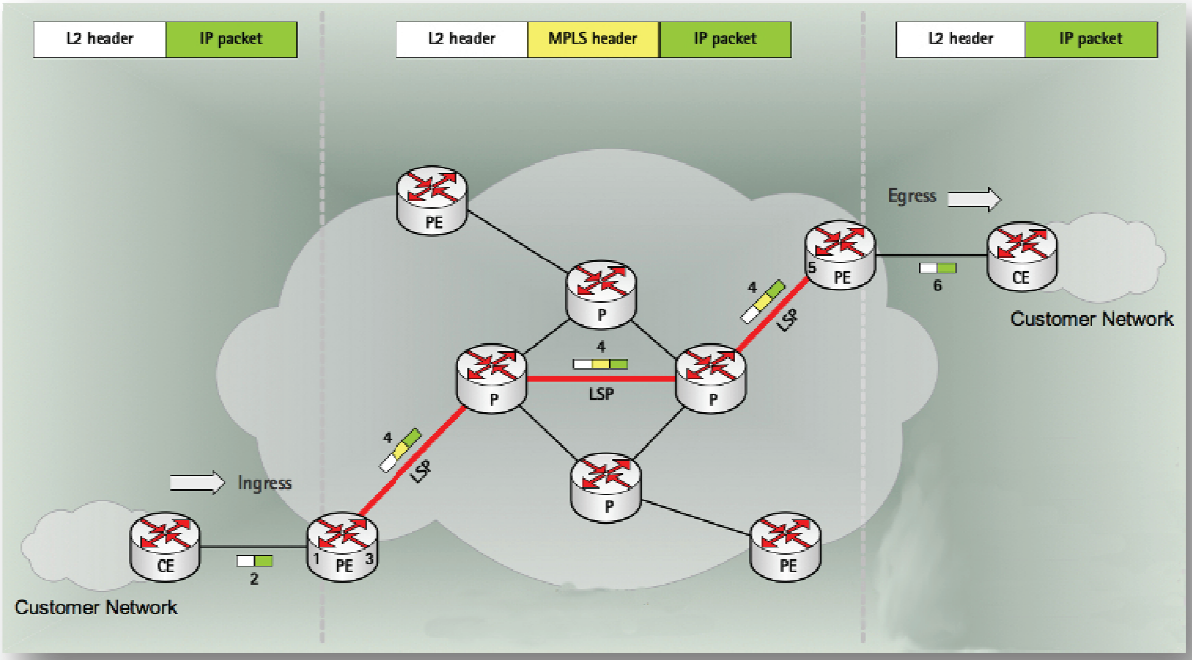
ΑΛΕΞΑΝΔΡΕΙΟ Τ.Ε.Ι. ΘΕΣΣΑΛΟΝΙΚΗΣ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πτυχιακή εργασία

Multiprotocol Label Switching



Επιμέλεια
Κατσαρός Αλέξανδρος
Αρ. Μητρώου: 03/2365

Επιβλέπων καθηγητής
Χαρχαλάκης Στέφανος

Θεσσαλονίκη 2009

Πτυχιακή εργασία

Multiprotocol Label Switching

Επιμέλεια
Κατσαρός Αλέξανδρος
Αρ. Μητρώου: 03/2365

Επιβλέπων καθηγητής
Χαρχαλάκης Στέφανος

Πρόλογος

Στα μέσα της δεκαετίας του 1990, ορισμένοι ISPs (Internet Service Providers) μετεξέλιξαν τα δίκτυά τους και αντικατέστησαν τους δρομολογητές στον πυρήνα των δικτύων τους με το μοντέλο επικάλυψης (overlay model) όπου χρησιμοποιείται IP (Internet Protocol) δρομολόγηση πάνω από δίκτυα ATM (Asynchronous transfer mode). Οι ISPs προχώρησαν σ' αυτή την αλλαγή επειδή χρειάστηκαν μεγαλύτερο εύρος ζώνης, ευκολία στον προσδιορισμό της απόδοσης προώθησης δεδομένων και έλεγχο κυκλοφορίας για την υποστήριξη της εκρηκτικής αύξησης που πραγματοποιούνταν στα δίκτυά τους. Ένας σημαντικός λόγος της καταλληλότητας της IP δρομολόγησης πάνω από δίκτυα ATM για την ικανοποίηση των παραπάνω απαιτήσεων ήταν η χρήση ενός αλγόριθμου προώθησης με ανταλλαγή ετικετών από τα δίκτυα ATM. Όμως, καθώς οι πάροχοι δικτυακών υπηρεσιών μεγάλωναν με εκθετικούς ρυθμούς και άρχισε να εμφανίζεται στο εμπόριο εξειδικευμένος εξοπλισμός για δικτυακές εφαρμογές, η λύση του μοντέλου IP δρομολόγησης πάνω από δίκτυα ATM (IP-over-ATM) με τα κληρονομικά προβλήματα επεκτασιμότητας, δεν έδειχνε να είναι και η πιο λογική μελλοντικά.

Καθώς οι πάροχοι δικτυακών υπηρεσιών συνέχιζαν να υιοθετούν το μοντέλο IP-over-ATM, άρχισαν να εμφανίζονται νέες τεχνολογίες σχεδιασμένες για το βασικό κορμό του Διαδικτύου. Για να μπορέσει να πάρει το προβάδισμα μια επιχείρηση στον κόσμο των δικτύων, έπρεπε να παρουσιάσει μια νέα λύση η οποία να μπορεί να συνδυάζει το κόστος και την απόδοση ενός μεταγωγέα ATM με τον έλεγχο ενός IP δρομολογητή και ταυτόχρονα να ελαχιστοποιεί την πολυπλοκότητα αντιστοίχησης που απαιτούσε το μοντέλο IP-over-ATM. Στα τέλη του 1996, ένας αριθμός επιχειρήσεων παρουσίαζε ιδιόκτητες λύσεις για μεταγωγή πολλαπλών επιπέδων, οι οποίες συνδύαζαν την μεταγωγή ATM και την IP δρομολόγηση. Μια από αυτές τις λύσεις ήταν η μέθοδος Tag Switching (Μεταγωγή Ετικέτας), που υλοποιήθηκε από την εταιρεία Cisco Systems. Ένα δίκτυο που χρησιμοποιεί την μεταγωγή ετικέτας αποτελείται από δρομολογητές ετικέτας στα άκρα του δικτύου (Tag Edge Routers) και ενδιάμεσους δρομολογητές μεταγωγής ετικέτας (Tag Switching Routers), όπου την ευθύνη για την επισύναψη ταμπέλας σε κάθε πακέτο την έχουν οι δρομολογητές στα άκρα του δικτύου. Για

τον προσδιορισμό του επόμενου προορισμού της κυκλοφορίας (επόμενο βήμα) χρησιμοποιούνται τα συνηθισμένα IP πρωτόκολλα.

Στις αρχές του 1997, το IETF (Internet Engineering Task Force) εγκαθίδρυσε την ομάδα εργασίας MPLS για να παράγει ένα ενοποιημένο και αλληλεπιδραστικό πρωτόκολλο μεταγωγής πολλαπλών επιπέδων, το πρωτόκολλο Μεταγωγής Ετικέτας Πολλαπλών Πρωτοκόλλων (Multiprotocol Label Switching - MPLS).

Περίληψη

Το MPLS είναι ένας μηχανισμός ο όποιος κατευθύνει και μεταφέρει δεδομένα από έναν κόμβο του δικτύου σε έναν άλλο. Μπορεί να εγκαταστήσει με ευκολία εικονικές συνδέσεις μεταξύ απομακρυσμένων κόμβων. Αποδίδει ετικέτες στα πακέτα, οι οποίες περιγράφουν την διαδρομή που θα ακολουθήσουν στο δίκτυο. Επίσης, μπορεί να ενθυλακώσει πακέτα από διαφορετικά πρωτόκολλα δικτύου. Το MPLS δεν χωράει σε κάποιο από τα επίπεδα του μοντέλου OSI, γιατί σε ένα MPLS δίκτυο βρίσκονται σε λειτουργία τόσο πρωτόκολλα επιπέδου σύνδεσης όσο και επιπέδου δικτύου.

Το MPLS προσθέτει στα πακέτα μια MPLS κεφαλίδα η οποία αποτελείται από μια ή περισσότερες ετικέτες. Αυτή η κεφαλίδα ονομάζεται στοίβα ετικετών. Κάθε ετικέτα της στοίβας αποτελείται από τέσσερα πεδία:

- Τιμή ετικέτας (20 bit)
- Experimental bits (3 bit), τα οποία χρησιμοποιούνται για ποιότητα υπηρεσίας (QoS/Quality of Service)
- Bottom of Stag flag (1 bit), αν είναι 1 τότε η ετικέτα είναι η τελευταία της στοίβας
- TTL (Time to Live) bits (8 bit)

Η ετικέτα λαμβάνει ακέραιες τιμές από 0 ως 1048575. Κάποιες ετικέτες είναι δεσμευμένες (0 ως 15) και εκτελούν κάποια ιδιαίτερη λειτουργία.

Οι κόμβοι εισόδου και εξόδου ενός πακέτου στο MPLS δίκτυο ονομάζονται οριακοί δρομολογητές (Label Edge Routers/LERs), και είναι αυτοί που αποδίδουν μια ετικέτα κατά την είσοδο του πακέτου και την αφαιρούν κατά την έξοδο του αντίστοιχα. Οι δρομολογητές οι οποία δρομολογούν ένα πακέτο σύμφωνα με την MPLS ετικέτα ονομάζονται δρομολογητές μεταγωγής ετικέτας (Label Switch Routers/LSRs). Οι ετικέτες διανέμονται μεταξύ των LERs και των LSRs με την βοήθεια ενός πρωτοκόλλου διανομής ετικετών. Σκοπός αυτής της διανομής είναι η δημιουργία μιας διαδρομής (Label Switched Path/LSP). Ένα LSP είναι μια σειρά

από LSRs οι οποία μεταγάγουν ένα επισημασμένο πακέτο μέσω του MPLS δικτύου ή σε ένα μέρος αυτού.

Όταν ένα IP πακέτο μπαίνει στο MPLS δίκτυο, ο οριακός δρομολογητής εισαγωγής επεξεργάζεται το πακέτο και του αποδίδει μια ετικέτα σύμφωνα με την διεύθυνση προορισμού του. Όσο το πακέτο κινείται εντός του MPLS δικτύου, η προώθηση του θα γίνεται σύμφωνα με την ετικέτα και όχι με την διεύθυνση IP. Κάθε LSR που λαμβάνει το πακέτο διαβάζει την ετικέτα και σύμφωνα με τον πίνακα προώθησης του την αντικαθιστά και προωθεί το πακέτο στον επόμενο LSR. Όταν το πακέτο φθάσει στον οριακό δρομολογητή εξόδου, η ετικέτα αφαιρείται και η προώθηση του πακέτου γίνεται βάση της IP διεύθυνσης του.

Κάποιες σημαντικές εφαρμογές του MPLS είναι το Traffic Engineering, το MPLS VPN και το VPLS (Virtual Private LAN Service). Η χρήση Traffic Engineering βοηθά τα MPLS δίκτυα στην ελαχιστοποίηση της συμφόρησης του δικτύου και στη μεγιστοποίηση της απόδοσης του. Η τεχνική Traffic Engineering χρησιμοποιεί της πληροφορίες δρομολόγησης με τέτοιο τρόπο ώστε να γίνει πιο αποδοτική η αντιστοίχηση της κυκλοφορίας στους διαθέσιμους δικτυακούς πόρους. Η λειτουργία αυτής της τεχνικής περιλαμβάνει διανομή πληροφορίας συνδέσεων, υπολογισμό διαδρομών, σηματοδοσία LSP και διαχωρισμό κίνησης πληροφορίας.

Το MPLS VPN είναι μια από τις πιο διαδεδομένες εφαρμογές MPLS δικτύων. Παρέχει επεκτασιμότητα και χωρίζει το δίκτυο σε μικρότερα μέρη, κάτι το οποίο είναι απαραίτητο για μεγάλα επιχειρησιακά δίκτυα. Υπάρχουν δυο τύποι MPLS VPN, τα Layer 3 MPLS VPN και τα MPLS-based Layer 2 VPN. Για να επιτευχθεί η υλοποίηση ενός Layer 3 MPLS VPN, χρειάζονται κάποια βασικά στοιχεία στους PE δρομολογητές. Αυτά είναι: Virtual Routing and Forwarding Tables (VRFs), διανομή διαδρομών με τη χρήση του BGP, Route Distinguisher (RD), Route Targets (RT), προώθηση επισημασμένων πακέτων. Όλα τα πακέτα προωθούνται με δύο ετικέτες: την IGP ετικέτα στην κορυφή της στοίβας ετικετών και την VPN ετικέτα στη βάση της στοίβας. Η IGP ετικέτα χρησιμοποιείται για την προώθηση του πακέτου μέσω του LSP, ενώ η VPN ετικέτα για την ταυτοποίηση του πίνακα VRF στον PE δρομολογητή. Το MPLS-based Layer 2 VPN χρησιμοποιεί το MPLS δίκτυο για να προσφέρει υπηρεσίες επιπέδου σύνδεσης στους πελάτες. Η υπηρεσία είναι μια τεχνολογία δευτέρου επιπέδου, όπως Frame Relay, ATM ή Ethernet VLAN. Διαφέρει όμως από τις παραπάνω γιατί μεταφέρεται μέσω ενός MPLS δικτύου.

Το VPLS (Virtual Private LAN Service) εξομοιώνει ένα τοπικό δίκτυο μέσω ενός MPLS δικτύου με την χρήση pseudowires. Για παράδειγμα, αν ένας πελάτης με διαφορετικές Ethernet περιοχές συνδεθεί σε ένα MPLS δίκτυο στο οποίο έχει εφαρμοστεί το VPLS, θα βλέπει όλες τις Ethernet περιοχές του σαν να ήταν συνδεδεμένες με ένα εικονικό Ethernet Switch.

Abstract

Multiprotocol Label Switching (MPLS) is a mechanism which directs and carries data from one network node to the next. It makes it easy to create "virtual links" between distant nodes. MPLS assigns short labels to network packets that describe how to forward them through the network. It can encapsulate packets of various network protocols. MPLS does not fit in the OSI layering too well because the Layer3 and Layer 2 encapsulation are still present with labeled packets.

MPLS works by prefixing packets with an MPLS header, containing one or more 'labels'. This is called a label stack. Each label stack entry contains four fields:

- A 20-bit label value.
- A 3-bit for QoS (Quality of Service) priority (experimental).
- A 1-bit *bottom of stack* flag. If this is set, it signifies that the current label is the last in the stack.
- An 8-bit TTL (time to live) field.

Labels are unsigned integer in the range 0 through 1048575. Some of these labels are reserved (in the 0 through 15 range) and they have a special meaning.

The entry and exit points of an MPLS network are called Label Edge Routers (LER), which, respectively, push an MPLS label onto an incoming packet and pop it off the outgoing packet. Routers that perform routing based only on the label are called Label Switch Routers (LSR). Labels are distributed between LERs and LSRs using the “Label Distribution Protocol” (LDP) in order to create LSPs. A label switched path (LSP) is a sequence of LSRs that switch a labeled packet through an MPLS network or part of an MPLS network.

When an IP packet enters an LSP, the ingress router examines the packet and assigns it a label based on its destination. The label transforms the packet from one that is forwarded based on its IP routing information to one that is forwarded based on information associated with the label. The packet then is

forwarded to the next router in the LSP. This router and all subsequent routers in the LSP do not examine any of the IP routing information in the labeled packet. Rather, they use the label to look up information in their label forwarding table. Then, they replace the old label with a new label and forward the packet to the next router in the path. When the packet reaches the egress router, the label is removed, and the packet again becomes a native IP packet and is again forwarded based on its IP routing information.

Major applications of MPLS are Traffic Engineering, MPLS VPN and Virtual Private LAN Service (VPLS). MPLS networks can use native TE mechanisms to minimize network congestion and improve network performance. TE modifies routing patterns to provide efficient mapping of traffic streams to network resources. The operation of MPLS TE involves link information distribution, path computation, LSP signaling, and traffic selection.

MPLS VPN, or MPLS Virtual Private Networks, is the most popular and widespread implementation of MPLS technology. MPLS VPN can provide scalability and divide the network into separate smaller networks, which is often necessary in the larger enterprise networks. There are two types of MPLS VPN, Layer 3 MPLS VPN and MPLS-based Layer 2 VPNs. To achieve Layer 3 MPLS VPN, you need some basic building blocks on the PE routers. These building blocks are the following: VRF, route distinguisher (RD), route targets (RT), route propagation through MP-BGP, and forwarding of labeled packets. All packets are forwarded with two labels: the IGP label as the top label and the VPN label as the bottom label. The IGP label is used to forward the packet through the LSP and the VPN label is used to separate the VRF table of the PE router. An MPLS-based Layer 2 VPN uses an MPLS network to deliver Layer 2 services to the customers. The service is a Layer 2 technology, such as Frame Relay, ATM, or Ethernet VLAN. Layer 2 MPLS VPN is, therefore, similar to a traditional Frame Relay or ATM VPN, but the difference is that the service provider network is MPLS-based, rather than being bound by the access technology.

Virtual Private LAN Service (VPLS) emulates a LAN segment across the MPLS backbone across pseudowires. For example, when the customer with different Ethernet sites connects to an MPLS backbone where VPLS is deployed, it appears as if all the sites are interconnected through a virtual Ethernet switch.

Ευρετήριο Περιεχομένων

Ευρετήριο Σχημάτων και Πινάκων

1. Βασικά Στοιχεία του MPLS

2. Αρχιτεκτονική & Λειτουργία MPLS

3. Πρωτόκολλα Διανομής Ετικετών

4. Traffic Engineering με MPLS

5. MPLS VPN

6. Virtual Private LAN Service (VPLS)

Εισαγωγή

Σκοπός της πτυχιακής αυτής εργασίας είναι η μελέτη του πρωτοκόλλου MPLS και η παρουσίαση του τρόπου λειτουργίας του. Εκτός από την βιβλιογραφική έρευνα του πρωτοκόλλου MPLS, υπήρξε και η σκέψη πρακτικής εφαρμογής του στο δίκτυο στου ΑΤΕΙ Θεσσαλονίκης. Η σκέψη όμως αυτή εγκαταλείφθηκε γιατί οι συσκευές και το λειτουργικό σύστημα των διαθέσιμων δρομολογητών δεν το υποστήριζαν. Το MPLS είναι μια αναπτυσσόμενη τεχνολογία εν έτη 2009, η οποία έχει ήδη εισαχθεί σε δίκτυα παρόχων υπηρεσιών διαδικτύου (ISPs) στην Ελλάδα. Στα κεφάλαια που ακολουθούν περιγράφεται η λειτουργία του MPLS και οι σημαντικότερες εφαρμογές του.

Στο πρώτο κεφάλαιο περιγράφονται τα βασικά στοιχεία του MPLS και λειτουργεί εισαγωγικά, περιγράφοντας σε γενικές γραμμές τι είναι το MPLS. Το δεύτερο κεφάλαιο αναφέρεται στην αρχιτεκτονική και στον τρόπο λειτουργίας του MPLS, ενώ στο τρίτο αναλύεται το πρωτόκολλο διανομής ετικετών (LDP) το οποίο είναι υπεύθυνο για την εγκαθίδρυση των σχέσεων μεταξύ των γειτονικών LSRs και για την διανομή των ετικετών του MPLS. Στο τέταρτο κεφάλαιο παρουσιάζεται η εφαρμογή Traffic Engineering, η οποία ωφελεί στην πιο αποδοτική αντιστοίχηση της κυκλοφορίας στους διαθέσιμους δικτυακούς πόρους. Στο πέμπτο κεφάλαιο αναλύεται το MPLS VPN, το οποίο προσφέρει ευελιξία σε επιχειρήσεις που διαθέτουν απομακρυσμένα παραρτήματα και πρέπει να επικοινωνούν με ασφάλεια. Τέλος, στο έκτο κεφάλαιο περιγράφεται το VPLS, με το οποίο εξομοιώνεται ένα τοπικό δίκτυο.

1

Βασικά Στοιχεία του MPLS

1.1 Εισαγωγή

Ιστορικά, το MPLS (Multi-Protocol Label Switching) προήλθε από την προσπάθεια της εκμετάλλευσης στο έπακρο των πλεονεκτημάτων των υψηλής ταχύτητας ATM μεταγωγέων (ATM Switches) στα IP δίκτυα κορμού. Το ευρύ κοινό δεν ήταν ικανοποιημένο από την τεχνική MPoA (MultiProtocol over ATM) του ATM Forum, η οποία φαινόταν πολύπλοκη και ακριβή στην εφαρμογή. Εναλλακτικές προτάσεις βρήκαν μεγάλη απήχηση, όπως η τεχνική IP Switch της Ipsilon την οποία ακολούθησε και ένα πλήθος άλλων τεχνικών, όπως η Tag Switching της Cisco Systems. Όλες αυτές οι προσεγγίσεις έδωσαν και το έναυσμα για την δημιουργία ενός προτύπου από το IETF, το οποίο θα εξηγούσε την μεταγωγή ετικέτας (Label Switching). Το συγκεκριμένο πρότυπο του IETF είναι γνωστό σήμερα σαν MPLS (Multi-Protocol Label Switching).

1.2 Τα επίπεδα της δρομολόγησης

Η δρομολόγηση επιπέδου δικτύου μπορεί να χωριστεί σε δυο βασικά επίπεδα: το επίπεδο του ελέγχου (Control Plane) και το επίπεδο της προώθησης (Forwarding Plane). Το Forwarding Plane είναι υπεύθυνο για την πραγματική προώθηση των πακέτων από την είσοδο στη έξοδο ενός μεταγωγέα ή δρομολογητή. Η πληροφορία που απαιτείται για την προώθηση παρέχεται από δύο πηγές: έναν πίνακα προώθησης (forwarding table) που διατηρεί ένας δρομολογητής και την πληροφορία την οποία κουβαλάει το ίδιο το πακέτο. Το Control Plane είναι υπεύθυνο για την κατασκευή και την διατήρηση του πίνακα προώθησης.

Κάθε δρομολογητής ενός δικτύου ενσωματώνει και τα δύο παραπάνω επίπεδα. Το Control Plane αποτελείται από ένα ή περισσότερα πρωτόκολλα

δρομολόγησης τα οποία βοηθούν στην ανταλλαγή της πληροφορίας δρομολόγησης μεταξύ των δρομολογητών και στον μετασχηματισμό αυτών των πληροφοριών ώστε να δημιουργηθεί ο πίνακας προώθησης. Το Forwarding Plane αποτελείται από διαδικασίες τις οποίες χρησιμοποιεί ένας δρομολογητής, ώστε να αποφασίσει για την προώθηση ενός πακέτου. Γενικά για το Forwarding Plane υπάρχουν τρεις περιπτώσεις: unicast προώθηση (προώθηση πακέτων σε έναν προορισμό), unicast προώθηση με τύπο υπηρεσίας (Type of Service/ToS [2]) και multicast προώθηση (προώθηση πακέτων σε πολλούς προορισμούς).

1.3 Forwarding Equivalence Class (FEC)

Οι διαδικασίες του Forwarding Plane αποτελούν γενικά ένα τρόπο ομαδοποίησης των πακέτων που οφείλει να προωθήσει ένας δρομολογητής σε έναν αριθμό διακριτών συνόλων. Από τη μεριά του Forwarding Plane, πακέτα που ανήκουν στο ίδιο σύνολο αντιμετωπίζονται από τον δρομολογητή με τον ίδιο τρόπο (π.χ. προωθούνται στον ίδιο επόμενο κόμβο), ακόμα και αν οι πληροφορίες επιπέδου δικτύου των πακέτων ενός συνόλου διαφέρουν μεταξύ τους. Αυτά τα σύνολα ονομάζονται FECs (Forwarding Equivalence Classes).

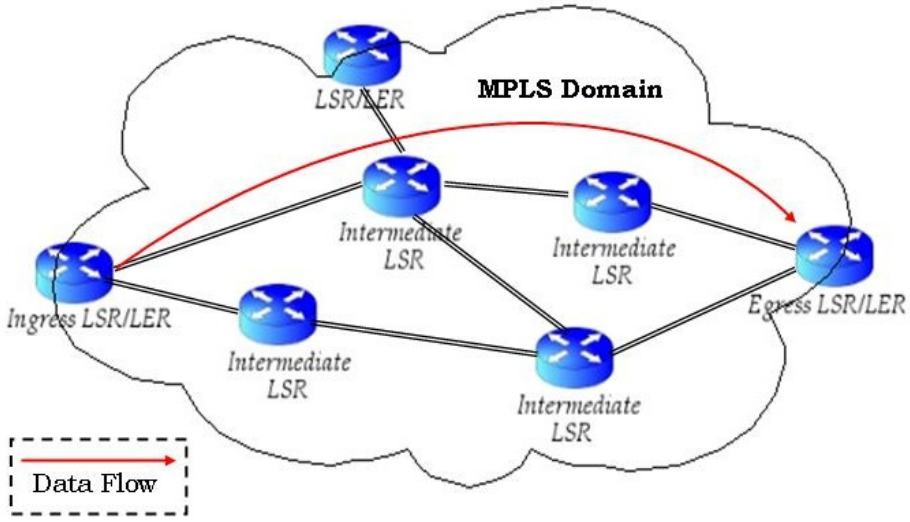
1.4 Μεταγωγή Ετικέτας (Label Switching): Forwarding Plane

Ο διαχωρισμός της δρομολόγησης στα επίπεδα Control και Forwarding μπορεί να εφαρμοστεί όχι μόνο στη συμβατική τεχνική δρομολόγησης (με IP διευθύνσεις), αλλά και σε τεχνικές μεταγωγής ετικέτας όπως το MPLS. Ο αλγόριθμος που χρησιμοποιείται γενικά στην προώθηση πακέτων με μεταγωγή ετικέτας βασίζεται σε δύο πηγές: έναν πίνακα προώθησης, ο οποίος διατηρείται από έναν δρομολογητή μεταγωγής ετικέτας (Label Switching Router/LSR), και την ενσωματωμένη σε κάθε πακέτο ετικέτα.

Ένας LSR είναι ένας δρομολογητής ο οποίος υποστηρίζει MPLS. Είναι ικανός να διαβάσει τις MPLS ετικέτες, να εκτελέσει κάποια λειτουργία σε αυτές, καθώς επίσης να λάβει και να αποστείλει επισημασμένα πακέτα. Σε ένα MPLS δίκτυο διακρίνουμε τρία είδη LSR, τα οποία φαίνονται στην εικόνα 1.1.

- Intermediate LSR: είναι ένας ενδιάμεσος του MPLS δικτύου LSR, ο οποίος λαμβάνει ένα επισημασμένο πακέτο, εκτελεί κάποια εργασία στην ετικέτα και αποστέλλει το επισημασμένο πακέτο στον επόμενο κόμβο σύμφωνα με τον πίνακα προώθησης.

- Ingress LSR: είναι ένας δρομολογητής μεταγωγής ετικέτας, ο οποίος βρίσκεται στη είσοδο ενός MPLS δικτύου. Λαμβάνει ένα πακέτο χωρίς ετικέτα, προσθέτει μια ετικέτα στο πακέτο και το προωθεί.
- Egress LSR: είναι ένας δρομολογητής μεταγωγής ετικέτας, ο οποίος βρίσκεται στη έξοδο ενός MPLS δικτύου. Λαμβάνει ένα πακέτο με ετικέτα, την αφαιρεί και το προωθεί σύμφωνα με πληροφορίες του επιπέδου δικτύου.



Εικόνα 1.1. Τα είδη των δρομολογητών σε ένα MPLS δίκτυο

Οι δρομολογητές οι οποίοι βρίσκονται στην είσοδο και στην έξοδο ενός MPLS δικτύου ονομάζονται και οριακοί δρομολογητές ετικέτας (Label Edge Routers/LERs). Στο σενάριο της εικόνας 1.1 υπάρχουν τρεις LERs, όμως για την συγκεκριμένη συνεδρία ένας από αυτούς παίζει τον ρόλο του ingress LSR και ένας άλλος του egress LSR.

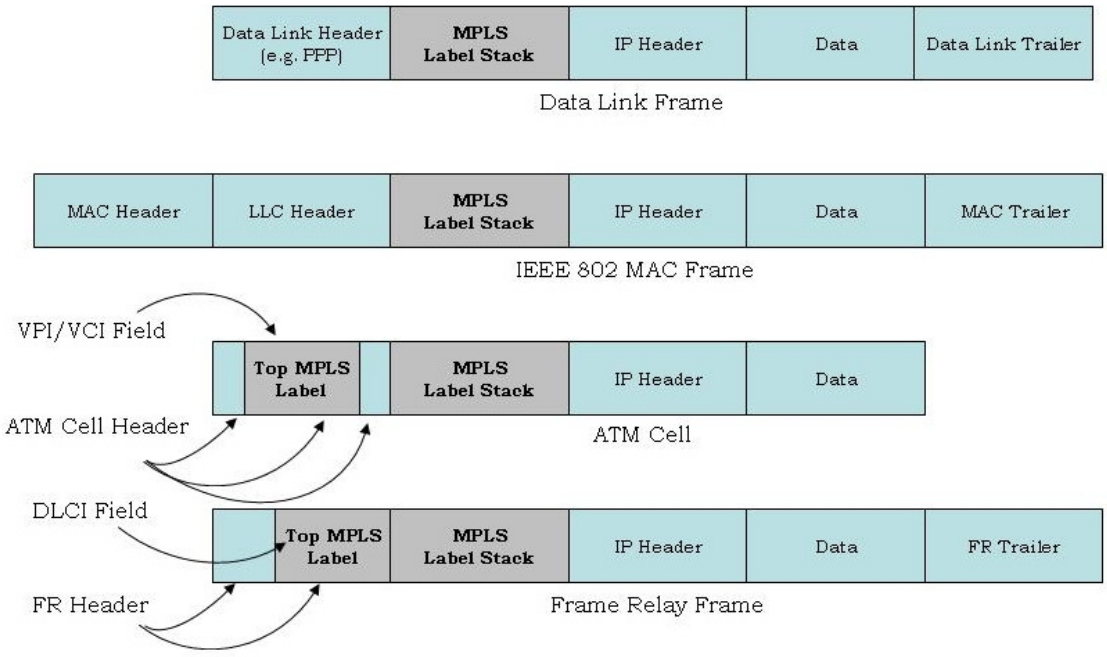
1.4.1 Ετικέτα του MPLS

Η ετικέτα είναι μια μικρή και καθορισμένου μεγέθους τιμή των 32 bit η οποία είναι τοπικής σημασίας. Μια ετικέτα δεν κωδικοποιεί κατευθείαν τις πληροφορίες επιπέδου δικτύου (π.χ. δεν κωδικοποιεί την διεύθυνση επιπέδου δικτύου). Ένα πακέτο μπορεί να μην έχει μια μόνο ετικέτα αλλά και περισσότερες. Γενικά υπάρχει μια στοίβα ετικετών. Οι LSRs επεξεργάζονται την ετικέτα στην κορυφή της στοίβας. Στην εικόνα 1.2 φαίνονται τα πεδία που συνθέτουν μια ετικέτα. Αν το πεδίο S (Bottom of Stack) μιας ετικέτας είναι 1, τότε η συγκεκριμένη ετικέτα είναι η τελευταία της στοίβας, ενώ αν είναι 0 υπάρχουν και άλλες ετικέτες κάτω από αυτήν.

Εικόνα 1.2. Η ετικέτα του MPLS

Ένα από τα σημαντικότερα θέματα προώθησης σε ένα δίκτυο μεταγωγής ετικέτας είναι η ικανότητα των πακέτων να ενσωματώσουν την ετικέτα με τον πιο αποδοτικό τρόπο.

Γενικά, η στοίβα ετικετών τοποθετείται πάντα μεταξύ του 2ου και 3ου επιπέδου, ανεξάρτητα από τα αντίστοιχα πρωτόκολλα που βρίσκονται σε χρήση. Αποτελεί μέρος των δεδομένων που μεταφέρονται από το πρωτόκολλο 2ου επιπέδου. Παρόλα αυτά, κάθε LSR επεξεργάζεται την ετικέτα στην κορυφή της στοίβας ώστε να πάρει μια απόφαση προώθησης. Έτσι, η κορυφαία ετικέτα μπορεί να διαχωριστεί από την υπόλοιπη στοίβα και να τοποθετηθεί σε ένα σημείο που η προσπέλαση της είναι πιο γρήγορη και πιο εύκολη. Επειδή το MPLS είναι σχεδιασμένο να λειτουργεί με διαφορετικά πρωτόκολλα 2ου επιπέδου, η εισαγωγή της κορυφαίας ετικέτας εξαρτάται από το πρωτόκολλο που χρησιμοποιείται. Στην εικόνα 1.3 φαίνεται η στοίβα ετικετών και η τοποθέτηση αυτών για διάφορες τεχνολογίες σύνδεσης.



Εικόνα 1.3. Η κωδικοποίηση των ετικετών ανάλογα με την τεχνολογία 2ου επιπέδου

Για παράδειγμα, αν το πρωτόκολλο 2ου επιπέδου έχει κάποιο πεδίο ικανό να ενσωματώσει μια ετικέτα, τότε αυτό το πεδίο μπορεί να χρησιμοποιηθεί για την κωδικοποίηση της ετικέτας ή μέρος αυτής. Παράδειγμα τέτοιων τεχνολογιών 2ου επιπέδου είναι το ATM [3] και το Frame Relay [7]. Στο Frame Relay μέρος της κορυφαίας ετικέτας (Label Value) ενσωματώνεται στη θέση του DLCI. Παρόλα αυτά, τα υπόλοιπα πεδία της κορυφαίας ετικέτας (EXP, S, TTL) και άλλες ετικέτες που μπορεί να έχει η στοίβα, τοποθετούνται μεταξύ 2ου και 3ου επιπέδου. Παρόμοια είναι η τοποθέτηση της κορυφαίας ετικέτας και στο ATM. Για τεχνολογίες όπως Ethernet [13] ή PPP [34], η κορυφαία ετικέτα τοποθετείται μαζί με την υπόλοιπη στοίβα μεταξύ 2ου και 3ου επιπέδου.

1.4.2 Αλγόριθμος Προώθησης Μεταγωγής Ετικέτας

Ο αλγόριθμος της προώθησης ο οποίος χρησιμοποιείται από την τεχνική μεταγωγής ετικέτας, βασίζεται στην αντικατάσταση ετικέτας. Όταν ένας LSR λάβει ένα πακέτο εξάγει την ετικέτα που αυτό μεταφέρει και την χρησιμοποιεί σαν δείκτη στον πίνακα προώθησης του. Κατά την εύρεση αυτού του δείκτη, που αντιπροσωπεύει την ετικέτα στον πίνακα προώθησης, διαπιστώνεται η εξερχόμενη ετικέτα που θα αντικαταστήσει την εισερχόμενη και η διασύνδεση εξόδου (Output Interface).

Ο πίνακας προώθησης ενός LSR ονομάζεται ILM (Incoming Label Map). Στη γενική του μορφή, ο πίνακας ILM αποτελείται από μια σειρά εγγραφών. Κάθε εγγραφή αποτελείται από μια εισερχόμενη ετικέτα και από μια ή περισσότερες υποεγγραφές, κάθε μια από τις οποίες περιέχει την εξερχόμενη ετικέτα και τη διασύνδεση εξόδου. Ο λόγος της πιθανής ύπαρξης υποεγγραφών για κάθε εγγραφή του ILM, είναι για την υποστήριξη multicast προώθησης πακέτων. Επιπλέον, κάθε LSR μπορεί να διατηρεί έναν ILM για κάθε διασύνδεση (per-interface) ή να έχει έναν ILM για όλες τις διασυνδέσεις του (per-platform). Στη τελευταία περίπτωση η προώθηση κάθε πακέτου δεν εξαρτάται μόνο από την εισερχόμενη ετικέτα, αλλά και από την εισερχόμενη διασύνδεση η οποία θα περιλαμβάνεται στον ILM.

Η διαδρομή που ακολουθούν τα πακέτα μέσα στο δίκτυο καθορίζεται από την αλλαγή των ετικετών. Εφόσον η αντιστοίχιση εισερχόμενης και εξερχόμενης ετικέτας σε κάθε LSR είναι μόνιμη (όπως καθορίζεται στον πίνακα ILM), μπορεί κανείς να πει ότι η διαδρομή καθορίζεται από την ετικέτα που θα προσθέσει στο πακέτο ο ingress LSR. Μια τέτοια διαδρομή ονομάζεται διαδρομή μεταγωγής ετικέτας (Label Switched Path/LSP). Ένα LSP είναι μονόδρομο, δηλαδή η

κυκλοφορία γίνεται μόνο προς μια κατεύθυνση. Το MPLS αλλάζει το τρόπο δρομολόγησης από κόμβο σε κόμβο με το να επιτρέπει στους δρομολογητές να προσδιορίζουν LSP διαδρομές στο δίκτυο, που βασίζονται στην ποιότητα υπηρεσίας (Quality of Service/QoS) και στις ανάγκες για εύρος ζώνης των εφαρμογών. Η επιλογή των διαδρομών μπορεί να λάβει υπόψη της ιδιότητες του 2ου επιπέδου, ιδιαίτερα όσον αφορά στη ποιότητα υπηρεσίας και στο φόρτο εργασίας των δρομολογητών.

Όταν η εισαγωγή εγγραφών στον πίνακα ILM έχει ολοκληρωθεί, τότε κατά την διάρκεια της μετάδοσης χρησιμοποιούνται αποκλειστικά οι ετικέτες του ILM. Η διαδικασία της εισαγωγής εγγραφών στον ILM πραγματοποιείται στατικά με κατάλληλες ρυθμίσεις από τον διαχειριστή ή δυναμικά με την βοήθεια ενός πρωτοκόλλου διανομής ετικετών. Οι λειτουργίες του πρωτόκολλου διανομής ετικετών ανήκουν στο Control Plane ενός δρομολογητή και αναλύονται σε επόμενη παράγραφο.

Η απλότητα του αλγόριθμου προώθησης που χρησιμοποιείται από την τεχνική μεταγωγής ετικέτας, διευκολύνει στην φθηνή εφαρμογή του αλγόριθμου κατευθείαν στο υλικό (hardware). Ένα ουσιώδες χαρακτηριστικό του αλγόριθμου προώθησης είναι ότι κάθε LSR μπορεί να συλλέξει όλες τις πληροφορίες που απαιτούνται για την προώθηση, με μια μόνο αναζήτηση στην μνήμη. Και αυτό γιατί μια εγγραφή στον πίνακα προώθησης περιέχει όλες τις απαιτούμενες πληροφορίες προώθησης, ακόμα και πληροφορία για τους πόρους που θα χρησιμοποιήσει το πακέτο. Η ικανότητα της συλλογής πληροφοριών προώθησης και δέσμευσης πόρων με μια μόνο πρόσβαση στη μνήμη, κάνει την μεταγωγή ετικέτας ιδανική τεχνολογία ως προς την απόδοση προώθησης.

1.4.3 Ενιαίος Αλγόριθμος Προώθησης

Στη συμβατική αρχιτεκτονική δρομολόγησης, οι λειτουργίες Control Plane (πχ. unicast δρομολόγηση, unicast δρομολόγηση με ToS, multicast δρομολόγηση), απαιτούν διαφορετικούς αλγόριθμους προώθησης (πίνακας 1.1). Για παράδειγμα, για την unicast προώθηση ο δρομολογητής συγκρίνει την διεύθυνση προορισμού ενός πακέτου με τις διευθύνσεις δικτύου (Prefixes) του πίνακα δρομολόγησης. Το αποτέλεσμα αυτού του αλγόριθμου είναι η κατάλληλη διασύνδεση εξόδου ώστε το πακέτο να κινηθεί σωστά προς το δίκτυο προορισμού. Για unicast προώθηση με ToS ο δρομολογητής εκτελεί την ίδια διαδικασία, με την διαφορά ότι ο αλγόριθμος οφείλει να εκτελέσει και πρόσθετους ελέγχους που αφορούν στο ToS.

Πίνακας 1.1. Αλγόριθμοι προώθησης σε συμβατική λειτουργία δρομολόγησης

Routing function	Unicast routing	Unicast routing with ToS	Multicast routing
Forwarding algorithm	Longest match on destination address	Longest match on destination address & exact match on ToS bits	Longest match on source address (network) & exact match on source address, destination address and incoming interface

Αντίθετα στη μεταγωγή ετικέτας κυριαρχεί η έλλειψη διαφορετικών αλγόριθμων προώθησης, υπάρχει μόνο ένας αλγόριθμος προώθησης (πίνακας 1.2). Μπορεί κανείς να υποθέσει ότι η ύπαρξη ενός και μόνο αλγόριθμου προώθησης περιορίζει σημαντικά τη λειτουργικότητα της βασισμένης σε ετικέτες προώθησης. Μια τέτοια υπόθεση είναι λανθασμένη. Αντιθέτως, η λειτουργικότητα που μπορεί να υποστηριχθεί με την μεταγωγή ετικέτας έχει την δυνατότητα να γίνει ακόμα πιο πλούσια από τις συμβατικές τεχνικές.

Πίνακας 1.2. Αλγόριθμος προώθησης στο MPLS

Routing function	Unicast routing	Unicast routing with ToS	Multicast routing
Forwarding algorithm	Common forwarding (Label Swapping)		

Οι λειτουργίες του Forwarding Plane στην μεταγωγή ετικέτας δεν ορίζουν κάποιο περιορισμό όσον αφορά στην αντιστοίχηση των FEC με ετικέτες. Η αντιστοίχηση των FEC με ετικέτες είναι μια διαδικασία η οποία αφορά αποκλειστικά το Control Plane και συζητείται σε επόμενη παράγραφο.

1.4.4 Πολυπρωτόκολλο

Από τα παραπάνω μπορεί κανείς να συμπεράνει ότι η προώθηση σε ένα δίκτυο μεταγωγής ετικέτας δεν εξαρτάται από κάποια συγκεκριμένη τεχνολογία επιπέδου δικτύου. Για παράδειγμα, η προώθηση θα πραγματοποιηθεί με τον ίδιο τρόπο ανεξάρτητα αν το μεταφερόμενο πακέτο είναι IP (Internet Protocol) ή IPX (Internetwork Packet Exchange). Παράλληλα το πολυπρωτόκολλο μεταγωγής ετικέτας είναι ικανό να λειτουργήσει και με κάθε πρωτόκολλο επιπέδου σύνδεσης. Αυτές του οι ιδιότητες αντανακλούν και στο όνομα του: MPLS (Πολυπρωτόκολλο Μεταγωγής Ετικέτας)(πίνακας 1.3).

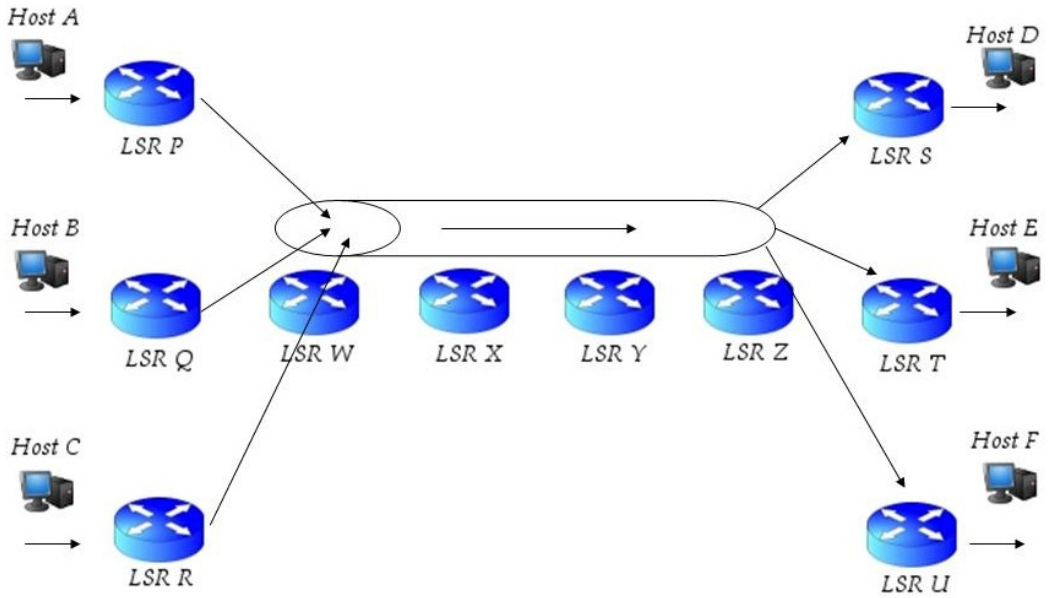
Πίνακας 1.3. Ανεξαρτησία MPLS από πρωτόκολλα σύνδεσης & δικτύου

IPX	AppleTalk		IPv4	IPv6
Label Switching				
Ethernet	FDDI	Point-to-Point	ATM	Frame Relay

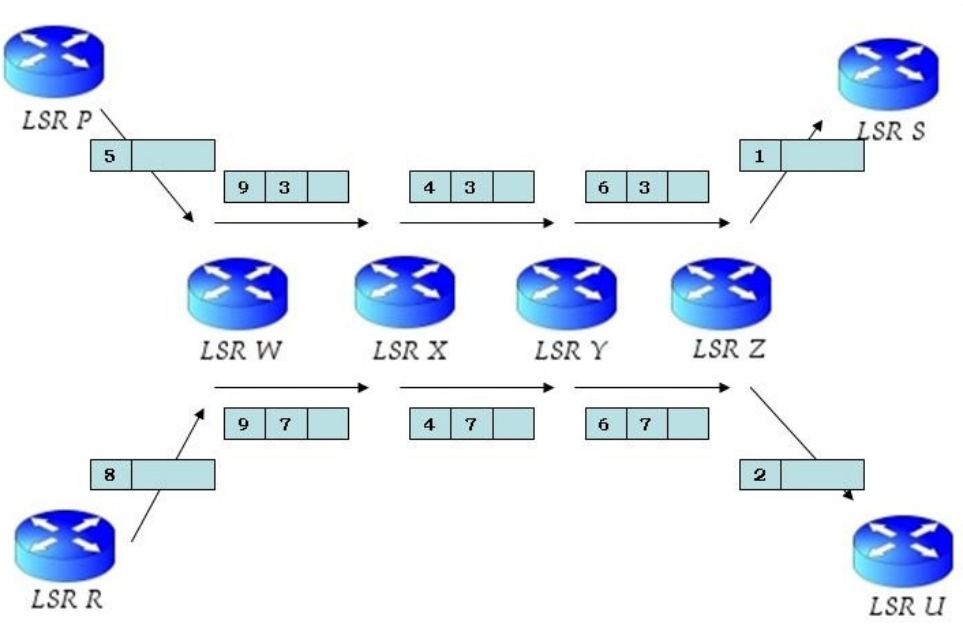
1.4.5 Ιεραρχία LSPs και Tunnels

Το MPLS επιτρέπει στα LSPs να είναι συγχωνευμένα ή να σχηματίζουν τούνελ (Tunnels). Είναι ένας χρήσιμος μηχανισμός ο οποίος επιτρέπει στα LSPs να αντιμετωπιστούν με τον ίδιο τρόπο στον κορμό του δικτύου, ενώ παράλληλα να διαφυλάξουν τα ξεχωριστά τους χαρακτηριστικά στα άκρα. Αυτό προσδίδει στο κορμό του δίκτυο ευελιξία (δεν απαιτείται να προσδιοριστούν όλοι οι ενδιάμεσοι LSRs και έτσι μπορούν να υπάρξουν αρκετά LSPs προς επιλογή) και βελτιώνει την διαχείριση των συνδέσεων.

Στην εικόνα 1.4 φαίνεται ένα Tunnel μεταξύ των LSR W και LSR Z. Στο πρωτόκολλο δρομολόγησης αυτοί οι δύο LSR φαίνονται σαν γειτονικοί. Αυτό επιτρέπει στα LSPs να εγκατασταθούν μέσω του Tunnel απλά σαν να έκαναν ένα βήμα από τον LSR W στον LSR Z. Ένας τρόπος για την εγκατάσταση των LSPs μέσω του Tunnel, είναι να εγκατασταθεί το Tunnel σαν μια εικονική σύνδεση μεταξύ των LSR W και LSR Z.



Εικόνα 1.4. LSP Tunnel μεταξύ δύο LSR του MPLS δικτύου



Εικόνα 1.5. Προώθηση MPLS πακέτου σε ένα LSP Tunnel

Το πακέτο μπαίνει στο Tunnel από τον LSR W (εικόνα 1.5). Ο LSR W αντικαθιστά την ετικέτα στη στοίβα, η οποία αναφέρεται στην εικονική σύνδεση με τον LSR Z. Η ετικέτα αυτή είναι η ετικέτα του Tunnel. Ο LSR W προσθέτει άλλη μια ετικέτα στη στοίβα η οποία χρησιμοποιείται για την προώθηση του πακέτου μέσω του LSP, το οποίο έχει δημιουργηθεί μεταξύ των LSR W και LSR Z. Όταν το πακέτο φθάσει στον LSR Z, η ετικέτα στην κορυφή της στοίβας αφαιρείται και μένει στο πακέτο η ετικέτα του Tunnel. Το επόμενο βήμα του πακέτου είναι βασισμένο στην ετικέτα του Tunnel.

1.5 Μεταγωγή Ετικέτας (Label Switching): Control Plane

Όπως προαναφέρθηκε, η ανάλυση της δρομολόγησης σε δύο επίπεδα, αυτά του Control Plane και του Forwarding Plane, μπορεί να εφαρμοστεί όχι μόνο στη συμβατική αρχιτεκτονική δρομολόγησης αλλά και στην μεταγωγή ετικέτας (MPLS). Ο ρόλος του Control Plane στη μεταγωγή ετικέτας είναι η διανομή πληροφορίας δρομολόγησης μεταξύ των LSRs και ένα πλήθος διαδικασιών οι οποίες χρησιμοποιούνται για την μετατροπή αυτής της πληροφορίας στον τελικό πίνακα προώθησης, που με τη σειρά του χρησιμοποιείται από το Forwarding Plane.

Αν κανείς συγκρίνει τις λειτουργίες του Control Plane μιας συμβατικής αρχιτεκτονικής δρομολόγησης με τις αντίστοιχες της μεταγωγής ετικέτας δεν θα βρει ουσιώδεις διαφορές. Στην πραγματικότητα η μεταγωγή ετικέτας περιλαμβάνει

όλα τα πρωτόκολλα δρομολόγησης που χρησιμοποιούνται από μια κοινή αρχιτεκτονική δρομολόγησης.

Στον πίνακα 1.4 παρουσιάζονται οι λειτουργίες του Control Plane στο MPLS.

Πίνακας 1.4. Οι λειτουργίες του Control Plane στο MPLS

Network layer routing protocols (e.g. OSPF, BGP)	Procedures for creating binding between label and FECs	Procedures for distributing information about created label binding
Maintenance of forwarding table		

Άρα οι λειτουργίες ελέγχου που πραγματοποιεί ένας LSR είναι:

- Δημιουργία αντιστοιχίσεων μεταξύ ετικετών και FECs
- Ανακοίνωση στους υπόλοιπους LSR για τις αντιστοιχίσεις που έχει κάνει
- Χρήση των δυο παραπάνω για την κατασκευή και διατήρηση του πίνακα προώθησης

Τα πρωτόκολλα δρομολόγησης τρίτου επίπεδου παρέχουν στους LSRs τις αντιστοιχίσεις μεταξύ των FECs και των διευθύνσεων των επόμενων κόμβων. Οι διαδικασίες για την δημιουργία μιας αντιστοίχησης μεταξύ ετικέτας και FEC και η διανομή των αντιστοιχίσεων μεταξύ των μεταγωγέων ετικέτας, παρέχουν στους LSRs την πληροφορία που απαιτείται για την κατασκευή του πίνακα προώθησης.

1.5.1 Αντιστοιχίσεις Ετικετών/FEC: Edge Routers

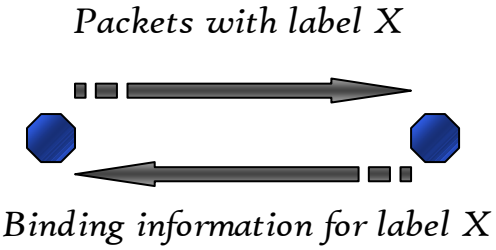
Ως τώρα έχει αναφερθεί ο τρόπος με τον οποίο πραγματοποιείται η μεταγωγή στον κορμό ενός MPLS δικτύου, δηλαδή η τεχνική αντικατάστασης ετικετών. Όμως ο τρόπος με τον οποίο τοποθετείται η αρχική ετικέτα σε ένα πακέτο είναι μια διαφορετική διαδικασία. Αυτή η διαδικασία πραγματοποιείται στους οριακούς δρομολογητές (Label Edge Routers).

Ένας οριακός δρομολογητής (LER) δεν ενσωματώνει μόνο τις λειτουργίες Control Plane και Forwarding Plane του MPLS, αλλά και τις αντίστοιχες λειτουργίες μια συμβατικής τεχνολογίας δρομολόγησης. Όταν ένας LER λάβει ένα πακέτο χωρίς ετικέτα τότε χρησιμοποιεί τους αλγόριθμους δρομολόγησης που διαθέτει για να αποφασίσει σε ποιο FEC ανήκει το πακέτο και ποιος είναι ο επόμενος κόμβος που αυτό πρέπει να σταλεί. Αν ο επόμενος κόμβος είναι ένας LSR τότε ο LER συμβουλεύεται τον πίνακα προώθησης του MPLS και αντιστοιχεί στο πακέτο μια ετικέτα, ανάλογα με το FEC στο οποίο ανήκει. Εδώ φαίνεται και ένα από τα

σημαντικότερα προτερήματα του MPLS: η αντιστοίχηση ενός πακέτου σε ένα FEC γίνεται μια φορά κατά την είσοδο του πακέτου στο MPLS δίκτυο και στη συνέχεια η μεταγωγή βασίζεται στην ετικέτα. Αντίθετα αν ο επόμενος κόμβος του LER στον οποίο πρέπει να σταλεί το πακέτο δεν είναι ένας LSR, τότε το πακέτο αποστέλλεται σύμφωνα με τη συμβατική τεχνολογία προώθησης (π.χ. IP προώθηση).

1.5.2 Διανομή Ετικετών

Κάθε εγγραφή στον πίνακα προώθησης ενός LSR περιέχει μια εισερχόμενη ετικέτα και μια ή περισσότερες εξερχόμενες. Για αυτές τις ετικέτες ορίζονται δύο τύποι: οι ετικέτες τις οποίες έχει αποδώσει ο συγκεκριμένος LSR για ένα FEC (local bindings) και οι ετικέτες τις οποίες έχει λάβει ο LSR από άλλους (remote bindings). Γενικά στον πίνακα προώθησης, οι εισερχόμενες ετικέτες ανήκουν στα local bindings, δηλαδή τις έχει αντιστοιχήσει ο ίδιος στα FEC, και οι εξερχόμενες στα remote bindings. Αυτός ο τρόπος αντιστοίχισης των ετικετών ονομάζεται downstream binding, και αυτό γιατί κάθε ετικέτα για ένα FEC αποδίδεται αναδρομικά από τον downstream LSR. Δηλαδή, η ανάθεση των ετικετών γίνεται με αντίθετη διεύθυνση από την διεύθυνση της ροής των επισημασμένων πακέτων. Η τεχνική downstream binding φαίνεται στην εικόνα 1.6.



Εικόνα 1.6. Downstream αντιστοίχηση ετικετών

Κάθε LSR διατηρεί έναν χώρο ελευθέρων ετικετών, δηλαδή ετικετών που δεν έχουν αντιστοιχηθεί με κάποιο FEC. Αυτός ο χώρος ετικετών περιέχει όλες τις ετικέτες που μπορούν να αποδοθούν ως τοπικές αντιστοιχίσεις (local bindings). Επίσης ένας LSR μπορεί να κάνει τις αντιστοιχίσεις ανά διασύνδεση (per-interface) ή ανά συσκευή (per-platform). Έτσι στην πρώτη περίπτωση θα έχει χώρους ετικετών όσους και οι διασυνδέσεις που μετέχουν στο MPLS δίκτυο.

Τη στιγμή που ένας LSR έχει κάνει τις αντιστοιχίσεις μεταξύ των τοπικά επιλεγμένων ετικετών και των FEC (local bindings), είναι σε θέση να ειδοποιήσει τους υπόλοιπους LSRs για αυτές τις αντιστοιχίσεις. Με αυτή τη διαδικασία θα ενημερώσει τους υπόλοιπους LSRs για τις απομακρυσμένα επιλεγμένες

αντιστοιχίσεις τους (remote bindings). Η διανομή των αντιστοιχίσεων μπορεί να πραγματοποιηθεί γενικά με δύο τρόπους:

- Ενσωμάτωση σε πρωτόκολλα δρομολόγησης
- Πρωτόκολλο διανομής ετικετών

Ενσωμάτωση σε πρωτόκολλα δρομολόγησης: ένας τρόπος διανομής των ετικετών είναι η ενσωμάτωση της λειτουργίας αυτής σε πρωτόκολλα δρομολόγησης. Έτσι η διανομή των ετικετών παραμένει συνεπής σε σχέση με την διανομή της πληροφορίας δρομολόγησης. Οι αντιστοιχίσεις μεταξύ ετικετών και FEC σε καμία περίπτωση δεν θα διανεμηθούν πριν την σύγκλιση του δικτύου, όσον αφορά στις πληροφορίες δρομολόγησης. Επίσης γίνεται πιο απλή η λειτουργία του δικτύου, εφόσον δεν χρησιμοποιείται κάποιο επιπλέον πρωτόκολλο για τη διανομή ετικετών.

Δεν είναι όλα τα πρωτόκολλα δρομολόγησης ικανά να ενσωματώσουν την λειτουργία της διανομής ετικετών. Για παράδειγμα, link state πρωτόκολλα δρομολόγησης δεν ενδείκνυνται για διανομή ετικετών, ενώ distance vector πρωτόκολλα τα οποία στέλνουν ολόκληρο τον πίνακα δρομολόγησης τους, δηλαδή τις αντιστοιχίσεις FEC και επόμενου κόμβου στους υπόλοιπους δρομολογητές, είναι προτιμότερα (για κάθε εγγραφή φέρει μια ετικέτα).

Επιπλέον, υπάρχει περίπτωση η επέκταση ενός πρωτοκόλλου για να ενσωματώσει τις πληροφορίες ετικέτας να μην είναι δυνατή λόγω τις πιθανής αλλαγής της αρχιτεκτονικής των μηνυμάτων που ανταλλάσσονται.

Πρωτόκολλα διανομής ετικετών: ο δεύτερος τρόπος είναι η χρήση ενός ξεχωριστού πρωτοκόλλου για την διανομή των ετικετών. Με αυτόν τον τρόπο είναι ικανή και η υποστήριξη διανομής ετικετών με πρωτόκολλα δρομολόγησης τα οποία δεν μπορούν από μόνα τους να διανέμουν ετικέτες. Αυτός ο λόγος είναι και η μόνη δικαιολογία για να χρησιμοποιήσει κανείς ένα τέτοιο ξεχωριστό πρωτόκολλο διανομής ετικετών. Αυτός ο τρόπος κάνει πιο δύσκολο τον συγχρονισμό μεταξύ πρωτοκόλλου δρομολόγησης και πρωτοκόλλου διανομής ετικετών. Επίσης αυξάνεται η πολυπλοκότητα του δικτύου, εφόσον εισάγεται ένα νέο πρωτόκολλο στο δίκτυο. Το LDP (Label Distribution Protocol) είναι ένα πρωτόκολλο αποκλειστικά για τη διανομή ετικετών, το οποίο αναλύεται σε επόμενο κεφάλαιο.

1.5.3 MPLS & Διευθύνσεις Επιπέδου Δικτύου

Παρόλο που στο MPLS η μεταγωγή βασίζεται στις ετικέτες, σε καμία περίπτωση δεν αντικαθίσταται οι διαδικασίες εγκαθίδρυσης και διατήρησης πληροφορίας δρομολόγησης. Έτσι η μεταγωγή ετικέτας δεν αντικαθιστά την διευθυνσιοδότηση τρίτου επιπέδου (π.χ. IP διευθύνσεις), καθώς αυτή παίζει σημαντικό ρόλο στις Control Plane λειτουργίες του MPLS.

Αν κανείς ήθελε να τοποθετήσει το MPLS ανάμεσα στα επτά επίπεδα του προτύπου OSI, τότε θα έπρεπε να δημιουργήσει μια νέα στάθμη ανάμεσα στα επίπεδα σύνδεσης και δικτύου. Το MPLS μπορεί να χρησιμοποιηθεί για να δημιουργήσει πίνακες προώθησης σε ATM ή Frame Relay μεταγωγείς χρησιμοποιώντας την υπάρχουσα κεφαλίδα ATM ή DLCI αντίστοιχα, ή σε απλούς IP δρομολογητές προσθέτοντας σημάνσεις σε IP πακέτα.

1.6 MPLS & Traffic Engineering (TE)

Το MPLS παρέχει τη δυνατότητα εφαρμογής Traffic Engineering (TE). Η βασική ιδέα πίσω από την τεχνική TE είναι η αποδοτικότερη χρήση της διαδικτυακής υποδομής και η εφαρμογή πολιτικών διαχείρισης του δικτύου. Το MPLS ενσωματώνοντας TE έχει τη δυνατότητα να εγκαθιδρύσει LSPs χρησιμοποιώντας μια διαδρομή η οποία δεν είναι η βέλτιστη διαδρομή του αλγόριθμου δρομολόγησης. Η τεχνική TE μπορεί να εξασφαλίσει πόρους στο δίκτυο αποκλειστικά για ένα συγκεκριμένο LSP, ώστε η ροή των δεδομένων και η τυχόν ποιότητα υπηρεσίας να είναι εγγυημένα. Μια άλλη εφαρμογή του TE είναι η δημιουργία πολλαπλών LSPs για την παράλληλη μεταφορά πακέτων μεταξύ μιας πηγής και ενός προορισμού. Σημαντική είναι και η χρήση του TE για ανάκτηση ή αναδρομολόγηση μιας διαδρομής σε περίπτωση αποτυχίας.

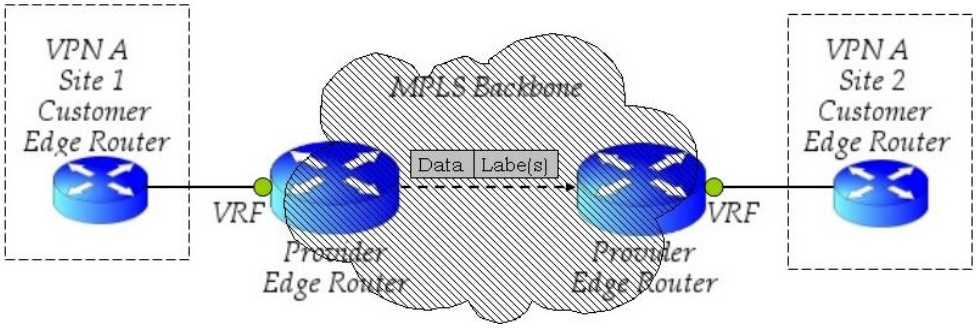
Σε γενικές γραμμές, η ενσωμάτωση του TE στο MPLS υπερτερεί ως προς προηγούμενες εφαρμογές TE, γιατί οι παραπάνω εφαρμογές μπορούν να καθορισθούν μια φορά στο σημείο εισόδου του LSP και όχι σε κάθε κόμβο του δικτύου ξεχωριστά.

1.7 MPLS VPN

Τα MPLS VPNs ή MPLS Virtual Private Networks είναι μια από τις πιο δημοφιλής και διαδεδομένες εφαρμογές της τεχνολογίας του MPLS. Βοηθούν στη

διαίρεση ενός δικτύου σε μικρότερα υποδίκτυα, τα οποία πολλές φορές είναι απαραίτητα σε μεγάλα δίκτυα όπου υπάρχει ανάγκη απομόνωσης ορισμένων τμημάτων της δικτυακής υποδομής. Πέραν της ασφάλειας που προσφέρουν μεταξύ των περιοχών των πελατών, τα MPLS VPNs προσφέρουν επίσης μεγαλύτερη ευελιξία σε σχέση με προηγούμενες εφαρμογές VPN. Νέες περιοχές μπορούν πολύ εύκολα να προστεθούν και η διαχείριση της όλης υποδομής γίνεται πιο απλή.

Με το MPLS μπορούν να δημιουργηθούν ιδιωτικά ιδεατά δίκτυα (VPNs) βασισμένα σε IP. Οι πάροχοι υπηρεσιών διαδικτύου (ISPs) μπορούν να δημιουργήσουν IP Tunnels σε όλο το δίκτυο τους, χωρίς την ανάγκη για εφαρμογές κρυπτογράφησης ή εφαρμογές τελικών χρηστών. Μια από τις κοινές εφαρμογές του MPLS VPN επιτυγχάνεται χρησιμοποιώντας την έννοια της εικονικής δρομολόγησης/προώθησης (Virtual Routing/Forwarding - VRF) και στο γεγονός ότι η προώθηση στον κορμό του δικτύου γίνεται χρησιμοποιώντας πακέτα με ετικέτες (εικόνα 1.7). Η τεχνολογία VRF εγγυάται ότι οι πληροφορίες δρομολόγησης των διαφόρων πελατών διαχωρίζονται και το MPLS στον κορμό του δικτύου εγγυάται την προώθηση των πακέτων σύμφωνα με την ετικέτα και όχι με πληροφορίες των IP κεφαλίδων.



Εικόνα 1.7. Εφαρμογή Layer 3 MPLS VPN

Τα MPLS VPNs χωρίζονται σε δύο κατηγορίες:

- Layer 3 MPLS VPN
- Layer 2 MPLS VPN

Το Layer 3 MPLS VPN, γνωστό και σαν L3VPN, συνδυάζει το πρωτόκολλο δρομολόγησης BGP [26], την βασισμένη σε ετικέτες προώθηση στον κορμό του MPLS δικτύου και την τεχνική VRF, για να δημιουργήσει VPN βασισμένα στο IP. Αυτή η τεχνική είναι πιο αποδοτική και παρέχει περισσότερες υπηρεσίες σε σύγκριση με άλλους τύπους VPN όπως το IPsec VPN.

Το Layer 2 MPLS VPN, γνωστό και σαν L2VPN, είναι μια point-to-point Pseudowire υπηρεσία. Κάποιες εφαρμογές L2VPN είναι το Any Transport over MPLS (AToM) της Cisco Systems και το Layer 2 Tunneling Protocol Version 3 (L2TPv3) [19]. Το L2VPN παρέχει μεθόδους μεταφοράς πλαισίων επιπέδου σύνδεσης μέσω ενός MPLS δικτύου. Οι δύο κατηγορίες MPLS VPN αναλύονται σε επόμενο κεφάλαιο.

1.8 Virtual Private LAN Service (VPLS)

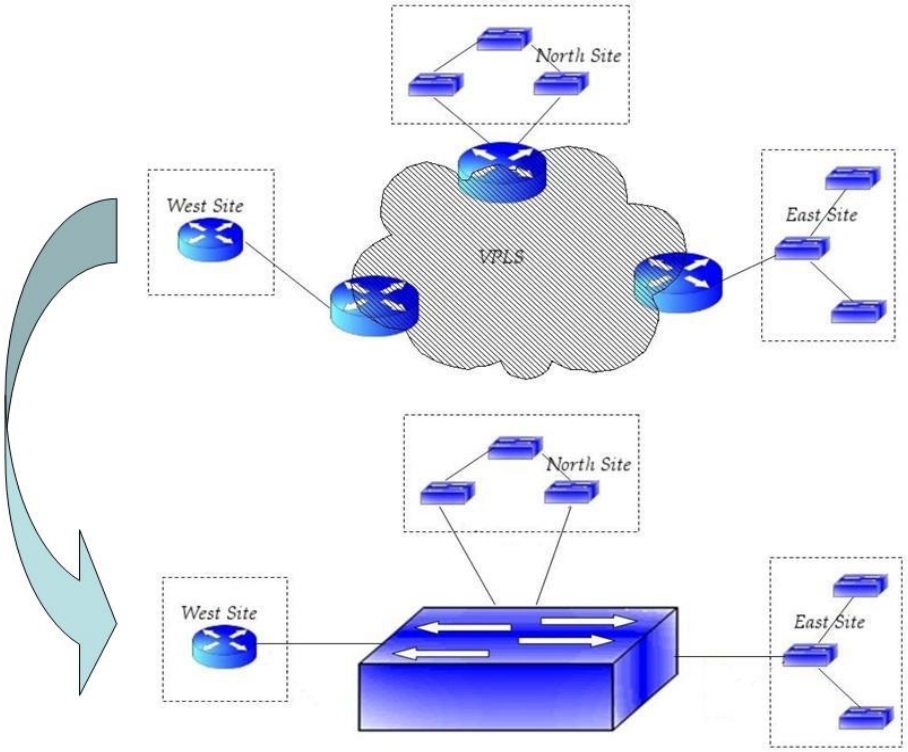
Το VPLS είναι μια υπηρεσία η οποία εξομοιώνει ένα Ethernet LAN. Υπάρχει η ανάγκη αυτής της υπηρεσίας για ποικίλους λόγους. Καταρχήν το Layer 3 MPLS VPN είναι μια υπηρεσία η οποία βασίζεται στο IP. Κανένα άλλο πρωτόκολλο τρίτου επιπέδου δεν μπορεί να μεταφερθεί μέσω ενός MPLS δικτύου με αυτήν την υπηρεσία. Η υπηρεσία AToM (Layer 2 MPLS VPN) επιτρέπει τη μεταφορά όλων των πρωτοκόλλων επιπέδου δικτύου μιας και είναι ικανή να μεταφέρει πλαίσια δευτέρου επιπέδου μέσω ενός MPLS δικτύου. Το μειονέκτημα αυτής της υπηρεσίας είναι ότι είναι point-to-point.

Σε περίπτωση που ένας πελάτης επιθυμούσε να συνδέσει τα τμήματα Ethernet που διαθέτει σε ένα μεγαλύτερο τμήμα (segment), θα έπρεπε να σκεφτεί τα παρακάτω: αν αυτά τα τμήματα βρίσκονται γεωγραφικά κοντά, θα μπορούσε να τοποθετήσει ένα Ethernet Switch ανάμεσα τους. Το Ethernet Switch θα προωθούσε τα unicast πλαίσια, τα multicast πλαίσια και τα broadcast πλαίσια. Στη περίπτωση όμως που τα τμήματα δεν είναι κοντά, δεν μπορεί να τοποθετηθεί κάποιο Ethernet Switch. Σε αυτή τη περίπτωση έρχεται το VPLS, το οποίο λειτουργεί σαν μια λογική γέφυρα πάνω από το MPLS και εξομοιώνει ένα Ethernet LAN. Στην εικόνα 1.8 παρουσιάζεται ένα VPLS δίκτυο, όπου η λειτουργικότητα του παρομοιάζεται με ένα Ethernet μεταγωγέα.

Ένα Ethernet Switch εκτελεί τις παρακάτω λειτουργίες:

- Προώθηση πλαισίων Ethernet
- Προώθηση unicast πλαισίων με άγνωστη διεύθυνση MAC
- Διανομή multicast και broadcast πλαισίων σε περισσότερες από μια διασυνδέσεις
- Πρόβλεψη βρόχων (Loop Prevention)
- Δυναμική εκμάθηση MAC διευθύνσεων

Μια υπηρεσία VPLS θα πρέπει επίσης να έχει τα παραπάνω χαρακτηριστικά.



Εικόνα 1.8. Λειτουργικότητα VPLS δικτύου

1.9 Generalized MPLS (GMPLS)

Κατά τα τέλη της δεκαετίας του 1990 τα δίκτυα που βασίζονταν στη πολύπλεξη μήκους κύματος (WDM) ήταν αρκετά δημοφιλή. Οι κατασκευαστές και οι παροχείς υπηρεσιών ξεκίνησαν να αναζητούν μια έξυπνη τεχνολογία, η οποία θα μείωνε το κόστος εφαρμογής και θα προσέφερε νέες υπηρεσίες. Διαπίστωσαν ότι η βασική λειτουργία μεταγωγής σε ένα WDM δίκτυο ήταν παρόμοια με την λειτουργία μιας MPLS συσκευής. Ένας μεταγωγέας WDM αντιστοιχεί ένα εισερχόμενο μήκος κύματος από μια εισερχόμενη διασύνδεση σε ένα εξερχόμενο μήκος κύματος και μια εξερχόμενη διασύνδεση, παρόμοια με την αντιστοίχιση εισερχόμενης και εξερχόμενης ετικέτας στο MPLS. Αυτή η αρχική παρατήρηση έδωσε το έναυσμα για την δημιουργία νέων δυνατοτήτων του MPLS και έτσι εμφανίστηκε το MPλS ή MPLambdaS.

Στη συνέχεια εμφανίστηκαν και άλλες τεχνολογίες οπτικής μεταγωγής. Έτσι η τεχνική MPλS διευρύνθηκε ώστε να καλύπτει μεταγωγή σε οπτικές ίνες, TDM δίκτυα, μεταγωγή δευτέρου επιπέδου και την υπάρχουσα μεταγωγή πακέτων και κελιών. Έτσι το θέμα γενικεύτηκε και το όνομα που πήρε ήταν Generalized MPLS [18].

1.10 Επίλογος

Στο παρόν κεφάλαιο περιγράφηκαν τα βασικά στοιχεία της τεχνολογίας του MPLS και επίσης έγινε μια αναφορά στα επίπεδα της δρομολόγησης. Αναφέρθηκαν βασικά στοιχεία που απαρτίζουν ένα MPLS δίκτυο όπως οι ενδιάμεσοι δρομολογητές μεταγωγής ετικέτας (LSRs), οι οριακοί δρομολογητές (LERs) και οι διαδρομές μεταγωγής ετικέτας (LSPs). Παρουσιάστηκε ο αλγόριθμος μεταγωγής ετικέτας στη γενική του μορφή και ένας απλός τρόπος διανομής ετικετών μεταξύ των LSR. Έγινε μια περιληπτική αναφορά στις σημαντικότερες εφαρμογές του MPLS όπως Traffic Engineering, MPLS VPN και VPLS, οι οποίες θα αναλυθούν σε επόμενα κεφάλαια. Στο επόμενο κεφάλαιο αναλύεται η ετικέτα του MPLS και η λογική λειτουργίας του.

2

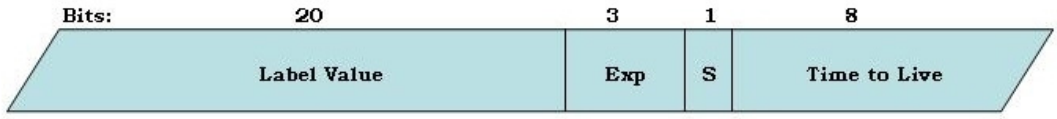
Αρχιτεκτονική & Λειτουργία MPLS

2.1 Εισαγωγή

Στο παρόν κεφάλαιο παρουσιάζεται η λειτουργία του MPLS. Η έννοια της μεταγωγής ετικέτας (Label Switching) σημαίνει ότι τα πακέτα που κινούνται στο δίκτυο είναι επισημασμένα, χωρίς να παίζει ρόλο αν αυτά τα πακέτα ήταν ipv4, ipv6 πακέτα ή πλαίσια δευτέρου επιπέδου. Αναλύεται η δομή της ετικέτας και ο τρόπος με τον οποίο διανέμεται ανάμεσα στους δρομολογητές. Επίσης αναφέρονται χαρακτηριστικά των πακέτων όπως ο χρόνος ζωής (TTL) και το MTU.

2.2 Η ετικέτα του MPLS

Η ετικέτα του MPLS (εικόνα 2.1) είναι μια ακολουθία των 32 bit με μια συγκεκριμένη εσωτερική δομή.



Εικόνα 2.1. Η δομή μιας MPLS ετικέτας

Τα πρώτα 20 bit είναι η κυρίως ετικέτα, η οποία χρησιμοποιείται για την μεταγωγή. Η τιμή που μπορεί να έχει κυμαίνεται από 0 ως 2^{20}-1 ή 1048575. Παρόλα αυτά, οι πρώτες 16 (0-15) τιμές είναι δεσμευμένες. Τα τρία EXP bit, που ακολουθούν την κυρίως ετικέτα, είναι πειραματικά. Στην πραγματικότητα χρησιμοποιούνται αποκλειστικά για την αναπαράσταση της ποιότητας υπηρεσίας (QoS). Το S bit ή Bottom of Stack δηλώνει την ύπαρξη ή όχι επόμενης ετικέτας στη στοίβα. Αν το S bit είναι 0 τότε ακολουθεί κι άλλη ετικέτα στη στοίβα, ενώ αν είναι 1 τότε η ετικέτα είναι η τελευταία της στοίβας. Τα τελευταία οχτώ bit είναι

αφιερωμένα στο χρόνο ζωής ενός πακέτου (TTL). Η λειτουργία του TTL είναι ακριβώς ίδια με αυτή ενός IP πακέτου. Δηλαδή σε κάθε δρομολογητή μειώνεται κατά 1 και σε περίπτωση που φθάσει 0 το πακέτο απορρίπτεται.

2.2.1 Η στοίβα ετικετών

Κάποιοι LSR μπορεί να χρειαστούν περισσότερες από μια ετικέτες για τη μεταγωγή του πακέτου μέσω του MPLS δικτύου. Αυτό γίνεται προσθέτοντας τις ετικέτες σε μια στοίβα, η μορφή της οποίας φαίνεται στην εικόνα 2.2. Η επεξεργασία γίνεται πάντα με βάση την ετικέτα στην κορυφή της στοίβας. Αν το πλήθος ετικετών της στοίβας είναι m, τότε μπορεί κανείς να αναφερθεί στην ετικέτα στη βάση της στοίβας σαν ετικέτα επιπέδου 1 και στην ετικέτα της κορυφή σαν ετικέτα επιπέδου m.

Label	EXP	0	TTL
Label	EXP	0	TTL
.....			
Label	EXP	1	TTL

Εικόνα 2.2. Η στοίβα ετικετών του MPLS

Μερικές εφαρμογές του MPLS χρειάζονται περισσότερες από μια ετικέτες στη στοίβα για να προωθήσουν τα πακέτα. Παράδειγμα τέτοιων εφαρμογών είναι το MPLS VPN και το AToM.

Η στοίβα ετικετών τοποθετείται μπροστά από την πληροφορία επιπέδου δικτύου και μετά τη πληροφορία επιπέδου σύνδεσης. Η τεχνολογία επιπέδου σύνδεσης μπορεί να είναι οποιαδήποτε τεχνολογία που υποστηρίζει ο LSR (PPP, HDLC, Ethernet, κοκ.). Έστω ότι το πρωτόκολλο επιπέδου δικτύου είναι το IPv4 και η τεχνολογία επιπέδου σύνδεσης είναι PPP, τότε η στοίβα ετικετών βρίσκεται μετά την κεφαλίδα του PPP και πριν την κεφαλίδα του IPv4. Έτσι επειδή η στοίβα ετικετών τοποθετείται πριν το επίπεδο δικτύου, πρέπει να υπάρξουν νέες τιμές στο πεδίο Data Link Layer Protocol Field οι οποίες να υποδεικνύουν το MPLS πακέτο που ακολουθεί. Η τιμή Data Link Layer Protocol Field παριστάνει το είδος του φορτίου ενός πλαισίου δευτέρου επιπέδου. Στον πίνακα 2.1 φαίνονται οι τιμές του Data Link Layer Protocol Field για κάποιες τεχνολογίες σύνδεσης, όταν αυτό που ακολουθεί είναι ένα MPLS πακέτο.

Πίνακας 2.1. Οι τιμές του Data Link Layer Protocol Field για MPLS πακέτα

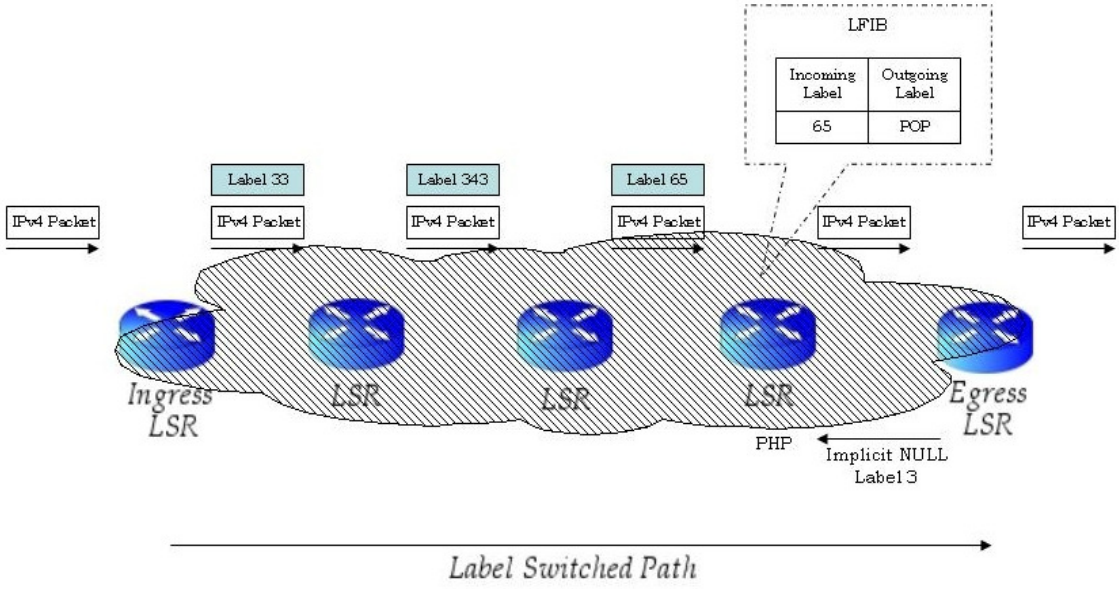
Layer 2 Encapsulation Type	Layer 2 Protocol Identifier Name	Value (hex)
PPP	PPP Protocol Field	0281
Ethernet	Ethertype Value	8847
HDLC	Protocol	8847
Frame Relay	NLPID(Network Level Protocol ID)	80

2.2.2 Δεσμευμένες ετικέτες

Όπως προαναφέρθηκε οι πρώτες 16 ετικέτες, δηλαδή από 0 ως 15 είναι δεσμευμένες. Υπό κανονικές συνθήκες δεν χρησιμοποιούνται από τον LSR για την προώθηση πακέτων. Όταν αποδοθεί μια από αυτές τις ετικέτες πραγματοποιείται μια συγκεκριμένη λειτουργία. Αξίζει να σημειώσουμε τις παρακάτω δεσμευμένες ετικέτες:

- Implicit NULL: είναι η ετικέτα με τιμή 3. Ένας οριακός δρομολογητής εξόδου (Egress LSR) αποδίδει την ετικέτα 3 σε ένα FEC εάν θέλει να σταλούν τα πακέτα του FEC χωρίς ετικέτα. Οι ετικέτες αποδίδονται με διεύθυνση αντίθετη της κυκλοφορίας των πακέτων. Για κάθε συνεδρία, ένας LSR (upstream LSR) κάνει μια αίτηση για ετικέτα στον επόμενο του (downstream LSR) και αυτός του αποδίδει μια ετικέτα. Έτσι αν σε έναν LSR έχει αποδοθεί η ετικέτα 3, τότε αυτός ο LSR θα στείλει πακέτα στον επόμενο του τα οποία δεν θα έχουν ετικέτες.

  Γενικά όταν ένας egress LSR λάβει ένα επισημασμένο πακέτο τότε το πρώτο που θα κάνει είναι να ψάξει στον πίνακα ILM και να βρει την αντιστοίχηση εισερχόμενης ετικέτας με εισερχόμενη διασύνδεση και εξερχόμενης ετικέτας με εξερχόμενη διασύνδεση. Αν ο egress LSR προωθήσει το πακέτο εκτός του MPLS δικτύου, η απόφαση προώθησης θα γίνει βάση της διεύθυνσης δικτύου. Έτσι θα αφαιρέσει την ετικέτα του πακέτου και θα ψάξει τον επόμενο κόμβο σύμφωνα με την διεύθυνση επιπέδου δικτύου. Εν συνεπεία, η πρώτη αναζήτηση στον ILM είναι περιττή. Σε αυτό στοχεύει και η ετικέτα implicit NULL. Ο egress LSR την αποδίδει στον προηγούμενο του (penultimate) και αυτός μόλις θελήσει να στείλει πακέτα στον egress βλέπει την ετικέτα με τιμή 3 και αντί να την αντικαταστήσει στο πακέτο βγάζει και την προϋπάρχουσα και στέλνει το πακέτο. Η μέθοδος αυτή ονομάζεται Penultimate Hop Popping (PHP) και παρουσιάζεται στην εικόνα 2.3.



Εικόνα 2.3. Η μέθοδος PHP

- Explicit NULL: είναι η ετικέτα με τιμή 0. Όταν κάποιος LSR χρησιμοποιεί την ετικέτα implicit NULL, τότε θα αφαιρέσει μια ετικέτα από τη στοίβα και θα μείνουν οι επόμενες ετικέτες της στοίβας. Αν το πακέτο περιείχε μια ετικέτα στη στοίβα του, τότε θα προωθεί χωρίς ετικέτες στον επόμενο LSR, ο οποίος έχει αποδώσει την implicit NULL ετικέτα. Αφαιρώντας όμως την ετικέτα του πακέτου χάνεται και η πληροφορία της ποιότητας υπηρεσίας (QoS) που βρίσκεται στα EXP bits. Σε αυτήν την περίπτωση μπορούμε να χρησιμοποιήσουμε την explicit null ετικέτα. Ο egress LSR στέλνει αυτήν την ετικέτα στον προηγούμενο του και εκείνος όταν δει στον πίνακα προώθησης του την ετικέτα με τιμή 0, κάνει κανονικά την αντικατάσταση και προωθεί το πακέτο. Ο egress LSR όταν θα λάβει επισημασμένο πακέτο με ετικέτα 0, θα διαβάσει τα EXP bits για να βρει την ποιότητα υπηρεσίας και θα αφαιρέσει την ετικέτα.
- Router Alert Label: είναι η ετικέτα με τιμή 1. Μπορεί να βρίσκεται οπουδήποτε μέσα στη στοίβα εκτός από το τέλος της στοίβας. Όταν μια ετικέτα με τιμή 1 βρίσκεται στην κορυφή της στοίβας, τότε ο LSR πρέπει να ελέγξει καλύτερα το πακέτο. Έτσι το πακέτο ελέγχεται χρησιμοποιώντας κάποιες διαδικασίες λογισμικού. Η ετικέτα αυτή είναι παρόμοια με την επιλογή Router Alert ενός IP πακέτου.
- OAM (Operation and Maintenance) Label: έχει τιμή 13 και χρησιμοποιείται για κυρίως έλεγχο σφαλμάτων και εποπτεία της απόδοσης του δικτύου.

2.3 Αντιστοιχίσεις ετικετών-FEC / Πίνακας Προώθησης MPLS

Όσον αφορά στον πίνακα που δημιουργείται στους LSR για την αντιστοίχηση των FEC με ετικέτες και τον τελικό πίνακα προώθησης θα εξηγηθούν οι παρακάτω όροι: Next Hop Label Forwarding entry (NHLFE), Incoming Label Map(ILM), FEC to NHLFE (FTN).

- NHLFE (Next Hop Label Forwarding entry): χρησιμοποιείται για την προώθηση ενός πακέτου και περιέχει την παρακάτω πληροφορία:
  - Το επόμενο βήμα του πακέτου
  - Τη λειτουργία που πρέπει να πραγματοποιηθεί στη στοίβα ετικετών (αντικατάσταση, αφαίρεση, κοκ.).
  - Το επίπεδο σύνδεσης που πρέπει να χρησιμοποιηθεί όταν αποστέλλεται το πακέτο
- ILM (Incoming Label Map): αντιστοιχεί κάθε εισερχόμενη ετικέτα σε ένα σύνολο από NHLFE. Χρησιμοποιείται για την προώθηση πακέτων τα οποία είναι επισημασμένα. Αν ο ILM αντιστοιχήσει μια συγκεκριμένη ετικέτα σε περισσότερα από ένα NHLFE, τότε ένα από αυτά πρέπει να επιλεχθεί πριν την προώθηση του πακέτου. Το ότι μπορεί υπάρχει αυτή η ένα προς πολλά αντιστοίχηση είναι κάποιες φορές χρήσιμο, όπως όταν είναι επιθυμητό να μοιραστεί η κίνηση μεταξύ δύο ή περισσοτέρων διαδρομών ή για multicast προώθηση.
- FTN (FEC to NHLFE): αντιστοιχεί κάθε FEC σε ένα ή περισσότερα NHLFE. Χρησιμοποιείται για την προώθηση πακέτων τα οποία ακόμα δεν έχουν ετικέτα (στους ingress LSRs), αλλά αποκτούν μια πριν προωθηθούν.

Σύμφωνα με τη Cisco Systems θα μπορούσε κανείς να συνοψίσει τα παραπάνω σε δύο πίνακες, τον Label Information Base(LIB) και τον Label Forwarding Information Base (LFIB).

- LIB: ο πίνακας αυτός περιέχει τις εισερχόμενες ετικέτες (local bindings) και όλες τις πιθανές εξερχόμενες ετικέτες (remote bindings) για κάθε FEC.
- LFIB: είναι ο πίνακας που χρησιμοποιείται για την προώθηση των επισημασμένων πακέτων. Περιέχει τις εισερχόμενες και τις εξερχόμενες ετικέτες για κάθε LSP. Η εισερχόμενη ετικέτα είναι το local binding του συγκεκριμένου LSR και η εξερχόμενη ένα από τα remote bindings το οποίο έχει επιλεχθεί από τον πίνακα LIB. Η επιλογή αυτή εξαρτάται κυρίως από την καλύτερη διαδρομή την οποία φανερώνει ο πίνακας δρομολόγησης.

Στη συνεχεία, όσον αφορά στους πίνακες προώθησης, θα χρησιμοποιηθεί η ονοματολογία της Cisco Systems, δηλαδή LIB και LFIB.

2.4 MPLS Modes

Ένας LSR χρησιμοποιεί τρεις καταστάσεις (modes) για τη διανομή ετικετών σε άλλους LSRs, την διατήρηση των ετικετών στους πίνακες προώθησης και την ανάθεση ετικετών σε FEC. Παρακάτω αναλύονται αυτές οι τρεις καταστάσεις:

- Κατάσταση Διανομής Ετικέτας (Label Distribution Mode)
- Κατάσταση Διατήρησης Ετικέτας (Label Retention Mode)
- Κατάσταση Ελέγχου LSP (LSP Control Mode)

2.4.1 Label Distribution Mode

Το MPLS υποστηρίζει δύο τεχνικές για τη διανομή ετικετών:

- Downstream on Demand (DoD)
- Unsolicited Downstream (UD)

Όταν χρησιμοποιείται η τεχνική DoD κάθε LSR κάνει μια αίτηση ετικέτας, για κάποιο συγκεκριμένο FEC, στον επόμενο του LSR (downstream LSR). Έτσι κάθε LSR λαμβάνει μια ετικέτα για κάθε FEC (remote binding) από τον downstream LSR του, ο οποίος είναι ο επόμενος LSR όπως αυτός καθορίζεται από κάποιο πρωτόκολλο δρομολόγησης.

Αντίθετα όταν χρησιμοποιείται η UD τεχνική, κάθε LSR διανέμει τις αντιστοιχήσεις που έχει κάνει στους γειτονικούς του LSR, χωρίς αυτοί να ζητήσουν κάποια ετικέτα. Έτσι ο LSR λαμβάνει ετικέτες για κάθε FEC από κάθε γειτονικό του LSR.

Στην περίπτωση της DoD τεχνικής ο LIB πίνακας έχει μόνο ένα remote binding ανά FEC, ενώ στην UD τεχνική πιθανόν να υπάρχουν περισσότερα από ένα. Τέλος, η τεχνική διανομής ετικέτας μπορεί να εξαρτάται από τη διασύνδεση και την συγκεκριμένη εφαρμογή.

2.4.2 Label Retention Mode

Δυο τεχνικές διατήρησης ετικέτας είναι πιθανές:

- Liberal Label Retention (LLR)
- Conservative Label Retention (CLR)

Στην τεχνική LLR, ένας LSR κρατάει όλες τις απομακρυσμένες αντιστοιχήσεις (remote bindings) που λαμβάνει και τις εγκαθιστά στον LIB. Μια από αυτές τις απομακρυσμένες αντιστοιχήσεις, η οποία έχει ληφθεί από τον downstream LSR του, θα εγκατασταθεί στον LFIB. Οι υπόλοιπες κρατούνται στον LIB για λόγους ασφάλειας (πχ. σε περίπτωση που αποτύχει κάποια σύνδεση και χρειαστεί να αλλάξει το επόμενο βήμα για κάποιο FEC, αυτό θα βρίσκεται ήδη στον πίνακα LIB).

Όσον αφορά στην τεχνική CLR, ο LSR που την υιοθετεί δεν κρατά όλες τις απομακρυσμένες αντιστοιχήσεις στον LIB, παρά μόνο αυτήν που σχετίζεται με το επόμενο βήμα για κάποιο συγκεκριμένο FEC

Σε γενικές γραμμές, η τεχνική LLR παρέχει πιο γρήγορη προσαρμογή σε αλλαγές δρομολόγησης, ενώ η CLR αποθηκεύει λιγότερες ετικέτες, κάνοντας καλύτερη χρήση της διαθέσιμης μνήμης ενός LSR.

2.4.3 LSP Control Modes

Μπορεί να δημιουργηθεί μια τοπική αντιστοίχηση ετικέτας/FEC (local binding) με δύο τρόπους:

- Independent LSP Control Mode
- Ordered LSP Control Mode

Ένας LSR μπορεί να κάνει μια τοπική αντιστοίχηση για ένα FEC ανεξάρτητα από τους άλλους (Independent LSP Control). Σε αυτήν την περίπτωση ένας LSR κάνει την αντιστοίχηση για ένα FEC εφόσον αναγνωρίζει το συγκεκριμένο FEC, δηλαδή εφόσον το πρόθεμα δικτύου για αυτό το FEC υπάρχει στον πίνακα δρομολόγησης του.

Αντίθετα στην τεχνική Ordered LSP Control, ένας LSR κάνει μια αντιστοίχηση για ένα FEC μόνον στην περίπτωση που ο ίδιος είναι ο egress LSR για το

συγκεκριμένο FEC ή αν έχει ήδη λάβει ένα remote binding για το συγκεκριμένο FEC από τον downstream LSR του.

Το μειονέκτημα της Independent Control τεχνικής είναι ότι κάποιοι LSR ξεκινούν να επισημαίνουν πακέτα πριν δημιουργηθεί ολόκληρο το LSP. Έτσι το πακέτο δεν θα προωθηθεί όπως πρέπει και μπορεί επίσης και να απορριφθεί.

Οι τεχνικές Independent LSP Control Mode και Ordered LSP Control Mode μπορούν να λειτουργήσουν ταυτόχρονα σε ένα MPLS δίκτυο. Είναι τοπικό ζήτημα, δηλαδή αφορά στον κάθε LSR ξεχωριστά.

2.5 Επιλογή διαδρομής

Η επιλογή της διαδρομής αναφέρεται στη μέθοδο επιλογής ενός LSP για ένα συγκεκριμένο FEC. Υπάρχουν δυο τεχνικές:

- Βήμα προς βήμα δρομολόγηση (Hop by hop routing)
- Ακριβής δρομολόγηση (Explicit routing)

Στην βήμα προς βήμα δρομολόγηση κάθε κόμβος μπορεί ανεξάρτητα να επιλέξει τον επόμενο κόμβο για κάποιο FEC. Αυτός είναι ο τρόπος με τον οποίο λειτουργούν και τα IP δίκτυα. Αντίθετα, στην ακριβή δρομολόγηση δεν επιλέγει κάθε LSR τον επόμενο του αλλά ένας LSR, ο ingress ή ο egress, επιλέγει όλους ή μερικούς από τους ενδιάμεσους LSRs για να συνθέσει ένα LSP.

Εάν ένας LSR επιλέξει ολόκληρο το LSP, τότε το LSP λέγεται αυστηρώς καθορισμένο. Αν ένας LSR καθορίσει μερικούς από τους ενδιάμεσους LSRs, το LSP λέγεται χαλαρά καθορισμένο. Η σειρά των LSR ενός LSP, όσον αφορά στην ακριβή δρομολόγηση, μπορεί να οριστεί στατικά με χρήση κατάλληλων ρυθμίσεων ή δυναμικά από κάποιον κόμβο.

Η χρήση ακριβής δρομολόγησης μπορεί να φανεί χρήσιμη για διάφορους σκοπούς, όπως traffic engineering και για εφαρμογή πολιτικών διαχείρισης. Επίσης στο MPLS μια ακριβής διαδρομή μπορεί να καθοριστεί τη στιγμή ανάθεσης των ετικετών και παράλληλα δεν χρειάζεται να καθοριστεί για κάθε IP πακέτο ξεχωριστά.

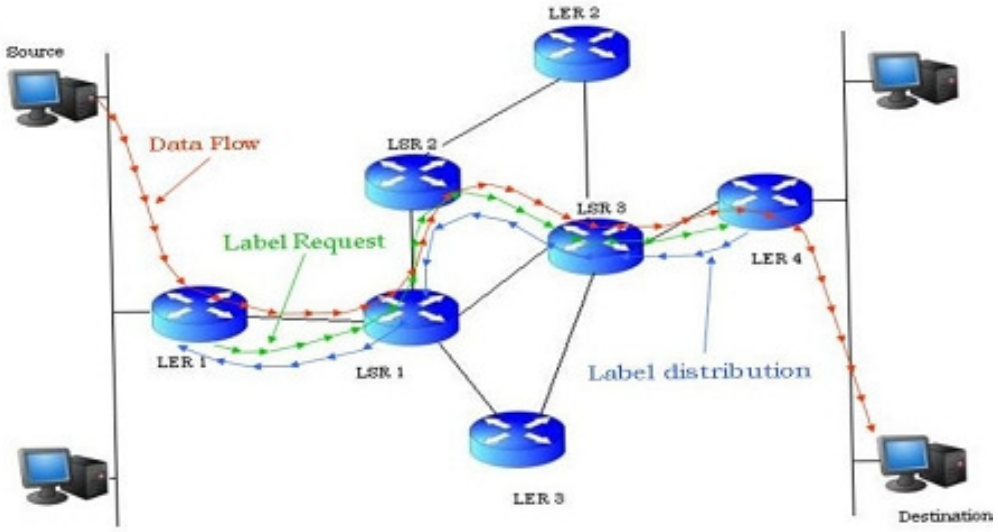
2.6 Λειτουργία MPLS

Κατά την διαδρομή ενός πακέτου μέσω ενός MPLS δικτύου συμβαίνουν τα ακόλουθα:

1. Δημιουργία ετικετών και διανομή
2. Δημιουργία πινάκων σε κάθε LSR
3. Δημιουργία LSP
4. Εισαγωγή ετικέτας / Αναζήτηση στον πίνακα
5. Προώθηση πακέτου

Δεν είναι απαραίτητο όλη η κίνηση από μια πηγή να μεταφερθεί μέσω του ίδιου LSP. Ανάλογα με τα χαρακτηριστικά της κίνησης, διαφορετικά LSP μπορεί να δημιουργηθούν με διαφορετικές απαιτήσεις ποιότητας υπηρεσίας.

Πριν ξεκινήσει οποιαδήποτε κίνηση οι δρομολογητές αποφασίζουν στην αντιστοίχηση μιας ετικέτας σε κάποιο συγκεκριμένο FEC ώστε να δημιουργηθούν οι πίνακες. Οι downstream LSRs ξεκινούν την αντιστοίχηση και τη διανομή ετικετών, όπως φαίνεται στην εικόνα 2.4 με τα μπλε βελάκια.



Εικόνα 2.4. Αιτήσεις/Διανομές ετικετών και ροή κινήσεως

Επιπρόσθετα, χαρακτηριστικά της κίνησης και τυχόν δυνατότητες των LSRs γίνονται γνωστές στους υπόλοιπους χρησιμοποιώντας το πρωτόκολλο διανομής ετικετών. Για την ανταλλαγή των μηνυμάτων LDP χρησιμοποιείται το πρωτόκολλο επιπέδου μεταφοράς TCP [16], έτσι ώστε να προσφέρεται αξιοπιστία στη μεταφορά.

Κατά την παραλαβή των αντιστοιχίσεων κάθε LSR δημιουργεί εγγραφές στον πίνακα LIB. Ο LIB περιλαμβάνει όλα τα remote bindings που έχει λάβει για κάποιο FEC. Για παράδειγμα, ο LSR 1 (εικόνα 2.4) θα λάβει για κάποιο FEC (το FEC το οποίο περιλαμβάνει την διεύθυνση του προορισμού όπως φαίνεται στην εικόνα 2.4) αντιστοιχήσεις από τους LSR 2, LSR 3, LER 3. Στη συνέχεια θα δημιουργήσει τον πίνακα LFIB ο οποίος θα περιέχει μια από τις παραπάνω αντιστοιχήσεις (αυτήν που επιλέγεται σαν καλύτερη από το πρωτόκολλο δρομολόγησης). Στο παραπάνω σενάριο θα εισάγει στον LFIB την αντιστοίχηση ετικέτας/FEC που έλαβε από τον LSR 2. Ο LFIB θα περιέχει την εισερχόμενη ετικέτα και εισερχόμενη διασύνδεση και την εξερχόμενη ετικέτα και εξερχόμενη διασύνδεση για το συγκεκριμένο FEC. Οι παραπάνω εγγραφές μπορούν να ανανεωθούν σε περίπτωση κάποιας αλλαγής στη δρομολόγηση.

Όπως φαίνεται και από τα μπλε βελάκια, τα LSP δημιουργούνται με φορά αντίθετη της ροής δεδομένων. Εφόσον έχει δημιουργηθεί το LSP, κάθε LSR που θα λάβει ένα επισημασμένο πακέτο θα αναζητήσει την εισερχόμενη ετικέτα στον LFIB και θα την αντικαταστήσει με την εξερχόμενη. Όταν το πακέτο φθάσει στον LER 4 θα αφαιρεθεί η ετικέτα και το πακέτο θα προωθηθεί στον προορισμό του.

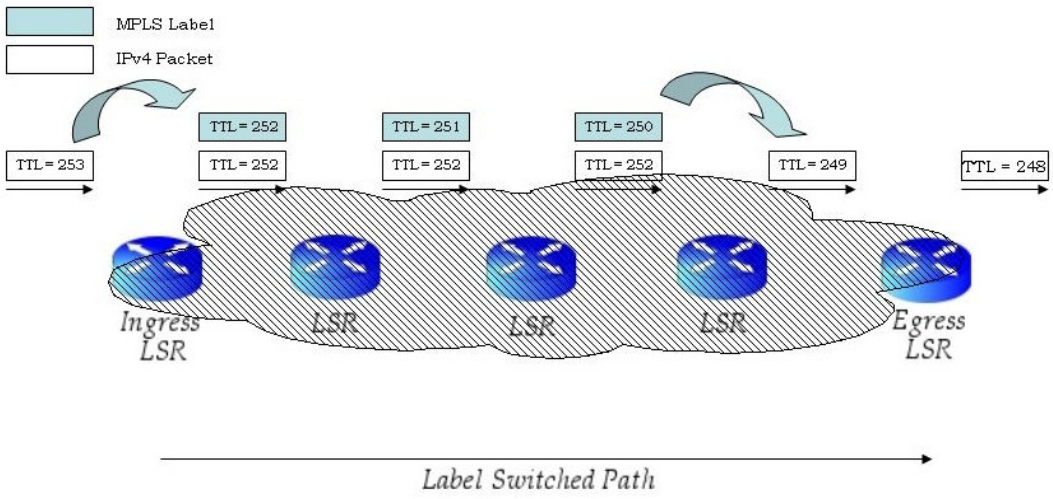
Έστω ένα πακέτο αποστέλλεται από την πηγή στον προορισμό του, σύμφωνα με το παραπάνω σενάριο. Εισέρχεται στο MPLS δίκτυο από τον LER 1 και φεύγει από τον LER 4. Έστω ότι ο LER 1 δεν έχει κάποια ετικέτα για το συγκεκριμένο FEC στο οποίο θα αντιστοιχήσει το πακέτο μιας και είναι η πρώτη του εμφάνιση και θα κάνει αίτηση για μια ετικέτα. Σε ένα IP δίκτυο θα γινόταν μια σύγκριση της IP διεύθυνσης με ένα πρόθεμα στον πίνακα δρομολόγησης για να βρεθεί ο επόμενος δρομολογητής που θα έπρεπε να σταλεί το πακέτο. Έστω ότι αυτός ο επόμενος δρομολογητής είναι ο LSR 1. Έτσι ο LER 1 θα κάνει μια αίτηση για ετικέτα στον LSR 1. Αυτή η αίτηση θα φτάσει αναδρομικά στον LER 4, όπως φαίνεται από τα πράσινα βελάκια. Κάθε ενδιάμεσος LSR θα λάβει μια ετικέτα από τον downstream LSR του (τον επόμενο του). Έτσι το LSP θα εγκατασταθεί από τον LER 4 προς τον LER 1, όπως φαίνεται από τα μπλε βελάκια, χρησιμοποιώντας το LDP ή κάποιο άλλο πρωτόκολλο διανομής. Στη συνέχεια ο LER 1 θα εισάγει στο πακέτο την ετικέτα, που έχει λάβει από τον LSR 1, και θα το προωθήσει στον LSR 1. Η αντικατάσταση της ετικέτας θα πραγματοποιείται μέχρι το πακέτο να φθάσει στον LER 4 ο οποίος θα αφαιρέσει την ετικέτα και θα προωθήσει το πακέτο στον προορισμό του. Η διαδρομή που θα ακολουθήσει το πακέτο φαίνεται από τα κόκκινα βελάκια.

2.7 Χρόνος Ζωής Πακέτων (TTL)

Στη συμβατική IP προώθηση κάθε πακέτο μεταφέρει στην κεφαλίδα του ένα πεδίο, το οποίο ονομάζεται Time to Live (TTL). Είναι ο χρόνος ζωής του πακέτου. Όταν το πακέτο περνά από έναν δρομολογητή, το TTL μειώνεται κατά ένα. Στη περίπτωση που το TTL φθάσει μηδέν πριν την παράδοση του πακέτου στον προορισμό του, το πακέτο απορρίπτεται και αποστέλλεται στην πηγή του πακέτου ένα ICMP [25] μήνυμα (type:11, code:0).

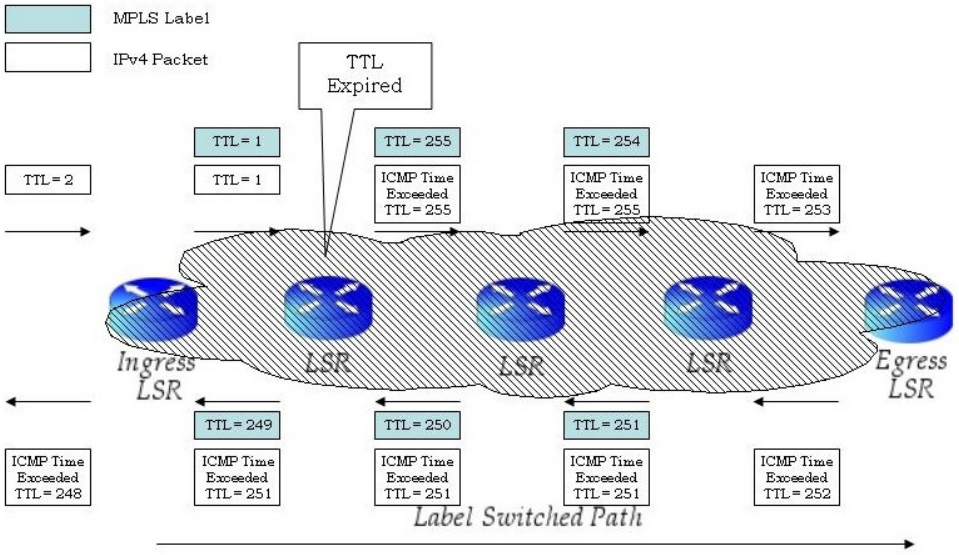
Ο μηχανισμός αυτός προσφέρει ένα επίπεδο προστασίας κατά των βρόγχων που ίσως υπάρχουν λόγω εσφαλμένης ρύθμισης των συσκευών, αποτυχίας αυτών ή αργής σύγκλησης των αλγόριθμων δρομολόγησης. Το TTL χρησιμοποιείται και για άλλες λειτουργίες, όπως η εκτέλεση της εντολής *traceroute*.

Στο MPLS η χρήση του TTL είναι ίδια με αυτήν ενός δικτύου IP. Μέσα το MPLS δίκτυο το TTL πεδίο της ετικέτας μειώνεται κατά ένα καθώς περνάει από κάθε LSR. Κατά την είσοδο του στο MPLS δίκτυο το πεδίο TTL του IP αντιγράφεται στο πεδίο TTL του MPLS αφού μειωθεί κατά ένα. Παρόμοια και κατά την έξοδο του, το TTL του MPLS αντιγράφεται στο IP (εικόνα 2.5). Υπάρχει επίσης και ένας άλλος τρόπος, σύμφωνα με τον οποίο δεν αντιγράφεται το TTL στην ετικέτα του MPLS, αλλά το TTL του MPLS γίνεται 255 και μειώνεται σε κάθε LSR. Έτσι φθάνοντας στον egress LSR η ετικέτα εξάγεται και εκείνη τη στιγμή μειώνεται κατά ένα και το TTL του IP πακέτου. Με αυτόν τον τρόπο, ολόκληρο το MPLS δίκτυο φαίνεται στο TTL σαν ένας κόμβος.



Εικόνα 2.5. Χρήση του πεδίου TTL σε ένα MPLS δίκτυο

Στην περίπτωση που θα λήξει ο χρόνος ζωής του πακέτου μέσα στο MPLS δίκτυο δημιουργείται πάλι ένα ICMP μήνυμα (type:11, code:0), με την μόνη διαφορά ότι δεν επιστρέφει κατευθείαν στον αποστολέα του και αυτό γιατί ο ενδιάμεσος LSR, στον οποίο απορρίφθηκε το πακέτο, μπορεί να μην γνωρίζει τον τρόπο να στείλει στον αποστολέα το μήνυμα. Μία τέτοια περίπτωση είναι το MPLS VPN, στο οποίο οι ενδιάμεσοι LSRs δεν διαθέτουν VPN πίνακες δρομολόγησης. Έτσι, το ICMP μήνυμα προωθείται πάνω στο LSP που ακολουθούσε το απορριφθέν πακέτο προς τον egress LSR (εικόνα 2.6). Ο egress LSR στέλνει το μήνυμα πίσω στον αποστολέα πάλι διαμέσου του MPLS δικτύου.



Εικόνα 2.6. Λήξη TTL εντός MPLS δικτύου

2.8 MPLS MTU

Το MTU (Maximum Transmission Unit) αναπαριστά το μέγιστο μέγεθος των πλαισίων ή πακέτων τα οποία περνούν από μια διασύνδεση χωρίς να τεμαχιστούν σε μικρότερα κομμάτια. Στα MPLS δίκτυα ο όρος MTU αναφέρεται στα επισημασμένα πακέτα. Αν έχουμε για παράδειγμα ένα IP δίκτυο το οποίο ενσωματώνει MPLS, τα πακέτα που προωθούνται έχουν μια ή περισσότερες ετικέτες και αυτό συνεπάγεται μεγαλύτερο μέγεθος (αριθμός ετικετών * 4 Bytes).

Για την αποφυγή τεμαχισμού των πακέτων απαιτείται η αύξηση του MTU στους LSRs σύμφωνα με τον αριθμό ετικετών της στοίβας. Για παράδειγμα, αν το πρωτόκολλο σύνδεσης είναι το Ethernet, το εξ' ορισμού MTU είναι 1500. Αν γνωρίζουμε ότι θα χρειαστούν δύο ετικέτες στη στοίβα για την προώθηση των πακέτων τότε μπορούμε να αυξήσουμε το MTU κατά 8 byte (4 byte κάθε ετικέτα). Στην εικόνα 2.7 φαίνεται η αύξηση του MTU σε ένα δρομολογητή της Cisco.

```
london#show mpls interfaces fastEthernet 2/6 detail
Interface FastEthernet2/6:
        IP labeling enabled
        LSP Tunnel labeling not enabled
        BGP labeling not enabled
        MPLS not operational
        MTU = 1500
london#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
london(config)#interface FastEthernet2/6
london(config-if)#mpls mtu 1508
london(config-if)#^Z
london#
london#show mpls interfaces fastEthernet 2/6 detail
Interface FastEthernet2/6:
        IP labeling enabled
        LSP Tunnel labeling not enabled
        BGP labeling not enabled
        MPLS not operational
        MTU = 1508
```

Εικόνα 2.7. Αύξηση MPLS MTU

2.9 Επίλογος

Στο παρόν κεφάλαιο αναλύθηκαν θέματα που αφορούν στην ετικέτα του MPLS. Μια ετικέτα είναι μέρος της στοίβας ετικετών που τοποθετείται στην κεφαλίδα ενός πακέτου. Υπάρχουν δεσμευμένες ετικέτες οι οποίες χρησιμοποιούνται για ειδικές λειτουργίες όπως η τεχνική PHP (Penultimate Hop Popping). Για την διανομή των ετικετών και την δημιουργία του LSP οι LSRs διαθέτουν κάποιες διαφορετικές καταστάσεις, όπως Downstream on Demand ή Unsolicited Downstream διανομή ετικετών. Δυο τεχνικές υπάρχουν για την επιλογή ενός LSP, η βήμα προς βήμα δρομολόγηση και η ακριβής δρομολόγηση. Επίσης περιγράφηκε ο τρόπος λειτουργίας του MPLS, από την δημιουργία μιας ετικέτας ως την προώθηση ενός πακέτου. Επίσης, εφόσον τα πακέτα μεγαλώνουν σε μέγεθος με την πρόσθεση ετικετών πρέπει να προσέξει κανείς και το MTU της σύνδεσης ώστε να αποφευχθεί η κατάτμηση των επισημασμένων πακέτων. Οι βασικές εντολές ρύθμισης του MPLS παρουσιάζονται στο **Παράρτημα 1**.

Πέρα από τις καταστάσεις διανομής ετικετών, σημαντικό ρόλο παίζουν και τα πρωτόκολλα που χρησιμοποιούνται για την λειτουργία της διανομής. Τέτοια πρωτόκολλα, όπως το LDP, αναλύονται στο επόμενο κεφάλαιο.

3

Πρωτόκολλα Διανομής Ετικετών

3.1 Εισαγωγή

Έστω ένα απλό IP δίκτυο το οποίο ενσωματώνει MPLS (IP over MPLS). Αυτό το δίκτυο αποτελείται από LSRs που τρέχουν κάποιο IGP (Interior Gateway Protocol) (πχ. OSPF [21], IS-IS [8], EIGRP [12]). Το IGP είναι είνα σύνολο πρωτοκόλλων δρομολόγησης τα οποίο χρησιμοποιούνται εντός ενός αυτόνομου συστήματος. Κατά την είσοδο ενός πακέτου στο δίκτυο, ο ingress LSR αναζητά στο πακέτο την διεύθυνση προορισμού, προσθέτει μια ετικέτα και προωθεί το πακέτο. Ο επόμενος LSR και ο κάθε ενδιάμεσος LSR παραλαμβάνει το επισημασμένο πακέτο, αντικαθιστά την εισερχόμενη ετικέτα με κάποια εξερχόμενη και προωθεί με τη σειρά του το πακέτο. Ο egress LSR με την σειρά του αφαιρεί την ετικέτα του πακέτου και το προωθεί σύμφωνα με την διεύθυνση IP. Για να πραγματοποιηθεί αυτή η διαδικασία, οι γειτονικοί LSRs πρέπει να συμφωνήσουν ποια ετικέτα θα χρησιμοποιήσουν για κάθε πρόθεμα IGP, δηλαδή με ποια εξερχόμενη ετικέτα θα αντικατασταθεί κάθε εισερχόμενη. Άρα χρειάζεται ένας μηχανισμός ο οποίος θα καθοδηγεί τους LSRs στην απόφαση τους για την λειτουργία που θα εκτελέσουν πάνω στα επισημασμένα πακέτα. Ο μηχανισμός αυτός είναι το πρωτόκολλο διανομής ετικετών. Όπως έχει προαναφερθεί υπάρχουν δύο τρόποι εφαρμογής ενός πρωτοκόλλου διανομής των ετικετών:

- Ενσωμάτωση την λειτουργίας διανομής σε υπάρχον πρωτόκολλο δρομολόγησης
- Χρήση ενός ξεχωριστού πρωτοκόλλου για τη διανομή ετικετών

Όσον αφορά στη πρώτη περίπτωση, δεν έχει μετατραπεί κάποιο IGP (Interior Gateway Protocol) ώστε να υποστηρίξει την διανομή ετικετών. Αντίθετα το BGP είναι ένα πρωτόκολλο δρομολόγησης το οποίο μπορεί ταυτόχρονα να μεταφέρει προθέματα και να διανέμει ετικέτες. Το BGP χρησιμοποιείται κυρίως για την διανομή ετικετών στο MPLS VPN.

Στη δεύτερη περίπτωση ή οποία και απασχολεί περισσότερο ανήκουν πρωτόκολλα όπως το LDP, το CR-LDP και το RSVP. Τα πρωτόκολλα αυτά τρέχουν ταυτόχρονα και συνεργάζονται με κάποιο πρωτόκολλο δρομολόγησης.

3.2 Label Distribution Protocol (LDP)

Το LDP χρησιμοποιείται για να διανέμει ετικέτες οι οποίες αντιστοιχίζονται με FEC σύμφωνα με συγκεκριμένα αιτήματα των LSRs (κατ' απαίτηση) ή απλά διανέμονται τη στιγμή που νέες διαδρομές γίνονται γνωστές. Ο σκοπός της ετικέτας που διανέμεται είναι η αντιστοίχηση της με ένα FEC. Δυο LSRs οι οποίοι ανταλλάσσουν τέτοιες αντιστοιχήσεις ονομάζονται LDP Peers ενώ LDP Session ονομάζεται η συγκεκριμένη συνεδρία για αυτούς τους δυο, η οποία γίνεται και προς τις δύο κατευθύνσεις.

Υπάρχουν τέσσερις κατηγορίες μηνυμάτων στο LDP:

- Discovery messages, μηνύματα που ανακοινώνουν και διατηρούν την παρουσία ενός LSR στο δίκτυο
- Session messages, μηνύματα για την εγκαθίδρυση, διατήρηση και τερματισμό των συνεδριών μεταξύ των LDP peers
- Advertisement messages, μηνύματα για την δημιουργία, αλλαγή και διαγραφή αντιστοιχίσεων μεταξύ ετικετών και FECs
- Notification messages, μηνύματα που παρέχουν οδηγίες και πληροφορίες σφαλμάτων

3.2.1 Εύρεση των LSRs που τρέχουν LDP (LDP Discovery)

Οι LSRs, οι οποίοι τρέχουν το LDP, στέλνουν LDP Hello μηνύματα από όλες τις διασυνδέσεις στις οποίες έχει ενεργοποιηθεί το LDP. Τα Hello μηνύματα είναι μηνύματα UDP [35] τα οποία στέλνονται σε όλους τους δρομολογητές του υποδικτύου (multicast/all routers on this subnet), δηλαδή με IP διεύθυνση 224.0.0.2. Η UDP πόρτα που χρησιμοποιείται για το LDP είναι η 646.

Όταν ένας LSR λάβει ένα Hello μήνυμα σε κάποια συγκεκριμένη διασύνδεση, τότε συμπεραίνει ότι στην άλλη άκρη της σύνδεσης βρίσκεται ένας άλλος LSR ο οποίος τρέχει το LDP. Έτσι οι δύο LSRs που συμμετέχουν στην σύνδεση, εγκαθιστούν μια LDP σχέση γειτνίασης μεταξύ τους (LDP adjacency). Το Hello μήνυμα περιέχει ένα μηχανισμό αντίστροφης χρονομέτρησης, ο οποίος ονομάζεται

Holdtime. Αν δεν ληφθεί κάποιο Hello μήνυμα πριν λήξει ο Holdtime, ο LSR που διατηρεί τον Holdtime διαγράφει τον άλλο LSR από την λίστα με τους LDP γείτονες του. Η εξ' ορισμού τιμή της μεταβλητής Holdtime για τα Hello μηνύματα είναι 15 δευτερόλεπτα, ενώ κάθε 5 δευτερόλεπτα οι LSRs στέλνουν Hello μηνύματα από τις LDP διασυνδέσεις τους. Αν δύο LDP peers έχουν διαφορετικές τιμές για τις μεταβλητές Holdtime, τότε επιλέγεται η μικρότερη από αυτές για τη συγκεκριμένη συνεδρία.

Επίσης οι LSRs, στους οποίους έχει ενεργοποιηθεί το LDP, έχουν ένα αναγνωριστικό LDP (LDP Identifier) ή LDP ID. Το LDP ID διαφημίζεται μέσα από τα Hello μηνύματα. Το αναγνωριστικό αυτό αποτελείται από 6 byte, από τα οποία τα 4 byte ταυτοποιούν με μοναδικό τρόπο τον κάθε LSR και τα άλλα 2 byte υποδεικνύουν το είδος απόδοσης ετικετών, δηλαδή αν οι ετικέτες αποδίδονται ανά συσκευή (per-platform) ή ανά διασύνδεση (per-interface). Έτσι αν τα δύο τελευταία byte είναι 0 τότε το διάστημα ετικετών είναι ανά συσκευή (per-platform), ενώ αν είναι διαφορετικά του 0 είναι ανά διασύνδεση (per-interface). Στην τελευταία περίπτωση μπορούν να χρησιμοποιηθούν πολλαπλά αναγνωριστικά LDP από κάποιον LSR για διαφορετικές συνεδρίες LDP, των οποίων τα πρώτα 4 byte είναι τα ίδια και τα δυο τελευταία φανερώνουν το διαφορετικό διάστημα ετικετών. Όσον αφορά στα 4 πρώτα byte του LDP ID, αυτά είναι συνήθως η IP διεύθυνση μιας ενεργής διασύνδεσης. Αν υπάρχουν ρυθμισμένα loopback interfaces, τότε αυτό με την μεγαλύτερη διεύθυνση IP επιλέγεται σαν LDP ID.

3.2.2 Εγκατάσταση και Διατήρηση Συνεδρίας

Μέτα την εύρεση του ζεύγους των LSRs με τη βοήθεια των Hello μηνυμάτων, οι LSRs επιχειρούν να εγκαταστήσουν μια LDP συνεδρία μεταξύ τους. Ένας από τους δύο επιχειρεί να ανοίξει μια TCP σύνδεση (πόρτα 646) με τον άλλο LSR. Μετά την εγκατάσταση της TCP σύνδεσης ξεκινά η διαπραγμάτευση ορισμένων LDP παραμέτρων, όσον αφορά στη συγκεκριμένη συνεδρία, με την ανταλλαγή μηνυμάτων τα οποία ονομάζονται LDP Initialization μηνύματα. Κάποιοι από τους παραμέτρους που διαπραγματεύονται περιλαμβάνουν:

- Χρονικές τιμές
- Τεχνικές διανομής ετικετών
- Εύρος DLCI τιμών σε περίπτωση LC-Frame Relay

Αν οι δύο LDP peers συμφωνήσουν στις παραμέτρους της συνεδρίας, συνεχίζουν να κρατούν ανοιχτή την TCP σύνδεση. Αν τελικά δεν συμφωνήσουν, συνεχίζουν την προσπάθεια τους για την εγκατάσταση της συνεδρίας αλλά σε

χαμηλό ρυθμό. Η LDP συνεδρία είναι μια TCP σύνδεση μεταξύ δύο IP διευθύνσεων των δύο LSRs (αν το πρωτόκολλο επιπέδου δικτύου είναι το IP).

Μια LDP συνεδρία διατηρείται είτε από την παραλαβή LDP πακέτων ή μηνυμάτων διατήρησης συνεδρίας (keepalive messages). Κατά την παραλαβή LDP πακέτων ή keepalive μηνυμάτων η μεταβλητή χρόνου Holdtime ξεκινά πάλι από την αρχή το μέτρημα όπως έχει ήδη αναφερθεί. Ο εξ' ορισμού χρόνος του Holdtime, όσον αφορά στα keepalive μηνύματα, είναι 180 δευτερόλεπτα.

Στην εικόνα 3.1 φαίνεται ένας LDP peer με αναγνωριστικό router ID 10.200.254.2. Η τοπική πόρτα TCP που χρησιμοποιείται είναι η 646 και η απομακρυσμένη η 11537. Ο holdtime είναι 180 δευτερόλεπτα και τα μηνύματα keepalive αποστέλλονται ανά 60 δευτερόλεπτα.

```
london#show mpls ldp neighbor 10.200.254.5 detail
    Peer LDP Ident: 10.200.254.5:0; Local LDP Ident 10.200.254.2:0
        TCP connection: 10.200.254.5.11537 - 10.200.254.2.646
        State: Oper; Msgs sent/rcvd: 16/19; Downstream; Last TIB rev sent 50
        Up time: 00:00:36; UID: 9; Peer Id 1;
        LDP discovery sources:
          Ethernet0/1/2; Src IP addr: 10.200.215.2
            holdtime: 15000 ms, hello interval: 5000 ms
        Addresses bound to peer LDP Ident:
          10.200.254.5    10.200.215.2    10.200.216.1
        Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
```

Εικόνα 3.1. Εμφάνιση χαρακτηριστικών ενός γειτονικού LSR

3.2.3 Διανομή Αντιστοιχίσεων Ετικετών

Η διανομή των αντιστοιχίσεων, που έχουν γίνει σε κάθε LSR, είναι και ο βασικός στόχος του LDP. Σε προηγούμενο κεφάλαιο έχουν αναφερθεί οι διαφορετικές καταστάσεις του MPLS (MPLS Modes) με τις οποίες μπορεί να γίνει η διανομή ετικετών και η δημιουργία ενός LSP:

- Label Distribution Mode
- Label Retention Mode
- LSP Control Mode

Κάθε μια από τις παραπάνω καταστάσεις έχει δύο πιθανές λύσεις. Έτσι κάθε LSR είναι πιθανόν να υλοποιεί τα παρακάτω:

- Unsolicited Downstream (UD) ή Downstream on Demand (DD) Distribution

- Liberal Label Retention (LLR) ή Conservative Label Retention (CLR)
- Independent LSP Control ή Ordered LSP Control

Αν και ένας LSR μπορεί να υλοποιεί οποιαδήποτε από τις παραπάνω καταστάσεις, ο στόχος είναι η διανομή των ετικετών. Οι αντιστοιχίσεις είναι ένα σύνολο από (LDP ID ,ετικέτα) ανά πρόθεμα. Ένας LDP δρομολογητής πιθανόν να λαμβάνει αρκετές αντιστοιχίσεις ετικετών για κάθε πρόθεμα και συγκεκριμένα μια αντιστοίχηση από κάθε LDP peer. Αυτές οι αντιστοιχίσεις αποθηκεύονται στον πίνακα LIB. Η αποθήκευση των αντιστοιχήσεων εξαρτάται και από την κατάσταση διατήρησης ετικέτας (Label Retention Mode) που χρησιμοποιείται.

Για κάθε LSR υπάρχει ένας LDP peer, ο οποίος είναι ο downstream LSR για κάποιο συγκεκριμένο πρόθεμα δικτύου. Παρόλα αυτά, αν υλοποιείται load balancing θα υπάρχουν περισσότεροι από έναν downstream LSRs. Ο downstream LSR για κάποιον LSR είναι ο επόμενος κόμβος αυτού όπως έχει υπολογιστεί στον πίνακα δρομολόγησης. Η αντιστοίχηση που συσχετίζεται με τον downstream LSR θα είναι αυτή που θα εισαχθεί στον πίνακα LFIB. Το πρόβλημα που εισέρχεται είναι ότι οι αντιστοιχήσεις διανέμονται σαν (LDP ID, ετικέτα), χωρίς τις IP διευθύνσεις των διασυνδέσεων του downstream LSR. Έτσι για να βρεθεί η εξερχόμενη ετικέτα, για κάποιο συγκεκριμένο πρόθεμα δικτύου, πρέπει να αντιστοιχίσει κανείς το LDP ID με την διεύθυνση της διασύνδεσης του downstream LSR. Αυτό μπορεί να επιτευχθεί αν κάθε LDP peer παρέχει πληροφορίες για όλες τις διευθύνσεις του. Μηνύματα τα οποία ονομάζονται μηνύματα διευθύνσεων (Address Messages) είναι υπεύθυνα για αυτήν την διανομή. Στην εικόνα 3.2 φαίνονται οι IP διευθύνσεις του LDP peer (bound addresses), όπως παρουσιάζονται σε ένα Cisco IOS.

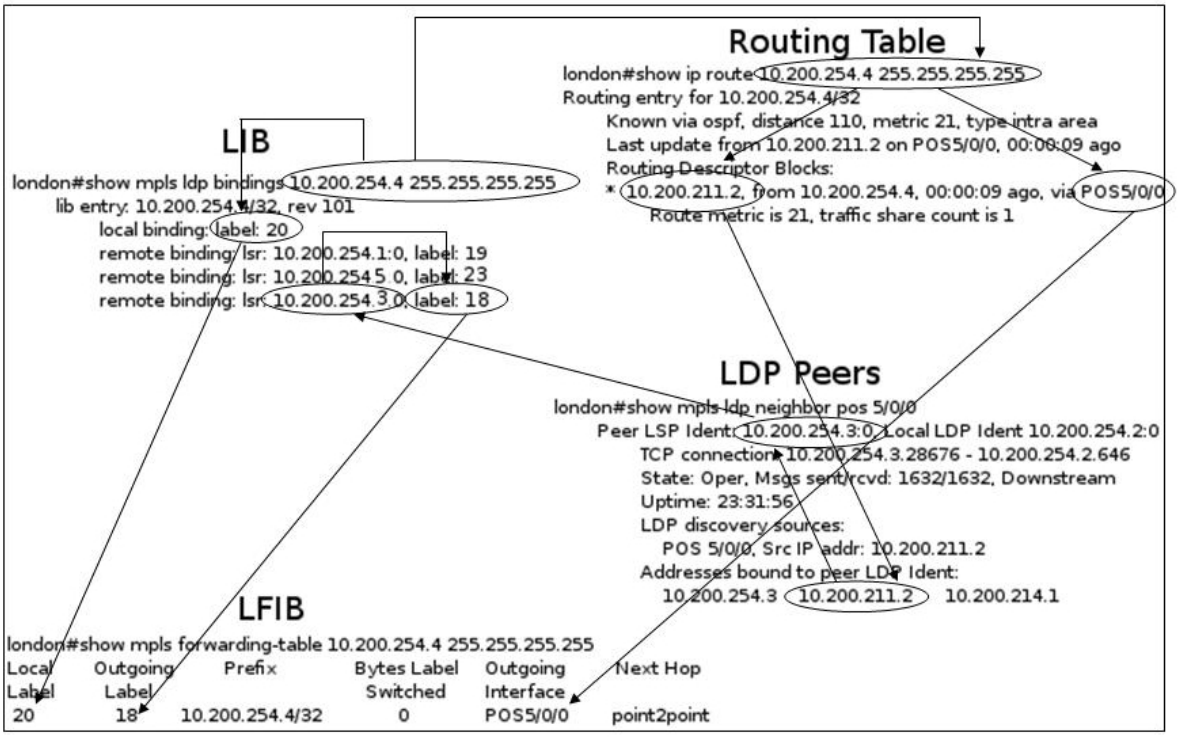
```
new-york#show mpls ldp neighbor detail
    Peer LDP Ident: 10.200.254.2:0; Local LDP Ident 10.200.254.1:0
        TCP connection: 10.200.254.2.646 - 10.200.255.1.64481
        State: Oper; Msgs sent/rcvd: 1303/1289; Downstream; Last TIB rev sent 743
        Up time: 17:20:24; UID: 101; Peer Id 0;
        LDP discovery sources:
          Ethernet1/1; Src IP addr: 10.200.210.2
            holdtime: 15000 ms, hello interval: 5000 ms
          Ethernet1/2; Src IP addr: 10.200.218.2
            holdtime: 15000 ms, hello interval: 5000 ms
        Addresses bound to peer LDP Ident:
          10.200.254.2    10.200.210.2    10.200.218.2    10.200.211.1
          10.200.215.1
        Peer holdtime: 180000 ms; KA interval: 60000 ms; Peer state: estab
```

Εικόνα 3.2. IP διευθύνσεις των διασυνδέσεων ενός downstream LSR

Κάθε LSR αποδίδει μια ετικέτα (local binding) σε κάθε πρόθεμα IGP που βρίσκεται στον πίνακα δρομολόγησης του. Όλα τα local bindings εγκαθίστανται στον πίνακα LIB του δρομολογητή. Κάθε μια από αυτές τις ετικέτες που αποδίδονται στα προθέματα IGP διαφημίζονται με το LDP στους LDP Peers. Αυτές οι αντιστοιχήσεις για τους LDP peers είναι τα remote bindings και αποθηκεύονται επίσης στον LIB πίνακα τους.

```
london#show mpls ldp bindings
  lib entry: 10.200.210.0/24, rev 4
        local binding:  label: imp-null
        remote binding: lsr: 10.200.254.5:0, label: 16
        remote binding: lsr: 10.200.254.1:0, label: imp-null
        remote binding: lsr: 10.200.254.3:0, label: 19
  lib entry: 10.200.211.0/24, rev 12
        local binding:  label: imp-null
        remote binding: lsr: 10.200.254.5:0, label: 18
        remote binding: lsr: 10.200.254.1:0, label: 32
        remote binding: lsr: 10.200.254.3:0, label: imp-null
  lib entry: 10.200.254.1/32, rev 31
        local binding:  label: 24
        remote binding: lsr: 10.200.254.5:0, label: 22
        remote binding: lsr: 10.200.254.1:0, label: imp-null
        remote binding: lsr: 10.200.254.3:0, label: 26
...
```

Εικόνα 3.3. Εγγραφές ενός LIB πίνακα



Εικόνα 3.4. Σχέση μεταξύ των πινάκων προς δημιουργία του LFIB

Στη εικόνα 3.3 φαίνεται ένας LIB πίνακας και στην εικόνα 3.4 φαίνεται η σχέση μεταξύ των πινάκων με σκοπό την δημιουργία του πίνακα LFIB για ένα FEC το οποίο περιλαμβάνει το πρόθεμα 10.200.254.4/32. Η εισερχόμενη ετικέτα (local binding) βρίσκεται κατευθείαν από τον LIB, ενώ η εξερχόμενη (remote binding) βρίσκεται συνδυάζοντας τον πίνακα δρομολόγησης, τις bound addresses του LDP peer και τελικά τον LIB.

Ας σημειωθεί εδώ ότι η τεχνική split horizon δεν υφίσταται. Με το LDP αποδίδονται ετικέτες σε όλα τα προθέματα διευθύνσεων που βρίσκονται στον πίνακα δρομολόγησης και οι αντιστοιχήσεις διανέμονται σε όλους τους LDP peers. Έτσι ένας LDP peer που αποδίδει μια ετικέτα για ένα πρόθεμα δικτύου, τη διανέμει στους LDP peers ακόμα και αν κάποιος από αυτούς είναι ο ίδιος που τον πληροφόρησε για το συγκεκριμένο πρόθεμα.

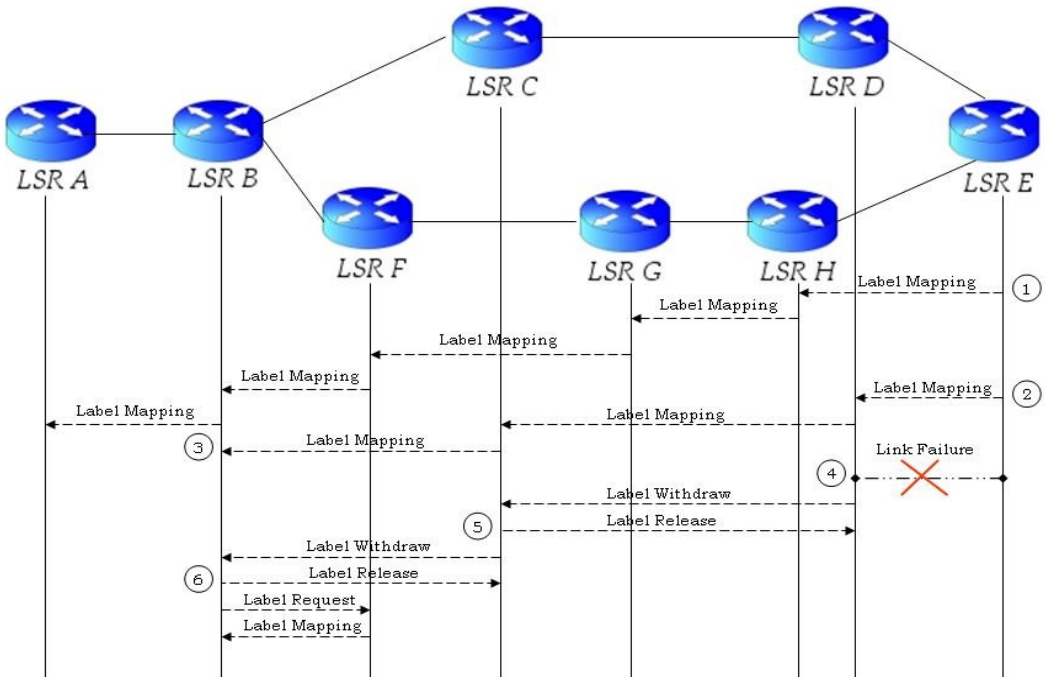
3.2.4 Απόσυρση Ετικετών (Label Withdrawing)

Οι LDP Peers, οι οποίοι λαμβάνουν αντιστοιχίσεις ετικετών, μπορούν να κρατήσουν αυτές τις αντιστοιχίσεις μέχρι την διακοπή μιας συγκεκριμένης LDP συνεδρίας ή μέχρι την απόσυρση μιας συγκεκριμένης ετικέτας. Για παράδειγμα, μια τέτοια απόσυρση μπορεί να συμβεί αν η ετικέτα αλλάξει λόγω κάποιου σφάλματος στη σύνδεση μεταξύ δύο LSRs.

Έτσι, όταν κάποιος LSR αποφασίσει ότι μια ετικέτα δεν είναι έγκυρη, την αποσύρει στέλνοντας μηνύματα απόσυρσης ετικέτας (Label Withdraw Messages). Όταν ένας LSR (ο upstream LSR σε σχέση με αυτόν που αποσύρει την ετικέτα) λάβει ένα μήνυμα απόσυρσης ετικέτας, οφείλει να σταματήσει τη χρήση αυτής και να απαντήσει στον downstream LSR, ώστε να γίνει ξεκάθαρο ότι ή απόσυρση ολοκληρώθηκε. Αυτή η απάντηση επιτυγχάνεται με την αποστολή ενός μηνύματος αποδέσμευσης ετικέτας (Label Release Message). Το συγκεκριμένο μήνυμα είναι μια αντιγραφή του μηνύματος αποδέσμευσης ετικέτας με την μόνη διαφορά ότι έχει έναν διαφορετικό κωδικό.

Στην εικόνα 3.5 φαίνεται ένα απλό MPLS δίκτυο, το οποίο χρησιμοποιεί Unsolicited Downstream διανομή ετικετών. Επίσης, παρουσιάζεται η χρήση των μηνυμάτων Label Mapping, Label Withdraw, Label Release και Label Request. Αρχικά ο LSR E διανέμει μια αντιστοίχηση ετικέτας/FEC στέλνοντας ένα Label Mapping μήνυμα στον LSR H (Βήμα 1). Με την σειρά του ο LSR H κάνει μια αντιστοίχηση ετικέτας/FEC και την στέλνει στον LSR G, ο LSR G στον LSR F, ο LSR F στον LSR B και τελικά ο LSR B στον LSR A. Επιπρόσθετα, ο LSR E κάνει και άλλη μια αντιστοίχηση ετικέτας/FEC, και τη στέλνει αυτή τη φορά στον LSR D

(Βήμα 2). Με την σειρά τους οι upstreams LSRs του LSR D διανέμουν την αντιστοίχηση ως τον LSR B.



Εικόνα 3.5. Σενάριο απόσυρσης ετικετών

Όταν η διαφήμιση του παραπάνω FEC από τον LSR C φθάσει στον LSR B (Βήμα 3), ο LSR B αποφασίζει ότι η διαδρομή μέσω του LSR C είναι προτιμότερη γιατί είναι πιο σύντομη. Έτσι εγκαθιστά στον LFIB την ετικέτα που απέστειλε ο LSR C και διαγράφει τελείως την ετικέτα που ελήφθη από τον LSR F (Conservative Label Retention). Ο LSR A δεν γνωρίζει κάτι για αυτή την απόφαση του LSR B, η απόφαση αυτή αντανακλάται μόνο στους πίνακες του LSR B.

Μετά από ένα χρονικό διάστημα η σύνδεση μεταξύ των LSR E και LSR D αποτυγχάνει (Βήμα 4). Έτσι ο LSR D αποφασίζει να αποσύρει την ετικέτα που είχε πριν ανακοινώσει στον LSR C, αποστέλλοντας ένα Label Withdraw μήνυμα. Ο LSR C ανταποκρίνεται κατευθείαν με ένα Label Release μήνυμα (Βήμα 5) και με την σειρά του αποσύρει την ετικέτα που είχε ανακοινώσει στον LSR B, οποίος και την διαγράφει (Βήμα 6). Εφόσον ο LSR B είναι συνδεδεμένος σε περισσότερους από έναν downstream LSRs κάνει μια προσπάθεια να λάβει μια άλλη ετικέτα από κάποιον άλλο downstream LSR. Όπως προαναφέρθηκε, ο LSR B χρησιμοποιεί Conservative Retention κατάσταση για τις ετικέτες, δηλαδή δεν έχει στους πίνακες του την προηγούμενη απόδοση ετικέτας από τον LSR F. Η ετικέτα αυτή είχε απορριφθεί όταν επιλέχθηκε το LSP μέσω του LSR C. Έτσι ο LSR B στέλνει ένα Label Request μήνυμα στον LSR F, ο οποίος του απαντά με ένα Label Mapping

μήνυμα. Έτσι ο LSR B ανανεώνει τους πίνακες του και εγκαθιστά το LSP μέσω του LSR F.

3.2.5 Μηνύματα Πληροφοριών (Notification Messages)

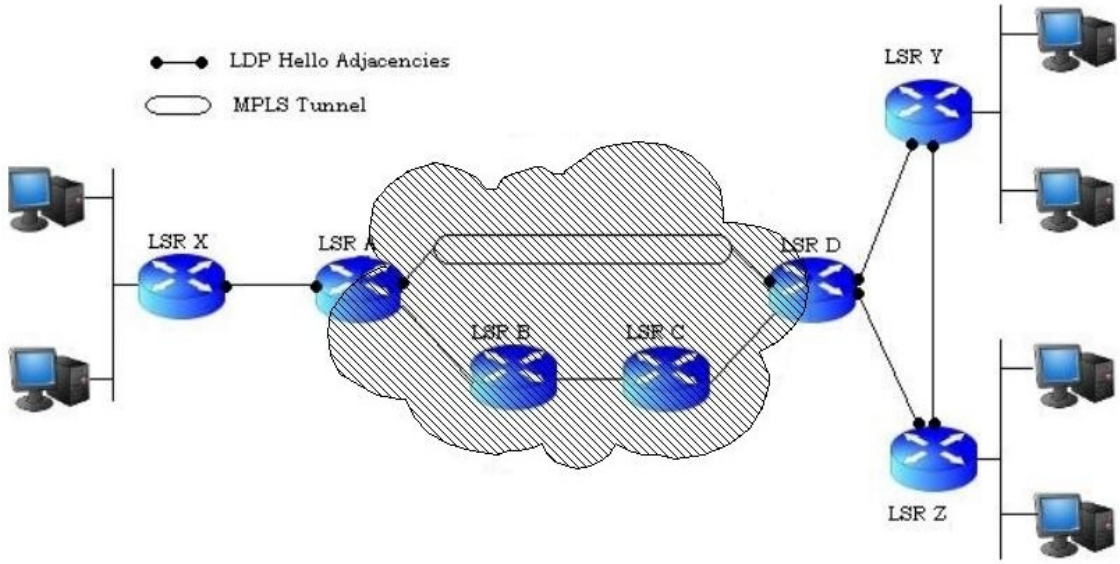
Τα μηνύματα πληροφοριών χρειάζονται για την εποπτεία των LDP συνεδριών. Επισημαίνουν διάφορα σημαντικά συμβάντα στον εκάστοτε LDP peer. Τα συμβάντα αυτά μπορεί να σηματοδοτούν σφάλματα (Error Notifications) η απλές συμβουλευτικές πληροφορίες (Advisory Notifications). Σε περίπτωση που συμβεί ένα σημαντικό σφάλμα, θα πρέπει να τερματιστεί μια συγκεκριμένη συνεδρία μεταξύ δύο LDP peers. Αντίθετα οι συμβουλευτικές πληροφορίες χρησιμοποιούνται για την αποστολή πληροφοριών για την συνεδρία ή για την αποστολή ενός μηνύματος στον LDP peer. Τα παρακάτω συμβάντα σηματοδοτούνται με την αποστολή μηνυμάτων πληροφοριών:

- Κατεστραμμένο PDU ή μήνυμα
- Εξάντληση χρόνου συνεδρίας (keepalive timer)
- Μονομερής διακοπή συνεδρίας
- Μηνύματα αρχικοποίησης
- Εσωτερικά σφάλματα
- Ανίχνευση βρόχων
- Διάφορα άλλα συμβάντα

3.2.6 Targeted LDP Sessions

Συνήθως μια LDP συνεδρία εγκαθίσταται μεταξύ δύο άμεσα συνδεδεμένων LSRs. Σε ένα δίκτυο στο οποίο IGP διαδρομές χρειάζεται να επισημανθούν συμβαίνει ακριβώς αυτό, γιατί η προώθηση των επισημασμένων πακέτων γίνεται βήμα προς βήμα. Έτσι αν οι αντιστοιχίσεις διανέμονται από κόμβο σε κόμβο, τα LSPs εγκαθίστανται χρησιμοποιώντας στη σειρά όλους τους ενδιάμεσους LSRs. Όμως σε μερικές περιπτώσεις απομακρυσμένες LDP συνεδρίες (targeted LDP Sessions) χρειάζεται να εγκατασταθούν. Αυτές είναι LDP συνεδρίες μεταξύ LSRs οι οποίοι δεν είναι άμεσα συνδεδεμένοι, αλλά είναι συνδεδεμένοι με ένα MPLS tunnel (εικόνα 3.6). Έτσι στο σενάριο της εικόνας 3.6 οι LSRs X και A ανταλλάσσουν κανονικά μηνύματα Hello και εγκαθιστούν μια LDP συνεδρία μεταξύ τους, όπως ακριβώς συμβαίνει και με τους LSRs D, Y και Z ανά δύο. Στην περίπτωση όμως των LSR A και LSR D το tunnel που χρησιμοποιείται για να προωθήσει τα πακέτα εγκαθιστά μια εικονική γειτονική σχέση μεταξύ αυτών. Έτσι οι δύο LSRs στέλνουν απομακρυσμένα Hello μηνύματα (targeted Hellos) και

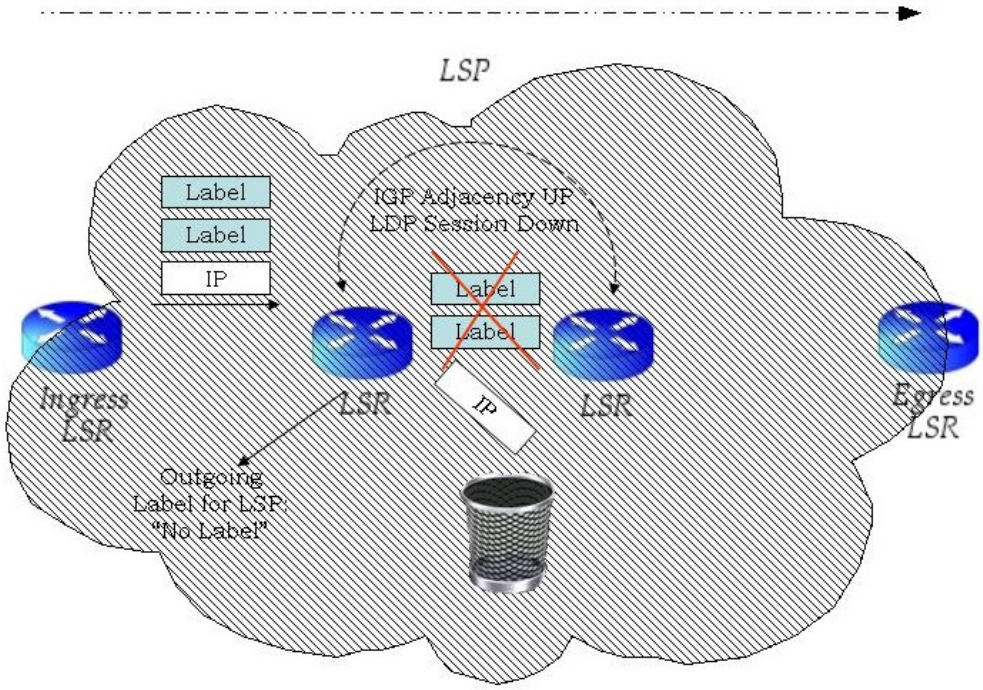
εγκαθιστούν μια targeted LDP συνεδρία. Παραδείγματα όπου χρησιμοποιούνται targeted LDP συνεδρίες είναι τα Traffic Engineering και MPLS VPNs.



Εικόνα 3.6. Targeted LDP Session μεταξύ δυο LSR

3.2.7 Συγχρονισμός LDP και IGP

Ένα πρόβλημα που μπορεί να παρουσιαστεί στα MPLS δίκτυα είναι ο μη ταυτόχρονος συγχρονισμός του LDP και του IGP του δικτύου. Ο συγχρονισμός εδώ σημαίνει ότι η προώθηση ενός πακέτου από μια διασύνδεση θα συμβεί μόνο εάν το LDP και το IGP συμφωνούν ότι αυτή είναι η διασύνδεση η οποία πρέπει να χρησιμοποιηθεί. Ένα συχνό πρόβλημα στα MPLS δίκτυα που τρέχουν το LDP είναι ότι αν μια LDP συνεδρία αποτύχει σε μια σύνδεση, το IGP δεν παύει να βλέπει αυτή τη σύνδεση σαν την καλύτερη διαδρομή στον πίνακα δρομολόγησης, από την οποία συνεχίζει να προωθεί πακέτα για κάποια προθέματα. Έτσι τα επισημασμένα πακέτα τα οποία θα προωθούταν μέσω αυτής της σύνδεσης, τώρα θα προωθηθούν χωρίς ετικέτα. Στη πιο συχνή περίπτωση όπου το δίκτυο είναι ένα απλό IPv4 over MPLS δεν υπάρχει σημαντικό πρόβλημα, γιατί οι LSRs γνωρίζουν πως να προωθήσουν πακέτα βάση της IP διεύθυνσής τους. Έτσι αφαιρείται η ετικέτα μέχρι να επισημανθούν ξανά σε κάποιον επόμενο LSR. Όμως σε περιπτώσεις όπως το MPLS VPN ή το VPLS οι LSRs δεν έχουν τη γνώση να προωθήσουν τα πακέτα και έτσι αυτά απορρίπτονται (εικόνα 3.7).



Εικόνα 3.7. Απόρριψη πακέτου λόγω μη συγχρονισμού LDP και IGP

Στην περίπτωση του MPLS VPN τα πακέτα βασίζονται στο IP, όμως πρέπει να προωθηθούν σύμφωνα με τον πίνακα VRF. Παρόλα αυτά, ο πίνακας VRF είναι προσωπικός για κάθε πελάτη και παρουσιάζεται μόνο στους οριακούς LSRs. Έτσι αν αφαιρεθεί η ετικέτα σε πακέτα εντός του MPLS δικτύου, αυτά θα απορριφθούν. Γενικά, σε περίπτωση που η συνεδρία LDP δεν είναι ενεργή (LDP session down), ενώ η IGP σχέση είναι ενεργή μεταξύ δύο LSRs (IGP adjacency up), μπορεί να προκύψουν σημαντικά προβλήματα και αρκετά πακέτα να χαθούν.

Παρόμοιο πρόβλημα μπορεί να υπάρξει και σε μια επανεκκίνηση των LSRs. Το IGP εγκαθιστά πιο γρήγορα τις γειτονικές σχέσεις από ότι το LDP τις συνεδρίες, υπονοώντας ότι η IGP προώθηση συμβαίνει ήδη πριν ο πίνακας LFIB μαζέψει τις πληροφορίες που απαιτούνται για την προώθηση βάση της ετικέτας.

Η λύση στο παραπάνω πρόβλημα, είναι ο συγχρονισμός LDP και IGP, δηλαδή η εγγύηση ότι δεν θα γίνει προώθηση μη επισημασμένης πληροφορίας όταν η συνεδρία LDP είναι ανενεργή για μια σύνδεση και επίσης θα γίνει η προώθηση από άλλη σύνδεση που έχει γίνει η εγκαθίδρυση της LDP συνεδρίας.

Το πρόβλημα του συγχρονισμού δεν συμβαίνει στην περίπτωση του BGP, γιατί το BGP είναι το ίδιο που φροντίζει και για την διανομή των αντιστοιχίσεων.

Έτσι το BGP είτε ενεργό είτε όχι δεν έχει πρόβλημα συγχρονισμού, εφόσον η εγκατάσταση ενός προθέματος στον πίνακα δρομολόγησης συνδέεται άμεσα με την αντιστοίχηση μιας ετικέτας για αυτό το πρόθεμα.

Όταν η τεχνική συγχρονισμού LDP και IGP είναι ενεργοποιημένη για μια διασύνδεση, το IGP διαφημίζει αυτή τη σύνδεση με μέγιστο κόστος (maximum metric) μέχρι να επιτευχθεί ο συγχρονισμός ή μέχρι να ενεργοποιηθεί η LDP συνεδρία σε αυτή τη σύνδεση. Ένα από τα IGP πρωτόκολλα που πραγματοποιείται η τεχνική συγχρονισμού LDP και IGP είναι το OSPF. Το μέγιστο κόστος για το OSPF είναι το 65536 (hex 0xFFFF). Έτσι καμία διαδρομή μέσω της συγκεκριμένης διασύνδεσης, που το LDP είναι ανενεργό, δεν χρησιμοποιείται εκτός και αν είναι η μόνη διαδρομή (δηλαδή δεν υπάρχουν άλλες διαδρομές με καλύτερο κόστος). Όταν τελικά η LDP συνεδρία εγκατασταθεί και οι αντιστοιχήσεις έχουν διανεμηθεί, το IGP διαφημίζει τη σύνδεση με το πραγματικό της κόστος.

3.3 CR-LDP (Constraint-Based LDP)

Το CR-LDP είναι μια επέκταση του LDP ώστε να του προσφέρει νέες δυνατότητες, όσον αφορά στην εγκατάσταση των LSPs. Για παράδειγμα, είναι ικανό να εγκαθιδρύσει LSP βασισμένα σε συγκεκριμένες σταθερές, σε σταθερές ποιότητας υπηρεσίας και άλλες σταθερές. Είναι μια επέκταση η οποία δημιουργήθηκε για την υποστήριξη του traffic engineering, την οποία δεν παρείχε το LDP. Η υλοποίηση τεχνικών traffic engineering γίνεται κυρίως με τη βοήθεια του πρωτοκόλλου RSVP-TE (RSVP με επεκτάσεις traffic engineering). Η περαιτέρω ανάπτυξη του πρωτοκόλλου CR-LDP από το IETF έχει σταματήσει. Σύμφωνα με το RFC 3468 (The Multiprotocol Label Switching (MPLS) Working Group Decision on MPLS Signaling Protocols), το IETF συνεχίζει τις προσπάθειες ανάπτυξης του RSVP-TE, ενώ σταματάει την έρευνα πάνω στο CR-LDP.

3.4 RSVP-TE (Resource Reservation Protocol with TE Extensions)

Είναι το ιδανικό πρωτόκολλο για ένα traffic engineered MPLS δίκτυο. Το RSVP ασχολείται με την από άκρο σε άκρο δέσμευση των πόρων του δικτύου για διάφορες ροές κυκλοφορίας, ένα ζήτημα παρόμοιο με αυτό του traffic engineering. Όμως δεν κατονομάζει όλες τις προϋποθέσεις που απαιτούνται για το MPLS και κυρίως την διανομή αντιστοιχίσεων ετικετών και τον έλεγχο καθορισμένων διαδρομών (Explicit Routes). Έτσι οι επεκτάσεις που συντέλεσαν στη δημιουργία του RSVP-TE αφορούν στα παρακάτω χαρακτηριστικά:

- Διαχείριση ετικετών
- Αίτηση και έλεγχος διαδρομών
- Διατήρηση συνδεσιμότητας μεταξύ RSVP-TE LSRs

Κάποιες από τις λειτουργίες του RSVP-TE παρουσιάζονται στο επόμενο κεφάλαιο όπου αναλύεται η τεχνική Traffic Engineering, εκεί που ουσιαστικά γίνεται και αναγκαία η χρήση του πρωτοκόλλου RSVP-TE.

3.5 Επίλογος

Θέμα του κεφαλαίου ήταν τα πρωτόκολλα διανομής ετικετών. Αναλύθηκε το LDP και ο τρόπος λειτουργίας του. Σημαντικό ρόλο στη δημιουργία και την αποτελεσματικότητα ενός LSP παίζει όχι μόνο η διανομή ετικετών από το LDP, αλλά και η απόσυρση τους. Οι εντολές ρύθμισης του LDP παρουσιάζονται στο **Παράρτημα 2**. Ένα άλλο πρωτόκολλο που χρησιμοποιείται για την διανομή ετικετών είναι το RSVP-TE, το οποίο εμφανίζεται περισσότερο σε MPLS δίκτυα τα οποία υλοποιούν Traffic Engineering. Αυτό είναι ένα θέμα το οποίο αναλύεται στο επόμενο κεφάλαιο.

4

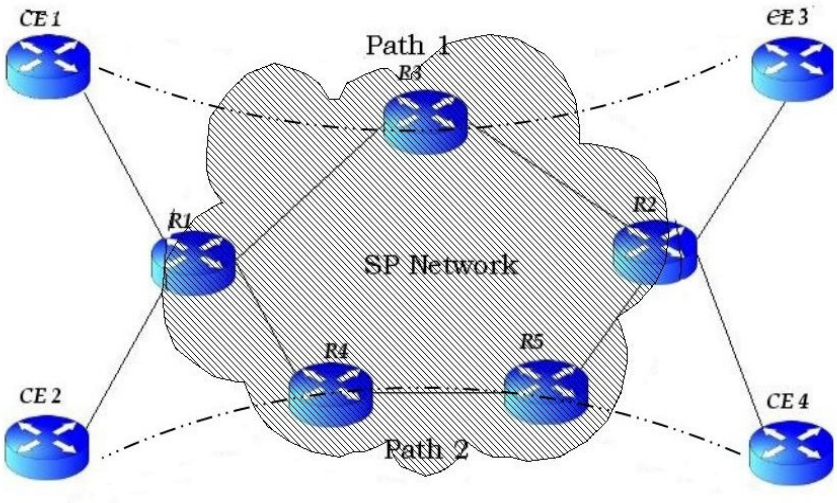
Traffic Engineering με MPLS

4.1 Εισαγωγή

Το TE (Traffic Engineering) είναι μια τεχνική στήριξης της κυκλοφορίας σε ένα δίκτυο κορμού με σκοπό την αποδοτικότερη χρήση του εύρους ζώνης μεταξύ των δρομολογητών. Πριν το MPLS TE, το TE υλοποιούταν με το IP ή με το ATM μεταξύ δυο οριακών δρομολογητών του δικτύου.

Το TE με IP εφαρμοζόταν κυρίως για την εκμετάλλευση του κόστους των διασυνδέσεων όταν υπήρχαν πολλαπλές διαδρομές μεταξύ δυο τερματικών σημείων του δικτύου. Επιπρόσθετα μπορούσαν να δημιουργηθούν στατικές διαδρομές, ώστε να πραγματοποιηθεί η κυκλοφορία μέσω μιας συγκεκριμένης διαδρομής.

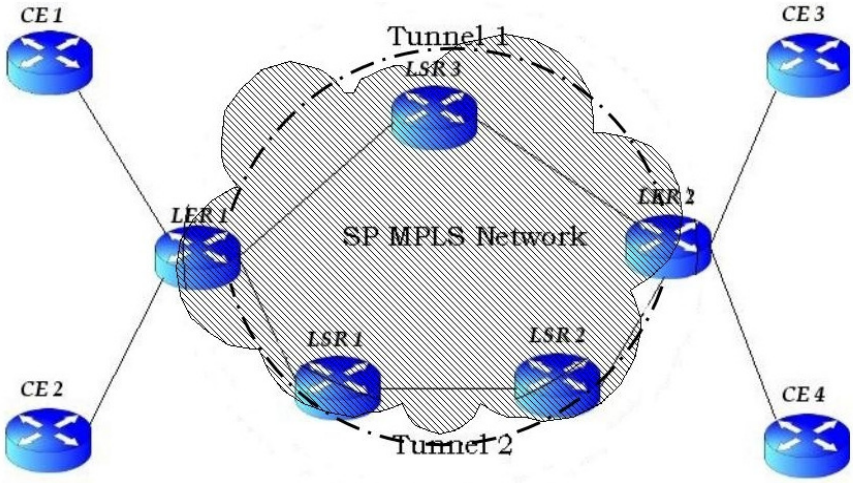
Στο σενάριο της εικόνας 4.1 παρουσιάζεται ένα απλό IP δίκτυο ενός παροχέα υπηρεσιών και τέσσερις συνδεδεμένοι δρομολογητές πελατών. Δύο διαδρομές υπάρχουν μεταξύ του CE 1 και CE 3 μέσω του δικτύου του παρόχου. Αν όλες οι συνδέσεις στο δίκτυο έχουν το ίδιο κόστος, τότε η προτιμότερη διαδρομή θα ήταν αυτή με τους λιγότερους κόμβους, δηλαδή το Path 1. Το ίδιο θα ισχύει και για την επικοινωνία του CE 2 με τον CE 4. Σε περίπτωση τώρα που όλες οι συνδέσεις είναι T3 και ο CE 1 στέλνει στον CE 3 πληροφορία με ρυθμό 45 Mbps, ενώ ταυτόχρονα ο CE 2 στέλνει στον CE 4 με ρυθμό 10 Mbps, κάποια πακέτα θα απορριφθούν στον R1 επειδή η καλύτερη διαδρομή αποστολής και για τους δύο (CE 1 & CE 2) είναι το Path 1. Το Path 2 δεν θα χρησιμοποιηθεί για την συγκεκριμένη μετάδοση. Σε αυτό το σημείο θα μπορούσε να βοηθήσει το TE αξιοποιώντας το διαθέσιμο εύρος ζώνης.



Εικόνα 4.1. IP δίκτυο ενός παροχέα υπηρεσιών

Για να υλοποιηθεί το TE στο παραπάνω σενάριο, κάνοντας load balancing ή χρησιμοποιώντας με κάποιο τρόπο και τις δυο διαδρομές, θα χρειαζόταν να περιληφθούν κάποια χαρακτηριστικά του IGP, όπως η αλλαγή του κόστους του Path 2 ώστε να είναι ίδιο με το Path 1. Πολλές φορές όμως κάτι τέτοιο μπορεί να μην είναι βολικό για τον εκάστοτε πάροχο υπηρεσιών και για μεγάλο αριθμό δρομολογητών.

Στο MPLS TE ένας οριακός δρομολογητής ελέγχει τη διαδρομή της πληροφορίας προς κάποιον συγκεκριμένο προορισμό του δικτύου. Όταν το παραπάνω σενάριο (εικόνα 4.1) μετατραπεί σε ένα MPLS TE δίκτυο τότε δημιουργείται το σενάριο της εικόνας 4.2 όπου τα TE LSPs ή TE Tunnels (Tunnel 1 και Tunnel 2) καθορίζουν διαδρομές οι οποίες μπορούν να χρησιμοποιηθούν για την κίνηση μεταξύ των LER 1 και LER 2.



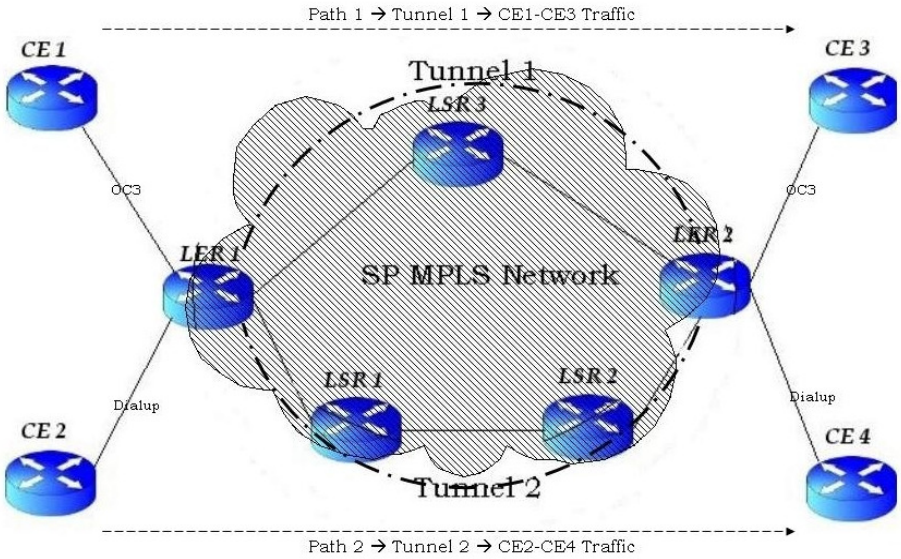
Εικόνα 4.2. MPLS δίκτυο με TE Tunnel

4.2 MPLS TE

Σε ένα συνηθισμένο σενάριο IP προώθησης τα πακέτα προωθούνται ανά κόμβο, σε κάθε έναν από τον οποίο πραγματοποιείται μια αναζήτηση στον πίνακα δρομολόγησης. Έτσι, όπως αναφέρθηκε και νωρίτερα αυτό μπορεί να οδηγήσει σε μη αποδοτική χρήση του διαθέσιμου εύρους ζώνης μεταξύ των δρομολογητών του δικτύου. Σε γενικές γραμμές, οι μη καλύτερες διαδρομές σε IP δίκτυα δεν αξιοποιούνται όπως πρέπει. Για να μην απορρίπτονται τα πακέτα λόγω της μη αποδοτικής χρήσης του διαθέσιμου εύρους ζώνης και για την καλύτερη απόδοση του δικτύου, μπαίνει σε λειτουργία η τεχνική TE. Σκοπός του TE είναι να οδηγήσει μια ροή κυκλοφορίας που προορίζεται για την καλύτερη διαδρομή, όπως αυτή υπολογίζεται από τα διάφορα πρωτόκολλα δρομολόγησης, σε μια υποδεέστερη και εφόσον αυτό θα οδηγήσει στη καλύτερη απόδοση του δικτύου. Η τεχνική TE παρακολουθεί τις ροές μεταξύ δυο δρομολογητών ώστε να κάνει αποδοτική τη χρήση του εύρους ζώνης στον πυρήνα ενός δικτύου. Το κλειδί για την εφαρμογή μιας αποδοτικής TE μεθοδολογίας είναι η συλλογή πληροφοριών, όσον αφορά στα χαρακτηριστικά της κίνησης που δημιουργείται στον πυρήνα του δικτύου, με σκοπό την εγγύηση του εύρους ζώνης για κάθε ροή. Όπως φαίνεται στο σενάριο της εικόνας 4.2, τα TE Tunnels (Tunnel 1 και Tunnel 2) μπορούν ρυθμιστούν στον LER 1, ώστε να καθορίσουν δύο διαδρομές.

Στα TE Tunnels που ρυθμίζονται στους δρομολογητές, η ροή της κυκλοφορίας γίνεται προς μια κατεύθυνση (Unidirectional). Έτσι για να έχουμε αμφίδρομη κίνηση μεταξύ των δρομολογητών LER 1 και LER 2 πρέπει να ρυθμιστούν και άλλα δύο TE Tunnels στον LER 2. Στα MPLS δίκτυα, όλες οι ρυθμίσεις που χρειάζεται να γίνουν για τα Tunnel αφορούν στους οριακούς δρομολογητές. Τα TE Tunnels ή και LSP Tunnels θα χρησιμοποιηθούν για να συνδέσουν τους οριακούς δρομολογητές του πυρήνα του δικτύου ενός παρόχου υπηρεσιών.

Το MPLS TE μπορεί επίσης να χρησιμοποιηθεί για να αντιστοιχίσει ροές κυκλοφορίας με TE Tunnels ανάλογα με τον προορισμό. Αυτό παρουσιάζεται στο σενάριο της εικόνας 4.3. Ο CE 1 αποστέλλει δεδομένα στον CE 3, ενώ και δύο συνδέονται στο MPLS δίκτυο με OC3 συνδέσεις. Αντίστοιχα ο CE 2 αποστέλλει στον CE 4 και οι σύνδεση τους με το MPLS δίκτυο πραγματοποιείται με Dialup συνδέσεις. Η κίνηση των CE 1-CE 3 γίνεται από το Tunnel 1, ενώ των CE 2-CE 4 από το Tunnel 2.



Εικόνα 4.3. Δύο MPLS TE Tunnels για τον διαχωρισμό της κυκλοφορίας

Τα TE Tunnels είναι ροές δεδομένων μεταξύ μιας συγκεκριμένης πηγής και ενός συγκεκριμένου προορισμού, τα οποία μπορούν να έχουν συγκεκριμένες ιδιότητες και χαρακτηριστικά. Οι απαιτήσεις εύρους ζώνης ή η τάξη υπηρεσίας (CoS) των δεδομένων μπορεί να ανήκουν στα χαρακτηριστικά ενός Tunnel. Οι διάφορες ροές δεδομένων προωθούνται μέσω της διαδρομής που ορίζει το Tunnel χρησιμοποιώντας τη μεταγωγή ετικέτας. Τα TE Tunnel μπορούν να αναδρομολογήσουν πακέτα από οποιαδήποτε διαδρομή στο δίκτυο, η οποία σχετίζεται με κάποιο LSP, εκτός και αν έχει οριστεί η ακριβής διαδρομή που πρέπει να ακολουθήσουν.

Ο σημαντικότερος λόγος για να ενσωματώσει κανείς σε ένα δίκτυο την τεχνική MPLS TE, είναι για να ελέγχει τις διαδρομές που ρέει η κυκλοφορία στο δίκτυο. Επίσης μπορεί να εγκαθιδρύσει δευτερεύουσες διαδρομές μεταξύ δυο δρομολογητών σε περίπτωση που η αρχική διαδρομή αποτύχει.

Πρωτόκολλα όπως το OSPF και το IS-IS με επεκτάσεις ώστε να υποστηρίξουν TE, μεταφέρουν πληροφορία σχετική με τα Tunnel που ρυθμίζονται σε έναν δρομολογητή. Αυτές οι επεκτάσεις περιλαμβάνουν χρήσιμη πληροφορία για τη δημιουργία του Tunnel, όπως το εύρος ζώνης για μια σύνδεση. Έτσι αν μια σύνδεση δεν διαθέτει τους απαιτούμενους πόρους για μια συγκεκριμένη μετάδοση, δεν επιλέγεται ως μέρος του TE Tunnel. Η σηματοδότηση σε ένα περιβάλλον MPLS TE πραγματοποιείται με το RSVP (Resource Reservation Protocol), το οποίο έχει επεκταθεί ώστε να υποστηρίζει χαρακτηριστικά TE Tunnel.

Σε ένα MPLS δίκτυο ο ingress LSR απαιτεί πληροφορίες σχετικά με τους πόρους που είναι διαθέσιμοι στις συνδέσεις του δικτύου, ώστε να αποφασίσει ποιες από αυτές μπορούν να συμμετάσχουν σε ένα MPLS Tunnel. Αυτές τις πληροφορίες τις παρέχει ένα IGP, όπως το OSPF ή το IS-IS. Όσον αφορά στο IS-IS, έχει προστεθεί ένα νέο TLV (type 22) για την μετάδοση πληροφορίας σχετικής με τους διαθέσιμους πόρους και την κατάσταση των συνδέσεων. Η ίδια πληροφορία παρέχεται από το OSPF με ένα άλλο TLV, το οποίο αναφέρεται σαν OSPF LSA type 10. Ένα TLV είναι ένα αντικείμενο το οποίο αποτελείται από μια τριάδα: τύπο (type), μήκος (length) και τιμή (value). Η προσθήκη TLV σε ένα πρωτόκολλο αποτελεί έναν εύκολο τρόπο για την επέκταση του πρωτοκόλλου. Έτσι, η διανομή της παραπάνω πληροφορίας χρησιμοποιώντας IGP ανανεώσεις, βοηθά τον ingress LSR να συλλέξει την πληροφορία που απαιτείται ώστε να καθορίσει τα Tunnel μέσω ενός συνόλου LSRs.

Το MPLS TE είναι εμπνευσμένο από την τεχνική CBR (Constraint Based Routing), κατά την οποία είναι πιθανή η ύπαρξη πολλαπλών διαδρομών μεταξύ ενός συγκεκριμένου ζεύγους αποστολέα-παραλήπτη. Με την τεχνική CBR, η λειτουργία ενός IP δικτύου αναβαθμίζεται και προστίθενται τεχνικές για την εύρεση διαδρομών μεταξύ πηγής και προορισμού. Η CBR απαιτεί ένα IGP, όπως τα προαναφερόμενα για την λειτουργία της. Η τεχνική αυτή αποτελεί τον κυρίως ορισμό ενός TE Tunnel και καθορίζεται στους ingress LSRs του MPLS δικτύου. Η διαθεσιμότητα των πόρων και η πληροφορία της κατάστασης των συνδέσεων υπολογίζεται από τον Constrained SPF αλγόριθμο [10], ο οποίος με βάση παραμέτρους όπως το εύρος ζώνης, πολιτικές διαχείρισης και πληροφορίες τοπολογίας, καθορίζει πιθανές διαδρομές από την πηγή στον προορισμό. Το αποτέλεσμα του CSPF είναι ένα σύνολο διευθύνσεων, οι οποίες αντιστοιχούν κατά σειρά σε κάθε επόμενο δρομολογητή δημιουργώντας ένα LSP, το οποίο αντιστοιχεί στο TE Tunnel. Το σύνολο των διευθύνσεων καθορίζεται στον εκάστοτε ingress LSR, ενώ οι ενδιάμεσοι LSRs δεν χρειάζεται να εκτελέσουν κάποια λειτουργία αναζήτησης διαδρομής. Τέλος, το RSVP με TE επεκτάσεις χρησιμοποιείται για να δεσμεύσει πόρους στη διαδρομή του LSP και για να αντιστοιχίσει ετικέτες στο Tunnel.

4.3 Λειτουργία RSVP-TE

Σε γενικές γραμμές, το RSVP δεσμεύει εύρος ζώνης για μια διαδρομή μεταξύ μιας πηγής και ενός προορισμού. Τα RSVP μηνύματα αποστέλλονται από τον ingress LSR κατά μήκος του δικτύου για την ταυτοποίηση των διαθέσιμων πόρων από την πηγή στον προορισμό (στην προκειμένη περίπτωση ingress LSR δεν

θεωρείται απαραίτητα ένας από τους ingress LSRs του MPLS δικτύου, άλλα ο LSR από τον οποίο ξεκινά το TE Tunnel). Ο ingress LSR είναι πάντα η πηγή του Tunnel και αντίστοιχα ο προορισμός είναι το τέλος του Tunnel. Μετά την αποστολή των μηνυμάτων, τα αποτελέσματα αποθηκεύονται στα μηνύματα καθώς ταξιδεύουν στο δίκτυο.

Τα σημαντικότερα μηνύματα που συντελούν στην εφαρμογή του RSVP για να υποστηρίξει TE είναι:

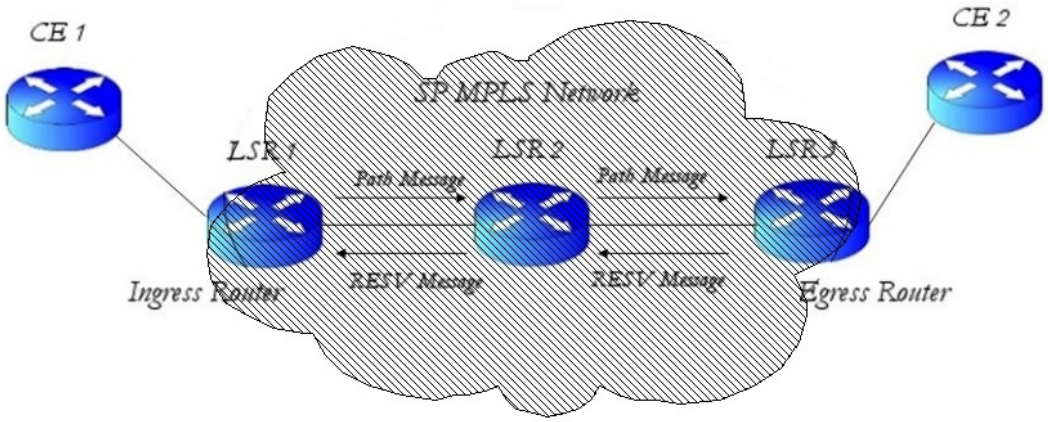
- RSVP Path Message
- RSVP Reservation Message
- RSVP Error Messages
- RSVP Tear Messages

Πέρα από την δέσμευση των απαιτούμενων πόρων, το RSVP βοηθά στην αντιστοίχηση ετικετών ώστε να δημιουργηθεί το TE LSP μέσω των δρομολογητών του δικτύου.

4.3.1 Μηνύματα RSVP

RSVP Path Message: δημιουργείται από τον ingress LSR και προωθείται στο δίκτυο μέσω του πιθανού TE Tunnel. Σε κάθε κόμβο, το Path Message ελέγχει την διαθεσιμότητα των προαπαιτουμένων πόρων και αποθηκεύει αυτή την πληροφορία.

RSVP Reservation Message: δημιουργείται από τον egress LSR του MPLS TE δικτύου και χρησιμοποιείται για να επιβεβαιώσει την αίτηση δέσμευσης πόρων, η οποία στάλθηκε νωρίτερα με τα μηνύματα Path. Όπως φαίνεται και στην εικόνα 4.4, το Path Message δημιουργείται από τον LSR 1 (Ingress Router) και προωθείται στον downstream LSR, όπου και ελέγχει τη διαθεσιμότητα των πόρων. Το RSVP Path Message λειτουργεί ταυτόχρονα και σαν μήνυμα αίτησης ετικέτας για το MPLS TE δίκτυο. Ας σημειωθεί εδώ, ότι όλα τα MPLS TE δίκτυα λειτουργούν με την downstream on demand μέθοδο απόδοσης ετικέτας, έτσι η αίτηση απόδοσης ετικέτας δημιουργείται από τον ingress LSR και προωθείται σε κάθε downstream. Προς απάντηση των Path Messages, ο egress LSR δημιουργεί τα Reservation Messages (RESV). Τα μηνύματα αυτά εκτελούν τη λειτουργία απόδοσης ετικετών. Εφόσον η διαδικασία απόδοσης και διανομής ετικετών πραγματοποιείται με την downstream on demand μέθοδο, η αντιστοίχηση ετικετών σε ένα TE Tunnel ξεκινά από τον egress LSR και προχωρά προς τον upstream LSR. Η διαδικασία αυτή συνεχίζεται σε κάθε κόμβο μέχρι τον ingress LSR.

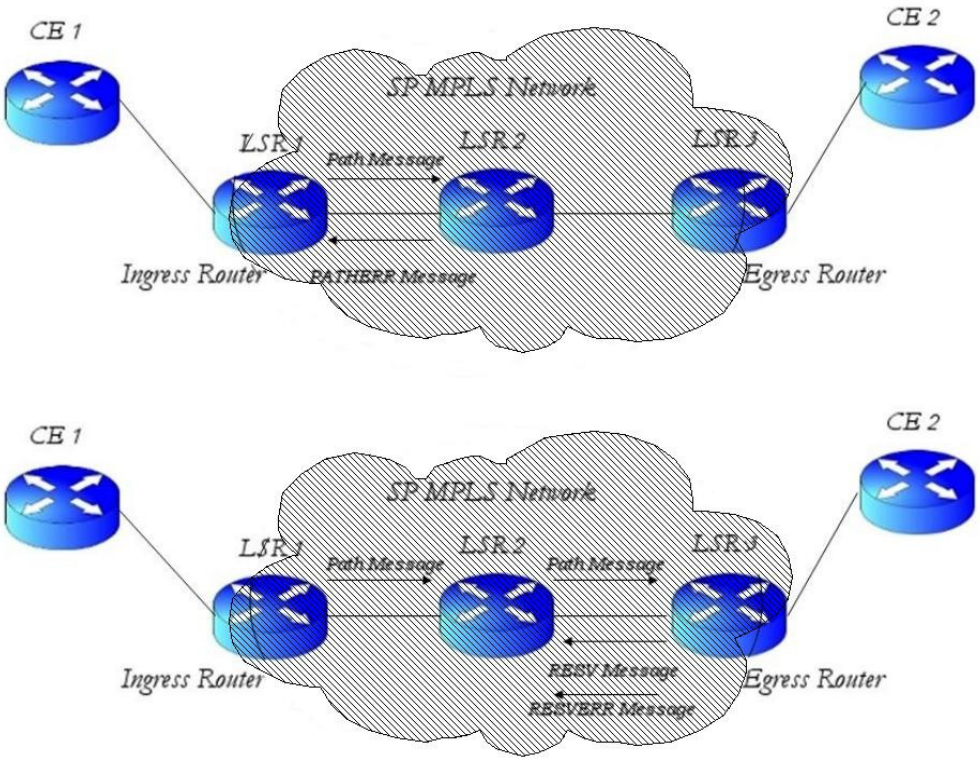


Εικόνα 4.4. RSVP Μηνύματα (Path Message, RESV Message)

RSVP Error Messages: σε περίπτωση που η διαθεσιμότητα πόρων δεν ανταποκρίνεται στις απαιτήσεις του Tunnel προς δημιουργία, τότε ο LSR δημιουργεί ένα μήνυμα RSVP Error και το αποστέλλει στον LSR από τον οποίο έλαβε κάποια αίτηση (Path Message). Σύμφωνα με το σενάριο της εικόνας 4.5, σε περίπτωση που ο LSR 2 δεν είναι ικανός να ανταπεξέλθει, στους αιτούμενος από τον LSR 1 πόρους όπως αυτοί καθορίζονται στο Path Message, τότε δημιουργεί ένα PATH ERROR μήνυμα και το στέλνει στον upstream LSR (LSR 1).

Υπάρχει περίπτωση τα Path Messages να φθάσουν στον egress LSR (LSR 3) και αυτός να στείλει στον LSR 2 ένα RESV Message, όμως κατά το μεσοδιάστημα ο LSR 3 να εντοπίσει έλλειψη πόρων. Σε αυτή τη περίπτωση στέλνει ένα Reservation Error message στον LSR 2 και απορρίπτει την επικείμενη δέσμευση, όπως παρουσιάζεται στο δεύτερο σενάριο της εικόνας 4.5.

RSVP Tear Messages : το RSVP δημιουργεί δύο τύπους τέτοιων μηνυμάτων, τα Path Tear μηνύματα και τα Reservation Tear μηνύματα. Τα μηνύματα αυτά καθαρίζουν τις Path και Reservation καταστάσεις των LSRs. Ο λόγος που γίνεται αυτό είναι για να ελευθερωθούν δεσμευμένοι πόροι, ώστε νέες αιτήσεις να πραγματοποιηθούν.



Εικόνα 4.5. RSVP Μηνύματα (PATHERR Message, RESVERR Message)

4.3.2 Λειτουργία RSVP σε ένα MPLS TE Περιβάλλον

Όπως προαναφέρθηκε, το αποτέλεσμα του CSPF αλγόριθμου στον ingress LSR, είναι ένα σύνολο από διευθύνσεις IP οι οποίες ταυτοποιούν κάθε επόμενο κόμβο της διαδρομής του TE Tunnel. Αυτή η λίστα διευθύνσεων υπολογίζεται και είναι γνωστή μόνο στον ingress LSR (ή πηγή του TE Tunnel). Οι υπόλοιποι δρομολογητές του δικτύου δεν εκτελούν κάποιο CBR υπολογισμό. Ο ingress LSR παρέχει τις απαιτούμενες πληροφορίες στους υπόλοιπους δρομολογητές του TE Tunnel μέσω αιτήσεων και επιβεβαιώσεων διαθέσιμων πόρων χρησιμοποιώντας το RSVP. Το RSVP με επεκτάσεις, που το καθιστούν κατάλληλο για TE, δεσμεύει τους απαραίτητους πόρους σε κάθε LSR της διαδρομής και αποδίδει αντιστοιχίσεις ετικετών στο TE Tunnel.

Οι επεκτάσεις του RSVP, που καθιστούν κατάλληλη τη σηματοδοσία σε ένα MPLS δίκτυο με TE παρουσιάζονται στον πίνακα 4.1. Αυτές τις επεκτάσεις μπορεί κανείς να τις συναντήσει και σαν αντικείμενα RSVP (RSVP Objects).

Πίνακας 4.1. Αντικείμενα RSVP

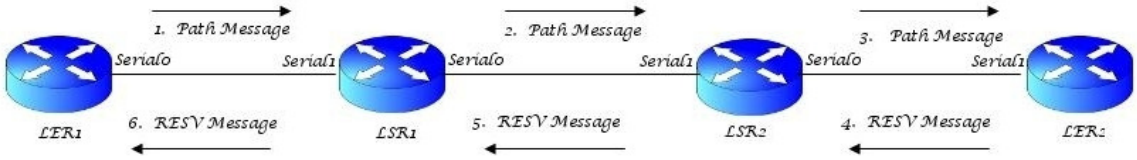
Object	Message	Function
LABEL_REQUEST	PATH	Χρησιμοποιείται για την αντιστοίχηση μιας ετικέτας με το TE Tunnel ή LSP και δημιουργείται από τον ingress LSR του Tunnel στο μήνυμα Path
LABEL	RESERVATION	Χρησιμοποιείται για να αποδώσει ετικέτες σε ένα TE Tunnel ή LSP και δημιουργείται από τον egress LSR στο μήνυμα Reservation
EXPLICIT_ROUTE	PATH	Μεταφέρεται στα μηνύματα Path και χρησιμοποιείται για την αίτηση ή την επιβεβαίωση μιας συγκεκριμένης διαδρομής για ένα TE Tunnel
RECORD_ROUTE	PATH, RESERVATION	Είναι παρόμοιο με την επιλογή εγγραφής ενός ICMP μηνύματος Ping. Προστίθεται στα Path ή Reservation μηνύματα και ειδοποιεί τον αποστολέα για την ακριβή διαδρομή ενός TE Tunnel
SESSION_ATTRIBUTE	PATH	Καθορίζει συγκεκριμένες παραμέτρους συνεδρίας τοπικά στο TE Tunnel

Ένα Path Message εμπεριέχει τα παρακάτω αντικείμενα του πίνακα 4.2.

Πίνακας 4.2. Στοιχεία ενός Path Message

Object	Message
SESSION	Καθορίζει την πηγή και τον προορισμό ενός LSP Tunnel. Συνήθως αποτελείται από την IP διεύθυνση της loopback διασύνδεσης της πηγής και του προορισμού.
SESSION_ATTRIBUTE	Καθορίζει τα χαρακτηριστά του συγκεκριμένου TE Tunnel, όπως οι απαιτήσεις σε εύρος ζώνης και οι πόροι που πρέπει να δεσμευθούν από το Tunnel
EXPLICIT_ROUTE	Αποτελεί μια λίστα των διευθύνσεων των κόμβους που καθορίζουν τη διαδρομή, οι οποίοι είτε έχουν καθοριστεί στατικά είτε έχουν υπολογιστεί δυναμικά με χρήση του CSPF
RECORD_ROUTE	Αποτελείται από τη διεύθυνση της διασύνδεσης εξόδου του τοπικού δρομολογητή
SENDER-TEMPLATE	Το αντικείμενο αυτό αναφέρεται στην διεύθυνση διασύνδεσης, η οποία θα χρησιμοποιηθεί σαν LSP-ID για το Tunnel. Η τιμή αυτή καθορίζεται από τον ingress router

Παρακάτω παρουσιάζεται η λειτουργία των μηνυμάτων Path και Reservation (εικόνα 4.6) καθώς και οι τιμές των διαφόρων αντικειμένων (πίνακας 4.3).



Εικόνα 4.6. Σενάριο αίτησης και απόδοσης RSVP

Πίνακας 4.3. Οι τιμές των αντικειμένων του σεναρίου της εικόνας 4.6

Path Message 1	**Object**	**Value**	**Path Message 2**	**Object**	**Value**
	SESSION	Source-LER1 Lo0 / Dest-LER2 Lo0		SESSION	Source-LER1 Lo0 / Dest-LER2 Lo0
	SESSION_ATTRIBUTE	Bandwidth		SESSION_ATTRIBUTE	Bandwidth
	EXPLICIT_ROUTE	LSR1 Serial1:LSR2 Serial1:LER2 Serial1		EXPLICIT_ROUTE	LSR2 Serial1:LER2 Serial1
	RECORD_ROUTE	LER1 Serial0		RECORD_ROUTE	LER1 Serial0:LSR1 Serial0
	LABEL	LABEL_REQUEST		LABEL	LABEL_REQUEST
	Sender Template	LER1 Loopback0		Sender Template	LER1 Loopback0

Path Message 3	**Object**	**Value**	**RESV Message 4**	**Object**	**Value**
	SESSION	Source-LER1 Lo0 / Dest-LER2 Lo0		SESSION	Source-LER1 Lo0 / Dest-LER2 Lo0
	SESSION_ATTRIBUTE	Bandwidth		SESSION_ATTRIBUTE	Bandwidth
	EXPLICIT_ROUTE	LER2 Serial1		RECORD_ROUTE	LER2 Serial1
	RECORD_ROUTE	LER1 Serial0:LSR1 Serial0:LSR2 Serial0			
	LABEL	LABEL_REQUEST		LABEL	POP
	Sender Template	LER1 Loopback0		Sender Template	LER1 Loopback0

RESV Message 5	**Object**	**Value**	**RESV Message 6**	**Object**	**Value**
	SESSION	Source-LER1 Lo0 / Dest-LER2 Lo0		SESSION	Source-LER1 Lo0 / Dest-LER2 Lo0
	SESSION_ATTRIBUTE	Bandwidth		SESSION_ATTRIBUTE	Bandwidth
	RECORD_ROUTE	LSR2 Serial1:LER2 Serial1		RECORD_ROUTE	LSR1 Serial1:LSR2 Serial1:LER2 Serial1

	LABEL	18		LABEL	22
	Sender Template	LER1 Loopback0		Sender Template	LER1 Loopback0

Βήμα 1: Ο ingress LSR (LER1) αποδίδει τις κατάλληλες τιμές στα αντικείμενα του μηνύματος Path (Path Message 1) και το στέλνει στον επόμενο κόμβο της διαδρομής του LSP Tunnel.

Βήμα 2: Όταν ο LSR1 λάβει το Path Message, ελέγχει το αντικείμενο EXPLICIT_ROUTE για να δει τον επόμενο κόμβο του Tunnel. Στο RSVP μήνυμα Path υπάρχει ένα bit, το οποίο ονομάζεται L-bit. Αν το L-bit είναι 1 τότε ο δρομολογητής δεν είναι άμεσα συνδεδεμένος με τον επόμενο. Σε μια τέτοια περίπτωση ο δρομολογητής πρέπει να τρέξει τον αλγόριθμο CSPF για να καθορίσει τον επόμενο κόμβο του Tunnel. Στην αντίθετη περίπτωση, όπου το L-bit είναι 0, ο δρομολογητής καταλαβαίνει ότι ο επόμενος κόμβος του LSP Tunnel είναι άμεσα συνδεδεμένος. Στη συνέχεια αφαιρεί τις εγγραφές του αντικειμένου EXPLICIT_ROUTE που αντιστοιχούν σε τοπικές διασυνδέσεις και προωθεί το μήνυμα σύμφωνα με την επόμενη εγγραφή (διεύθυνση) του EXPLICIT_ROUTE. Επίσης πριν την προώθηση ανανεώνει και το αντικείμενο RECORD_ROUTE, εισάγοντας ως τελευταία εγγραφή τη διεύθυνση από την τοπική διασύνδεση εξόδου που θα στείλει το μήνυμα (Path Message 2). Η ίδια διαδικασία επαναλαμβάνεται και στον LSR2 (Path Message 3).

Βήμα 3: Όταν το μήνυμα Path φθάσει στον προορισμό του (LER2), ξεκινά η αρχικοποίηση ενός μηνύματος RESV. Εδώ ξεκινάει και η διαδικασία απόδοσης ετικετών (δηλαδή στον egress Router με downstream on demand). Έτσι ο LER2 δημιουργεί ένα μήνυμα RESV και αποδίδει μια POP ετικέτα (τιμή 3 για IPv4 πακέτα) στο LSP Tunnel (Penultimate Pop Hopping). Το αντικείμενο RECORD_ROUTE αρχικοποιείται ξανά και ως πρώτη εγγραφή εισάγεται, από τον LER2, η διασύνδεση εξόδου του μηνύματος RESV.

Βήμα 4: Όταν το μήνυμα φθάσει στον LSR2, ή ετικέτα από τον LER2 αποθηκεύεται (remote binding) και αποδίδεται μια νέα ετικέτα για την σύνδεση μεταξύ LSR1 και LSR2 (local binding). Επίσης ανανεώνεται το αντικείμενο RECORD_ROUTE, καθώς ο LSR2 εισάγει ως αρχική εγγραφή τη διασύνδεση εξόδου του RESV μηνύματος. Η διαδικασία επαναλαμβάνεται μέχρι το μήνυμα να φθάσει στον LER1.

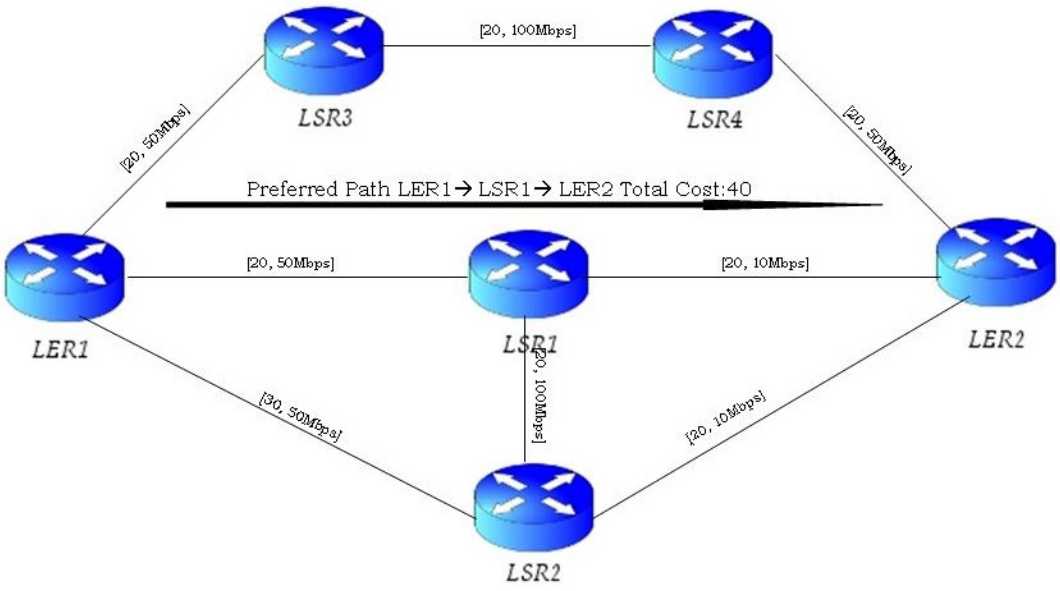
Βήμα 5: Όταν το Reservation μήνυμα φθάσει στον LER1, τότε το αντικείμενο RECORD_ROUTE εμπεριέχει τη TE LSP διαδρομή που ικανοποιεί τα συγκεκριμένα SESSION_ATTRIBUTES. Οι αντιστοιχήσεις των ετικετών

χρησιμοποιούνται για την προώθηση των πακέτων μέσω του MPLS LSP, το οποίο δημιουργήθηκε χρησιμοποιώντας με τη βοήθεια του RSVP Traffic Engineering, αντί του απλού τρόπου δημιουργίας ενός LSP.

4.4 Constraint-Based SPF

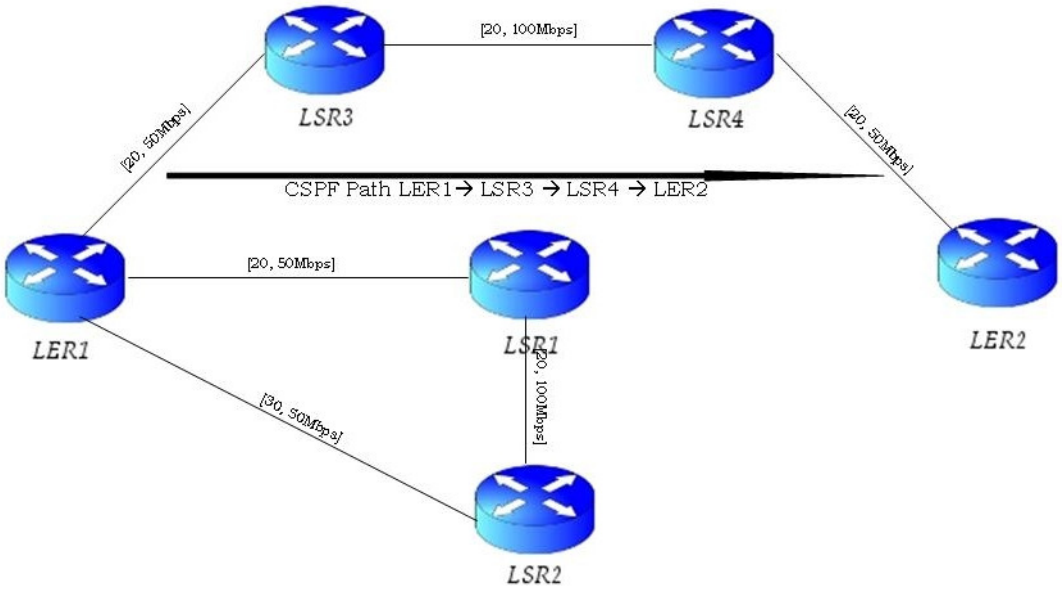
Σε μια κανονική SPF διαδικασία, ένας δρομολογητής τοποθετείται στην κορυφή του δένδρου με τις μικρότερου κόστους διαδρομές που υπολογίστηκαν βάση του κόστους της κάθε διαδρομής.

Κατά τη διάρκεια μιας κανονικής διαδικασίας SPF, στο δίκτυο του σεναρίου της εικόνας 4.7, λαμβάνεται υπόψη μόνο το κόστος των συνδέσεων. Έτσι η προτεινόμενη διαδρομή είναι από τον LER1 στον LER2 είναι η: LER1 – LSR1 – LSR2. Το ζεύγος τιμών στις συνδέσεις του σεναρίου της εικόνας 4.7 αποτελούν το κόστος και το εύρος ζώνης αντίστοιχα. Στον συγκεκριμένο υπολογισμό δεν μετράτε καθόλου το εύρος ζώνης, παρά μόνο το κόστος.



Εικόνα 4.7. Εύρεση καλύτερης διαδρομής σύμφωνα με τον SPF αλγόριθμο

Αν όριζε κανείς κάποιες παραμέτρους για την επιλογή της κατάλληλης διαδρομής και σε αυτές τις παραμέτρους δεν περιλάμβανε μόνο το κόστος αλλά και την απαίτηση όλες οι ενδιάμεσες συνδέσεις να υποστηρίζουν τουλάχιστον 50Mbps εύρος ζώνης, κάποιες από τις παραπάνω συνδέσεις της εικόνας 4.7 δεν θα περιλαμβάνονταν στην επιλογή. Έτσι θα προέκυπτε το σενάριο της εικόνας 4.8.



Εικόνα 4.8. Εύρεση διαδρομής σύμφωνα με τον CSPF αλγόριθμο

Με τους παραπάνω περιορισμούς η μόνο επιτρεπτή διαδρομή για το συγκεκριμένο TE LSP είναι η: LER1 – LSR3 – LSR4 – LER2.

Με το CSPF χρησιμοποιούνται περισσότερα κριτήρια παρά μόνο του κόστους για τον καθορισμό των διαδρομών που μπορεί να πάρει ένα TE LSP. Ο ingress LSR αποφασίζει ποια θα είναι η διαδρομή που θα εγκατασταθεί μετά την εξέταση των κριτηρίων και την απόρριψη των συνδέσεων που δεν τα ικανοποιούν. Το αποτέλεσμα του CSPF αλγόριθμου είναι ένα ταξινομημένο σύνολο διευθύνσεων που αντιστοιχούν σε κάθε επόμενο κόμβο του LSP Tunnel. Έτσι, πολλαπλά TE LSPs μπορούν να προκύψουν από την χρήση του CSPF, τα οποία θα καθορίζουν πιθανές συνδέσεις στο δίκτυο που ικανοποιούν τα συγκεκριμένα κριτήρια. Σε περίπτωση που βρεθούν πολλές διαδρομές που ικανοποιούν τα κριτήρια, τότε επιλέγεται αυτή που τα ικανοποιεί στο έπακρο και αν δεν υπάρχει διαφορά ανάμεσα τους, το CSPF κάνει μια τυχαία επιλογή. Επιπλέον, ο διαχειριστής μπορεί να δημιουργήσει και στατικά ένα TE Tunnel ή LSP στον ingress Router, με το να ρυθμίσει μια σειρά από LSRs. Έτσι μπορεί κάποιος να δημιουργήσει ένα στατικό εφεδρικό TE Tunnel σε περίπτωση που το αρχικό αποτύχει.

Τα αποτελέσματα του CSPF περνούν στη συνέχεια στο RSVP, το οποίο ξεκινά τη διαδικασία αιτήσεων και δέσμευσης πόρων όπως έχει προαναφερθεί. Το RSVP χρησιμοποιείται, μετά το αποτέλεσμα του CSPF ή δεδομένης μιας λίστας LSRs από τον διαχειριστή, για τη σηματοδοσία και την εγκαθίδρυση του TE LSP. Ας σημειωθεί ξανά ότι το TE LSP είναι μονόδρομο.

Μπορεί κανείς να συνοψίσει τη δημιουργία ενός MPLS TE Tunnel LSP σε ένα δίκτυο στα ακόλουθα:

1. Πραγματοποίηση CSPF υπολογισμού στον ingress LSR, βασισμένο σε κριτήρια που καθορίζονται από τις απαιτήσεις του TE Tunnel. Αυτός ο υπολογισμός πραγματοποιείται από το IGP που χρησιμοποιείται, είτε OSPF ή IS-IS.

2. Μετά τον υπολογισμό του LSP, τα αποτελέσματα της CSPF διαδικασίας, δηλαδή το σύνολο των διευθύνσεων των δρομολογητών, περνούν στο RSVP.

3. Το RSVP με τη σειρά του εκτελεί τις αιτήσεις και επιβεβαιώσεις δέσμευσης πόρων για το LSP, ώστε να αποφασίσει αν το LSP που καθορίστηκε από τον CSPF αλγόριθμο ικανοποιεί τις συγκεκριμένες απαιτήσεις του TE Tunnel προς δημιουργία

4. Μετά την λήψη ενός Reservation μηνύματος, το RSVP σηματοδοτεί την εγκαθίδρυση του TE Tunnel.

Ο λόγος χρήσης του OSPF ή του IS-IS για την υλοποίηση του CSPF είναι γιατί τα συγκεκριμένα πρωτόκολλα δρομολόγησης ανήκουν στην κατηγορία των link state πρωτοκόλλων δρομολόγησης (στέλνουν την κατάσταση όλων των συνδέσεων ενός δρομολογητή στους γειτονικούς δρομολογητές, κάτι το οποίο δεν κάνουν τα distance vector πρωτόκολλα τα οποία στέλνουν μόνο την καλύτερη διαδρομή). Αν σε ένα δίκτυο δεν υλοποιείται TE τότε μπορεί να χρησιμοποιηθεί και κάποιο distance vector πρωτόκολλο όπως το EIGRP.

Τα OSPF και IS-IS πρέπει με κάποιο τρόπο να διαδώσουν στις ανανεώσεις τους και τα κριτήρια, απαραίτητα για τον CSPF υπολογισμό, των συνδέσεων των δρομολογητών. Όσον αφορά στο OSPF, τρεις νέες link state advertisements (LSAs) έχουν καθοριστεί και ονομάζονται Opaque LSAs. Οι επεκτάσεις αυτές, οι οποίες περιγράφονται στο RFC 2370, προσδίδουν στο OSPF ένα γενικό μηχανισμό ώστε να μεταφέρει πληροφορία, την οποία μπορεί να επεξεργαστεί το ίδιο ή άμεσα κάποια εφαρμογή. Αυτά τα LSAs είναι και αυτό που χρειάζεται το MPLS TE για να τοποθετήσει την πληροφορία των κριτηρίων στο OSPF. Παρόμοια για το IS-IS, έχουν δημιουργηθεί κάποιες επεκτάσεις που του επιτρέπουν να μεταφέρει την πληροφορία του MPLS TE. Οι επεκτάσεις αυτές, οι οποίες αφορούν σε δύο νέα IS-IS TLVs, περιγράφονται στο RFC 3784.

4.5 Εφαρμογή του MPLS TE / Fast ReRoute (FRR)

Η τεχνική TE ενεργοποιείται συνήθως στον πυρήνα του δικτύου, που η χωρητικότητα των συνδέσεων είναι υψηλή. Αν μια σύνδεση ή ένας δρομολογητής αποτύχει, η κίνηση αναδρομολογείται γύρω από το σημείο αποτυχίας. Σε γενικές γραμμές, αυτή η αναδρομολόγηση συμβαίνει σχετικά γρήγορα. Στις περισσότερες όμως περιπτώσεις αρκετή πληροφορία χάνεται στο σημείο τις αποτυχίας. Για κίνηση που προέρχεται από εφαρμογές πραγματικού χρόνου, όπως VoIP εφαρμογές, κάτι τέτοιο είναι σίγουρα ανεπιθύμητο. Υπάρχει περίπτωση οι συνδέσεις να προστατεύονται στο φυσικό επίπεδο, όπως με τον μηχανισμό APS (Automatic Protection Switching) [32], όμως το να υπάρχει προστασία στο επίπεδο του MPLS είναι καλύτερο. Ο μηχανισμός APS είναι μια μέθοδος προστασίας για συνδέσεων σε επίπεδο υλικού. Το μειονέκτημα αυτού του μηχανισμού είναι ότι για κάθε προστατευόμενη σύνδεση, μια εφεδρική σύνδεση μένει σε αδράνεια μέχρι να χρειαστεί σε περίπτωση αποτυχίας.

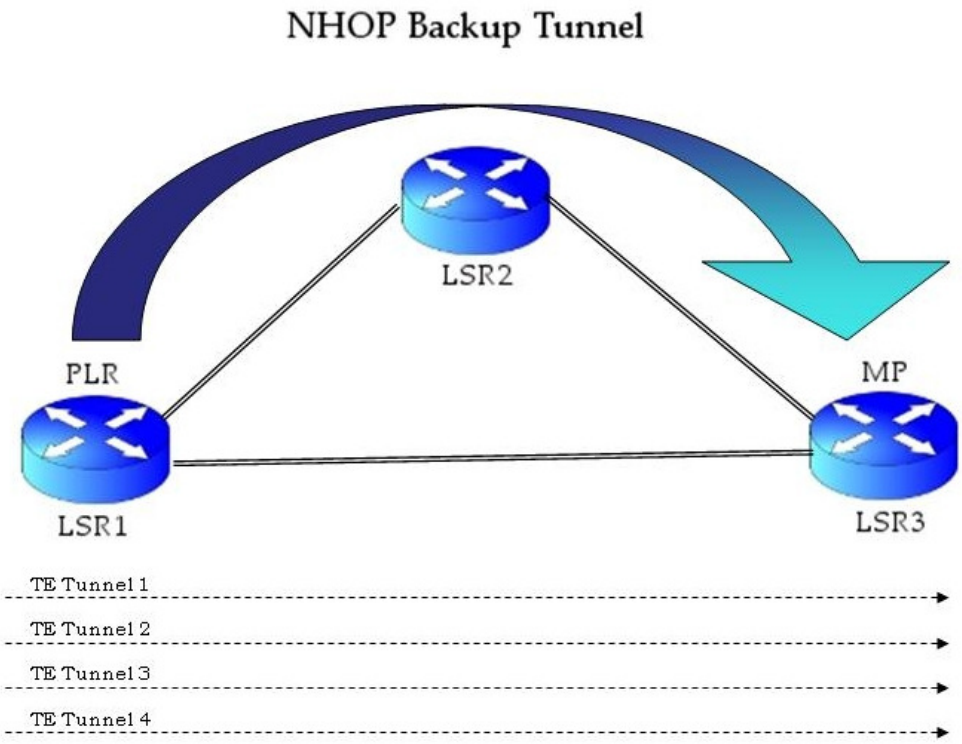
Με την τεχνική TE προσφέρεται μια πιο αποδοτική μέθοδος προστασίας των κόμβων και των συνδέσεων (Link & Node Protection). Δεν χρειάζεται πλέον εφεδρική σύνδεση, η οποία να μένει σε αδράνεια για κάθε ενεργή σύνδεση. Δημιουργείται εκ των προτέρων ένα εφεδρικό TE Tunnel για κάθε σύνδεση ή κόμβο. Έτσι δεν χάνεται χρόνος για την δημιουργία του εφεδρικού Tunnel τη στιγμή που θα αποτύχει μια σύνδεση ή ένας κόμβος. Είτε χρησιμοποιείται η προστασία σύνδεσης (Link Protection) είτε η προστασία κόμβου (Node Protection), η αναδρομολόγηση συμβαίνει όσο πιο κοντά είναι δυνατόν στο σημείο αποτυχίας και η ταχύτητα της αφορά δέκατα του χιλιοστού του δευτερολέπτου.

4.5.1 Link Protection FRR

Με την προστασία σύνδεσης, προστατεύεται μια συγκεκριμένη σύνδεση που χρησιμοποιείται για TE. Έτσι όλα τα TE Tunnels που διασχίζουν τη συγκεκριμένη σύνδεση, προστατεύονται από ένα εφεδρικό Tunnel. Η τεχνική αυτή ονομάζεται και facility backup, γιατί προστατεύεται μια σύνδεση με όλα τα TE Tunnel που μπορεί να τη διασχίζουν. Στο σενάριο της εικόνας 4.9, η σύνδεση μεταξύ των LSR1 και LSR3, προστατεύεται από το εφεδρικό Tunnel LSR1-LSR2-LSR3. Το συγκεκριμένο Tunnel προστατεύει μόνο τα TE Tunnel με κατεύθυνση από τον LSR1 στον LSR3. Έτσι για να προστατευτεί και η αντίθετη κατεύθυνση πρέπει να δημιουργηθεί άλλο ένα εφεδρικό Tunnel (LSR3-LSR2-LSR2).

Στην περίπτωση της προστασίας σύνδεσης, το εφεδρικό Tunnel ονομάζεται και Next Hop Bypass Tunnel (NHOP) και ξεκινά πάντα από το τοπικό σημείο ανακατασκευής (Point of Local Repair, PLR). Στην περίπτωση του σεναρίου της εικόνας 4.9 το τοπικό σημείο ανακατασκευής είναι ο LSR1. Το εφεδρικό Tunnel συνδέει πάντα τον PLR με τον επόμενο του δρομολογητή, δηλαδή τον δρομολογητή στο άλλο άκρο της σύνδεσης. Αυτός ο δρομολογητής ονομάζεται και σημείο ένωσης (Merge Point, MP), γιατί είναι το σημείο που ενώνονται οι δύο συνδέσεις (πρωταρχική και εφεδρική). Το εφεδρικό Tunnel είναι μια ακριβής διαδρομή που σηματοδοτείται από το RSVP. Όταν δημιουργείται το εφεδρικό Tunnel, οι ετικέτες αποδίδονται με τον συνήθη τρόπο, με το RSVP.

Ο PLR θα χρησιμοποιήσει για μικρό χρονικό διάστημα το εφεδρικό Tunnel για να μεταφέρει την κίνηση των TE Tunnels. Η προστασία είναι προσωρινή, γιατί μετά την αποτυχία της σύνδεσης ο PLR στέλνει μηνύματα PATHERR στον ingress Router του TE Tunnel. Όταν ο ingress Router λάβει τα μηνύματα σφάλματος, υπολογίζει και σηματοδοτεί μια νέα διαδρομή για το LSP Tunnel. Έτσι γίνεται η αναδρομολόγηση ολόκληρου του LSP στο δίκτυο.



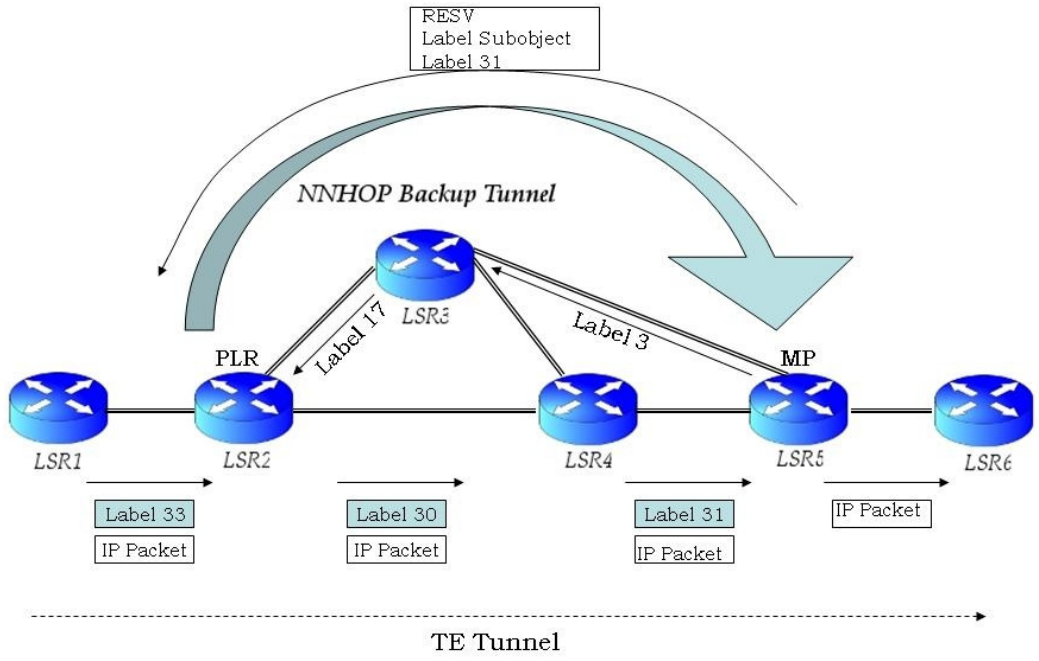
Εικόνα 4.9. Link Protection FRR

Ένα μειονέκτημα της χρήσης προστασίας σύνδεσης είναι ότι το NHOP Tunnel προστατεύει μια ολόκληρη σύνδεση. Οποιαδήποτε στιγμή, ένα πλήθος

από TE Tunnel με συγκεκριμένες απαιτήσεις εύρους ζώνης μπορεί να διασχίζει τη προστατευόμενη σύνδεση. Επιπλέον, το εφεδρικό Tunnel δεν δεσμεύει εύρος ζώνης. Έτσι όταν τα προστατευόμενα Tunnels χρησιμοποιήσουν το εφεδρικό, είναι πιθανόν να μην υπάρχει αρκετό διαθέσιμο εύρος ζώνης για την προώθηση όλης της κίνησης. Έτσι μπορεί κάποια πακέτα να απορριφθούν. Παρόλα αυτά, τα προστατευόμενα Tunnels θα χρησιμοποιήσουν το εφεδρικό προσωρινά, μέχρι οι ingress Routers των Tunnels να δεσμεύσουν ικανοποιητικό εύρος ζώνης και να αναδρομολογήσουν τα TE Tunnels.

4.5.2 Node Protection FRR

Με το FRR Node Protection καταφέρνει κανείς να προστατέψει όχι μια σύνδεση, αλλά έναν ολόκληρο δρομολογητή. Η τεχνική επιτυγχάνεται με την δημιουργία ενός εφεδρικού Tunnel, του οποίου ingress Router είναι ο προηγούμενος δρομολογητής του προστατευόμενου δρομολογητή. Το Tunnel ονομάζεται και Next Next Hop Backup Tunnel (NNHOP). Έτσι στην προστασία κόμβου ο MP δρομολογητής είναι ο NNHOP δρομολογητής (Εικόνα 4.10).

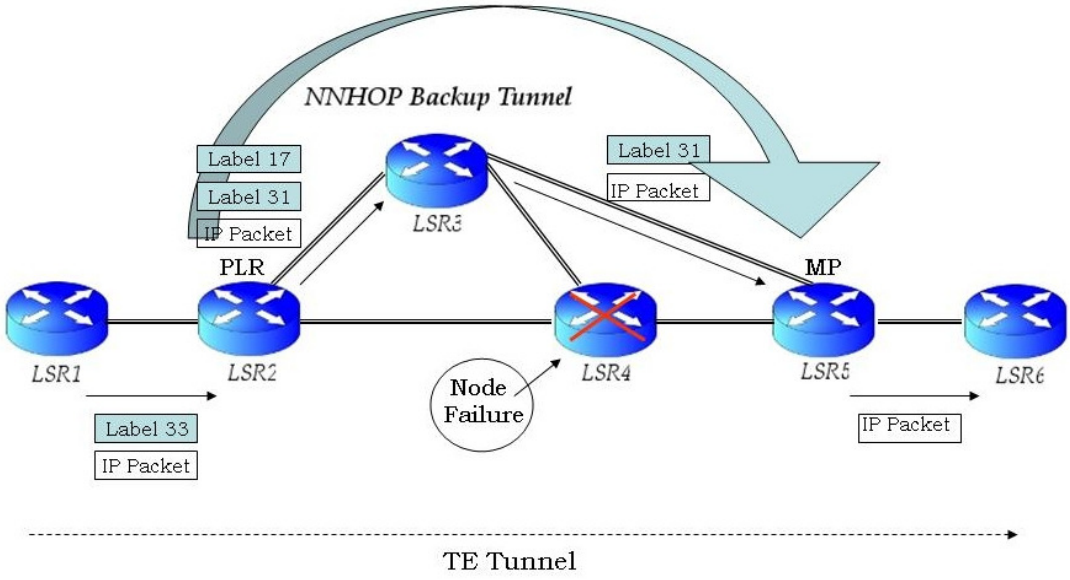


Εικόνα 4.10. Node Protection FRR 1

Στο σενάριο της εικόνας 4.10 ένα TE Tunnel ξεκινά από τον LSR1 και καταλήγει στον LSR6. Ο προστατευόμενος κόμβος είναι ο LSR4. Το NNHOP Backup Tunnel ξεκινά από τον LSR2 (PLR) και καταλήγει στον LSR5 (NNHOP ή MP). Το back Tunnel αποτρέπει στον LSR4 την συμμετοχή στο Tunnel, επισημαίνοντας τον εκτός της ακριβής διαδρομής. Αυτό επιτυγχάνεται εισάγοντας

το Router ID του LSR4 σε μια λίστα από κόμβους, από τους οποίους δεν επιτρέπεται να περάσει το Tunnel.

Ένα θέμα το οποίο κάνει πιο περίπλοκη την τεχνική προστασίας κόμβου, είναι ότι τα πακέτα δεν φθάνουν στον NHOP LSR (LSR3) αλλά στον NNHOP (LSR5). Άρα ο PLR πρέπει να γνωρίζει τη σωστή ετικέτα που θα τοποθετήσει στα πακέτα, ώστε αυτά να φθάνουν στον NNHOP με την ίδια ετικέτα στην κορυφή της στοίβας όπως αν έφθαναν από τον LSR4 (όταν δηλαδή δεν χρησιμοποιείται το backup Tunnel). Για να λυθεί αυτό το πρόβλημα, η ετικέτα διαφημίζεται από τον MP στον PLR μέσα σε ένα υποαντικείμενο του αντικειμένου Record Route ενός RESV μηνύματος. Όταν τα πακέτα φθάνουν στον PLR και πρέπει να αναδρομολογηθούν στο backup Tunnel, ο PLR αντικαθιστά την εισερχόμενη ετικέτα με την ετικέτα με την ετικέτα που έλαβε από τον MP και στη συνέχεια προσθέτει την ετικέτα του NNHOP backup Tunnel (Εικόνα 4.11).



Εικόνα 4.11. Node Protection FRR 2

4.6 Επίλογος

Στο παρόν κεφάλαιο αναλύθηκε η τεχνική Traffic Engineering και το πρωτόκολλο RSVP. Το TE είναι μια τεχνική στήριξης της κυκλοφορίας σε ένα δίκτυο κορμού με σκοπό την αποδοτικότερη χρήση του εύρους ζώνης μεταξύ των δρομολογητών. Μπορεί να αξιοποιήσει καλύτερα τις διαδρομές οι οποίες δεν επιλέγονται ως καλύτερες από το υπάρχον πρωτόκολλο δρομολόγησης. Η κίνηση σε ένα περιβάλλον MPLS TE γίνεται μέσω των TE Tunnels. Τα TE Tunnels είναι διαδρομές που δημιουργούνται βάση κριτηρίων και περιορισμών που απαιτούνται

για συγκεκριμένες ροές κυκλοφορίας. Σημαντικό ρόλο στη δημιουργία των TE Tunnel παίζει και ο αλγόριθμος CSPF.

Επιπρόσθετα, στο παρόν κεφάλαιο αναφέρθηκε και η εφαρμογή Fast ReRoute του MPLS TE. Η FRR είναι μια χρήσιμη εφαρμογή για γρήγορη επαναδρομολόγηση και ελαχιστοποίηση της χαμένης πληροφορίας από κάποια αποτυχία σύνδεσης ή κόμβου. Οι εντολές ρύθμισης του MPLS TE παρουσιάζονται στο **Παράρτημα 3**. Το επόμενο κεφάλαιο αναφέρεται στο MPLS VPN, μια άλλη σημαντική και πλέον εμπορική εφαρμογή του MPLS

5
MPLS VPN

5.1 Εισαγωγή

Τα BGP/MPLS IP VPNs [28], γνωστά σαν MPLS L3 VPNs ή L3VPN, είναι μια από τις πιο διαδεδομένες εφαρμογές MPLS δικτύων. Τα VPNs προϋπήρχαν του MPLS. Η επιτυχία των L3VPNs έγκειται στην επεκτασιμότητα και την απλότητα που παρέχεται από τον συνδυασμό του BGP και του MPLS στα διάφορα VPN σενάρια. Τα L3VPNs επεκτάθηκαν στα L2VPNs και στο VPLS.

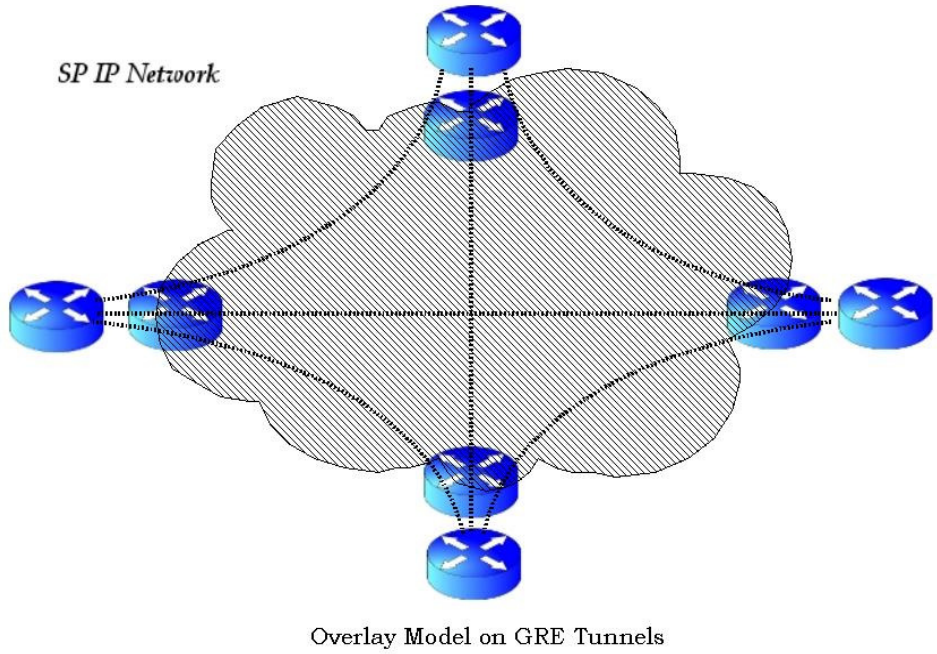
Τα BGP/MPLS VPNs είναι βασισμένα στο VPN Peer Model, το οποίο παρουσιάζεται αμέσως μετά. Ο κυριότερος λόγος αυτής της συσχέτισης είναι γιατί τα VPNs τα οποία είναι βασισμένα στους PE δρομολογητές (Provider Edge Router), όπως το VPN Peer Model, παρουσιάζουν ευκολία στη δρομολόγηση, όσον αφορά στους πελάτες (Customers), και επίσης ευκολία στην πρόσθεση νέων VPN περιοχών.

Η πρώτη δημοσίευση του μοντέλου BGP/MPLS VPN έγινε ανεπίσημα στο RFC 2547, στο οποίο παρουσιαζόταν μια VPN λύση από τη Cisco. Στη συνέχεια μια ομάδα εργασίας ξεκίνησε στην IETF, η οποία ονομαζόταν ppvpn (Provider-Provisioned VPNs). Η ομάδα εργασίας χωρίστηκε στη συνέχεια στις ομάδες L2VPN και L3VPN.

5.2 Το Μοντέλο Overlay VPN

Στο Overlay VPN μοντέλο ο πάροχος υπηρεσιών προσφέρει point-to-point συνδέσεις μεταξύ των δρομολογητών των διαφόρων περιοχών. Οι point-to-point συνδέσεις μπορεί να είναι κυκλώματα Frame Relay ή ATM, μισθωμένες γραμμές IP-over-IP Tunnels όπως τα GRE (Generic Route Encapsulation/Εικόνα 5.1) [14]. Έτσι προκύπτει ένα εικονικό δίκτυο κορμού για το δίκτυο των πελατών, το οποίο

κάθεται πάνω από τη δικτυακή δομή του παρόχου. Σχεδιάζονται έτσι σχέσεις γειτνίασης μεταξύ των δρομολογητών των διαφορετικών περιοχών των πελατών (CE Routers, Customer Edge Routers), ώστε να ανταλλάσσουν πληροφορίες δρομολόγησης και να επιτρέπεται η επικοινωνία μεταξύ των διαφορετικών περιοχών. Με αυτόν τον τρόπο δεν εγκαθιδρύονται γειτονικές σχέσεις μεταξύ των δρομολογητών των πελατών (CE Routers) και του παρόχου υπηρεσιών (PE Routers). Έτσι οι διαδρομές των CE Routers δεν φαίνονται στους PE Routers. Στην εικόνα 5.1 φαίνεται ένα Overlay Model με GRE Tunnels.



Εικόνα 5.1. Το μοντέλο Overlay VPN

Η υπηρεσία VPN στο Overlay μοντέλο παρέχεται από τους CE Routers. Ένα VPN του οποίου ο έλεγχος και οι αποφάσεις παρέχονται από τους CE Routers ονομάζεται CE-Based VPN. Έτσι οι πελάτες στη ουσία σχεδιάζουν και τρέχουν το δικό τους VPN, κάτι για το οποίο μπορεί να μην έχουν τη διάθεση και την ικανότητα. Έτσι ο εκάστοτε πάροχος υπηρεσιών ίσως αναλάβει την διαχείριση του εικονικού δικτύου κορμού του πελάτη, και έτσι καταλήγει στη διαχείριση ενός μεγάλου ποσού CE δρομολογητών. Κάτι τέτοιο δεν είναι επιθυμητό.

Ανεξάρτητα από το ποιος διαχειρίζεται τους CE δρομολογητές, ένα μοντέλο το οποίο τοποθετεί τον έλεγχο στις συσκευές των πελατών έχει περιορισμούς. Έστω ένα σενάριο όπου υπάρχουν αρκετές περιοχές πελατών και όλοι οι δρομολογητές είναι εικονικά συνδεδεμένοι μεταξύ τους. Σε κάθε τέτοια περίπτωση ο αριθμός των ομότιμων σχέσεων μεταξύ των δρομολογητών είναι μεγάλος. Αυτό μπορεί να προκαλέσει πρόβλημα στο IGP, λόγω της μεγάλης πληροφορίας

δρομολόγησης που πρέπει να ανταλλάξει σε περίπτωση κάποιας αλλαγής. Ένας άλλος περιορισμός αφορά στον μεγάλο αριθμό ρυθμίσεων που πρέπει να γίνει σε περίπτωση εισαγωγής κάποιας νέας περιοχής στο VPN.

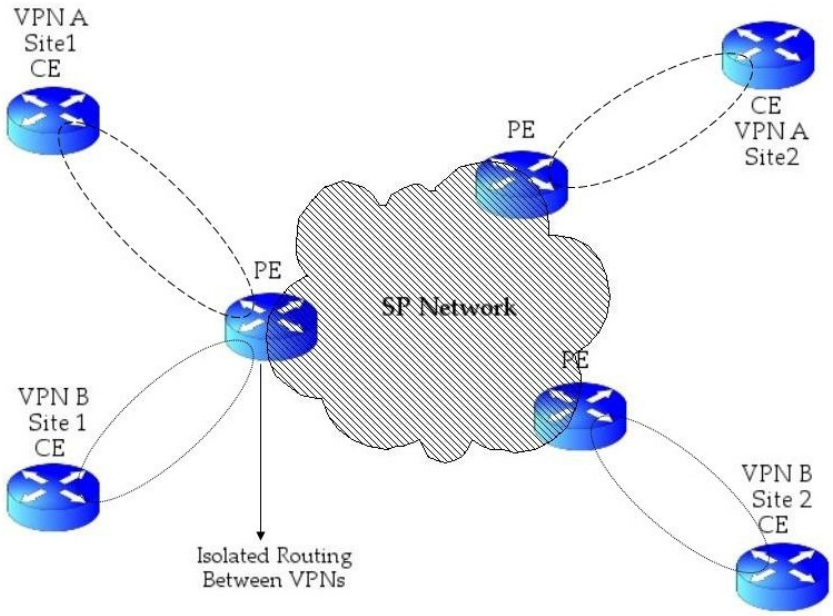
Το μοντέλο overlay επιτυγχάνει τους βασικούς στόχους για τη δημιουργία ενός VPN. Παρέχει επικοινωνία μεταξύ διαφορετικών περιοχών των πελατών, επιτρέπει την ύπαρξη private διευθύνσεων και εγγυάται την ασφάλεια της κίνησης μεταξύ των περιοχών του VPN. Το διαχειριστικό κόστος είναι αρκετά μεγάλο εφόσον απαιτείται η διαχείριση μεγάλου αριθμού δρομολογητών και ρυθμίσεων σε περίπτωση κάποιας αλλαγής.

5.3 Το Μοντέλο Peer VPN

Το Peer Model επιχειρεί να ξεπεράσει τα μειονεκτήματα του Overlay Model. Δεν απαιτείται η άμεση ανταλλαγή πληροφοριών δρομολόγησης μεταξύ των δρομολογητών των πελατών. Οι γειτονικές σχέσεις που αναπτύσσονται αφορούν στους άμεσα συνδεδεμένους δρομολογητές. Έτσι ένας CE Router εγκαθιστά μια γειτονική σχέση με τον άμεσα συνδεδεμένο PE Router. Η πλήρες κομβική συνδεσμολογία (εικονικών κυρίως συνδέσεων) που υπήρχε στο Overlay Model καταρρίπτεται. Από την μεριά του παρόχου υπηρεσιών η δρομολόγηση γίνεται εύκολη υπόθεση. Η διαχείριση της διανομής των πληροφοριών δρομολόγησης περνά στη μεριά του παρόχου και γενικά η λειτουργία περνά στους PE Routers.

Η εισαγωγή μιας νέας περιοχής σε ένα VPN απαιτεί ρυθμίσεις στον PE Router και CE Router της καινούργιας περιοχής και όχι σε όλους τους CE Routers του πελάτη. Επιπλέον, αν απαιτείται η αύξηση του εύρους ζώνης μεταξύ κάποιων περιοχών, αυτό μπορεί να επιτευχθεί στη σύνδεση του PE και του CE Router και δεν χρειάζεται η αναβάθμιση πολλών κυκλωμάτων ή μισθωμένων γραμμών. Στην εικόνα 5.2 παρουσιάζεται ένα σενάριο Peer Model VPN, στο οποίο τον έλεγχο τον έχουν οι PE δρομολογητές.

Η τεχνική του Peer Model είναι πιο αποδοτική λύση από τη μεριά της διαχείρισης, άλλα οφείλει ταυτόχρονα να εγγυάται και για την συνδεσιμότητα και την ασφάλεια που απαιτείται σε ένα VPN σχήμα. Η κίνηση πρέπει να ρέει μεταξύ περιοχών του ίδιου VPN, και να απαγορεύεται μεταξύ διαφορετικών VPN. Έτσι πρέπει να εισαχθούν κάποιοι περιορισμοί στη κίνηση. Αυτό μπορεί να επιτευχθεί είτε εισάγοντας κάποιους περιορισμούς στην κίνηση την χρονική στιγμή της προώθησης, δηλαδή χρησιμοποιώντας access lists στις συνδέσεις μεταξύ CE και PE, είτε εισάγοντας περιορισμούς στην διανομή της πληροφορίας δρομολόγησης.



Εικόνα 5.2. Το Μοντέλο Peer VPN

Μια από της αρχικές Peer Model VPN λύσεις εγγυόταν την ασφάλεια της πληροφορίας μεταξύ των διαφορετικών VPN περιοχών με τη χρήση των access lists. Οι access lists επενεργούν πάνω σε IP πακέτα την στιγμή της προώθησης, με το να επιτρέπουν ή όχι την κίνηση βασισμένες σε κριτήρια όπως η διεύθυνση πηγής και προορισμού. Η λύση η οποία βασίζονταν σε access lists έγινε γρήγορα δύσκολη στην διαχείριση. Έτσι έγινε η προσπάθεια απαλλαγής από τις access lists και η εύρεση μιας τεχνικής η οποία εγγυόταν ότι η κίνηση που λάμβαναν οι PE Routers προοριζόταν μόνο για ένα συγκεκριμένο VPN. Αυτός ο στόχος μπορεί να επιτευχθεί με την σύνδεση κάθε VPN περιοχής στον αποκλειστικό της φυσικό ή εικονικό PE δρομολογητή. Όμως, πρέπει να υπάρξει η εγγύηση ότι δεν θα δημιουργηθεί κάποια κατάσταση δρομολόγησης, η οποία θα επιτρέψει κίνηση μεταξύ PE δρομολογητών διαφορετικών VPN. Έτσι μια άλλη λύση Peer Model VPN αναπτύχθηκε, η οποία ήταν βασισμένη σε κριτήρια διανομής πληροφοριών δρομολόγησης και συγκεκριμένα βασισμένη στα BGP Communities. Τα BGP Communities [9] είναι πρόσθετα χαρακτηριστικά τα οποία μπορούν να προστεθούν στις IP διαδρομές που διανέμονται από το BGP. Σε αυτό το μοντέλο, οι PE δρομολογητές δέχονται και εγκαθιστούν διαδρομές που ανήκουν στα συγκεκριμένα VPNs που υπηρετούν. Αυτό το μοντέλο είναι και η βάση για τα BGP/MPLS-based VPNs.

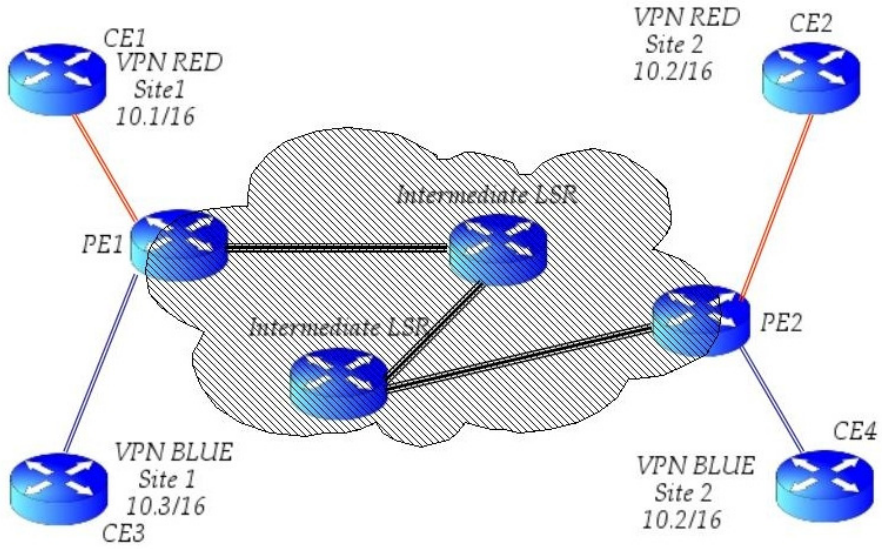
5.4 L3VPNs

Για να επιτευχθεί η υλοποίηση ενός Layer 3 MPLS VPN, χρειάζονται κάποια βασικά στοιχεία στους PE δρομολογητές. Αυτά είναι τα παρακάτω:

- Virtual Routing and Forwarding Tables (VRFs)
- Διανομή διαδρομών με τη χρήση του BGP
- Route Distinguisher (RD)
- Route Targets (RT)
- Προώθηση επισημασμένων πακέτων

5.4.1 Virtual Routing and Forwarding Tables (VRFs)

Η απομόνωση της κίνησης μεταξύ των διαφορετικών VPNs, σημαίνει ότι ένας πελάτης ενός VPN δεν πρέπει να είναι ικανός να στείλει πληροφορία σε ένα άλλο VPN. Στο σενάριο της εικόνας 5.3 υπάρχουν δυο VPNs πελατών, τα VPN RED και VPN BLUE.



Εικόνα 5.3. MPLS δίκτυο με δύο VPN

Κάθε PE δρομολογητής είναι συνδεδεμένος σε περιοχές και των δύο VPN. Αν υποθέσει κανείς ότι υπάρχει ένας εικονικός πίνακας δρομολόγησης/προώθησης σε κάθε PE Router, τότε υπάρχει πρόβλημα στην περίπτωση που υπάρχει επικάλυψη private διευθύνσεων μεταξύ των δύο VPN (όπως στην περίπτωση του CE2 και CE4). Επίσης, πρόβλημα συνεχίζει να υπάρχει και στην περίπτωση που δεν υπάρχει επικάλυψη. Αν υπάρχει επικάλυψη διευθύνσεων μεταξύ των δυο VPN,

τότε δεν μπορεί να εγκατασταθεί η πληροφορία προώθησης και για τα δυο VPN, γιατί δεν θα υπάρχει τρόπος να ξεχωρίσει κανείς τους δυο προορισμούς. Στην αντίθετη περίπτωση που δεν υπάρχει επικάλυψη, είναι πιθανόν για έναν σταθμό στο VPN RED να στείλει κάποια πληροφορία στο VPN BLUE, στέλνοντας απλά IP κίνηση με προορισμό το BLUE VPN. Έτσι όταν ο PE Router δει ένα πακέτο με διεύθυνση προορισμού το VPN BLUE, απλά προωθεί το πακέτο.

Και τα δύο παραπάνω προβλήματα μπορούν να λυθούν, αν συνδεθεί η κάθε περιοχή πελάτη στο δικό της φυσικό ή εικονικό PE Router. Όμως η αύξηση του αριθμού των PE δρομολογητών για κάθε νέο πελάτη που εισάγεται στο δίκτυο δεν ευνοεί την επεκτασιμότητα αλλά ούτε και τη διαχείριση του δικτύου.

Ένας πιο αποδοτικός τρόπος είναι η χρήση εικονοκών πινάκων δρομολόγησης/προώθησης ανά VPN (per-VPN Virtual routing and forwarding tables (VRFs)), ώστε να διατηρείται ξεχωριστά η πληροφορία δρομολόγησης και προώθησης για κάθε VPN. Αυτοί οι πίνακες συνυπάρχουν με τον γενικό πίνακα δρομολόγησης, ο οποίος χρησιμοποιείται για την κυκλοφορία πακέτων εκτός των VPN, και περιέχουν διαδρομές για τις τοπικές και απομακρυσμένες περιοχές των πελατών.

Όταν φθάνει ένα IP πακέτο από μια περιοχή πελάτη, ένας PE Router πρέπει να γνωρίζει τον VRF που αντιστοιχεί στη συγκεκριμένη περιοχή. Αυτό επιτυγχάνεται αν συσχετίσουμε κάθε διασύνδεση με έναν VRF μέσω ρυθμίσεων στους PE δρομολογητές. Όταν φθάνει ένα IP πακέτο σε έναν PE δρομολογητή το οποίο δεν σχετίζεται με κανέναν VRF, τότε η αναζήτηση πραγματοποιείται στον γενικό πίνακα δρομολόγησης. Στην εικόνα 5.4 φαίνεται μια διασύνδεση ενός PE δρομολογητή και οι ρυθμίσεις που έχουν γίνει σε αυτήν ώστε να συσχετίζεται με έναν VRF πίνακα του οποίου το όνομα είναι cust-one.

```
!
ip vrf cust-one
rd 1:1
route-target export 1:1
route-target import 1:1
!
interface Serial5/1
ip vrf forwarding cust-one
ip address 10.10.4.1 255.255.255.0
!
```

Εικόνα 5.4. Ορισμός VRF πίνακα για μια διασύνδεση

Η χρήση πολλαπλών πινάκων προώθησης στους PE δρομολογητές είναι απαραίτητη προϋπόθεση για την ύπαρξη όμοιων private διευθύνσεων μεταξύ των διαφορετικών VPN. Παρόλα αυτά η ύπαρξη αρκετών πινάκων προώθησης δεν εγγυάται άμεσα ότι κίνηση δεν μπορεί προωθηθεί από ένα VPN στο άλλο. Αν στο σενάριο της εικόνας 5.3, ο πίνακας προώθησης του VPN RED με κάποιο τρόπο περιέχει πληροφορία για προορισμούς του VPN BLUE, τότε τίποτα δεν μπορεί να εμποδίσει την προώθηση πληροφορίας από το VPN RED στο VPN BLUE. Εντέλει, είναι απαραίτητος ο έλεγχος της πληροφορίας που εγκαθίσταται σε κάθε VPN. Αυτό επιτυγχάνεται με την διανομή της πληροφορίας δρομολόγησης βάση κριτηρίων, ώστε οι πιθανοί προορισμοί των περιοχών των πελατών να διαφημίζονται μόνο εκεί που πρέπει να διαφημιστούν.

5.4.2 Διανομή διαδρομών με τη χρήση του BGP

Ένας τρόπος για αυτήν την περιορισμένη διανομή της πληροφορίας δρομολόγησης, είναι όλες οι VPN διαδρομές να μεταφέρονται μέσω ενός πρωτοκόλλου δρομολόγησης στο δίκτυο του παρόχου υπηρεσιών και να περιορίζεται η διανομή της πληροφορίας των προορισμών στους PE Routers. Αυτή είναι και η μέθοδος που εφαρμόζεται στα BGP/MPLS VPNs, όπου το BGP είναι το πρωτόκολλο που μεταφέρει τις VPN διαδρομές. Μερικές από τις ιδιότητες που κάνουν το BGP ιδανικό για τα VPN σενάρια είναι:

- Υποστηρίζει φιλτράρισμα διαδρομών με τη χρήση του community χαρακτηριστικού. Δηλαδή, μπορεί να κάνει περιορισμένη διανομή των πληροφοριών δρομολόγησης.
- Έχει τη δυνατότητα να μεταφέρει ένα μεγάλο πλήθος διαδρομών, και έτσι μπορεί να μεταφέρει διαδρομές από αρκετούς πελάτες.
- Μπορεί να ανταλλάξει πληροφορία μεταξύ δρομολογητών, οι οποίοι δεν είναι άμεσα συνδεδεμένοι. Κατά συνέπεια, η ανταλλαγή πληροφορίας δρομολόγησης μπορεί να γίνει μεταξύ των PE Routers.
- Είναι ικανό να μεταφέρει ετικέτες σύμφωνα με τις διαδρομές.
- Μπορεί να λειτουργήσει μεταξύ των οριακών συσκευών ενός παροχέα υπηρεσιών.

5.4.3 Διευθύνσεις VPN-IPv4 και Route Distinguisher (RD)

Όπως έχει προαναφερθεί, το BGP έχει αρκετές ιδιότητες που το κάνουν δελεαστικό για την μεταφορά των VPN διαδρομών στο δίκτυο ενός παροχέα υπηρεσιών. Παρόλα αυτά, το μόνο που κάνει είναι να εγκαθιστά και να διανέμει μια διαδρομή για ένα πρόθεμα δικτύου, το οποίο όμως μπορεί να προκαλέσει

πρόβλημα για private VPN διευθύνσεις που μπορεί να επικαλύπτονται ανάμεσα στα VPN.

Η λύση είναι να γίνει μια private διεύθυνση μοναδική. Η μοναδικότητα μιας private διεύθυνσης επιτυγχάνεται με το RD. Η βασική ιδέα είναι ότι κάθε πρόθεμα δικτύου από κάθε πελάτη λαμβάνει ένα μοναδικό αναγνωριστικό (RD), για να ξεχωρίζει από τα ίδια προθέματα άλλων πελατών. Ως αποτέλεσμα προκύπτει ένα νέο πρόθεμα, το οποίο αποτελεί συνδυασμό του IPv4 προθέματος και του RD, και ονομάζεται VPN-IPv4 πρόθεμα. Το BGP οφείλει να μεταφέρει τα VPN-IPv4 προθέματα μεταξύ των δρομολογητών.

Το RD είναι ένα πεδίο 64 bit, το οποίο χρησιμοποιείται για να κάνει τα VRF προθέματα μοναδικά όταν το BGP τα μεταφέρει. Το RD δεν υποδεικνύει τον VRF πίνακα στον οποίον ανήκει το πρόθεμα. Η λειτουργία του δεν είναι σαν αναγνωριστικό VPN, γιατί σε κάποια πιο περίπλοκα σενάρια VPN μπορεί να μην αρκεί μόνο ένα RD ανά VPN. Κάθε VRF πίνακας σε έναν PE δρομολογητή πρέπει να έχει ένα RD που να συσχετίζεται με αυτόν. Αυτό το πεδίο των 64 bit μπορεί να έχει δύο μορφές: ASN:nn ή IP-Address:nn, όπου το nn είναι ένας αριθμός και ASN (Internet Assigned Number) ο αριθμός αυτόνομου συστήματος. Η πιο συνηθισμένη μορφή είναι η ASN:nn. Συνήθως οι παροχείς υπηρεσιών χρησιμοποιούν ASN:nn, που ο autonomous system αριθμός έχει αποδοθεί από την Internet Assigned Numbers Authority (IANA) και ο nn είναι ο αριθμός που αποδίδεται μοναδικά στον VRF. Ο συνδυασμός του RD και του IPv4 προθέματος που αποτελεί το VPN-IPv4 πρόθεμα, έχει μήκος 96 bit. Για παράδειγμα αν το αναγνωριστικό RD για το IPv4 πρόθεμα 10.1.1.0/24 είναι 1:1, τότε το VPN-IPv4 πρόθεμα είναι 1:1:10.1.1.0/24.

Ένας πελάτης έχει το δικαίωμα να χρησιμοποιήσει διαφορετικά RDs για την ίδια IPv4 διαδρομή. Όταν μια VPN περιοχή είναι συνδεδεμένη σε δύο PE δρομολογητές, τότε οι διαδρομές από την VPN περιοχή μπορεί να έχουν δυο διαφορετικά RDs, αναλόγως από ποιον PE Router λαμβάνονται οι διαδρομές. Κάθε IPv4 διαδρομή μπορεί να πάρει δυο διαφορετικά RDs και έτσι μπορούν να υπάρξουν δυο εντελώς διαφορετικές VPN-IPv4 διαδρομές. Αυτό επιτρέπει στο BGP να τις εκλάβει σαν δυο διαφορετικές διαδρομές και να εφαρμόσει διαφορετικές πολιτικές στην κάθε μια.

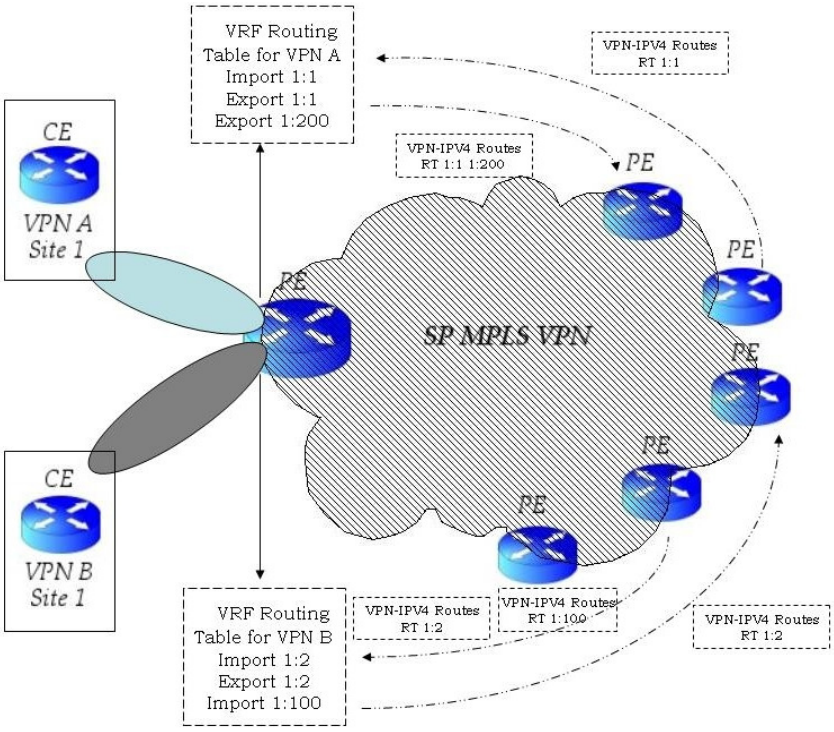
5.4.4 Route Targets (RTs)

Τα RD χρησιμοποιούνται για να ξεχωρίσουν τα VPN. Υπάρχει όμως περίπτωση να απαιτηθεί η επικοινωνία μεταξύ περιοχών διαφορετικών VPN. Μια

περιοχή του πελάτη A δεν θα ήταν ικανή να επικοινωνήσει με μια περιοχή του πελάτη B γιατί τα RD τους δεν θα ταίριαζαν. Η λειτουργία της επικοινωνίας συγκεκριμένων περιοχών διαφορετικών VPN, ονομάζεται extranet VPN. Αντίθετα, intranet VPN ονομάζεται η επικοινωνία μεταξύ περιοχών του ίδιου VPN. Η επικοινωνία μεταξύ περιοχών διαφορετικών VPN ελέγχεται από μια άλλη έννοια, αυτή των RTs.

Ένα RT είναι ένα extended community του BGP [31] , το οποίο υποδεικνύει ποιες διαδρομές πρέπει να εισαχθούν από το BGP στον VRF πίνακα. Τα extended community του BGP παρέχουν ένα μηχανισμό επισήμανσης της μεταφερόμενης πληροφορίας. Η εξαγωγή ενός RT (RT Export) σημαίνει ότι τα εξερχόμενα προθέματα VPN-IPv4 λαμβάνουν ένα επιπλέον BGP extended community όταν διανέμονται με το BGP (το RT, το οποίο έχει ρυθμιστεί στον PE Router). Η εισαγωγή ενός RT (RT Export) σημαίνει ότι τα εισερχόμενα VPN-IPv4 προθέματα από το BGP, ελέγχονται αν ταιριάζουν με ένα extended community (το RT, το οποίο έχει ρυθμιστεί στον PE Router). Αν υπάρξει ταίριασμα, το πρόθεμα τοποθετείται στον VRF πίνακα, αν όχι το πρόθεμα απορρίπτεται.

Στην εικόνα 5.5 φαίνεται ο έλεγχος των RTs για τις διαδρομές που εισάγονται στους VRF πίνακες από τους απομακρυσμένους PE Routers και με ποια RTs εξάγονται τα VPN-IPv4 προθέματα.

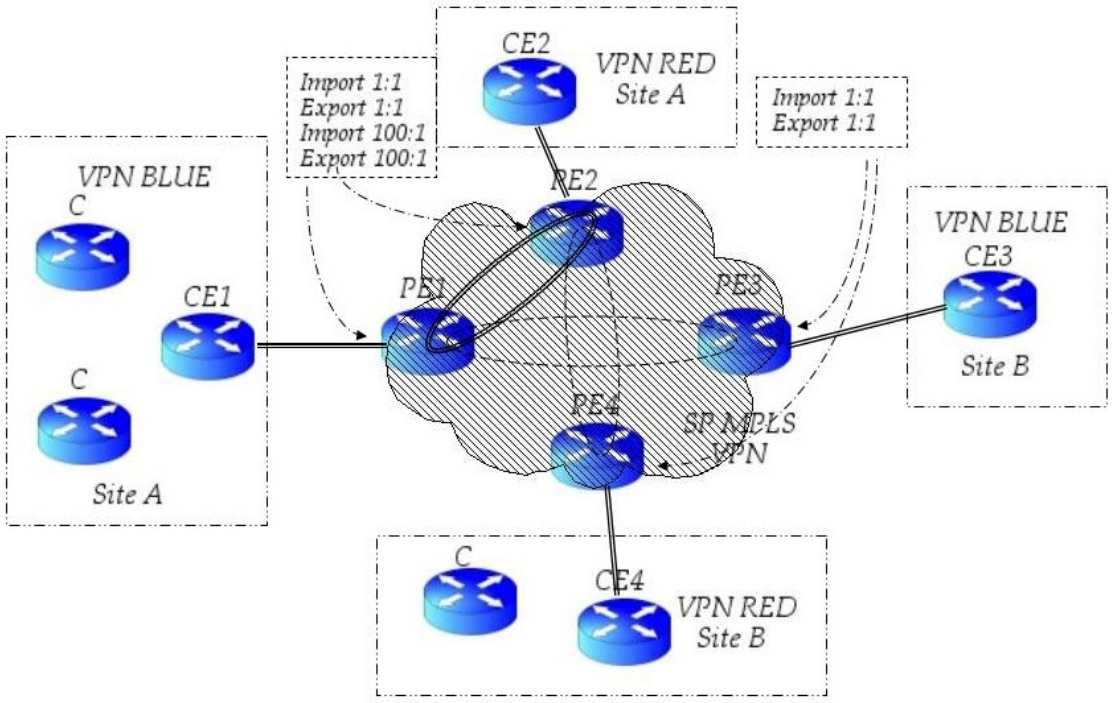


Εικόνα 5.5. Εισαγωγή και εξαγωγή RT 1

Όσον αφορά στο σενάριο της εικόνας 5.7 οι περιοχές A και B του VPN BLUE είναι ικανές να επικοινωνήσουν, καθώς επίσης και οι περιοχές A και B του VPN RED. Το RT που χρησιμοποιείται από το VPN BLUE είναι το 1:1, ενώ το VPN RED χρησιμοποιεί το RT 1:2. Σε περίπτωση, που η περιοχή A και μόνον αυτή από το VPN BLUE θέλει να επικοινωνήσει με την περιοχή A και μόνον αυτή από το VPN RED, τότε μπορούν να ρυθμιστούν κατάλληλα RTs στους VRF πίνακες των PE1 και PE2 αντίστοιχα. Εν συνεπεία, το RT 100:1 μπορεί να εισαχθεί και να εξαχθεί από τις περιοχές A των VRF RED και BLUE για να επιτευχθεί η επικοινωνία των συγκεκριμένων περιοχών των δύο VPN. Αυτό καλείται extranet. Στην εικόνα 5.6 φαίνονται οι ρυθμίσεις στους VRFs των δρομολογητών PE1 και PE2.

PE1	PE2
!	!
ip vrf BLUE	ip vrf RED
rd 1:1	rd 1:2
route-target export 1:1	route-target export 1:2
route-target export 100:1	route-target export 100:1
route-target import 1:1	route-target import 1:2
route-target import 100:1	route-target import 100:1
!	!

Εικόνα 5.6. Ρυθμίσεις VRF πινάκων στους δρομολογητές PE1 και PE2

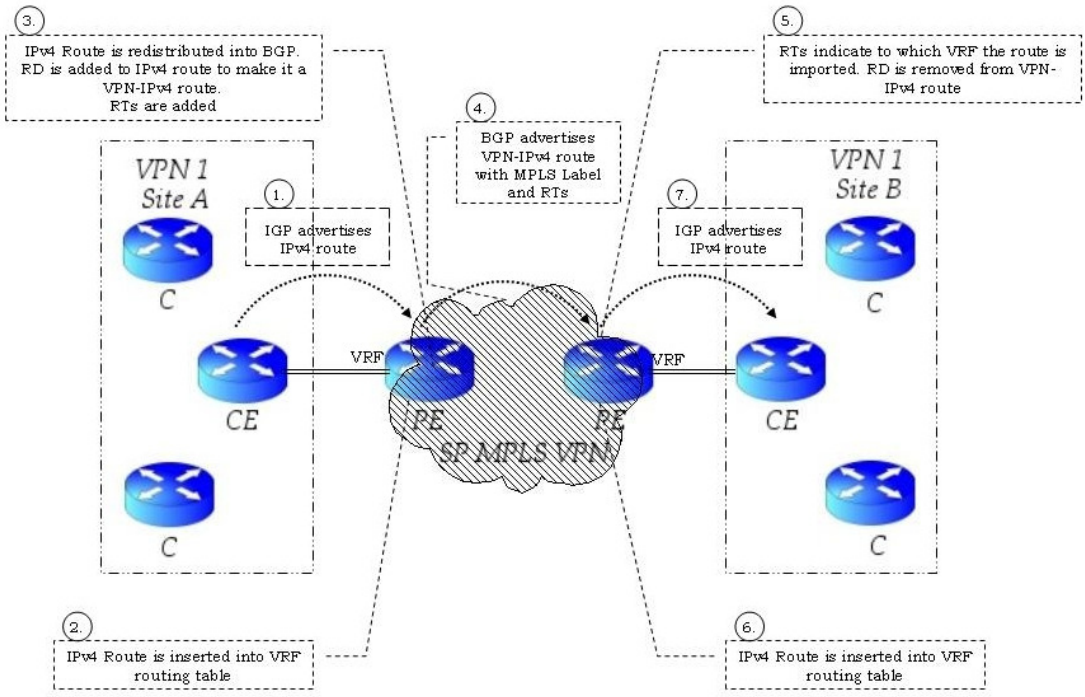


Εικόνα 5.7. Εισαγωγή και εξαγωγή RT 1

5.4.5 Διάδοση Διαδρομών σε ένα MPLS VPN

Οι VRF πίνακες διαχωρίζουν της διαδρομές των πελατών στους PE δρομολογητές. Το BGP φαίνεται να είναι το ιδανικό πρωτόκολλο δρομολόγησης για να μεταφέρει όλες αυτές τις διαδρομές (πιθανόν εκατοντάδες ή χιλιάδες). Η προσθήκη του RD στις IPv4 διαδρομές, η δημιουργία δηλαδή των VPN-IPv4 προθεμάτων, συντελεί με τη σειρά της στην ασφαλή μεταφορά των διαδρομών μέσω του MPLS VPN δικτύου.

Ένας PE Router λαμβάνει IPv4 διαδρομές από ένα CE Router μέσω ενός Interior Gateway Protocol (IGP). Αυτές οι IPv4 διαδρομές από την VPN περιοχή, τοποθετούνται στον VRF πίνακα δρομολόγησης. Ο VRF πίνακας που θα χρησιμοποιηθεί για μια συγκεκριμένη VPN περιοχή, εξαρτάται από τις ρυθμίσεις που έχουν γίνει στον PE Router (δηλαδή κάτω από ποιον VRF πίνακα έχει οριστεί η διασύνδεση που επικοινωνεί με τη συγκεκριμένη VPN περιοχή). Στις διαδρομές ενός VRF πίνακα προστίθεται το RD που έχει ρυθμιστεί για αυτόν τον πίνακα και σχηματίζονται τα VPN-IPv4, τα οποία διαφημίζονται με το BGP στους υπόλοιπους PE δρομολογητές του MPLS VPN δικτύου. Στους PE δρομολογητές αφαιρείται το RD από τα VPN-IPv4 προθέματα και οι IPv4 διαδρομές τοποθετούνται στους VRF πίνακες. Η εισαγωγή στους VRF πίνακες, εξαρτάται από τα εισαχθέντα RTs. Στη συνέχεια οι IPv4 διαδρομές διαφημίζονται στους CE Routers με κάποιο IGP πρωτόκολλο. Η όλη διαδικασία παρουσιάζεται στην εικόνα 5.8.



Εικόνα 5.8. Διάδοση IPv4 διαδρομών σε ένα MPLS δίκτυο

5.4.6 Προώθηση Πακέτων σε ένα MPLS VPN

Η προώθηση των πακέτων εντός του MPLS VPN είναι βασισμένη στις ετικέτες. Οι P Routers (Provider's Routers / ενδιάμεσοι LSRs) χρειάζονται μόνο την κατάλληλη πληροφορία για την αντικατάσταση των ετικετών για να προωθήσουν τα πακέτα. Ο συνήθης τρόπος είναι να ρυθμιστεί το LDP μεταξύ των ενδιάμεσων LSRs και των PE δρομολογητών έτσι ώστε όλη η κίνηση να γίνεται βασισμένη στις ετικέτες. Μπορεί να γίνει χρήση του RSVP με TE Extensions για μια υλοποίηση MPLS VPN με TE, όμως το πιο συνηθισμένο πρωτόκολλο διανομής ετικετών για MPLS VPN είναι το LDP. Τα πακέτα προωθούνται στον κορμό του MPLS δικτύου με μια ετικέτα που ορίζει το LSP από τον ingress PE στον egress PE δρομολογητή. Κάθε ενδιάμεσος LSR δεν χρειάζεται ποτέ να κάνει κάποια αναζήτηση σχετικά με την διεύθυνση δικτύου. Αυτός είναι ο τρόπος με τον οποίο γίνεται η μεταγωγή των πακέτων από τον ingress PE Router στον egress PE. Η παραπάνω ετικέτα που κουβαλούν τα πακέτα ονομάζεται IGP ετικέτα, γιατί συσχετίζεται με κάποιο IPv4 πρόθεμα στον γενικό πίνακα δρομολόγησης των P και PE δρομολογητών και είναι κάποιο IGP του δικτύου του παρόχου υπηρεσιών που το έχει διαφημίσει.

Ο τρόπος με τον οποίο ο egress PE δρομολογητής καταλαβαίνει σε ποιον VRF ανήκει το πακέτο δεν βρίσκεται στην IP κεφαλίδα του πακέτου αλλά ούτε προκύπτει από την IGP ετικέτα, η οποία χρησιμοποιείται μόνο για την προώθηση του πακέτου στο δίκτυο του παροχέα υπηρεσιών. Η λύση είναι η πρόσθεση άλλης μια ετικέτας στην στοίβα ετικετών του MPLS. Αυτή η ετικέτα προσδιορίζει σε ποιον VRF πίνακα ανήκει το πακέτο. Έτσι κάθε πακέτο ενός πελάτη προωθείται με δύο ετικέτες: την IGP ετικέτα στην κορυφή της στοίβας και την VPN ετικέτα στη βάση της στοίβας. Η VPN ετικέτα πρέπει να εισαχθεί από τον ingress PE για να μπορέσει ο egress PE να αντιστοιχίσει το πακέτο με έναν VRF πίνακα. Ο τρόπος με τον οποίο ο egress PE δρομολογητής ενημερώνει τον ingress PE για την VPN ετικέτα που πρέπει να χρησιμοποιηθεί για ένα συγκεκριμένο VRF πρόθεμα, έχει ήδη συζητηθεί. Γιατί το BGP που ήδη διαφημίζει τα VPN-IPv4 προθέματα, διαφημίζει επίσης και μια ετικέτα (την VPN ετικέτα ή BGP ετικέτα) που σχετίζεται με το συγκεκριμένο VPN-IPv4 πρόθεμα.

Ανακεφαλαιώνοντας, στην κίνηση μεταξύ των VRF κάθε πακέτο έχει δυο ετικέτες μέσα στο MPLS VPN δίκτυο. Στην κορυφή βρίσκεται η IGP ετικέτα, η οποία διανέμεται από κόμβο σε κόμβο με το LDP ή το RSVP TE μεταξύ όλων των PE και P δρομολογητών. Η ετικέτα στη βάση της στοίβας είναι η VPN ή BGP ετικέτα, η οποία διανέμεται με το BGP από τον ένα PE στον άλλο. Οι P

δρομολογητές χρησιμοποιούν την IGP ετικέτα για να προωθήσουν το πακέτο στον κατάλληλο egress PE δρομολογητή. Οι egress PE δρομολογητές χρησιμοποιούν την VPN ετικέτα για να προωθήσουν ένα IP πακέτο στον κατάλληλο CE δρομολογητή.

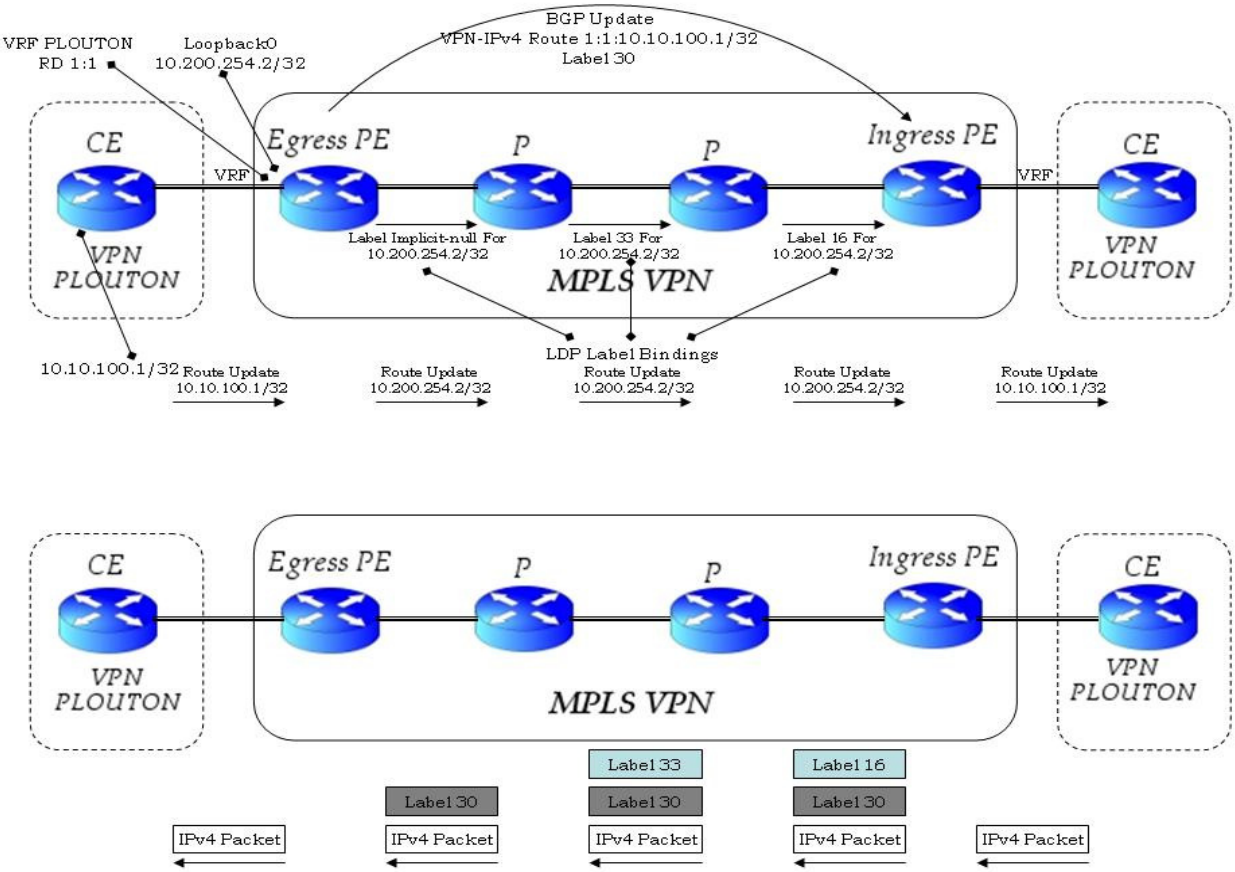
Παράδειγμα Προώθησης Πακέτων μέσω ενός MPLS VPN δικτύου

Στην εικόνα 5.9 παρουσιάζεται ένα σενάριο MPLS VPN δικτύου και η πορεία ενός πακέτου καθώς ταξιδεύει από την μια περιοχή ενός πελάτη στην άλλη. Το BGP πρέπει να τρέχει μεταξύ των PE Routers, οι οποίοι διαφημίζουν τις VPN-IPv4 διαδρομές και τις σχετικές με αυτές VPN ετικέτες. Ένα πρωτόκολλο διανομής ετικετών πρέπει να λειτουργεί μεταξύ των PE και P δρομολογητών. Στο σενάριο της εικόνας 5.9 το πρωτόκολλο διανομής ετικετών είναι το LDP. Μεταξύ των PE και των CE δρομολογητών πρέπει επίσης να τρέχει ένα πρωτόκολλο δρομολόγησης ώστε αν τοποθετεί τις διαδρομές των πελατών στους VRF πίνακες των PE δρομολογητών. Επίσης, αυτές οι διαδρομές πρέπει να διαδίδονται στο BGP και το αντίθετο. Στην εικόνα 5.9 φαίνονται οι διαφημίσεις των VPN-IPv4 διαδρομών και η VPN ετικέτα που αποδίδεται από τον egress PE στον ingress PE. Επίσης φαίνεται και η διαφήμιση της IGP διαδρομής, η οποία αναπαριστάται από το BGP Next Hop του egress PE (συνήθως loopback διεύθυνση). Η διεύθυνση BGP Next Hop του egress PE είναι η 10.200.254.2/32, την οποία κάποιο IGP διαφημίζει στον ingress PE. Οι ετικέτες για αυτήν την IGP διαδρομή διανέμονται από το LDP ανά κόμβο. Η IPv4 διαδρομή του πελάτη 10.10.100.1/32 διαφημίζεται από κάποιο IGP πρωτόκολλο από τον CE στον egress PE. Ο egress PE της προσθέτει το RD 1:1 μετατρέποντας την στην VPN-IPv4 διαδρομή 1:1:10.10.100.1/32 και την στέλνει στον ingress PE με ετικέτα 30 μέσω του BGP.

Όταν ένα IP πακέτο φθάνει στον ingress PE Router από τον CE, ο ingress PE αναζητά την IP διεύθυνση προορισμού στον VRF πίνακα του συγκεκριμένου VPN. Ο σωστός πίνακας βρίσκεται από τον PE Router κοιτώντας από ποια διασύνδεση έχει εισέλθει το πακέτο και με ποιον VRF πίνακα σχετίζεται αυτή η διασύνδεση. Η εγγραφή που αναζητείται στον VRF πίνακα συνήθως υποδεικνύει δύο ετικέτες, οι οποίες πρέπει να προστεθούν στο πακέτο (VPN ετικέτα:30, IGP ετικέτα:16). Η εικόνα 5.10 παρουσιάζει τον VRF πίνακα του ingress PE για το συγκεκριμένο VPN.

Έτσι, ο ingress PE προσθέτει στο πακέτο την VPN ετικέτα 30, όπως αυτή διαφημίστηκε από το BGP για την VPN-IPv4 διαδρομή. Στην συνέχεια προσθέτει στην κορυφή της στοίβας και την IGP ετικέτα, η οποία είναι η ετικέτα που

σχετίζεται με την IGP διαδρομή για την BGP Next Hop διεύθυνση. Έτσι προστίθεται η IGP ετικέτα 16, η οποία ως γνωστόν είναι τοπικής σημασίας.



Εικόνα 5.9. Παράδειγμα προώθησης πακέτων σε ένα MPLS VPN δίκτυο

```
Ingress-PE#show ip cef vrf plouton 10.10.100.1 255.255.255.0 detail
  10.10.100.1/32, epoch 0
    recursive via 10.200.254.2 label 30
      nexthop 10.200.214.1 POS0/1/0 label 16
```

Εικόνα 5.10. Εμφάνιση στοιχείων του VRF πίνακα plouton

Το πακέτο φεύγει από τον ingress PE με δυο ετικέτες στην στοίβα. Η IGP ετικέτα η οποία βρίσκεται στην κορυφή, αντικαθίσταται σε κάθε κόμβο. Με αυτήν την ετικέτα το IPv4 VPN πακέτο φθάνει στον σωστό egress PE Router. Συνήθως φθάνει στον egress PE με μια ετικέτα (την VPN ετικέτα), λόγω της τεχνικής PHP (Penultimate Hop Popping). Ο egress PE αναζητά την VPN ετικέτα στον LFIB και στέλνει το πακέτο, αφού έχει αφαιρεθεί η στοίβα ετικετών στον CE Router.

5.5 L2VPNs

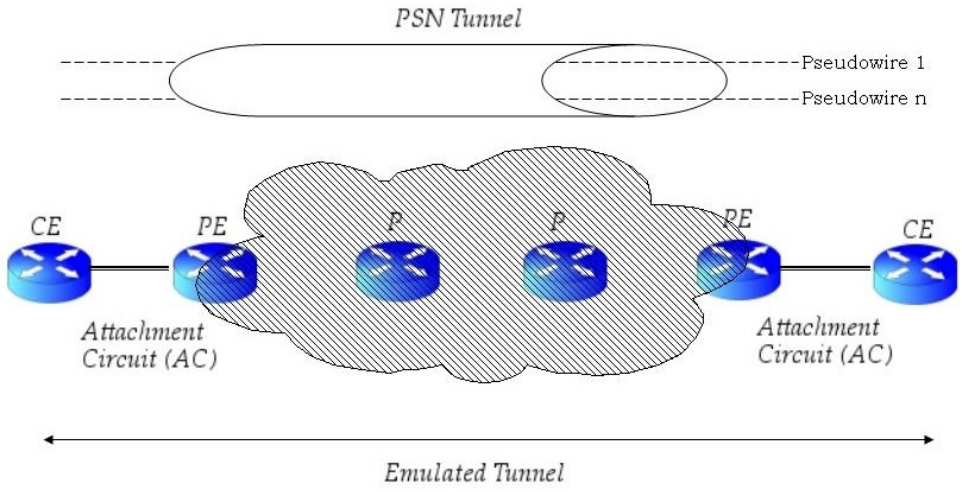
Τα Layer 3 VPN έχουν κάποιους περιορισμούς. Ο κυριότερος περιορισμός είναι ότι το μόνο πρωτόκολλο που υποστηρίζει είναι το IP. Επίσης, είναι πιθανή υπερφόρτωση των PE δρομολογητών. Σε σύγκριση με τα Layer 3 VPNs, τα Layer 2 VPNs είναι ικανά να μεταφέρουν οποιοδήποτε πρωτόκολλο (διαφορετικό του IP) μέσω της δικτυακής υποδομής. Ένα άλλο μειονέκτημα των Layer 3 VPNs είναι η ανάγκη της ύπαρξης πινάκων δρομολόγησης στους PE Routers για κάθε συνδεδεμένο VPN. Αυτό δεν ισχύει στα Layer 2 VPNs, διότι δεν αποθηκεύονται πίνακες δρομολόγησης των πελατών στους δρομολογητές του παροχέα υπηρεσιών.

Αρκετές τεχνικές Layer 2 VPN έχουν αναπτυχθεί για την μεταφορά πλαισίων επιπέδου 2 μέσω ενός δικτύου μεταγωγής πακέτων (Packet Switched Network/PSN). Μια τεχνική είναι η Any Transport over MPLS της Cisco Systems, με την οποία επιτυγχάνεται η μεταφορά πλαισίων επιπέδου 2 μέσω ενός MPLS δικτύου. Μια επίσης αναπτυσσόμενη τεχνική Layer 2 VPN είναι το Layer 2 Tunneling Protocol version 3 (L2TPv3). Το L2TPv3 χρησιμοποιείται για την μεταφορά πλαισίων μέσω ενός IP δικτύου κορμού. Και με τις δυο τεχνικές μπορούν να μεταφερθούν πλαίσια Ethernet, HDLC [6], PPP, ATM, Frame Relay και άλλων πρωτοκόλλων επιπέδου σύνδεσης.

Η αρχιτεκτονική του AToM και του L2TPv3 είναι βασισμένη στα Pseudowires. Τα Pseudowires μεταφέρουν την Layer 2 κίνηση από άκρη σε άκρη (από PE σε PE), μέσω ενός δικτύου μεταγωγής πακέτων (PSN), ανεξάρτητα αν είναι MPLS (AToM) ή IP (L2TPv3) δίκτυο. Είναι μια σύνδεση μεταξύ δύο PE δρομολογητών, η οποία εξομοιώνει ένα καλώδιο το οποίο μεταφέρει πλαίσια δευτέρου επιπέδου. Τα Pseudowires χρησιμοποιούν την έννοια των Tunnels. Τα πλαίσια επιπέδου 2 είτε ενθυλακώνονται μέσα σε ένα IP πακέτο (L2TPv3) ή επισημαίνονται (AToM). Έτσι επιτυγχάνεται η εξομοίωση των χαρακτηριστικών και της λειτουργίας ενός δικτύου δευτέρου επιπέδου μέσω ενός PSN δικτύου.

Στην εικόνα 5.11 παρουσιάζονται Pseudowires, τα οποία συνδέουν από άκρο σε άκρο ένα PSN δίκτυο. Το PSN μπορεί να είναι ένα IP ή ένα MPLS δίκτυο. Μέσα στο PSN Tunnel μπορεί να βρίσκονται ένα ή και περισσότερα Pseudowires, τα οποία συνδέουν τα ACs (Attachment Circuits) των PE δρομολογητών μεταξύ τους. Ένα AC μπορεί να είναι ATM, Frame-Relay, HDLC, PPP κ.ο.κ. Τα πλαίσια που λαμβάνονται στους PE Routers από το AC, ενθυλακώνονται και αποστέλλονται μέσω του Pseudowire στον απομακρυσμένο PE Router. Στον egress Router του

PSN Tunnel τα πλαίσια ξεχωρίζονται από την ενθυλάκωση τους και προωθούνται στο AC.



Εικόνα 5.11. Σύνδεση ακραίων δρομολογητών μέσω Pseudowires

Λίγο πριν την προώθηση των πλαισίων μέσω του pseudowire, οι PE δρομολογητές πρέπει να εγκαθιδρύσουν μια σχέση μεταξύ τους. Κατά την εγκαθίδρυση αυτής της σχέσης, οι PE Routers ανταλλάσσουν τις απαραίτητες πληροφορίες ώστε να συμφωνήσουν για το είδος της υπηρεσίας. Για παράδειγμα, πρέπει να συμφωνήσουν για την μέθοδο ενθυλάκωσης. Έτσι το αποτέλεσμα για μια υπηρεσία AToM, είναι ότι οι CE δρομολογητές ή μεταγωγείς είναι φαινομενικά άμεσα συνδεδεμένοι σε επίπεδο σύνδεσης, άσχετα αν το Pseudowire τις διαχωρίζει.

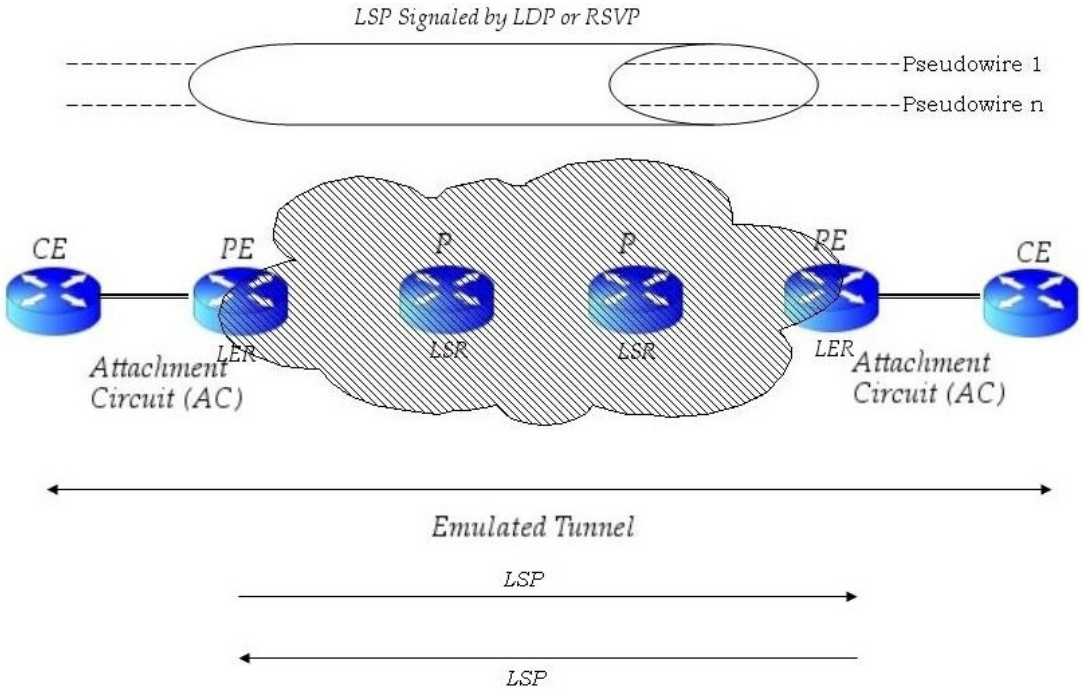
5.5.1 Any Transport over MPLS (AToM)

Σε δίκτυα που υλοποιούν την τεχνική AToM, όλοι οι δρομολογητές του παρόχου υπηρεσιών πρέπει να τρέχουν το πρωτόκολλο MPLS και ένα AC (Attachment Circuit) να συνδέεται με τους PE δρομολογητές. Οι PE δρομολογητές λαμβάνουν τα πλαίσια από τα AC, προσθέτουν σε αυτά ετικέτες και τα στέλνουν μέσω του PSN στον απομακρυσμένο PE δρομολογητή. Στον απομακρυσμένο PE δρομολογητή οι ετικέτες αφαιρούνται και τα πλαίσια στέλνονται στον CE δρομολογητή ή μεταγωγέα.

Κατά συνέπεια, στην περίπτωση του AToM το PSN Tunnel δεν είναι τίποτε άλλο από ένα LSP μεταξύ των δυο PE δρομολογητών. Για αυτό το λόγο και οι ετικέτες που συνδέονται με το LSP ονομάζονται και Tunnel Labels. Όσον αφορά στην σηματοδοσία του LSP, αυτή μπορεί να πραγματοποιηθεί με διάφορους τρόπους. Μπορεί να χρησιμοποιηθεί το LDP, για να αποδώσει ετικέτες στο LSP

βήμα προς βήμα. Επίσης, μπορεί να χρησιμοποιηθεί TE, και έτσι το RSVP να σηματοδοτήσει το LSP. Έτσι, η Tunnel Label χρησιμοποιείται για την ταυτοποίηση του LSP στο οποίο ανήκουν τα πλαίσια ενός συγκεκριμένου CE. Ένα PSN Tunnel (LSP), ίσως εμπεριέχει περισσότερα από ένα Pseudowires. Έτσι ένας PE δρομολογητής χρησιμοποιεί άλλη μια ετικέτα για να ξεχωρίσει τα Pseudowires. Η ετικέτα αυτή ονομάζεται VC ή PW γιατί η λειτουργία της είναι να ξεχωρίσει ένα Virtual Circuit (VC) ή ένα Pseudowire (PW).

Για την εγκατάσταση ενός Pseudowire πρέπει να υπάρχουν δύο LSP μεταξύ των PE Routers, ένα για κάθε κατεύθυνση. Ως γνωστόν, ένα LSP είναι μονόδρομο. Στην εικόνα 5.12 παρουσιάζεται η εξομοίωση των Pseudowires σε ένα MPLS δίκτυο.



Εικόνα 5.12. Εγκατάσταση δύο LSP για αμφίδρομη επικοινωνία

Προώθηση Επισημασμένων Πλαισίων

Όπως προαναφέρθηκε, καθώς ο PE δρομολογητής λαμβάνει ένα πλαίσιο από τον CE δρομολογητή, το προωθεί μέσω του MPLS δικτύου με δυο ετικέτες˙ την ετικέτα του Tunnel και την PW ετικέτα.

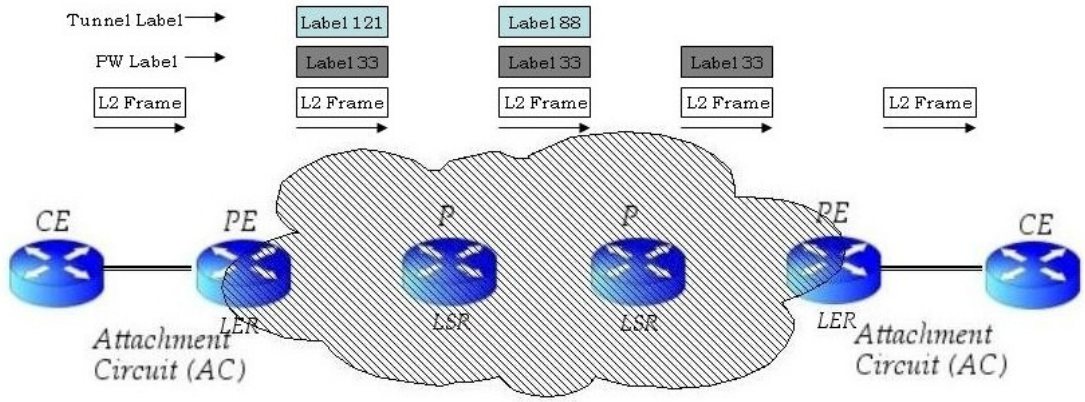
Σε ένα δίκτυο AToM, εκτός των άλλων, κάθε ζεύγος PE δρομολογητών πρέπει να τρέχουν μια συνεδρία targeted LDP μεταξύ τους. Αυτή η συνεδρία σηματοδοτεί χαρακτηριστικά του Pseudowire και διαφημίζει επίσης την PW ετικέτα. Η PW ετικέτα βρίσκεται πάντα στη βάση τη στοίβας ετικετών. Η δουλειά της είναι η ταυτοποίηση του Pseudowire και πιο συγκεκριμένα η ταυτοποίηση του AC που

συνδέεται με τον egress PE. Η Tunnel ετικέτα βρίσκεται στην κορυφή της στοίβας και ορίζει το LSP που θα κινηθούν τα επισημασμένα πλαίσια από τον ingress PE στον egress PE.

Στην εικόνα 5.13 παρουσιάζεται ένα παράδειγμα προώθησης ενός AToM πακέτου. Ο ingress LSR προσθέτει στο πλαίσιο την PW ετικέτα 33. Αυτή η ετικέτα δεν αλλάζει γιατί χρησιμοποιείται για την ταυτοποίηση του Pseudowire. Στην συνέχεια προσθέτει την ετικέτα του Tunnel, η οποία είναι αυτή που συσχετίζεται με κάποιο IGP πρόθεμα δικτύου του egress PE. Αυτό το πρόθεμα καθορίζεται στις ρυθμίσεις του AToM για το PSN Tunnel προς δημιουργία. Το MPLS πακέτο προωθείται βάση της κορυφαίας ετικέτας, βήμα προς βήμα μέχρι να φθάσει στον egress PE.

Λόγω της τεχνικής PHP (Penultimate Hop Popping), όταν το πακέτο φθάσει στον egress PE η Tunnel Label θα έχει ήδη αφαιρεθεί. Ο egress Router αναζητά την PW ετικέτα στον LFIB, την αφαιρεί και προωθεί το πακέτο στο κατάλληλο AC.

Οι P Routers από τη μεριά τους, δεν κοιτούν ποτέ την ετικέτα PW και δεν εκτελούν κάποια ιδιαίτερη λειτουργία πέρα από την αντικατάσταση ετικέτας. Οι P δρομολογητές επίσης, δεν γνωρίζουν καθόλου για την υπηρεσία AToM. Δεν χρειάζεται κάποιο ιδιαίτερο πρωτόκολλο διανομής ετικετών για αυτούς, εφόσον το μόνο που κάνουν είναι να συμβάλλουν στη δημιουργία του LSP και έτσι το LDP ή το RSVP αρκούν για την λειτουργία τους. Αντίθετα για τους PE Routers, πρέπει να υπάρξει μια συνεδρία targeted LDP για να διαφημίσει την ετικέτα PW στον απομακρυσμένο PE.



Εικόνα 5.13. Προώθηση ενός πακέτου με την τεχνική AToM

Στην εικόνα 5.14 φαίνεται πίνακας LFIB του egress PE. Η εισερχόμενη (local binding/33) PW ετικέτα αντιστοιχίζεται με ένα Layer 2 αναγνωριστικό, το οποίο υποδεικνύει το AC που θα προωθηθεί το πλαίσιο.

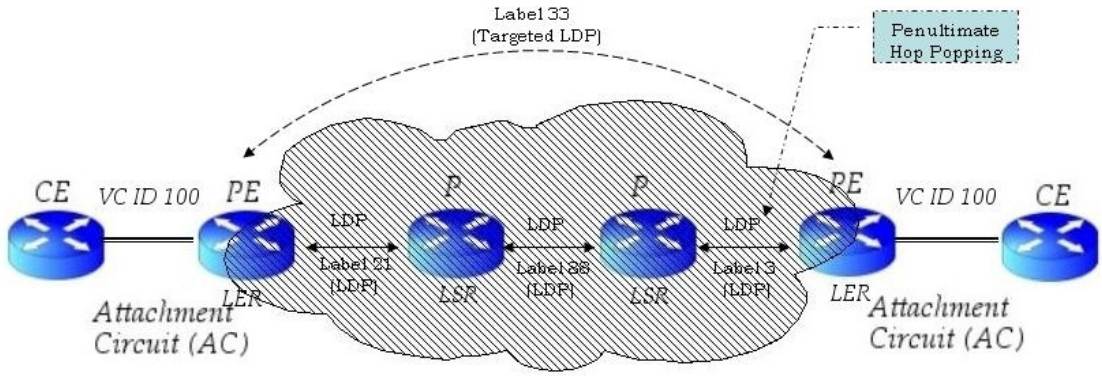
Egress PE#**show mpls forwarding-table interface serial 4/0/0**

Local tag	Outg. tag or VC	Prefix or Tunnel ID	Bytes tag switched	Out. interface	Next hop
33	Untagged	l2ckt(100)	2138118	Se4/0/0	point2point

Εικόνα 5.14. LFIB πίνακας του Egress PE

Η Σηματοδοσία του Pseudowire

Η σηματοδοσία του Pseudowire επιτυγχάνεται με την targeted LDP συνεδρία. Το LDP εγκαθιστά και διατηρεί τα Pseudowires μεταξύ των PE Routers. Η πιο σημαντική λειτουργία του LDP σε αυτό το σημείο είναι η διαφήμιση της ετικέτας PW, που σχετίζεται με το συγκεκριμένο Pseudowire. Η ετικέτα αυτή διαφημίζεται χρησιμοποιώντας ένα Label Mapping μήνυμα και υιοθετώντας την μέθοδο διανομής downstream unsolicited. Στο σενάριο της εικόνας 5.15 φαίνεται η διαφήμιση τον ετικετών PW και Tunnel. Η PW ετικέτα διαφημίζεται από τον egress PE στον ingress PE για ένα συγκεκριμένο AC με VC ID 100, με την targeted LDP συνεδρία. Η ετικέτα του Tunnel (LSP) διαφημίζεται από τον egress PE προς τον ingress PE χρησιμοποιώντας το LDP.



Εικόνα 5.15. Διαφήμιση της PW και της Tunnel ετικέτας

Το μήνυμα Label Mapping, το οποίο διαφημίζεται με την targeted LDP συνεδρία περιέχει κάποια TLVs. Ένα TLV είναι ένα αντικείμενο το οποίο αποτελείται από μια τριάδα: τύπο (type), μήκος (length) και τιμή (value). Η

προσθήκη TLV σε ένα πρωτόκολλο αποτελεί έναν εύκολο τρόπο για την επέκταση του πρωτοκόλλου. Αυτά είναι τα: Pseudowire identifier (PW ID) FEC TLV και Label TLV. Το πρώτο TLV ταυτοποιεί το Pseudowire στο οποίο αντιστοιχίζεται η ετικέτα, ενώ το δεύτερο είναι αυτό που χρησιμοποιεί το LDP για να διαφημίσει την ετικέτα (PW Label).

Το PW ID FEC TLV περιέχει τα παρακάτω στοιχεία:

- C-bit: αν το C-bit είναι 1 τότε υπάρχει μια λέξη ελέγχου (control word). Μια λέξη ελέγχου είναι ένα πεδίο των 32 bit και τοποθετείται ανάμεσα από την PW ετικέτα και το πλαίσιο επιπέδου σύνδεσης που μεταφέρεται. Απαιτείται η ύπαρξη της για κάποια πρωτόκολλα δευτέρου επιπέδου, ενώ είναι προαιρετική για άλλα. Μεταφέρει επιπλέον πληροφορίες, όπως πληροφορίες ελέγχου που μπορεί να απαιτούνται από κάποια πρωτόκολλα, και έναν αριθμό σειράς. Υπεύθυνος για την προσθήκη της λέξης ελέγχου είναι ο ingress Router και με την σειρά του ο egress Router την αφαιρεί, αφού πρώτα την επεξεργαστεί. Σε γενικές γραμμές μια λέξη ελέγχου εκτελεί τις παρακάτω λειτουργίες:

    - μεταφέρει bit ελέγχου από την κεφαλίδα επιπέδου σύνδεσης του πρωτοκόλλου που μεταφέρεται
    - εγγυάται την σειρά των μεταφερόμενων πλαισίων
    - συμπληρώνει μικρά πακέτα
    - εκτελεί λειτουργίες για την σωστή κατάτμηση και συλλογή πλαισίων, σε περίπτωση που απαιτείται κατάτμηση

- PW Type: είναι ένα πεδίο των 15 bit, το οποίο αναπαριστά τον τύπο του Pseudowire. Στον πίνακα 6.1 παρουσιάζονται οι πιο συνηθισμένοι τύποι Pseudowires

Πίνακας 5.1. Τύποι Pseudowires

PW Type	Description
0x0005	Ethernet
0x0004	Ethernet Tagged Mode
0x0006	HDLC
0x0007	PPP
0x000F	Frame Relay port mode
0x0019	Frame Relay DLCI

- Group ID: χρησιμοποιείται για την ταυτοποίηση μιας ομάδας από Pseudowires. Ένας PE Router θα μπορούσε να χρησιμοποιήσει το Group

ID για να αποσύρει όλες τις PW ετικέτες, που σχετίζονται με μια ομάδα από Pseudowires, με ένα και μόνο LDP Label Withdraw μήνυμα. Αυτή η τεχνική αναφέρεται σαν wild card label withdrawal.

- PW ID: είναι ένα πεδίο των 32 bit και μαζί με το PW Type ταυτοποιεί απόλυτα ένα Pseudowire.
- Interface Parameters: περιγράφουν κάποιες παραμέτρους που αφορούν στη διασύνδεση, όπως η μέγιστη μονάδα μετάδοσης (MTU) της διασύνδεσης προς τον CE δρομολογητή ή κάποια περιγραφή της διασύνδεσης.

Λόγω του ότι ένα LSP είναι μονόδρομο, η εγκαθίδρυση ενός Pseudowire επιτυγχάνεται μόνο με την εγκατάσταση ενός άλλου LSP προς την αντίθετη κατεύθυνση του αρχικού. Το PW ID FEC TLV χρησιμοποιείται, επίσης, για την αναγνώριση και το ταίριασμα των δύο αντίθετων LSPs μεταξύ του ζεύγους των ακραίων PEs. Στη εικόνα 5.16 φαίνεται το PW ID FEC TLV.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
PW TLV								C	PW Type															PW Length							
Group ID																															
PW ID																															
Interface Parameters ----------																															

Εικόνα 5.16. Το PW ID FEC TLV

MPLS MTU για Πακέτα AToM

Σε δίκτυα MPLS στα οποία υλοποιείται η υπηρεσία AToM, τα πλαίσια λαμβάνουν τουλάχιστον δυο ετικέτες για την μεταφορά τους μέσω του Pseudowire. Εκτός από την περίπτωση που οι δύο PE δρομολογητές είναι άμεσα συνδεδεμένοι. Έτσι το μέγεθος του πακέτου αυξάνεται τουλάχιστον κατά 8 bytes. Στην περίπτωση που υπάρχει και λέξη ελέγχου αυξάνει άλλα 4 bytes. Το φορτίο που μεταφέρεται με την υπηρεσία AToM, δεν είναι απλά ένα IP πακέτο όπως με τα L3VPN, αλλά ένα πλαίσιο δευτέρου επιπέδου. Έτσι κατά τον υπολογισμό του μέγιστου πιθανού πακέτου AToM πρέπει να συμπεριλάβουμε και τα bytes της κεφαλίδας του επιπέδου σύνδεσης. Για παράδειγμα στο Ethernet over MPLS, αν το μεταφερόμενο πλαίσιο είναι ένα Ethernet II πλαίσιο που κουβαλάει ένα IP πακέτο των 1500 bytes, τότε το μέγιστο φορτίο ενός AToM πακέτου θα είναι 1514 bytes. Τα 14 bytes είναι 12 για τις MAC διευθύνσεις πηγής και προορισμού και 2 για το Ethertype. Αν το μεταφερόμενο πλαίσιο είναι 802.1Q, τότε άλλα δυο byte πρέπει να προστεθούν για την VLAN σήμανση.

Για να εγγυηθεί κανείς ότι δεν θα χρειαστεί η κατάτμηση ενός πακέτου, πρέπει το MTU στις διασυνδέσεις του κορμού του δικτύου να είναι μεγαλύτερο από αυτό του μεγαλύτερου πιθανού πακέτου AToM. Έστω ότι ένα IP πακέτο των 1500 byte μεταφέρεται μέσω ενός Ethernet over MPLS (EoMPLS) Pseudowire με μια κεφαλίδα VLAN. Αν χρησιμοποιείται και λέξη ελέγχου, το μέγεθος του MPLS πακέτου θα είναι 1530 bytes. Αναλυτικά θα έχει ως εξής:

- 1500 bytes του IP πακέτου
- 8 bytes για τις δύο ετικέτες του MPLS
- 4 bytes για τη λέξη ελέγχου
- 4 bytes για την κεφαλίδα 802.1Q
- 14 bytes για την κεφαλίδα Ethernet II (χωρίς το FCS)

Κατά συνέπεια το MTU σε όλες τις διασυνδέσεις του MPLS δικτύου θα πρέπει να είναι τουλάχιστον 1530 bytes προς αποφυγή πιθανής κατάτμησης. Εναλλακτικά μπορεί να χρησιμοποιηθεί κάποιος αλγόριθμος εύρεσης MTU ή να γίνει στατικός περιορισμός του MTU στους ακραίες συσκευές.

Μεταφερόμενα Πρωτόκολλα Επιπέδου Σύνδεσης

Η υπηρεσία AToM υποστηρίζει αρκετά πρωτόκολλα επιπέδου σύνδεσης. Παρακάτω αναφέρεται περιληπτικά το φορτίο των AToM πακέτων για διαφορετικά πρωτόκολλα δευτέρου επιπέδου [15]:

- HDLCoMPLS: το φορτίο ενός AToM πακέτου που μεταφέρει ένα HDLC πλαίσιο είναι το ίδιο το HDLC πλαίσιο, εκτός από κάποια flags και του FCS. Τα flags και το FCS τα προσθέτει ο egress PE πριν στείλει το πακέτο στον CE δρομολογητή/μεταγωγέα.
- PPPoMPLS: παρόμοια το φορτίο στην περίπτωση που του PPPoMPLS είναι το PPP πλαίσιο, εκτός των flags, των διευθύνσεων, του πεδίου ελέγχου (control field) και του FCS. Όλα τα παραπάνω τα προσθέτει ο egress PE πριν αποστείλει το πακέτο στον CE δρομολογητή/μεταγωγέα.
- FRoMPLS: το Frame Relay μπορεί να μεταφερθεί μέσω ενός MPLS δικτύου με δύο τρόπους: DLCI to DLCI ή Port to Port.

  Με την DLCI to DLCI μέθοδο, ένα εικονικό κύκλωμα (VC) μεταφέρεται πάνω από ένα Pseudowire. Το φορτίο του AToM πακέτου είναι ένα Frame Relay πλαίσιο, του οποίου όμως αφαιρούνται τα flags, το FCS, ακόμα και η Frame Relay κεφαλίδα. Αντίθετα τα bits ελέγχου FECN, BECN, DE και CR αντιγράφονται στη λέξη ελέγχου. Μια κεφαλίδα προστίθεται μεταξύ της

λέξης ελέγχου και του Frame Relay φορτίου η οποία προσδιορίζει το Ethertype, δηλαδή το πρωτόκολλο δευτέρου ή τρίτου επιπέδου που αποτελεί το φορτίο. Όταν ο egress PE δρομολογητής λάβει το πακέτο χρησιμοποιεί την PW ετικέτα για να προσδιορίσει το VCID και κατόπιν την αφαιρεί. Στη συνέχεια η πληροφορία που βρίσκεται στη λέξη ελέγχου χρησιμοποιείται για την ανακατασκευή της κεφαλίδας Frame Relay πριν την αποστολή του πλαισίου στον CE Router.

Με την μέθοδο Port to Port, όλα τα VCs από μια πόρτα μεταφέρονται μέσω ενός Pseudowire. Έτσι δημιουργείται μια πολλά προς ένα αντιστοίχηση των VCs στο Pseudowire. Από την μεριά των PE δρομολογητών η ενθυλάκωση που χρησιμοποιείται για την μεταφορά του Frame Relay σε port to port κατάσταση είναι HDLC. Το Pseudowire μεταφέρει την κεφαλίδα του frame relay αφού αφαιρεθούν τα flags και το FCS πεδίο.

- EoMPLS: η μεταφορά Ethernet πάνω από MPLS είναι point to point. Δεν γίνεται multipoint μετάδοση και έτσι δεν εξομοιώνεται ένα τοπικό δίκτυο. Η εξομοίωση ενός τοπικού δικτύου με το MPLS είναι δυνατή και ονομάζεται VPLS.

  Το AC στην περίπτωση του EoMPLS μπορεί να είναι μια πόρτα Ethernet ή ένα 802.1Q VLAN. Για κάθε έναν από τους δυο τύπους το LDP σηματοδοτεί διαφορετικό PW Type στο PW ID FEC TLV. Στην πρώτη περίπτωση το PW Type είναι 5, ενώ αν υπάρχει Ethernet VLAN το PW Type είναι 4.

  Όταν ένας ingress PE Router λάβει ένα Ethernet πλαίσιο αφαιρεί τα: Preamble, Start of Frame Delimiter (SFD) και το πεδίο FCS. Στη συνέχεια προσθέτει μια λέξη ελέγχου, επισημαίνει το πλαίσιο και το προωθεί στο MPLS δίκτυο. Αν το πλαίσιο Ethernet είναι επισημασμένο με μια 802.1Q σήμανση, τότε και αυτή παραμένει. Στον egress PE αφαιρείται η ετικέτα PW και η λέξη ελέγχου. Το πλαίσιο Ethernet ανακατασκευάζεται και αποστέλλεται στον CE δρομολογητή/μεταγωγέα.

Ποιότητα Υπηρεσίας στο AToM

Υπάρχει η δυνατότητα της χρήσης ποιότητας υπηρεσίας (QoS) σε MPLS δίκτυα ώστε να καθοριστεί η προτεραιότητα των πακέτων. Στην περίπτωση του IP, η προτεραιότητα ενός πακέτου μπορεί να καθοριστεί από την παρουσία των DSCP (DiffServ CodePoint) bit στην κεφαλίδα του IP πακέτου. Στην περίπτωση

του MPLS, μπορεί κανείς να θέσει την προτεραιότητα από τα 3 EXP bits της ετικέτας. Έτσι οι τιμές που μπορεί να πάρει είναι μεταξύ του 0 και του 7. Όσον αφορά στο AToM, το φορτίο του MPLS πακέτου είναι ένα πλαίσιο. Υπάρχουν τρεις επιλογές για το μαρκάρισμα των EXP bits της ετικέτας:

- Στατική ρύθμιση των EXP bits
- Ρύθμιση των EXP bits σύμφωνα με τα DSCP bits του IP
- Ρύθμιση των EXP bits σύμφωνα με πληροφορία της κεφαλίδας του πλαισίου

Μπορεί κανείς να ρυθμίσει τα EXP bits στατικά χρησιμοποιώντας το Modular QoS Command Line Interface (MQC) των δρομολογητών της Cisco Systems. Απαιτείται η εισαγωγή πολιτικής δικτύου (Policy) στον ingress δρομολογητή, ώστε να θέτει τα EXP bits. Τα EXP bits θέτονται στην ετικέτα του PW αλλά και στην ετικέτα του Tunnel. Αυτό είναι σημαντικό γιατί στην περίπτωση που εφαρμόζεται η τεχνική PHP (εξ' ορισμού λειτουργία για πολλούς δρομολογητές), το πακέτο φθάνει στον egress Router χωρίς την ετικέτα του Tunnel. Άρα για να εγγυηθεί η παρουσία των EXP bits, πρέπει αυτά να εισαχθούν και στην PW ετικέτα. Το παρακάτω παράδειγμα της εικόνας 5.17, παρουσιάζει την ρύθμιση των EXP bits στην περίπτωση του EoMPLS. Η ρύθμιση έχει πραγματοποιηθεί εισάγοντας πολιτική δικτύου στον ingress LSR με το MQC.

```
PE#
!
class-map match-all EXP
  match any
!
policy-map set-EXP
  class EXP
  set mpls experimental 4
!
interface FastEthernet9/0/0
  no ip address
  xconnect 10.200.254.4 100 pw-class one
  service-policy input set-EXP
!
```

Εικόνα 5.17. Αρχείο ρύθμισης των EXP bits στο EoMPLS

Η ρύθμιση των EXP bits σύμφωνα με τα DSCP bits της IP κεφαλίδας είναι εφικτή μόνο εάν το φορτίο του πλαισίου είναι ένα IP πακέτο. Η πληροφορία της κεφαλίδας του πλαισίου ως χρήση για τα EXP bits, μπορεί να είναι για παράδειγμα

τα priority bits (P bits) της κεφαλίδας ενός 802.1Q πλαισίου. Σε περίπτωση που τα EXP bits της ετικέτας δε έχουν οριστεί, τα P bits της κεφαλίδας του 802.1Q αντιγράφονται στο πεδίο EXP bits της ετικέτας.

5.6 Επίλογος

Θέμα του κεφαλαίου είναι τα MPLS VPN τα οποία είναι από τις ποιο σημαντικές εφαρμογές του MPLS. Υπάρχουν δυο τύπο MPLS VPN: το Layer 3 MPLS VPN και MPLS-based Layer 2 VPN. Για να επιτευχθεί η υλοποίηση ενός Layer 3 MPLS VPN, χρειάζονται κάποια βασικά στοιχεία στους PE δρομολογητές. Αυτά είναι: VPN Routing and Forwarding Tables (VRFs), διανομή διαδρομών με τη χρήση του BGP, Route Distinguisher (RD), Route Targets (RT), προώθηση επισημασμένων πακέτων. Όλα τα πακέτα προωθούνται με δύο ετικέτες: την IGP ετικέτα στην κορυφή της στοίβας ετικετών και την VPN ετικέτα στη βάση της στοίβας. Το MPLS-based Layer 2 VPN χρησιμοποιεί το MPLS δίκτυο για να προσφέρει υπηρεσίες επιπέδου σύνδεσης στους πελάτες. Η υπηρεσία είναι μια τεχνολογία δευτέρου επιπέδου, όπως Frame Relay, ATM ή Ethernet VLAN. Διαφέρει όμως από τις παραπάνω γιατί μεταφέρεται μέσω ενός MPLS δικτύου. Οι βασικές εντολές ρύθμισης του MPLS VPN παρουσιάζονται στο **Παράρτημα 4**.

Παρόλο που με το MPLS-based Layer 2 VPN μεταφέρονται πλαίσια δευτέρου επιπέδου δεν μπορεί κανείς να υποστηρίξει ότι οι δύο απομακρυσμένες περιοχές που επικοινωνούν συμπεριφέρονται σαν τοπικό δίκτυο Ethernet, και αυτό γιατί η μετάδοση είναι point-to-point. Για multipoint μετάδοση προσφέρεται το VPLS, το οποία αναλύεται στο επόμενο κεφάλαιο.

6

Virtual Private LAN Service (VPLS)

6.1 Εισαγωγή

Ένα VPLS δίκτυο είναι ένα multipoint VPN δευτέρου επιπέδου, το οποίο εξομοιώνει υπηρεσίες τοπικών δικτύων (LAN) πάνω από ένα WAN δίκτυο. Το VPLS επιτρέπει στους παροχείς υπηρεσιών να διασυνδέσουν τοπικές περιοχές των πελατών τους πάνω από ένα δίκτυο PSN (Packet Switched Network), κάνοντας τους έτσι να αλληλεπιδρούν σαν να είναι μέρος του ίδιου τοπικού δικτύου. Με το VPLS δεν πραγματοποιείται καμία λειτουργία δρομολόγησης μεταξύ των πελατών και του παρόχου υπηρεσιών και επιπλέον ο πελάτης μπορεί να τρέχει οποιοδήποτε πρωτόκολλο δικτύου.

Το IETF έχει δημιουργήσει δυο ξεχωριστές ομάδες εργασίας για το VPLS, οι οποίες καταγράφονται στα RFC 4761 (Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling) και RFC 4762 (Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling). Και τα δυο RFC δεν παρουσιάζουν διαφορές όσον αφορά στη λειτουργία της προώθησης, αντίθετα είναι διαφορετικά ως προς τη λειτουργία του ελέγχου. Στην πρώτη περίπτωση χρησιμοποιείται το BGP σαν πρωτόκολλο σηματοδοσίας, ενώ στη δεύτερη το LDP.

6.2 Αρχιτεκτονική του VPLS

Το VPLS εξομοιώνει ένα τοπικό δίκτυο LAN ή θα μπορούσε να πει κάνεις ότι είναι ένα εικονικό Ethernet Switch. Ένα Ethernet Switch εκτελεί τις παρακάτω λειτουργίες:

- Προώθηση πλαισίων Ethernet
- Προώθηση unicast πλαισίων με άγνωστη διεύθυνση MAC

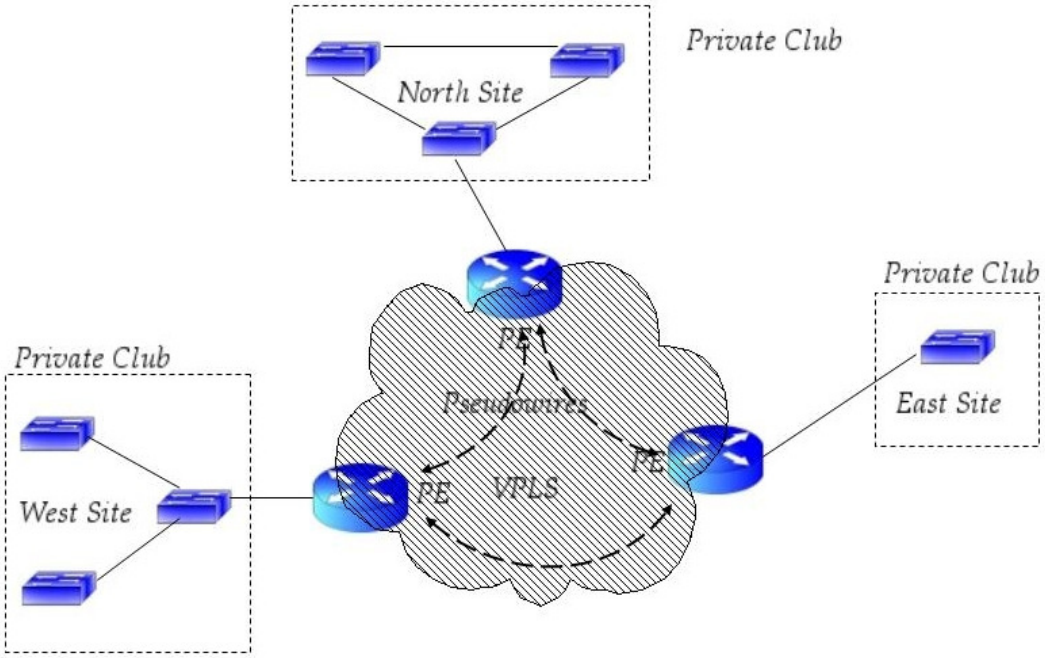
- Διανομή multicast και broadcast πλαισίων σε περισσότερες από μια διασυνδέσεις
- Πρόβλεψη βρόχων (Loop Prevention)
- Δυναμική εκμάθηση MAC διευθύνσεων

Η υπηρεσία VPLS πρέπει επίσης να έχει τα παραπάνω χαρακτηριστικά. Τα πλαίσια Ethernet λαμβάνουν δύο MPLS ετικέτες πριν γίνει η προώθηση τους μέσω του MPLS δικτύου κορμού. Η προώθηση των πλαισίων είναι ίδια με αυτή στην περίπτωση του AToM. Μια ετικέτα PW χρησιμοποιείται στην βάση της στοίβας ετικετών για τον διαχωρισμό του Pseudowire που ανήκει το κάθε πλαίσιο. Η ετικέτα του Tunnel στην κορυφή της στοίβας προσδιορίζει την προώθηση του επισημασμένου πακέτου από τον ingress PE στον egress PE.

Σε περίπτωση που ο PE δρομολογητής λάβει ένα πλαίσιο του οποίου η MAC διεύθυνση είναι άγνωστη, το πλαίσιο προωθείται σε όλες τις διασυνδέσεις που ανήκουν στο ίδιο LAN. Για ένα Ethernet Switch ένα σύνολο από διασυνδέσεις που ανήκουν στο ίδιο VLAN, αποτελούν ένα LAN. Όταν ρυθμίζεται το VPLS, πρέπει να καθοριστεί για κάθε διασύνδεση ή για κάθε VLAN σε ποιο VPLS στιγμιότυπο ανήκουν. Κατά συνέπεια, τα πλαίσια με άγνωστη διεύθυνση MAC προωθούνται στις διασυνδέσεις που ανήκουν στο ίδιο VPLS στιγμιότυπο. Σε ένα πραγματικό Ethernet Switch μια διασύνδεση είναι μια πραγματική φυσική διασύνδεση, αντίθετα στο VPLS μπορεί να είναι μια φυσική διασύνδεση ή ένα Pseudowire προς κάποιον PE δρομολογητή. Στο σενάριο της εικόνας 6.1 οι PE δρομολογητές συμμετέχουν σε ένα VPLS στιγμιότυπο το οποίο ονομάζεται Private Club. Ο πελάτης έχει τρεις περιοχές τοπικών δικτύων οι οποίες συνδέονται στους PE δρομολογητές. Οι PE δρομολογητές έχουν εγκαταστήσει Pseudowires για την μεταφορά των πλαισίων. Κάθε Pseudowire αποτελείται από δυο LSP, ένα προς κάθε κατεύθυνση.

Αν κάποια περιοχή του Private Club στείλει ένα broadcast πλαίσιο στον PE δρομολογητή, το πλαίσιο προωθείται από κάθε διασύνδεση του PE δρομολογητή η οποία ανήκει στο συγκεκριμένο VPLS στιγμιότυπο και επίσης από όλα τα Pseudowires που ανήκουν σε αυτό το στιγμιότυπο. Τα multicast πλαίσια προωθούνται σε όλες τις φυσικές διασυνδέσεις που είναι μέρος της ομάδας του multicast και στα αντίστοιχα Pseudowires. Κατά την προώθηση broadcast πλαισίων είναι σημαντικό να μεταδοθούν τα πλαίσια στην broadcast περιοχή. Αν οι PE δρομολογητές δεν είναι πλήρως κομβικά συνδεδεμένοι, όσον αφορά σε κάποιο VPLS στιγμιότυπο, τότε απαιτείται Spanning Tree πρωτόκολλο ώστε να αποφευχθούν οι βρόγχοι. Η πιο απλή λύση όμως είναι οι PE Routers να είναι πλήρως κομβικά συνδεδεμένοι, όπως στο σενάριο της εικόνας 6.1, και να λειτουργεί η τεχνική Split Horizon για την προώθηση επιπέδου σύνδεσης. Σε αυτήν

την περίπτωση σημαίνει ότι ένα πλαίσιο το οποία λήφθηκε από ένα Pseudowire, δεν προωθείται σε άλλα Pseudowires του ίδιου VPLS στιγμιοτύπου.



Εικόνα 6.1. Εφαρμογή VPLS σε ένα απλό MPLS δίκτυο

6.3 Η Προώθηση στο VPLS

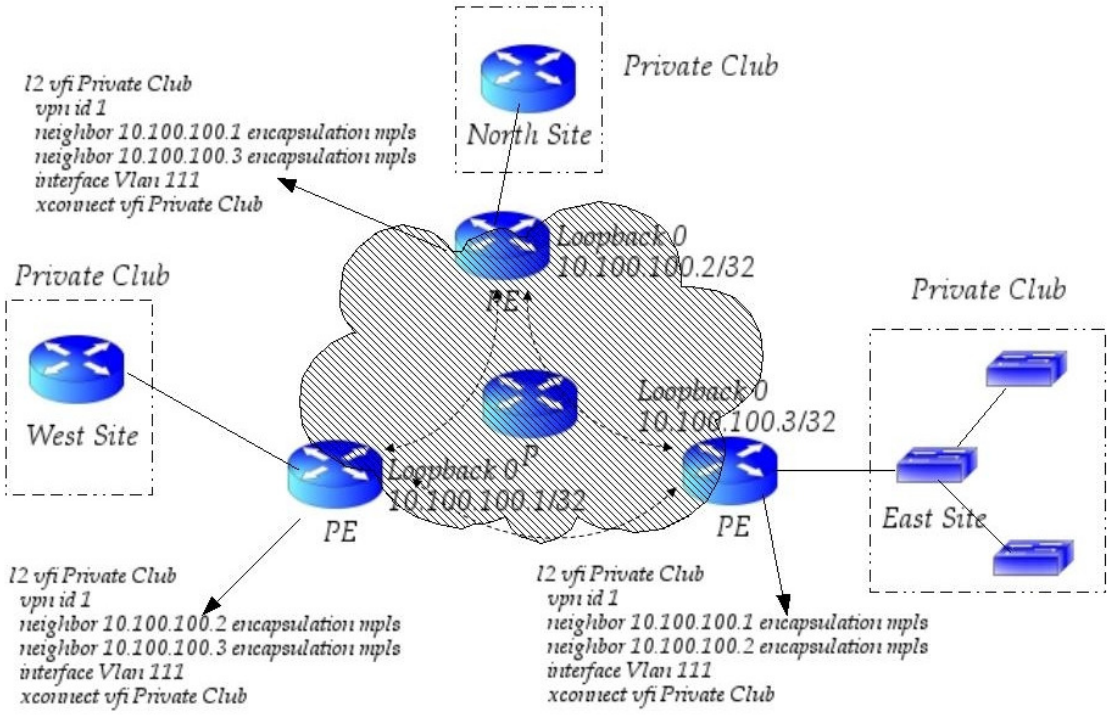
Όσον αφορά στην μεταφορά των πλαισίων σε ένα VPLS δίκτυο, είναι ίδια με αυτήν της μεταφοράς Ethernet πλαισίων μέσω ενός AToM δικτύου. Η διαφορά του VPLS είναι ότι δεν είναι point to point, όπως το AToM. Δυο ετικέτες προστίθενται σε κάθε Ethernet πλαίσιο. Η ετικέτα στην κορυφή της στοίβας καθορίζει το LSP που θα ακολουθήσει το πακέτο, ενώ η ετικέτα στη βάση της στοίβας (PW ετικέτα) καθορίζει το Pseudowire. Με άλλα λόγια, ο egress PE ελέγχει την PW ετικέτα για να αποφασίσει σε ποιο AC (Attachment Circuit/Ethernet Port ή VLAN) πρέπει να προωθήσει το πλαίσιο.

Κάθε PE δρομολογητής συνθέτει έναν MAC πίνακα, όπως ένα κανονικό Ethernet Switch. Ο πίνακας αυτός χρησιμοποιείται για την προώθηση από και προς της φυσικές Ethernet διασυνδέσεις και από και προς τα Pseudowires. Σε αρχιτεκτονικές δρομολογητών της Cisco Systems, κάθε πελάτης που συνδέεται σε ένα MPLS δίκτυο έχει ένα VFI (Virtual Forwarding Instance). Ένα VFI είναι μια συλλογή δεδομένων που χρησιμοποιούνται για την προώθηση των πλαισίων στο

Ethernet AC και στα Pseudowires. Τα δεδομένα του VFI παρέχονται από τις διαδικασίες ελέγχου και τις διαδικασίες προώθησης. Τα δεδομένα των διαδικασιών ελέγχου είναι οι ρυθμίσεις του PE Router και το πρωτόκολλο LDP (ή BGP) που σηματοδοτεί το Pseudowire, τα οποία παρέχουν στο VFI πληροφορίες ετικέτας και συμμετοχής σε ένα Pseudowire. Τα δεδομένα από την διαδικασία προώθησης προέρχονται από την προώθηση του πλαισίου και παρέχουν στο VFI πληροφορίες όπως οι διευθύνσεις MAC.

6.4 VPLS Control Plane

Όπως προαναφέρθηκε, για τη σωστή λειτουργία του VPLS απαιτείται οι PE δρομολογητές να είναι πλήρως κομβικά συνδεδεμένοι με Pseudowires, για κάποιο VPLS στιγμιότυπο. Όταν ρυθμίζεται κάποιο VPLS στιγμιότυπο σε κάποιον PE Router, πρέπει επίσης να καθοριστούν και οι γειτονικές σχέσεις αυτού στον PE. Αυτό σημαίνει ότι πρέπει να καθοριστούν όλοι οι γειτονικοί PE του συγκεκριμένου PE δρομολογητή για ένα συγκεκριμένο πάντα VPLS στιγμιότυπο. Με λίγα λόγια πρέπει να εγκατασταθούν targeted LDP συνεδρίες μεταξύ όλων των πιθανών ζευγαριών PE δρομολογητών που ανήκουν σε ένα VPLS στιγμιότυπο. Μια targeted LDP συνεδρία σηματοδοτεί το Pseudowire μεταξύ δυο PE δρομολογητών και διαφημίζει την PW ετικέτα.



Εικόνα 6.2. Ρυθμίσεις των δρομολογητών ενός VPLS δικτύου

Σε περίπτωση που ένα VPLS στιγμιότυπο σχετίζεται με μια VLAN διασύνδεση, τότε το τοπικό VC ID συσχετίζεται με το VPLS στιγμιότυπο. Το VC ID είναι το VPN Identifier και η συσχέτιση με το VPLS στιγμιότυπο γίνεται μέσω ρυθμίσεων. Κάθε Pseudowire για ένα τέτοιο VPLS στιγμιότυπο έχει ένα VC ID. Παρόλα αυτά η ετικέτα PW είναι διαφορετική για κάθε Pseudowire του ίδιου στιγμιότυπου. Στην εικόνα 6.2 παρουσιάζεται ένα VPLS σενάριο και οι ρυθμίσεις σε κάθε PE δρομολογητή. Το VLAN 111 συσχετίζεται με το VPLS στιγμιότυπο Private Club.

6.5 Ποιότητα Υπηρεσίας στο VPLS

Παρόμοια με το AToM είναι και η χρήση του QoS στο VPLS. Εξ΄ ορισμού τα P bits του 802.1Q αντιγράφονται στα EXP bits της ετικέτας του MPLS. Αν κανείς θέλει να αλλάξει την προτεραιότητα των πακέτων, μπορεί να κάνει χρήση του MQC.

6.6 Επίλογος

Το παρόν κεφάλαιο αναφέρεται στο VPLS, το οποίο είναι μια τεχνική που μπορεί να εξομοιώσει υπηρεσίες τοπικών δικτύων μέσω ενός WAN δικτύου. Εξηγήθηκε η αρχιτεκτονική του VPLS και ο τρόπος λειτουργίας του με την χρήση των pseudowires. Οι βασικές εντολές ρύθμισης του VPLS παρουσιάζονται στο **Παράρτημα 5**.

Συμπεράσματα

Διανύοντας την πρώτη δεκαετία του 2000 το MPLS έγινε αρκετά δημοφιλές και όλο και περισσότεροι πάροχοι υπηρεσιών το εφαρμόζουν στα δίκτυα τους. Ελληνικοί πάροχοι δικτυακών και τηλεπικοινωνιακών υπηρεσιών, όπως η OTENET, η Forthnet και η Hellas on Line έχουν ήδη ενσωματώσει το MPLS στα δίκτυα τους. Η υπηρεσία που προσφέρεται από τους παραπάνω παρόχους είναι το MPLS VPN. Η πρόσβαση των πελατών στο MPLS δίκτυο υλοποιείται μέσω μισθωμένων κυκλωμάτων αλλά και μέσω PSTN, ISDN ή ADSL ανάλογα με τις ανάγκες επικοινωνίας του κάθε σημείου παρουσίας του πελάτη. Επίσης οι πάροχοι υπηρεσιών έχουν ενσωματώσει και ποιότητα υπηρεσίας (QoS) στο MPLS δίκτυο τους. Χαρακτηριστικό παράδειγμα αποτελεί η Forthnet, η οποία προσφέρει τις παρακάτω τέσσερις τάξεις υπηρεσίας (CoS) :

- CoS Gold – Εγγυάται την ποιότητα του σήματος, την παράδοση των πακέτων και τον χρόνο παράδοσης των πακέτων. Ενδείκνυται για εφαρμογές όπως: τηλεφωνία και video conference.
- CoS Silver – Εγγυάται την παράδοση των πακέτων και τον χρόνο παράδοσης τους. Ενδείκνυται για εφαρμογές όπως: Oracle και SAP ERP.
- CoS Bronze – Ενδείκνυται για εφαρμογές όπως HTTP, FTP και email. Η τάξη υπηρεσίας Bronze μεταδίδει τα δεδομένα με τη βέλτιστη προσπάθεια (Best-Effort μετάδοση δεδομένων).

Ένα από τα σημαντικότερα πλεονεκτήματα του MPLS είναι ότι παρέχει στους διαχειριστές δικτύου ένα πλήθος εργαλείων Traffic Engineering. Επίσης προσφέρει και εγγυάται για την ποιότητα υπηρεσίας των δεδομένων, όπως οι τεχνολογίες σύνδεσης ATM και Frame Relay, χωρίς όμως να απαιτεί αφιερωμένες συνδέσεις.

Η τεχνολογία MPLS έχει δημιουργηθεί ειδικά για να προσδώσει μεγάλες δυνατότητες επεκτασιμότητας στην κατασκευή VPNs με συνέπεια να δίνει τη δυνατότητα δημιουργίας VPNs που αποτελούνται από αρκετές εκατοντάδες

σημεία με μειωμένο διαχειριστικό κόστος. Το MPLS VPN είναι μια από τις ποιο δημοφιλείς εφαρμογές του MPLS.

Επιπλέον μελλοντική μελέτη του πρωτοκόλλου MPLS θα μπορούσε να χωριστεί σε δύο σκέλη:

- Πρακτική εφαρμογή του MPLS σε ένα περιβάλλον που μπορεί να υποστηρίξει κάποιες από τις εφαρμογές του
- Μελέτη του GMPLS (Generalized MPLS)[1]

[1] Το GMPLS βασίζεται στο MPLS TE. Η διαφορά του με το MPLS TE είναι ότι έχει επεκταθεί ώστε να υποστηρίζει συστήματα όπως: Wavelength-Division Multiplexing Systems (DWDM), Photonic Cross-Connects (PXC), Optical Cross-Connects (OXC). Τα συστήματα που απαιτούνται για την λειτουργία του GMPLS, δεν είναι απλοί δρομολογητές ή ATM μεταγωγείς που τρέχουν MPLS. Τα συστήματα αυτά εκτελούν το GMPLS στο Control Plane. Δεν μεταγάγουν επισημασμένα πακέτα αλλά μήκη κύματος.

Βιβλιογραφία

[1] Καλογεράς, Δ., Ματσάκης, Δ., Παπαγεωργίου, Σ., Πολυράκης, Α. (2007). *Διάρθρωση MPLS. «Παροχή υπηρεσιών ανάπτυξης και διαχείρησης εικονικού κέντρου δικτύων του ακαδημαϊκού και ερευνητικού ΕΔΕΤ (V-NOC3)»*

[2] Almquist, P. (1992). IETF RFC 1349. *Type of Service in the Internet Protocol Suite.*

[3] *Asynchronous transfer mode*. In Broadband Forum. http://www.broadband-forum.org/

[4] Avici Systems Inc (2000). *Traffic Engineering with MPLS.* North Billerica: Avici Systems Inc.

[5] Awduche, D., Malcolm, J., McManus, J., O'Dell, M., McManus, J., UUNET (MCI Worldcom). (1999). IETF RFC 2702. *Requirements for Traffic Engineering Over MPLS.*

[6] Bramer B. (1997). School of Computing and Mathematical Sciences, De Montfort University, Leicester. *The HDLC Family of Protocols.* From http://www.cse.dmu.ac.uk/~cfi/Networks/DataLink/DataLink12.htm

[7] Brown, C., Consultant, Malis, A., Ascend Communications, Inc. (1998). IETF RFC 2427. *Multiprotocol Interconnect over Frame Relay*.

[8] Callon, R. (1990). IETF RFC 1195. *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments.*

[9] Chandra, R., Traina, P., Cisco Systems, Inc., Li, T. (1996). IETF RFC 1997. *BGP Communities Attribute.*

[10] *Constrained Shortest Path First*. (2009, July 20). In *Wikipedia, The Free Encyclopedia*. Retrieved 12:30, December 3, 2009, from http://en.wikipedia.org/w/index.php?title=Constrained_Shortest_Path_First&oldid=303045656.

[11] Davie, B. S., Farrel, A. (2008). *MPLS Next Steps.* Burlington: Elsevier Inc.

[12] *Enhanced Interior Gateway Routing Protocol*. (2009, December 2). In *Wikipedia, The Free Encyclopedia*. Retrieved 12:32, December 3, 2009, from http://en.wikipedia.org/w/index.php?title=Enhanced_Interior_Gateway_Routing_Protocol&oldid=329294340

[13] *Ethernet*. In IEEE 802.3 Ethernet Working Group. From http://www.ieee802.org/3/

[14] Farinacci, D., Li, T., Procket Networks, Hanks, S., Enron Communications, Meyer, D., Cisco Systems, Inc., Traina, P., Juniper Networks. (2000). IETF RFC 2784. *Generic Routing Encapsulation (GRE).*

[15] Ghein, L. D. (2006). *MPLS Fundamentals.* Street Indianapolis: Cisco Press.

[16] Information Sciences Institute, University of Southhern California. (1981). IETF RFC 793. *Transmission Control Protocol*.

[17] Lobo, L., Lakshman, U. (2005). *MPLS Configuration on Cisco IOS Software.* Indianapolis: Cisco Press.

[18] Mannie, E. (2004). IETF RFC 3945. *Generalized Multi-Protocol Label Switching (GMPLS) Architecture.*

[19] McGill, N., Pignataro, C., Cisco Systems, Inc. (2009). IETF RFC 5641. *Layer 2 Tunneling Protocol Version 3 (L2TPv3) Extended Circuit Status Values.*

[20] Minei, I., Lucek, J. (2005). *MPLS Enabled Applications.* England: John Wiley & Sons Ltd.

[21] Moy, J., Ascend Communications, Inc. (1998). IETF RFC 2328. *OSPF Version 2 .*

[22] *Multiprotocol Label Switching*. (2009, November 30). In *Wikipedia, The Free Encyclopedia*. Retrieved 12:37, December 3, 2009, from http://en.wikipedia.org/w/index.php?title=Multiprotocol_Label_Switching&oldid=328858499

[23] Networks, J. I. (2007). *Virtual Private LAN Service (VPLS).* California: Juniper Networks Inc.

[24] Osborne, E., Simha, A. (2002). *Traffic Engineering with MPLS.* Indianapolis: Cisco Press.

[25] Postel, J., ISI. (1981). IETF RFC 792. *Internet Control Message Protocol.*

[26] Rekhter, Y., Li, T., Hares, S. (2006). IETF RFC 4271. *A Border Gateway Protocol 4 (BGP-4) .*

[27] Rosen, E., Callon, R., Cisco Systems, Inc., Viswanathan, A., Force10 Networks, Inc., Callon, R., Juniper Networks, Inc. (2001). IETF RFC 3031. *Multiprotocol Label Switching Architecture* .

[28] Rosen, E., Cisco Systems, Inc, Rekther, Y. (2006). IETF RFC 4364. *BGP/MPLS IP Virtual Private Networks (VPNs).*

[29] Rosen, E., Tappan, D., Fedorkow, G., Cisco Systems, Inc., Rekhter, Y., Juniper Networks, Farinacci, D., Li, T., Procket Networks, Inc., Conta, A., Transwitch Corporation. (2001). IETF RFC 3032. *MPLS Label Stack Encoding* .

[30] Rosen, E., Rekther, Y., Cisco Systems, Inc. (1999). IETF RFC 2547. *BGP/MPLS VPN.*

[31] Sangli, S., Tappan, D., Cisco Systems, Rekhter, Y., Juniper Networks. (2006). IETF RFC 4360. *BGP Extended Communities Attribute.*

[32] Shah, S., Yip, M., Extreme Networks. (2003). IETF RFC 3619. *Extreme Networks' Ethernet Automatic Protection Switching (EAPS) Version 1.*

[33] Sharma, V., Metanoia, Inc., Hellstrand, F., Nortel Networks. (2003). IETF RFC 3469. *Framework for Multi-Protocol Label Switching (MPLS)-based Recovery* .

[34] Simpson, W., DayDreamer. (1994). IETF RFC 1661. *The Point-to-Point Protocol (PPP).*

[35] Postel, J., Information Sciences Institute. (1980). IETF RFC 768. *User Datagram Protocol*.

Παράρτημα 1

A. Βασικές Ρυθμίσεις IGP

Εντολή	Περιγραφή
OSPF	
R(config)#**router ospf** process id	Βασικές εντολές για την ενεργοποίηση του OSPF σε ένα δίκτυο.
R(config-router)#**network** ip-address wildcard mask **area** area-id	
IS-IS	
R(config)#**router isis** area-tag	Βασικές εντολές για την ενεργοποίηση του IS-IS σε ένα δίκτυο.
R(config-router)#**net** network-entity-title	
R(config)#**interface** interface-type number	
R(config-if)#**ip router isis** area-tag	

B. Βασικές Ρυθμίσεις MPLS

Εντολή	Περιγραφή
R(config)#**ip cef**	Πριν την ενεργοποίηση του MPLS στις διασυνδέσεις πρέπει να ενεργοποιηθεί η τεχνική CEF. Η CEF (Cisco Express Forwarding) είναι σημαντική για την μεταγωγή ετικετών και υπεύθυνη για την πρόσθεση και αφαίρεση ετικετών σε ένα MPLS δίκτυο. Ρυθμίζεται στους δρομολογητές σε global κατάσταση.
R(config-if)#**ip** route-cache cef	Εκτελείται σε interface κατάσταση και ενεργοποιεί την τεχνική CEF ανά διασύνδεση, σε περίπτωση που μετά την εκτέλεση της εντολής **ip cef** δεν έχει ενεργοποιηθεί η CEF σε κάποια διασύνδεση.
R(config)#**mpls ip** R(config-if)#**mpls ip**	Εκτελείται σε global ή interface κατάσταση για την ενεργοποίηση της MPLS μεταγωγής σε όλες ή συγκεκριμένες διασυνδέσεις αντίστοιχα. Στην ουσία η εντολή mpls ip ενεργοποιεί το πρωτόκολλο LDP σε όλες ή συγκεκριμένες διασυνδέσεις αντίστοιχα

Εντολή	Περιγραφή
R(config)#**no mpls ip propagate-ttl [forwarded| local]**	Κατά την εκτέλεση αυτής της εντολής, το TTL του IP πακέτου δεν αντιγράφεται στο TTL της ετικέτας. Το TTL της ετικέτας γίνεται 255. Με αυτόν τον τρόπο δεν διακρίνεται η εσωτερική δομή ενός mpls δικτύου (π.χ η εκτέλεση της εντολής traceroute θα φανερώσει μόνο τον ingress LSR). Η παράμετρος **forwarded** απαγορεύει την αντιγραφή του TTL μόνο στα μηνύματα που έρχονται στον ingress LSR και προωθούνται στο MPLS δίκτυο, ενώ επιτρέπει την αντιγραφή στα μηνύματα που παράγονται στον ingress LSR. Η παράμετρος **local** απαγορεύει την αντιγραφή του TTL μόνο στα μηνύματα που δημιουργούνται στον ingress LSR
R(config)#**mpls label range** min-label-value max-label-value	Καθορίζει το εύρος τιμών που μπορεί να χρησιμοποιηθεί από έναν LSR. Το εύρος μπορεί να είναι από 16 έως 1,048,575. Η χρήση της εντολής **no mpls label range** θέτει τις εξ' ορισμού τιμές
R(config)#**mpls ip ttl-expiration pop** labels(1-6)	Καθορίζει τον τρόπο προώθησης ενός πακέτου με συγκεκριμένο αριθμό ετικετών (1-6). Έτσι σε περίπτωση που λήξει το TTL, το ICMP μήνυμα αντί να ακολουθήσει το LSP και να σταλεί πίσω από τον egress LSR, αφαιρείται η ετικέτα και αποστέλλεται κατευθείαν πίσω. Απαραίτητη προϋπόθεση, ο LSR στον οποίο θα ρυθμιστεί η εντολή να έχει την διαδρομή του αποστολέα στον πίνακα δρομολόγησης του
R(config-if)#**mpls mtu** bytes	Καθορίζει το μέγεθος του πακέτου που μπορεί να περάσει από μια σύνδεση χωρίς κατάτμηση
R#**debug mpls packets**	Δημιουργεί μια έξοδο με πληροφορίες αποσφαλμάτωσης για κάθε πακέτο που επεξεργάζεται. Επειδή μπορεί να μην είναι επιθυμητό να γίνεται αυτό για κάθε πακέτο, μπορεί κανείς να δημιουργήσει μια access-list και να εφαρμόσει την αποσφαλμάτωση σε αυτήν. Παρακάτω φαίνεται η έξοδος της εντολής Router#**debug mpls packets 2700** Packet debugging is on with ACL 2700 Router# 1d02h: MPLS turbo: Et3/1: rx: Len 122 Stack {16 0 253} – ipv4 data 1d02h: MPLS turbo: Se4/0: tx: Len 108 Stack {24 0 252} – ipv4
R#**show mpls interfaces [detail]**	Επαληθεύει την ενεργοποίηση του MPLS στις διασυνδέσεις ενός δρομολογητή. Με την παράμετρο detail εμφανίζονται επιπλέον πληροφορίες, όπως το MPLS MTU. Παρακάτω φαίνεται η έξοδος της εντολής

Εντολή	Περιγραφή
	Router#**show mpls interfaces** Interface IP Tunnel Operational Ethernet0/1/2 Yes (ldp) Yes Yes Ethernet0/1/3 Yes (ldp) Yes Yes Ethernet0/1/4 Yes (ldp) No Yes POS5/0/0 Yes (ldp) Yes Yes
R#**show mpls forwarding-table**	Εμφανίζει τις πληροφορίες του πίνακα LFIB
R#**show mpls ip binding**	Εμφανίζει τις πληροφορίες του πίνακα LIB, δηλαδή όλες τις ετικέτες που είναι πιθανόν να χρησιμοποιηθούν για κάποιο συγκεκριμένο πρόθεμα. Μια από αυτές επιλέγεται και εγκαθίσταται στον πίνακα LFIB. Παρακάτω φαίνεται η έξοδος της εντολής Router#**show mpls ip bindings** lib entry: 10.200.210.0/24, rev 4 local binding: label: imp-null remote binding: lsr: 10.200.254.5:0, label: 16 remote binding: lsr: 10.200.254.1:0, label: imp-null remote binding: lsr: 10.200.254.3:0, label: 19 lib entry: 10.200.211.0/24, rev 12 local binding: label: imp-null remote binding: lsr: 10.200.254.5:0, label: 18 remote binding: lsr: 10.200.254.1:0, label: 32 remote binding: lsr: 10.200.254.3:0, label: imp-null lib entry: 10.200.254.1/24, rev 31 local binding: label: 24 remote binding: lsr: 10.200.254.5:0, label: 22 remote binding: lsr: 10.200.254.1:0, label: imp-null inuse remote binding: lsr: 10.200.254.3:0, label: 26

Παράρτημα 2

A. Ρυθμίσεις LDP

Εντολή	Περιγραφή
R(config)#**mpls ldp router-id** {interface | ip-address} **[force]**	Καθορίζει το LDP Router ID που χρησιμοποιείται για τις LDP συνεδρία. Σε περίπτωση που δεν καθοριστεί με αυτήν την εντολή, τότε το LDP Router ID είναι η μεγαλύτερη διεύθυνση από τις διασυνδέσεις. Με την παράμετρο **force** το ID αλλάζει κατευθείαν.
R(config-if)#**mpls ldp discovery transport-address {interface**|ip-address**}**	Καθορίζει το LDP Router ID που χρησιμοποιείται για μια LDP συνεδρία. Ρυθμίζεται ανά διασύνδεση
R(config)#**mpls ldp discovery {hello {holdtime**|**interval}}** seconds	Χρησιμοποιείται για την αλλαγή της περιόδου αποστολής Hello μηνυμάτων (Hello Interval) ή του χρόνου λήξης Hello (Hello Hold Time)
R(config)#**mpls ldp holdtime** seconds	Χρησιμοποιείται για την αλλαγή του keepalive timer μιας LDP συνεδρίας. Η τιμή του κυμαίνεται από 15 έως 2.147.283 δευτερόλεπτα. Η εξ' ορισμού τιμή είναι 180 δευτερόλεπτα.
R(config)#**mpls ldp backoff** initial-backoff maximum-backoff	Σε περίπτωση που δύο LDP Peers δεν συμφωνούν σε παραμέτρους για την εγκατάσταση συνεδρίας, συνεχίζουν τις προσπάθειες για την εγκατάσταση αλλά με μειωμένο ρυθμό. Με την εντολή **mpls ldp backoff** ρυθμίζεται ο αρχικός χρόνος (5 έως 2.147.283) με εξ' ορισμού 15 δευτερόλεπτα και ο μειωμένος (5 έως 2.147.283) με εξ' ορισμού 120 δευτερόλεπτα
R(config)#**mpls ldp neighbor [vrf** vpn-name**]** ip-addr targeted	Εγκαθιστά μια LDP συνεδρία μεταξύ δύο LSR, οι οποίοι δεν είναι άμεσα συνδεδεμένοι
R(config)#**mpls ldp discovery targeted-hello {holdtime**|**interval}** seconds | **{accept [from** acl**]}**	Καθορίζει τους χρόνους Hello Holdtime και Hello Interval. Παράλληλα μπορεί να χρησιμοποιηθεί με μια access-list, ώστε ο LSR να λαμβάνει targeted Hello μηνύματα μόνο από συγκεκριμένους LSR
R(config)#**mpls ldp neighbor [vrf** vpn-name**]** ip-addr **password** [0-7] pswd-string	Χρησιμοποιεί MD5 πιστοποίηση για την επικοινωνία μεταξύ δυο LSR. Το ίδιο password πρέπει να οριστεί και στους δυο για να είναι δυνατή η επικοινωνία

Εντολή	Περιγραφή
R(config)#**mpls ldp advertise-labels [vrf** vpn-name**] [interface** interface|**for** prefix-access-list **[to** peer-access-list**]]**	Η χρήση της καθορίζει για ποια προθέματα ο LSR θα αποδώσει ετικέτας. Τα προθέματα αυτά ή οι διευθύνσεις μπορούν να καθοριστούν σε μια standard access-list (prefix-access-list). Επίσης καθορίζει ποίοι LDP Peers πρέπει να λάβουν αυτά τα προθέματα (peer-access-list).
R(config)#**mpls ldp neighbor [vrf** vpn-name**]** nbr-addr **labes accept** acl	Φιλτράρει τις αντιστοιχήσεις ετικετών που λαμβάνονται από κάποιον γειτονικό LSR, ώστε να μην γεμίζει ο πίνακας LIB με άχρηστες αντιστοιχήσεις, και κρατά μόνο αυτές που αντιστοιχούν στα προθέματα διευθύνσεων που καθορίζονται στην access-list.
R(config-router)#**[no] mpls ldp sync**	Ενεργοποιεί/Απενεργοποιεί την τεχνική συγχρονισμού IGP-LDP. Το IGP πρωτόκολλο που υποστηρίζει αυτήν την τεχνική είναι το OSPF
R(config)#**mpls ldp igp sync holddown** msec	Ρυθμίζει ένα χρονικό περιθώριο ώστε αν δεν επιτευχθεί συγχρονισμός, να ξεκινήσει το IGP να διαδίδει τις διαδρομές. Σε αυτήν την περίπτωση οι διαδρομές θα διαδοθούν με το μέγιστο μέτρο
R#**debug mpls ldp sync interface** name	Παρέχει πληροφορίες αποσφαλμάτωσης της διαδικασίας του συγχρονισμού IGP-LDP
R(config)#**mpls ldp session protection [vrf** vpn-name**] [for** acl**] [duration** seconds**]**	Παρέχει προστασία LDP συνεδριών, δημιουργώντας μια targeted LDP συνεδρίας μέσω άλλων LSR (εφόσον αυτό είναι εφικτό). Στην access-list καθορίζονται οι LDP peers που πρέπει να προστατευτούν. Επίσης ρυθμίζεται και η διάρκεια που θα μείνει ενεργή η targeted LDP συνεδρία. Ο εξ' ορισμού χρόνος είναι το άπειρο.
R#**show mpls ldp discovery [detail]**	Εμφανίζει χαρακτηριστικά για τις διασυνδέσεις που μετέχουν σε LDP συνεδρίες, όπως αποστολή/λήψη Hello μηνυμάτων, περίοδος αποστολής Hello μηνυμάτων (Hello Interval), χρόνος λήξης Hello (Hello Hold Time), περίοδος αποστολή μηνυμάτων για την διατήρηση LDP συνεδρίας (Keepalive). Παρακάτω φαίνεται η έξοδος της εντολής Router#**show mpls ldp discovery detail** Local LDP Identifier: 10.200.254.2:0 Discovery Sources: Interfaces: Ethernet0/1/2 (ldp): xmit/recv Enabled: Interface config Hello interval: 5000 ms; Transport IP addr: 10.200.254.2 LDP Id: 10.200.254.5:0 Src IP addr: 10.200.215.2; Transport IP addr: 10.200.254.5 Hold Time: 15 sec; Proposed local/peer: 15/15 sec Reachable via 10.200.254.5/32
R#**show mpls ldp parameters**	Εμφανίζει πληροφορίες της LDP συνεδρίας

Εντολή	Περιγραφή
R#**show mpls ldp neighbor [detail]**	Εμφανίζει πρόσθετες πληροφορίας για έναν LDP Peer. Σημαντική πληροφορία της εξόδου αυτής της εντολής είναι οι Bound Addresses, δηλαδή οι διευθύνσεις των διασυνδέσεων του LDP Peer
R#**show mpls ldp bindings**	Εμφανίζει τις πληροφορίες του πίνακα LIB. Η διαφορά της με την εντολή **show mpls ip binding,** είναι ότι δεν δείχνει την ετικέτα που είναι σε χρήση (inuse)

Παράρτημα 3

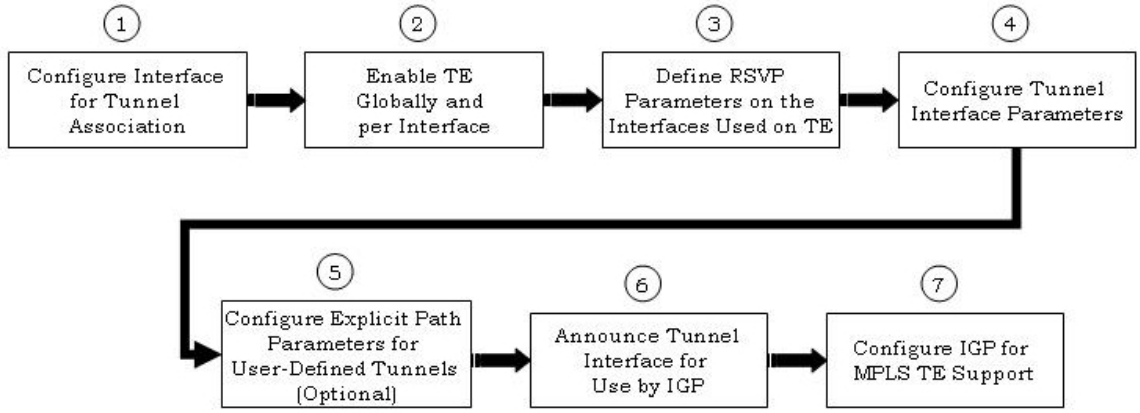
A. Ρυθμίσεις Traffic Engineering

Εντολή	Περιγραφή
R(config)#**mpls traffic-eng tunnels** R(config-if)#**mpls traffic-eng tunnels**	Ρύθμιση του MPLS TE γενικά στις διασυνδέσεις ενός δρομολογητή ή συγκεκριμένα σε κάποια διασύνδεση. Έτσι οι διασυνδέσεις γίνονται υποψήφιες για την δημιουργία ενός TE LSP
R(config-if)#**ip rsvp bandwidth [**reservable bandwidth 1-10000000 kbps] [max reservable bandwidth per flow 1-1000000 kbps]	Καθορίζει το μέγιστο εύρος ζώνης που θα δεσμέυσει το RSVP, για την όλη κίνηση ή για συγκεκριμένη ροή, σε συγκεκριμένη διασύνδεση.
R(config)#**inteface tunnel** number	Μπαίνει στην κατάσταση ρυθμίσεων μιας Tunnel διασύνδεσης
R(config-if)#**ip unnumbered loopback** number	Ρυθμίζεται η IP διεύθυνση της Tunnel διασύνδεσης να σχετίζεται με μια loopback διασύνδεση
R(config-if)#**tunnel mode mpls traffic-eng**	Ρυθμίζεται η κατάσταση της tunnel διασύνδεσης, ώστε να είναι ένα MPLS TE Tunnel
R(config-if)#**tunnel destination** ip-addr of remote loopback	Καθορίζει τον προορισμό (το άλλο άκρο) ενός MPLS TE Tunnel
R(config-if)#**tunnel mpls traffic-eng bandwidth** bandwidth	Καθορίζει το εύρος ζώνης που απαιτείται για την λειτουργία του Tunnel
R(config-if)#**tunnel mpls traffic-eng path-option** priority **dynamic [bandwidth** override bandwidth config value | **attributes** lsp attribute list name | **lockdown]**	Με την εκτέλεση αυτής της εντολής η δημαιουργία του TE LSP θα γίνει δυναμικά, κάνοντας χρήση του IGP και του CSPF αλγόριθμου. Επιπλέον, μπορούν να καθοριστούν προτεραιότητες και χαρακτηριστικά του Tunnel
R(config)#**ip explicit-path name** name **enable** R(config)#**ip explicit-path identifier** number **enable**	Είτε με την πρώτη είτε με την δεύτερη εντολή καθορίζεται μια συγκεκριμένη διαδρομή για ένα TE Tunnel
R(cfg-ip-expl-path)#**next address** ip-address R(cfg-ip-expl-path)#**exit**	Καθορίζονται οι διευθύνσεις για την δημιουργία ενός συγκεκριμένου MPLS TE Tunnel

Εντολή	Περιγραφή
R(config-if)#**tunnel mpls traffic-eng priority** setup priority-value [hold-priority value]	Καθορίζει την προτεραιότητα ενός MPLS TE Tunnel. Η παράμετρος setup priority καθορίζει πόσο σημαντικό είναι ένα Tunnel, ώστε να εγκατασταθεί έναντι κάποιων άλλων. Η παράμετρος hold priority καθορίζει τη σημαντικότητα ενός εγκατεστημένου Tunnel ώστε να διατηρήσει τις δεσμεύσεις που έχει κάνει. Οι τιμές των παραμέτρων κυμαίνονται από 0 έως 7. Χαμηλότερη τιμή σημαίνει και υψηλότερη προτεραιότητα
R(config-if)#**tunnel mpls traffic-eng autoroute announce**	Διαδίδει την διασύνδεση του Tunnel στον πίνακα δρομολόγησης του IGP, το οποίο δεν γίνεται εξ' ορισμού
R(config-router)#**mpls traffic-eng area** number	Ενεργοποιεί το OSPF για Traffic Engineering
R(config-router)#**mpls traffic-eng router-id** interface number	Καθορίζει το Router ID για την λειτουργία TE, στο OSPF ή στο IS-IS
R(config-router)#**mpls traffic-eng level [1|2]**	Καθορίζει τις IS-IS περιοχές Level1/Level2 που θα χρησιμοποιηθούν για την λειτουργία του TE
R(config-router)#**metric-style wide**	Ρυθμίζει το IS-IS ώστε να χρησιμοποιήσει enhanced TLVs
R(config-if)#**tunnel mpls traffic-eng fast-reroute**	Ενεργοποιεί την τεχνική Fast Reroute σε ένα Tunnel. Ρυθμίζεται στον ingress LSR του Tunnel
R(config-if)#**tunnel mpls traffic-eng fast-reroute node-protection**	Ενεργοποιεί την τεχνική Fast Reroute σε ένα Tunnel. Ρυθμίζεται στον ingress LSR του Tunnel. Χρησιμοποιείται σε αντίθεση με την εντολή **tunnel mpls traffic-eng fast-reroute** για την προστασία ενός ολόκληρου κόμβου και όχι μόνο μιας συνδεσης
R(config-if)#**mpls traffic-eng backup-path tunnel** interface number	Καθορίζει τη χρήση ενός εφεδρικού Tunnel σε περίπτωση αποτυχίας μιας διασύνδεσης. Ρυθμίζεται στην προστατευόμενη σύνδεση
R#**debug ip rsvp dump-messages**	Εμφανίζει πληροφορίες RSVP μηνυμάτων, όπως εξερχόμενα Path μηνύματα, εισερχόμενα RESV μηνύματα.
R#**show mpls traffic-eng tunnels tunnel** tunnel-num	Εμφανίζει πληροφορίες για την κατάσταση των TE Tunnel. Παρακάτω φαίνεται η έξοδος της εντολής Router1# **!** **interface Tunnel1** **ip unnumbered Loopback0** **tunnel destination 10.200.254.5** **tunnel mode mpls traffic-eng** **tunnel mpls traffic-eng autoroute announce** **tunnel mpls traffic-eng path-option 1 explicit name Router1-Router2** **tunnel mpls traffic-eng fast-reroute** **!** **ip explicit-path name Router1-Router2 enable** **next-address 10.200.210.2** **next-address 10.200.211.2** **!**

Εντολή	Περιγραφή
	Router1#**show ip explicit-paths name Router1-Router2** Path Router1-Router2 1: next-address 10.200.210.2 2: next-address 10.200.211.2 Router1#**show mpls traffic-eng tunnels tunnel 1** Name: Router1_t1 (Tunnel1) Destination: 10.200.254.5 Status: Admin: up Oper: up Path: valid Signaling: connected path option 1, type explicit Router1-Router2 InLabel: - OutLabel: POS4/0, 17 RSVP Signalling Info: Src 10.200.254.2, Dst 10.200.254.5, Tun_id 1, Tun_Inst 799 RSVP Path Info: My Address: 10.200.254.2 Explicit Route: 10.200.210.2 10.200.211.2 10.200.254.5 Record Route: NONE RSVP Resv Info: Record Route: 10.200.211.1(17) 10.200.211.2(0) Shortest Unconstrained Path Info: Path Weight: 2 (TE) Explicit Route: 10.200.210.2 10.200.211.2 10.200.254.5

Στην παρακάτω εικόνα παρουσιάζονται τα βασικά βήματα για τη δημιουργία ενός TE Tunnel και η σειρά εκτέλεσης των εντολών.



1. Router(config)#**interface loopback** number Router(config-if)#**ip address** ip-address

2.
Router(config)#**mpls traffic-eng tunnels**

Router(config)#**interface** type number
Router(config-if)#**ip address** ip-address mask
Router(config-if)#**mpls traffic-eng tunnels**

3.
Router(config)#**interface** type number
Router(config-if)#**ip rsvp bandwidth** [reservable bandwidth 1-10000000 kbps] [max reservable bandwidth per flow 1-1000000 kbps]

4.
Router(config)#**interface Tunnel** number
Router(config-if)#**ip unnumbered loopback** number
Router(config-if)#**tunnel mode mpls traffic-eng**
Router(config-if)#**tunnel destination** ip-address of remote loopback
Router(config-if)#**tunnel mpls traffic-eng path-option** priority **dynamic** [**bandwidth** override bandwidth config value | **attributes** lsp attribute list name | **lockdown**] | **explicit [identifier** | **name]** name
Router(config-if)#**tunnel mpls traffic-eng bandwidth** kbps
Router(config-if)#**tunnel mpls traffic-eng priority** setup-priority [hold-priority]

5.
Router(config)#**ip explicit-path name** name **enable**
Router(cfg-ip-expl-path)#**next address** ip-address
Router(cfg-ip-expl-path)#**next address** ip-address
Router(cfg-ip-expl-path)#**next address** ip-address
Router(cfg-ip-expl-path)#**next address** ip-address
Router(cfg-ip-expl-path)#**exit**

6.
Router(config)#**interface tunnel** number
Router(config-if)#**tunnel mpls traffic-eng autoroute announce**

7.
OSPF
Router(config)#**router ospf** process-id
Router(config-router)#**network** ip-address wild-card mask **area** area-id
Router(config-router)#**no auto-summary**
Router(config-router)#**mpls traffic-eng area** number
Router(config-router)#**mpls traffic-eng** router-id interface-number

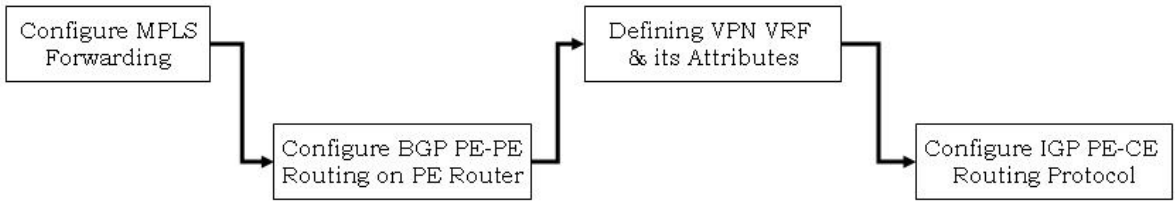
IS-IS
Router(config)#**router isis** process-id
Router(config-router)#**net** network-entity-title
Router(config)#**interface** type number

```
Router(config-if)#ip router isis process-id
Router(config)#router isis process-id
Router(config-router)#mpls traffic-eng level [1|2]
Router(config-router)#mpls traffic-eng router-id interface-number
Router(config-router)#metric-style wide
```

Παράρτημα 4

A. Ρυθμίσεις MPLS VPN Layer 3

Σε γενικές γραμμές τα βήματα που απαιτούνται για την λειτουργία ενός Layer 3 MPLS VPN είναι τα παρακάτω:



Εντολή	Περιγραφή
BGP PE-PE Routing on PE Router	
R(config)#**router bgp** as-number	Ενεργοποίηση του πρωτοκόλλου BGP και καθορισμός ενός αριθμού AS
R(config-router)#**neighbor** ip-address|peer-group-name **remote-as** as-number	Καθορίζει έναν απομακρυσμένο BGP γείτονα, ώστε να εγκατασταθεί μια BGP συνεδρία μεταξύ τους
R(config-router)#**neighbor** ip-address|peer-group-name **update-source** interface-type interface-number	Καθορίζει την διεύθυνση μιας διασύνδεσης, η οποία θα χρησιμοποιείται για την BGP συνεδρία. Συνήθως η διασύνδεση Loopback είναι αυτή που ορίζεται ως πηγή των μηνυμάτων. Η παράμετρος *ip-address* καθορίζει την αντίστοιχη διεύθυνση του γειτονικού BGP δρομολογητή
R(config-router)#**address-family vpnv4 [unicast]**	Εισάγει τον δρομολογητή στη κατάσταση **address-family** από την οποία ρυθμίζονται οι BGP συνεδρίες που πρόκειται να χρησιμοποιήσουν VPN-IPv4 προθέματα
R(config-router-af)#**neighbor** ip-address|peer-group-name **activate**	Έχοντας μπει στην κατάσταση **address-family** για τα VPN-IPv4 προθέματα, η διπλανή εντολή ενεργοποιεί την ανταλλαγή αυτής της πληροφορίας των προθεμάτων μεταξύ των γειτονικών BGP δρομολογητών
R(config-router-af)#**neighbor** ip-address|peer-group-name **next-hop-self**	Ρυθμίζει τον δρομολογητή σαν τον Next-Hop του γειτονικού BGP ή ενός συνόλου BGP δρομολογητών

Εντολή	Περιγραφή
R(config-router)#**address-family ipv4 vrf** vrf-name R(config-router-af)#**redistribute connected** R(config-router-af)#**exit-address-family**	Εισαγωγή στην κατάσταση **address-family** του BGP για τα IPv4 προθέματα των VRF πινάκων. Στην συνέχεια πραγματοποιείται η διάδοση των διαδρομών στο BGP, από το IGP πρωτόκολλο μεταξύ των PE και CE.
R#**show ip bgp**	Εμφανίζει τις πληροφορίες του BGP πίνακα δρομολόγησης. Παρακάτω φαίνεται η έξοδος της εντολής Router#**show ip bgp** Network Next Hop Metric LocPrf Weight Path 100.0.0.0/8 5.198.4.2 0 100 0 100 151.1.0.0/16 5.198.4.2 0 100 0 100 192.1.0.0/16 172.16.72.30 0 100 0 174
R#**show ip bgp neighbors [**neighbor-address] **[received-routes|routes|advertised-routes]**	Η εντολή χωρίς παραμέτρους (**show ip bgp neighbors**) εμφανίζει απλά πληροφορίες για όλες τις γειτονικές BGP συνδέσεις. Με την παράμετρο **received-routes** εμφανίζονται όλες οι διαδρομές οι οποίες έχουν μαθευτεί από κάποιον συγκεκριμένο γείτονα. Η παράμετρος **routes** εμφανίζει όλες τις διαδρομές που εμφανίζει και η παράμετρος **received-routes** εκτός αυτών που έχουν απορριφθεί. Η παράμετρος **advertised-routes** εμφανίζει τις διαδρομές οι οποίες έχουν διαφημιστεί σε έναν γειτονικό BGP. Παρακάτω φαίνεται η έξοδος της εντολής Router#**show ip bgp neighbors** BGP neighbor is 10.10.4.1, remote AS 1, external link BGP version 4, remote router ID 10.200.254.5 BGP State = Established, up for 00:00:37 Last read 00:00:30, hold time is 180, keepalive interval is 60 Neighbor capabilities: Route Refresh: advertised and received Address family IPv4 Unicast: advertised and received ipv4 MPLS Label capability: advertised and received …….
R#**show ip bgp summary**	Εμφανίζει την κατάσταση όλων των BGP συνδέσεων. Παρακάτω φαίνεται η έξοδος της εντολής Router#**show ip bgp summary** Neighbor V AS MsgR MsgS TblVer InQ OutQ Up/Dow State 193.0.16.1 4 1755 4859 1598 717029 0 0 1:27:2 Active 193.0.17.1 4 1755 2154 1698 717029 0 0 2d02 Idle 193.0.18.1 4 1755 1758 2154 717029 0 0 2:13:1 Active

Εντολή	Περιγραφή
R#**show ip bgp vpnv4 all**	Εμφανίζει όλες τις VPN-IPv4 διευθύνσεις του BGP. Παρακάτω φαίνεται η έξοδος της εντολής Router#**show ip bgp vpnv4 all** Network Next Hop Metric LocPrf Weight Path Route Distinguisher: 1:1 (default for vrf A) 100.0.0.0/8 0.0.0.0 0 100 0 32768 ? 151.1.0.0/16 10.10.2.1 0 100 0 65001 i 192.1.0.0/16 0.0.0.0 0 100 0 32768 ? Route Distinguisher: 2:2 (default for vrf B) 10.140.1.1/32 0.0.0.0 0 100 0 32768 ? Route Distinguisher: 9000:1 (default for vrf C) 10.239.9.1/32 10.239.1.1 0 100 0 65400 i
Defining VPN VRF & its Attributes	
R(config)#**ip vrf** vrf-name	Ρυθμίζει έναν εικονικό πίνακα δρομολόγησης/ προώθησης VRF
R(config-vrf)#**rd** route-distinguisher	Ρυθμίζει το Route Distinguisher, το οποίο καθορίζει μοναδικά έναν πίνακα VRF και συντελεί στη δημιουργία των VPN-IPv4 διευθύνσεων
R(config-vrf)#**route-target import|export|both** route-target-ext-community	Δημιουργεί ένα Route Target Extended Community και το προσθέτει στον πίνακα VRF εισάγοντας το, εξάγοντας το ή και τα δυο. Χρησιμοποιείται για την επικοινωνία διαφορετικών VPN
R(config-if)#**ip vrf forwarding** vrf-name	Συσχετίζει μια διασύνδεση με έναν συγκεκριμένο VRF πίνακα
R#**show ip vrf brief|detail|interfaces|id** [vrf-name] [output-modifiers]	Εμφανίζει τους VRF πίνακες ενός δρομολογητή και τις διασυνδέσεις που έχουν συσχετιστεί με αυτούς Παρακάτω φαίνεται η έξοδος της εντολής Router#**show ip vrf detai** vrfA VRF vrfA; default RD 100:1 default VPNID A1:3F6C Interfaces: Ethernet1/3 Connected addresses are in global routing table Export VPN route-target communities RT:100:1 Import VPN route-target communities RT:100:1 No import route-map
PE-CE OSPF Configuration	
R(config)#**router ospf** process-id **vrf** vrf-name	Ενεργοποίηση του OSPF ανά VRF πίνακα για τις περιοχές των πελατών
R(config-router)#**network** ip-address **area** area-id	Ρύθμιση δικτύων τα οποία θα διαφημίζει το OSPF
R(config-router)#**router-id** ip-address	Ως **router-id** ρυθμίζεται συνήθως η Loopback διασύνδεση του δρομολογητή

Εντολή	Περιγραφή
R(config)#**router ospf** process-id **vrf** vrf-name R(config-router)#**redistribute bgp** as-number **subnets [metric** metric-value**] [metric type 1**|**2]**	Με τις διπλανές εντολές διαδίδονται οι διαδρομές του BGP στο OSPF
R(config)#**router bgp** as-number R(config-router)#**address-family ipv4 vrf** vrf-name R(config-router-af)#**redistribute ospf** process-id [**match internal**|**external 1**|**external 2**]	Με τις διπλανές εντολές διαδίδονται οι διαδρομές του OSPF στο BGP

Στον παρακάτω πίνακα φαίνονται οι ρυθμίσεις ενός PE δρομολογητή, ενός P δρομολογητή (ενδιάμεσος LSR) και ενός CE δρομολογητή κάποιου VPN ενός πελάτη.

PE-Left Router

```
hostname PE
!
ip cef
!
ip vrf A
 rd 1:100
 route-target export 1:100
 route-target import 1:100
!
ip vrf B
 rd 1:200
 route-target export 1:200
 route-target import 1:200
!
interface Loopback0
 ip address 10.10.10.101 255.255.255.255
!
interface Loopback101
 description OSPF Router ID for VRF A
 ip vrf forwarding A
 ip address 172.16.101.1 255.255.255.255
!
interface Loopback201
 description OSPF Router ID for VRF B
 ip vrf forwarding B
```

```
 ip address 192.168.201.1 255.255.255.255
!
interface Serial0/0
 description connected to P
 ip address 10.10.10.1 255.255.255.252
 mpls ip
!
interface Serial1/0
 description connected to CE-A
 ip vrf forwarding A
 ip address 172.16.1.1 255.255.255.252
!
interface Serial2/0
 description connected to CE-B
 ip vrf forwarding B
 ip address 192.168.1.1 255.255.255.252
!
router ospf 101 vrf A
 router-id 172.16.101.1
 redistribute bgp 1 subnets
 network 172.16.0.0 0.0.255.255 area 0
!
router ospf 201 vrf B
 router-id 192.168.201.1
 redistribute bgp 1 subnets
 network 192.168.0.0 0.0.255.255 area 1
!
router ospf 1
 router-id 10.10.10.101
 network 10.0.0.0 0.255.255.255 area 0
!
router bgp 1
 no synchronization
 neighbor 10.10.10.102 remote-as 1
 neighbor 10.10.10.102 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
 neighbor 10.10.10.102 activate
 neighbor 10.10.10.102 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf B
 redistribute ospf 201 vrf B match internal external 1 external 2
 no auto-summary
 no synchronization
 exit-address-family
 !
```

```
 address-family ipv4 vrf A
 redistribute ospf 101 vrf A match internal external 1 external 2
 no auto-summary
 no synchronization
 exit-address-family
```

P Router

```
hostname P
!
interface Loopback0
 ip address 10.10.10.200 255.255.255.255
!
interface Serial0/0
 description connected to PE-Left
 ip address 10.10.10.2 255.255.255.252
 mpls ip
!
interface Serial1/0
 description connected to PE-Right
 ip address 10.10.10.6 255.255.255.252
 mpls ip
!
router ospf 1
 log-adjacency-changes
 network 10.0.0.0 0.255.255.255 area 0
```

CE-A

```
hostname CE-A
!
interface Ethernet0/0
 description VPN-A Site 1 network
 ip address 172.16.10.1 255.255.255.0
!
interface Serial1/0
 description connected to PE-Left
 ip address 172.16.1.2 255.255.255.252
!
router ospf 101
 network 172.16.1.0 0.0.0.255 area 0
 network 172.16.10.0 0.0.0.255 area 1
```

Β. Ρυθμίσεις MPLS VPN Layer 2 (AToM)

Εντολή	Περιγραφή
R(config)#[**no] pseudowire-class** [class-name]	Δημιουργεί, καθορίζει το όνομα της τάξης ενός Pseudowire και εισάγει τον χρήστη στον κατάσταση Pseudowire-Class. Σε περίπτωση που απαιτείται η δημιουργία περισσοτέρων του ενός Pseudowire, απαιτείται η χρήση του ονόματος της τάξης (*class-name*). Με την παράμετρο **no** διαγράφεται το Pseudowire.
R(config-pw-class)#**encapsulation mpls**	Καθορίζεται το MPLS ως το πρωτόκολλο ενθυλάκωσης των πλαισίων, για την μεταφορά τους μέσω του Pseudowire Tunnel
R(config-pw-class)#**internetworking ip|ethernet**	Ενεργοποιεί την επιπέδου 2 VPN λειτουργία. Σε περίπτωση που γίνει χρήση της παραμέτρου **ethernet** (Bridged Internetworking Mode), πλαίσια τα όποια δεν είναι Ethernet απορρίπτονται. Αντίστοιχα με την παράμετρο **ip** (Routed Internetworking Mode), πλαίσια τα οποία δεν περιέχουν IP πακέτα απορρίπτονται.
R#**show mpls l2transport vc** [vc-id] **[detail]**	Εμφανίζει πληροφορίες για τα επιπέδου 2 κυκλώματα (VCs), τα οποία έχουν ενεργοποιηθεί στον δρομολογητή για να προωθούν τα πλαίσια στον προορισμό τους. Παρακάτω φαίνεται η έξοδος της εντολής Router#**show mpls l2transport vc 100 detail** Local interface: Fa5/0.100 up, line protocol up, Eth VLAN 100 up Destination address: 10.10.10.101, VC ID: 100, VC status: up Output interface: Gi6/0, imposed label stack {16 16} Preferred path: not configured Default path: active Tunnel label: 16, next hop 10.10.10.6 Create time: 00:13:42, last status change time: 00:10:32 Signaling protocol: LDP, peer 10.10.10.101:0 up MPLS VC labels: local 20, remote 16 Group ID: local 0, remote 0 MTU: local 1500, remote 1500 Remote interface description: Sequencing: receive disabled, send disabled VC statistics: packet totals: receive 20, send 10 byte totals: receive 4802, send 1382 packet drops: receive 0, send 0
EoMPLS – Router Based Port Mode	
R(config)#interface fast|gigabit|ethernet number	Εισαγωγή στην κατάσταση μιας Ethernet διασύνδεσης
R(config-if)#xconnect remote-peer-id-address vc-id encapsulation mpls	Ενεργοποιεί την δρομολόγηση AToM πακέτων μέσω ενός συγκεκριμένου VC και με MPLS ενθυλάκωση
EoMPLS – Router Based VLAN Mode	
R(config)#**interface** interface-type.sub-interface	Δημιουργία μιας υποδιασύνδεσης και εισαγωγή στον κατάσταση υποδιασύνδεσης

Εντολή	Περιγραφή
R(config-subif)#**encapsulation dot1Q** VLAN ID	Ενεργοποίηση 802.1Q ενθυλάκωσης σε μια υποδιασύνδεση
R(config-subif)#**xconnect** remote-peer-id-address vc-id **encapsulation mpls**	Ενεργοποιεί την δρομολόγηση AToM πακέτων μέσω ενός συγκεκριμένου VC και με MPLS ενθυλάκωση
EoMPLS – Switch Based	
R(config)#**interface vlan** VLAN-ID	Εισαγωγή στην VLAN κατάσταση. Προϋποθέτει την ρύθμιση κάποιων διασυνδέσεων στο συγκεκριμένο VLAN
R(config-if)#**xconnect** remote-peer-id-address vc-id **encapsulation mpls**	Ενεργοποιεί την δρομολόγηση AToM πακέτων μέσω ενός συγκεκριμένου VC και με MPLS ενθυλάκωση
PPPoMPLS	
R(config)#**interface** interface-type	Εισαγωγή στην κατάσταση μιας διασύνδεσης
R(config)#**encapsulation ppp**	Ρύθμιση PPP ενθυλάκωσης στη διασύνδεση
R(config-if)#**xconnect** remote-peer-id-address vc-id **encapsulation mpls**	Ενεργοποιεί την δρομολόγηση AToM πακέτων μέσω ενός συγκεκριμένου VC και με MPLS ενθυλάκωση
HDLCoMPLS	
R(config)#**interface** interface-type	Εισαγωγή στην κατάσταση μιας διασύνδεσης
R(config)#**encapsulation hdlc**	Ρύθμιση HDLC ενθυλάκωσης στη διασύνδεση
R(config-if)#**xconnect** remote-peer-id-address vc-id **encapsulation mpls**	Ενεργοποιεί την δρομολόγηση AToM πακέτων μέσω ενός συγκεκριμένου VC και με MPLS ενθυλάκωση
FRoMPLS	
R(config)#**frame-relay switching**	Ενεργοποίηση του Frame-Relay στον δρομολογητή
R(config)#**interface** interface-type	Εισαγωγή στην κατάσταση μιας διασύνδεσης
R(config-if)#**encapsulation frame-relay**	Ενεργοποίηση Frame-Relay ενθυλάκωσης σε συγκεκριμένη διασύνδεση
R(config-if)#**frame-relay intf-type dce**	Ρύθμιση της διασύνδεσης ως DCE
R(config)#**connect** connection-name interface-type/name dlci **l2transport**	Καθορίζει ένα τοπικής σημασίας όνομα σύνδεσης και ένα επίσης τοπικής σημαίας DLCI. Καθορίζεται επιπλέον και το AC (Attachment Circuit)

Παράρτημα 5

A. Ρυθμίσεις VPLS

Εντολή	Περιγραφή
R(config)#**l2 vfi** name **manual**	Δημιουργία ενός VFI και εισαγωγή στην VFI κατάσταση
R(config-vfi)#**vpn id** number	Καθορίζεται το VPN-ID το οποίο λειτουργεί ως αναγνωριστικό μιας VPLS περιοχής στο δίκτυο
R(config-vfi)#**neighbor** remote-router-id **encapsulation mpls**	Καθορίζει το απομακρυσμένο άκρο του Tunnel, δηλαδή το απομακρυσμένο Router-ID. Επίσης καθορίζεται και η ενθυλάκωση του Tunnel
R(config-vfi)#**xconnect vfi** name	Καθορίζει το απομακρυσμένο VFI του Tunnel
R(config-if)#**l2protocol-tunnel [cdp|stp|vtp]**	Ενεργοποιεί την μεταφορά ορισμένων πρωτοκόλλων μέσω του Tunnel. Εξ' ορισμού δεν μεταφέρονται
R#**show vfi** name	Εμφανίζει πληροφορίες ενός VFI. Παρακάτω φαίνεται η έξοδος της εντολής Router#**show vfi** A VFI name: A, state:up Local attachment circuits: vlan 100 Neighbors connected via pseudowires: 10.10.10.102 10.10.10.103
R#**show mpls l2transport vc** [vc-id] **[detail]**	Εμφανίζει πληροφορίες για τα επιπέδου 2 κυκλώματα (Vcs). Παρακάτω φαίνεται η έξοδος της εντολής Router#**show mpls l2transport vc** 100 **detail** Local interface: VFI A up Destination address: 10.10.10.102, VC ID: 100, VC status: up Tunnel label: imp-null, next hop 10.10.10.2 Output interface: GE3/1, imposed label stack {21} Create time: 10:13:08, last status change time: 10:06:25 Signaling protocol: LDP, peer 10.10.10.102:0 up MPLS VC labels: local 21, remote 21 Group ID: local 0, remote 0 MTU: local 1500, remote 1500 Remote interface description: Sequencing: receive disabled, send disabled VC statistics: packet totals: receive 973, send 971 byte totals: receive 77383, send 77244 packet drops: receive 0, send 0

Εντολή	Περιγραφή
	Local interface: VFI A up Destination address: 10.10.10.103, VC ID: 100, VC status: up Tunnel label: imp-null, next hop 10.10.10.6 Output interface: GE3/2, imposed label stack {17} Create time: 10:13:09, last status change time: 10:06:45 Signaling protocol: LDP, peer 10.10.10.103:0 up MPLS VC labels: local 22, remote 17 Group ID: local 0, remote 0 MTU: local 1500, remote 1500 Remote interface description: Sequencing: receive disabled, send disabled VC statistics: packet totals: receive 90, send 977 byte totals: receive 8560, send 77712 packet drops: receive 0, send 0

Επεξήγηση Όρων

Όρος	Επεξήγηση
AC	Attachment Circuit: είναι ένα φυσικό ή εικονικό κύκλωμα που συνδέει έναν ακραίο δρομολογητή πελάτη με έναν δρομολογητή ενός παρόχου υπηρεσιών.
APS	Automatic Protection Switching: προστατεύει μια σύνδεση δεσμεύοντας μια άλλη σύνδεση με την ίδια χωρητικότητα (αφιερωμένη ή όχι).
ASN	Autonomous System Number: είναι ένα μοναδικό αναγνωριστικό ενός αυτόνομου συστήματος (AS), το οποίο χρησιμοποιείται από τα πρωτόκολλα δρομολόγησης. Το IANA (Internet Assigned Numbers Authority) είναι υπεύθυνο για την παροχή των αναγνωριστικών ASN.
ATM	Asynchronous Transfer Mode: είναι μια τεχνολογία σύνδεσης δευτέρου επιπέδου που βασίζεται στη μεταφορά δεδομένων μέσω κελιών καθορισμένου μεγέθους.
AToM	Any Transport over MPLS: είναι μια μέθοδος της Cisco Systems για την μεταφορά πλαισίων επιπέδου σύνδεσης πάνω από ένα MPLS δίκτυο.
BGP	Border Gateway Protocol: είναι το πρωτόκολλο δρομολόγησης το οποίο χρησιμοποιείται κυρίως μεταξύ διαφορετικών αυτόνομων συστημάτων.
CBR	Constraint Based Routing: αποτελεί μεθόδους δρομολόγησης βάση περιορισμών, όπως εύρος ζώνης.
CE	Customer Edge: είναι ο δικτυακός εξοπλισμός ο οποίος βρίσκεται στη μεριά του πελάτη και διασυνδέει τον πελάτη με τον πάροχο υπηρεσιών. Παραδείγματος χάριν, μπορεί να είναι ένας IP δρομολογητής ή ένας ATM μεταγωγέας,
CoS	Class of Service: καθορίζει ένα συγκεκριμένο σύνολο από χαρακτηριστικά κυκλοφορίας τα οποία εφαρμόζονται σε μια ροή δεδομένων
CR-LDP	Constraint based Label Distribution Protocol: αποτελεί επέκταση του πρωτοκόλλου LDP ώστε να επιτρέπει την χρήση περιορισμών στην επιλογή του LSP.
CSPF	Constrained Shortest Path First: προσθέτει περιορισμούς (π.χ. εύρος ζώνης) στον υπολογισμό της μικρότερου κόστους διαδρομής που υπολογίζει ο αλγόριθμος SPF.
DiffServ	Differentiated Services: παρέχει έναν μηχανισμό με τον οποίο τα πακέτα μαρκάρονται με ένα συγκεκριμένο επίπεδο σημαντικότητας. Χρησιμοποιεί το πεδίο DSCP του IP πακέτου.
DLCI	Data Link Connection Identifier: είναι ένα πεδίο των 10bit το οποίο καθορίζει τον προορισμό ενός πλαισίου σε Frame Relay δίκτυα. Είναι τοπικής σημασίας.
DSCP	Differentiated Services Code Point: είναι ένα πεδίο στην IP κεφαλίδα το οποίο επιτρέπει στους δρομολογητές να εφαρμόζουν διαφορετικές προτεραιότητες υπηρεσίας σε πακέτα. Επιτρέπει στους παρόχους υπηρεσιών να προσφέρουν διαφορετικές ποιότητες ανάλογα με την προτεραιότητα των πακέτων.
EIGRP	Enhanced Interior Gateway Protocol: είναι ένα προηγμένο IGP πρωτόκολλο δρομολόγησης της Cisco Systems, που συνδυάζει πλεονεκτήματα των distance vector και των link state πρωτοκόλλων δρομολόγησης.
EoMPLS	Ethernet over Multiprotocol Label Switching: είναι μια Any Transport over MPLS

Όρος	Επεξήγηση
	τεχνική με την οποία μεταφέρονται πλαίσια Ethernet πάνω από ένα MPLS δίκτυο
FEC	Forwarding Equivalence Class: είναι ένα σύνολο πακέτων, τα οποία λόγω συγκεκριμένων χαρακτηριστικών, τυγχάνουν την ίδια απόφαση προώθησης.
FRR	Fast ReRoute: είναι μια MPLS τεχνική η οποία παρέχει γρήγορη ανάκτηση της κυκλοφορίας (50ms) σε περίπτωση αποτυχίας μιας σύνδεσης ή ενός κόμβου.
FTN	FEC to Next Hop Label Forwarding Entry: αντιστοιχεί κάθε FEC σε ένα ή περισσότερα NHLFE. Χρησιμοποιείται για την προώθηση πακέτων τα οποία ακόμα δεν έχουν ετικέτα, αλλά αποκτούν μια πριν προωθηθούν.
GRE	Generic Routing Encapsulation: συναντάται κυρίως στις VPN εφαρμογές. Είναι ένας τρόπος ενθυλάκωσης IP πακέτων τα οποία μεταφέρονται με ασφάλεια (συνήθως IPSec) μέσω ενός Tunnel.
HDLC	High Level Data Link Control: είναι ένα πρωτόκολλο δευτέρου επιπέδου για point-to-point και multipoint παράδοση δεδομένων.
HDLCoMPLS	High Level Data Link Control over Multiprotocol Label Switching: είναι μια Any Transport over MPLS τεχνική με την οποία μεταφέρονται πλαίσια HDLC πάνω από ένα MPLS δίκτυο
ICMP	Internet Control Message Protocol: είναι ένα πρωτόκολλο που αναφέρει τυχόν σφάλματα και παρέχει και άλλες πληροφορίες σχετικές με την επεξεργασία των IP πακέτων.
IGP	Interior Gateway Protocol: σύνολο πρωτοκόλλων δρομολόγησης που χρησιμοποιούνται για την ανταλλαγή πληροφορίας δρομολόγησης εντός ενός αυτόνομου συστήματος. Παράδειγμα αποτελούν το OSPF και το IS-IS.
ILM	Incoming Label Map: αντιστοιχεί κάθε εισερχόμενη ετικέτα σε ένα σύνολο από Next Hop Label Forwarding Entries. Χρησιμοποιείται για την προώθηση πακέτων τα οποία είναι επισημασμένα.
IP	Internet Protocol: πρωτόκολλο τρίτου επιπέδου το οποίο παρέχει υπηρεσία επικοινωνίας χωρίς σύνδεση.
IPX	Internetwork Packet Exchange: πρωτόκολλο επιπέδου δικτύου το οποίο υποστηρίζεται από το NetWare network operating system της Novell και ήταν δημοφιλές κατά τη διάρκεια της δεκαετίας του 80’ ως και τα μέσα της δεκαετίας του 90’
IS-IS	Intermediate system to intermediate system: είναι ένα IGP πρωτόκολλο δρομολόγησης. Ανήκει στην κατηγορία των link-state πρωτοκόλλων δρομολόγησης.
ISP	Internet Service Provider: πάροχος υπηρεσιών διαδικτύου
L2VPN	Layer 2 Virtual Private Network: είναι μια υπηρεσίας ιδεατού ιδιωτικού δικτύου η οποία εξομοιώνει ένα δευτέρου επιπέδου μεταξύ των απομακρυσμένων τμημάτων ενός πελάτη
L3VPN	Layer 3 Virtual Private Network: είναι ένα ιδεατό ιδιωτικό δίκτυο τρίτου επιπέδου το οποίο βασίζεται στο IP
LDP	Label Distribution Protocol: είναι το πρωτόκολλο που χρησιμοποιείται για την διανομή των ετικετών του MPLS
LER	Label Edge Router: δρομολογητής εισόδου ή εξόδου ενός πακέτου σε ένα MPLS δίκτυο. Είναι υπεύθυνος για την εισαγωγή ή την εξαγωγή της ετικέτας.
LFIB	Label Information Forwarding Base:για κάθε FEC περιέχει μόνο τις ετικέτες που απαιτούνται για την προώθηση των πακέτων

Όρος	Επεξήγηση
LIB	Label Information Base: περιέχει το σύνολο εισερχόμενων και εξερχόμενων ετικετών για κάθε FEC
LSA	Link State Advertisement: παρέχουν τον βασικό τρόπο επικοινωνίας στο πρωτόκολλο δρομολόγησης OSPF
LSR	Label Switching Router: είναι δρομολογητές ενός MPLS δικτύου οι οποίοι είναι ικανοί να μεταγάγουν επισημασμένα πακέτα.
L2TPv3	Layer 2 Tunneling Protocol: είναι ένα εναλλακτικό πρωτόκολλο για μετάδοση πλαισίων δευτέρου επιπέδου πάνω από ένα IP δίκτυο.
MAC	Media Access Control: αναφέρεται στις φυσικές διευθύνσεις των δικτυακών συσκευών.
MPLS	Multiprotocol Label Switching: είναι ένα πρωτόκολλο ανεξάρτητο από τα επίπεδα του OZI το οποίο ορίζει έναν τρόπο μεταγωγής πακέτων βάση ετικετών.
MPoA	Multiprotocol over ATM: ασχολείται με την μεταφορά δεδομένων σε ένα Local Area Network Emulation.
MQC	Cisco Modular Quality of Service Command Line Interface: γραμμή εντολών για ρύθμιση χαρακτηριστικών ποιότητας υπηρεσίας.
MTU	Maximum Transmission Unit: ορίζει το μέγιστο μήκος πακέτων που μπορεί να διαχειριστεί μια συγκεκριμένη διασύνδεση.
NHLFE	Next Hop Label Forwarding Entry: χρησιμοποιείται για την προώθηση ενός πακέτου και περιέχει πληροφορίες όπως: το επόμενο βήμα του πακέτου, τη λειτουργία που πρέπει να πραγματοποιηθεί στη στοίβα ετικετών
OSI	Open System Interconnection: είναι ένα μοντέλο των εφτά επιπέδων το οποίο χωρίζει τις λειτουργίας της επικοινωνίας στα επίπεδα αυτά.
OSPF	Open shortest Path First: IGP πρωτόκολλο δρομολόγησης. Ανήκει στην κατηγορίας των link state πρωτοκόλλων δρομολόγησης.
PDU	Protocol Data Unit: περιλαμβάνει δεδομένα και πληροφορίες ελέγχου που μεταφέρονται ανάμεσα στα επίπεδα μιας στοίβας πρωτοκόλλων.
PE	Provider Edge: είναι ο δικτυακός εξοπλισμός ο οποίος βρίσκεται στη μεριά του παρόχου υπηρεσιών και διασυνδέει τον πάροχο υπηρεσιών με τον πελάτη.
PHP	Penultimate Hop Popping: τεχνική με την οποία αφαιρείται η ετικέτα ενός πακέτου στον προτελευταίο κόμβο πριν την έξοδο από το MPLS δίκτυο.
PPP	Point to Point Protocol: πρωτόκολλο δευτέρου επιπέδου το οποίο παρέχει point-to-point σύνδεση μεταξύ δρομολογητών σε σύγχρονα ή ασύγχρονα συστήματα.
PPPoMPLS	Point to Point Protocol over Multiprotocol Label Switching: είναι μια Any Transport over MPLS τεχνική με την οποία μεταφέρονται πλαίσια PPP πάνω από ένα MPLS δίκτυο
PSN	Packet Switch Network: δίκτυο στο οποίο πραγματοποιείται μεταγωγή πακέτων
QoS	Quality of Service: ποιότητα υπηρεσίας η οποία εφαρμόζει ένας πάροχος στα πακέτα των πελατών
RD	Route Distinguisher: είναι ένα μοναδικό αναγνωριστικό που προσθέτει το BGP στα IP προθέματα ώστε να γίνουν μοναδικά μεταξύ των διαφορετικών VPN
RSVP	Resource Reservation Protocol: είναι ένα σύνολο από κανόνες επικοινωνίας που επιτρέπουν την δέσμευση συνδέσεων και πόρων
RT	Route Target: είναι ένα extended community του BGP το οποίο επιτρέπει την επικοινωνία μεταξύ διαφορετικών VPN
TCP	Transmission Control Protocol: είναι ένα πρωτόκολλο μεταφοράς δεδομένων. Προσφέρει αξιοπιστία σε ένα περιβάλλον με σύνδεση.

Όρος	Επεξήγηση
TE	Traffic Engineering: χρησιμοποιεί της πληροφορίες δρομολόγησης με τέτοιο τρόπο ώστε να γίνει πιο αποδοτική η αντιστοίχηση της κυκλοφορίας στους διαθέσιμους δικτυακούς πόρους.
TLV	Type Length Value: είναι ένα αντικείμενο το οποίο αποτελείται από μια τριάδα: τύπο (type), μήκος (length) και τιμή (value).
ToS	Type of Service: είναι ένα πεδίο στην κεφαλίδα ενός IP πακέτου το οποίο χρησιμοποιείται για την εφαρμογή ποιότητας υπηρεσίας.
TTL	Time to Live: είναι ο χρόνος ζωής ενός πακέτου. Σε κάθε κόμβο μειώνεται. Όταν φθάσει μηδέν το πακέτο απορρίπτεται.
UDP	User Datagram Protocol: πρωτόκολλο επιπέδου μεταφοράς το οποίο χρησιμοποιείται για την μεταφορά πακέτων χωρίς σύνδεση
VCI	Virtual Channel Identifier: είναι ένα αναγνωριστικό της κεφαλίδας ενός ATM κελιού το οποίο καθορίζει σε ποιο εικονικό κύκλωμα ανήκει ένα κελί.
VFI	Virtual Forwarding Instance (όρος της Cisco Systems): είναι ένα εικονικό στιγμιότυπο το οποίο περιέχει τα δίκτυα τα οποία μέσω του VPLS αποτελούν εικονικά ένα τοπικό δίκτυο.
VPI	Virtual Path Identifier: πεδίο ενός ATM κελιού το οποίο καθορίζει σε ποια εικονική διαδρομή ανήκει το ATM κελί.
VPLS	Virtual Private Lan Service: εφαρμογή του MPLS που εξομοιώνει ένα τοπικό δίκτυο
VPN	Virtual Private Network: εικονικό ιδεατό δίκτυο
VRF	Virtual Routing and Forwarding: είναι εικονικοί πίνακες δρομολόγησης οι οποίοι ξεχωρίζουν τις πληροφορίες δρομολόγησης των πελατών διαφορετικών VPN.