ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

ΤΜΗΜΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΣΠΟΥΔΩΝ ΣΤΗΝ ΚΑΤΕΥΘΥΝΣΗ

«ΔΙΚΤΥΟΚΕΝΤΡΙΚΑ ΣΥΣΤΗΜΑΤΑ»

Μεταπτυχιακή Διπλωματική Εργασία

Μηχανισμοί Παροχής Ποιότητας Υπηρεσίας σε Δίκτυα Κορμού

Φοιτητής : Μπάκας Σωτήριος

Α.Μ. : ΜΕ09064

Επιβλέπων : Ρούσκας Άγγελος, Επίκουρος Καθηγητής

Αθήνα 2013

UNIVERSITY OF PIRAEUS

DEPARTMENT OF DIGITAL SYSTEMS

POSTGRADUATE PROGRAMME IN

«NETWORK-ORIENTED SYSTEMS»

DISSERTATION

Mechanisms for Quality of Service Provisioning in Core Networks

STUDENT : MPAKAS SOTIRIOS

Id.No : ME09064

Advisor : Rouskas Angelos, Assistant Professor

Athens 2013

Περίληψη

Στη σημερινή εποχή της παγκοσμιοποίησης, οι επιχειρήσεις επεκτείνονται με ταχύτατους ρυθμούς χωρίς προηγούμενο. Παράλληλη είναι και η εξέλιξη της τεχνολογίας˙ έτσι το Internet πρέπει να υποστηρίζει καινούριες και συνεχώς αναβαθμιζόμενες υπηρεσίες. Καθώς λοιπόν υπάρχει αυτή η τάση για ανάπτυξη και οι επιχειρήσεις εξαπλώνονται γεωγραφικά σε όλο και περισσότερους προορισμούς, η ανάγκη τους να συνδεθούν στις νέες τοποθεσίες μεγαλώνει. Ο αριθμός των τοποθεσιών αυξάνει συνεχώς με αποτέλεσμα την «υποβάθμιση» της επικοινωνίας και την προβληματική διαχείριση των αυξανόμενων απαιτήσεων του δικτύου. Επομένως, γίνεται επιτακτική η ανάγκη αναβάθμισης της τεχνολογίας για ποσοτική , ποιοτική , ασφαλέστερη και ταχύτερη επικοινωνία. Οι πάροχοι υπηρεσιών αντιμετωπίζουν περισσότερα προβλήματα, διότι πρέπει να εξυπηρετούν πολλαπλούς πελάτες και όλοι προσπαθούν να δημιουργήσουν υποδομές σε ολοένα και περισσότερες περιοχές.

Επίσης, ο ανταγωνισμός στην αγορά αυξάνεται συνεχώς, γεγονός που αναγκάζει τους παρόχους υπηρεσιών να προσφέρουν οικονομικά αποδοτικές και εύκολα διαχειρίσιμες λύσεις στους πελάτες τους.

Με τις εφαρμογές πολυμέσων να κερδίζουν τη δημοτικότητα, είναι πλέον απαραίτητο να υπάρχει ποιότητα υπηρεσιών (Quality of Service – QoS). Οι υπηρεσίες φωνής θα πρέπει να έχουν προτεραιότητα έναντι των άλλων υπηρεσιών, καθώς είναι πολύ ευαίσθητες στην καθυστέρηση. Επιπλέον, όλο και περισσότερες εφαρμογές βίντεο βρίσκουν τη θέση τους σε εταιρικά δίκτυα, όπως λύσεις Τηλεδιάσκεψης, που δίνουν τη δυνατότητα εξοικονόμησης χρόνου στις σύγχρονες εταιρίες, τις κάνουν πιο ευέλικτες στις αποφάσεις τους και μειώνουν το κόστος των ταξιδιών. Όπως είναι κατανοητό για αυτές τις εφαρμογές θα πρέπει επίσης να δοθεί προτεραιότητα.

Η αποδοτικότερη διαχείριση του εύρους ζώνης στα δίκτυα γίνεται όλο και πιο σημαντική, ειδικότερα όταν τίθεται το θέμα της δέσμευσης των διαθέσιμων πόρων

στο δίκτυο με σκοπό τη βελτίωση της απόδοσης. Πολλές φορές βλέπουμε σε δίκτυα με αρκετά μεγάλο φορτίο κυκλοφορίας και περιορισμένους πόρους, κάποιους από τους συνδέσμους να είναι υπερφορτωμένοι και κάποιοι άλλοι να παραμένουν αχρησιμοποίητοι.

Μια τεχνολογία που επιχειρεί να ανταποκριθεί με επάρκεια στην πρόκληση για αποδοτική διαχείριση της κίνησης αλλά και να δώσει απάντηση σε όλα τα παραπάνω ζητήματα είναι το Multiprotocol Label Switching (MPLS).

Στην παρούσα μεταπτυχιακή διπλωματική διατριβή, λοιπόν, εξετάζονται όσον αφορά στο θεωρητικό μέρος, τα γενικότερα χαρακτηριστικά και εφαρμογές του MPLS και στη συνέχεια, στο δεύτερο μέρος παρουσιάζονται τα σενάρια MPLS με τη χρήση του GNS3 εξομοιωτή, καταλήγοντας στο τελευταίο κεφάλαιο στα γενικότερα συμπεράσματα που προκύπτουν από τη μελέτη του MPLS μηχανισμού, για τον οποίο και εκπονήθηκε η συγκεκριμένη εργασία.

Κατά την εκπόνηση της παρούσης διπλωματικής εργασίας σχεδιάστηκε και υλοποιήθηκε μια σύνθετη τοπολογία που μας επέτρεψε να αναπτύξουμε και μελετήσουμε εξολοκλήρου τα ακόλουθα σενάρια:

1. MPLS - OSPF

2. MPLS - EIGRP

3. MPLS - RIPv2

4. MPLS - VPN

5. MPLS TE - CSPF (OSPF-TE) / Constraint-Based Routing

Abstract

In the era of globalization, companies are expanding rapidly. The same happens with the evolution of technology, so the Internet should support new and continuously upgraded services. Since, there is this tendency for growth and businesses are spreading geographically to more and more destinations, the need to connect to new locations grow. The number of locations is increasing which results to "deterioration" of communication and the problematic management of the increasing demands of the network. Therefore, it becomes imperative the technology upgrade, for quantitative, qualitative, safer and faster communication. Service providers face more problems because they have to serve multiple customers and all trying to create infrastructure in several different areas.

Moreover, the competition in the market area is increasing, forcing service providers to offer cost-effective and manageable solutions to their customers.

It seems that the multimedia applications gaining the popularity, thus it is now necessary to have quality of service (Quality of Service - QoS). The voice should have priority over other services, as it is very sensitive to delays. In addition, more and more video applications find their place in corporate networks as video conferencing solutions which give the possibility of time saving in modern companies, make them more flexible in their decisions and reduce the cost of travels. It is understood that for these applications should also be given priority.

The more efficient management of bandwidth in networks is becoming increasingly important, particularly when the issue arises of the commitment of available resources in the network in order to improve performance. Many times we see in networks with large enough traffic load and limited resources, some of the links to remain unused and some of them to be overloaded.

A technology that seeks to respond adequately to the challenge of efficient traffic management and to answer all the above questions is the Multiprotocol Label Switching (MPLS).

This postgraduate diploma thesis, examines in the theoretical part the general characteristics and applications of MPLS and in the second part are presented some MPLS scenarios using the GNS3 emulator, concluding with the final chapter with the main conclusions, arising from the study of the MPLS mechanism, for which was elaborated this dissertation.

For the elaboration of this dissertation, was designed and implemented a network topology which allowed us to develop and study the following scenarios:

1. MPLS - OSPF
2. MPLS - EIGRP
3. MPLS - RIPv2
4. MPLS - VPN
5. MPLS TE - CSPF (OSPF-TE) / Constraint-Based Routing

Ευχαριστίες

Αρχικά θα ήθελα να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή της διπλωματικής μου εργασίας κ. Ρούσκα Άγγελο, για την καθοδήγηση και την πολύτιμη συμβολή του στην διάρκεια της δημιουργίας της παρούσας εργασίας. Επίσης θα ήθελα να ευχαριστήσω και να εκφράσω την ευγνωμοσύνη μου στην οικογένειά μου, που όλα αυτά τα χρόνια μου συμπαραστέκονται ηθικά.

Αθήνα, Απρίλιος 2013

Περιεχόμενα

Ευρετήριο Εικόνων

Ευρετήριο Εικόνων Παραρτήματος Α

Πρόλογος

Η παρούσα μεταπτυχιακή διπλωματική διατριβή εκπονήθηκε στα πλαίσια του Προγράμματος Μεταπτυχιακών Σπουδών «Διδακτικής της Τεχνολογίας και Ψηφιακά Συστήματα» του τμήματος Ψηφιακών Συστημάτων του Πανεπιστημίου Πειραιώς. Το προσωπικό ενδιαφέρον και η πρόκληση για περαιτέρω γνώση του μηχανισμού MPLS αποτελούν τα κριτήρια επιλογής του συγκεκριμένου θέματος. Παράλληλα αυτή η διπλωματική εργασία θα μπορούσε να αποτελέσει ένα χρήσιμο εργαλείο μελέτης και βοήθειας για το τμήμα Ψηφιακών Συστημάτων, ως ένδειξη ελάχιστης ευγνωμοσύνης από τη πλευρά του συγγραφέα, πράγμα το οποίο θα προσέφερε ιδιαίτερη ικανοποίηση και ευχαρίστηση στον ίδιο.

Εισαγωγή

1. Τι είναι το MPLS

Αποτελεί μια εξελισσόμενη τεχνολογία, η οποία βοηθάει στην επιτάχυνση της ροής της κυκλοφορίας του δικτύου και καθιστώντας πιο εύκολο να τη διαχειριστεί. Το MPLS προβλέπει την εγκαθίδρυση ενός συγκεκριμένου μονοπατιού για μια δεδομένη ακολουθία πακέτων, τα οποία αναγνωρίζονται από μία ετικέτα που τοποθετείται σε καθένα από αυτά, εξοικονομώντας έτσι το χρόνο που απαιτείται για ένα δρομολογητή, να αναζητήσει τη διεύθυνση του επόμενου κόμβου για την προώθηση του πακέτου. Ονομάζεται Multiprotocol γιατί μπορεί να συνυπάρξει με IP , ATM και Frame Relay δικτυακά πρωτόκολλα. Επιτρέπει τα περισσότερα πακέτα να διαβιβάζονται στο επίπεδο 2 (Layer 2 Data Link Layer) και όχι στο επίπεδο 3 του δικτύου (Layer 3 - Network). Εκτός από την ταχύτερη κίνηση της κυκλοφορίας συνολικά, το MPLS καθιστά εύκολη τη διαχείριση της ποιότητας της υπηρεσίας (QoS).

Η τεχνική της μεταγωγής εικονικών κυκλωμάτων μέσω ετικετών είναι μια υβριδική τεχνική ανάμεσα στην μεταγωγή κυκλώματος και την μεταγωγή πακέτων που προσπαθεί να εκμεταλλευτεί τα καλύτερα στοιχεία κάθε μιας. Η μορφή αυτή χρησιμοποιεί, πολυπλέκει και μετάγει πακέτα για να κάνει καλύτερη εκμετάλλευση των ζεύξεων, αλλά δημιουργεί και συνδέσεις (εικονικά κυκλώματα) για να έχει έλεγχο του φόρτου κάθε ζεύξης και να κάνει πιο γρήγορη τη μεταγωγή των πακέτων μέσω ετικετών. Έτσι μπορεί να υποστηρίξει υπηρεσίες που απαιτούν ποιότητα (ζωντανές υπηρεσίες ροής φωνής και βίντεο) αλλά και την δημιουργία ιδιωτικών νοητών δικτύων (VPN-Virtual Private Networks), μια υπηρεσία με μεγάλη ζήτηση.

Ιστορικά , προέκυψε από τα πλεονεκτήματα των ATM μεταγωγέων (ATM Switches) στα IP δίκτυα. Η αγορά δεν ήταν ικανοποιημένη από τις τεχνικές του ATM που φαίνονταν πολύπλοκές και ακριβές και έτσι εναλλακτικές προτάσεις βρήκαν απήχηση όπως η τεχνική IP Switch της Ipsilon και η Tag Switching της Cisco.

Αποτέλεσμα αυτών ήταν η δημιουργία του προτύπου της IETF που είναι γνωστό ως MPLS (Multi-Protocol Label Switching).

1.1 Συστατικά στοιχεία και MPLS ορολογία

Forwarding Equivalence Class (FEC)

Το πλήθος των πακέτων που προωθούνται με τον ίδιο τρόπο. Μία ή περισσότερες FECs μπορεί να αντιστοιχηθούν σε ένα LSP.

MPLS Label

Είναι η επικεφαλίδα/ετικέτα που χρησιμοποιείται από τους LSR (Label Switch Router) για την προώθηση των πακέτων. Οι LSRs διαβάζουν μόνο τις ετικέτες αυτού του τύπου, και όχι τις επικεφαλίδες IP των πακέτων. Οι ετικέτες έχουν νόημα μόνο σε τοπικό επίπεδο, δηλαδή μόνο μεταξύ δύο συσκευών που επικοινωνούν.

Εικόνα 1 : MPLS Ετικέτα

Η 32-bit MPLS ετικέτα τοποθετείται μετά την επικεφαλίδα του δευτέρου επιπέδου και πριν την IP επικεφαλίδα. Περιλαμβάνει τα ακόλουθα πεδία:

1. Το πεδίο Label (20-bits) περιλαμβάνει την πραγματική τιμή του MPLS label.
2. Το πεδίο CoS (3-bits) μπορεί να επηρεάσει τους αλγορίθμους χρονοδρομολόγησης και απόρριψης που εφαρμόζονται στο πακέτο καθώς αυτό μεταδίδεται μέσα στο δίκτυο.
3. Το πεδίο Stack (1-bit) υποστηρίζει μια ιεραρχική στοίβα ετικετών.
4. Το πεδίο TTL (time-to-live) (8-bits) παρέχει τη συμβατική IP TTL λειτουργικότητα.

Label Switched Path (LSP)

Είναι το "μονοπάτι" που ορίζεται από τις ετικέτες που δημιουργούνται και ανατίθενται στο κάθε πακέτο, μεταξύ των τελικών σημείων του δικτύου. 'Ενα LSP

μπορεί να είναι ορισμένο είτε στατικά είτε δυναμικά. Το τελευταίο προσδιορίζεται αυτόματα χρησιμοποιώντας πληροφορίες δρομολόγησης. Τα στατικά LSPs χρησιμοποιούνται σπανιότερα.

Label Switch Router (LSR)

Αποτελεί την συσκευή κορμού του δικτύου που μετάγει πακέτα εφοδιασμένα με την κατάλληλη ετικέτα, σύμφωνα με τους προϋπολογισμένους πίνακες μεταγωγής.

Edge LSR

Είναι η συσκευή που τοποθετείται στο άκρο του κυρίως δικτύου, η οποία εκτελεί την αρχική επεξεργασία και κατηγοριοποίηση του κάθε πακέτου και του αναθέτει την πρώτη ετικέτα.

Label Distribution Protocol (LDP)

Είναι το πρωτόκολλο που έχει σαν ρόλο την απόδοση ετικετών στα πακέτα, καθώς και τη μετάφραση των πληροφοριών τους από τους LSRs. Αναθέτει ετικέτες στα πακέτα από τις δικτυακές συσκευές στις άκρες και στον πυρήνα του δικτύου, έτσι ώστε να καθοριστούν τα αναγκαία LSPs. Η απόδοση των ετικετών γίνεται σε συνδυασμό με κάποια πρωτόκολλα δρομολόγησης, όπως τα Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS), Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP) ή Border Gateway Protocol (BGP).

Label Information Base (LIB)

Πίνακας προώθησης πακέτων με βάση την ετικέτα σε κάθε LSR.
Αντιστοιχίζει τις ετικέτες εισόδου-εξόδου στον LSR.

Δρομολογητές CE (customer edge)

Είναι οι δρομολογητές που τους διαχειρίζεται ο πελάτης και ανήκουν συνήθως σε αυτόν. Δεν εχει σχέση με το MPLS ούτε με πακέτα με ετικέτες αλλά συνδέονται με τους LSR.

Δρομολογητές PE (provider edge)

Είναι οι δρομολογητές που αποτελούν τα σημεία εισόδου και εξόδου των VPNs. Ανήκουν διαχειριστικά στον ISP. Αποτελούν το πιο σημαντικό τμήμα στη «λογική» των MPLS VPNs.

Δρομολογητές P (provider)

Είναι οι δρομολογητές που αποτελούν το δίκτυο κορμού του ISP και ανήκουν και αυτοί διαχειριστικά σε αυτόν. Δεν συμμετέχουν στη λογική VPN - ο κύριος σκοπός τους είναι η προώθηση των MPLS ετικετών προς τους PE routers.

Το MPLS περιλαμβάνει μια ευρεία ποικιλία εφαρμογών, με κάθε εφαρμογή να εξετάζει έναν ή περισσότερους από τους πιθανούς παράγοντες που επηρεάζουν τις αποφάσεις προώθησης MPLS. Δύο από τους σημαντικότερους είναι :

- **MPLS IP unicast**
- **MPLS VPNs**

MPLS Unicast IP

Το MPLS μπορεί να χρησιμοποιηθεί για απλή unicast IP προώθηση. Με την λογική του MPLS Unicast IP Forwarding το MPLS προωθεί πακέτα βασισμένα σε ετικέτες. Παρόλο αυτά, όταν επιλέγονται τα εξωτερικά interfaces από όπου θα προωθηθούν τα πακέτα, το MPLS εξετάζει μόνο τις διαδρομές στο unicast IP πίνακα δρομολόγησης, έτσι, το τελικό αποτέλεσμα της χρήσης του MPLS είναι ότι το πακέτο ρέει πάνω από την ίδια διαδρομή όπως θα είχε και αν το MPLS δεν είχε χρησιμοποιηθεί. Καταλαβαίνουμε λοιπόν πως δεν παρέχει σημαντικά πλεονεκτήματα από μόνο του, όμως, πολλές από τις πιο χρήσιμες εφαρμογές MPLS, όπως MPLS VPNs και MPLS Traffic Engineering (TE), χρησιμοποιεί το MPLS unicast IP Forwarding ως ένα μέρος του δικτύου MPLS.

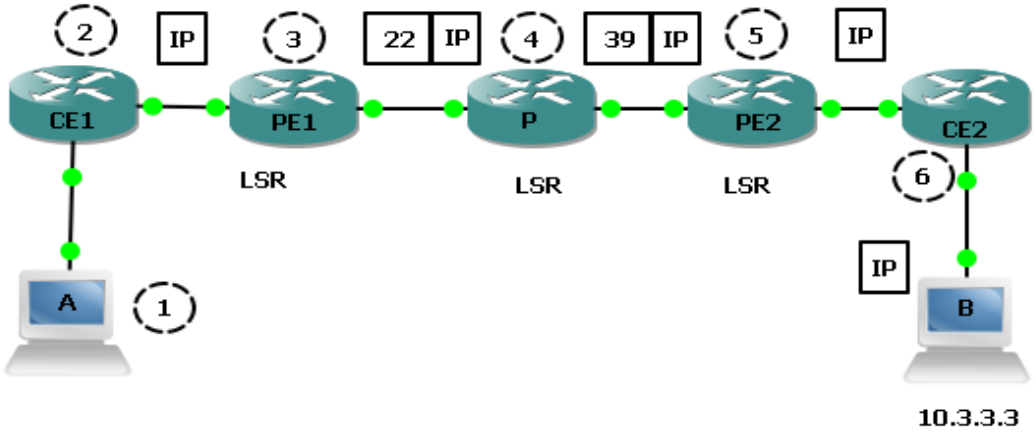
Το MPLS απαιτεί τη χρήση των πρωτοκόλλων επιπέδου ελέγχου (control plane) (για παράδειγμα, OSPF και LDP) για να μαθαίνει ετικέτες, να συσχετίζει αυτές

τις ετικέτες με συγκεκριμένα προθέματα προορισμού (prefixes), και να χτίζουν τους σωστούς πίνακες προώθησης. Το MPLS απαιτεί επίσης μια θεμελιώδη αλλαγή στην λογική προώθησης του πυρήνα επιπέδου δεδομένων (data plane). Στην συνέχεια θα εξετάσουμε το επίπεδο των δεδομένων, όπου ορίζει την λογική προώθησης πακέτου και μετά από αυτό θα εξετάσουμε τα πρωτόκολλα επίπεδο ελέγχου, και ιδιαίτερα το Label Distribution Protocol (LDP), το οποίο οι MPLS δρομολογητές χρησιμοποιούν για να ανταλλάσσουν τις ετικέτες για unicast IP προθέματα (prefixes). Με λίγα λόγια το επίπεδο ελέγχου (control plane) είναι εκεί που παίρνονται οι αποφάσεις για τις δρομολογήσεις και τις προωθήσεις των πακέτων ενώ το επίπεδο δεδομένων (data plane) είναι εκεί που πραγματοποιούνται όλες οι ενέργειες των δρομολογήσεων / προωθήσεων.

MPLS IP Forwarding: Επίπεδο δεδομένων (Data Plane)

Το MPLS ορίζει ένα εντελώς διαφορετικό πρότυπο προώθησης πακέτου. Ωστόσο οι Hosts δεν θα πρέπει να στέλνουν και να λαμβάνουν πακέτα με ετικέτες, έτσι σε κάποιο σημείο, κάποιοι δρομολογητές θα πρέπει να προσθέσουν μια ετικέτα στο πακέτο και, αργότερα, κάποιοι άλλοι δρομολογητές να αφαιρέσουν την ετικέτα. Οι MPLS δρομολογητές είναι οι δρομολογητές που προσθέτουν (push), αφαιρούν (pop) ή προωθούν πακέτα βασισμένα στις ετικέτες, χρησιμοποιώντας την λογική προώθησης MPLS.

Το πρότυπο προώθησης MPLS υποθέτει ότι οι hosts δημιουργούν πακέτα χωρίς ετικέτα MPLS, στη συνέχεια, κάποιοι δρομολογητές τοποθετούν μια ετικέτα MPLS, άλλοι δρομολογητές προωθούν το πακέτο με βάση την ετικέτα, και τέλος άλλοι δρομολογητές αφαιρούν την ετικέτα. Το τελικό αποτέλεσμα είναι ότι οι κεντρικοί υπολογιστές δεν έχουν επίγνωση της ύπαρξης του MPLS. Για να εκτιμήσουμε αυτή τη συνολική διαδικασία προώθησης παρακάτω θα δούμε αναλυτικά ένα παράδειγμα, με τα βήματα που δείχνει πώς ένα πακέτο προωθείται με τη χρήση MPLS.



Εικόνα 2 : Προώθηση πακέτου με τη χρήση MPLS

1. Ο Host A παράγει και στέλνει ένα πακέτο χωρίς ετικέτα που προορίζεται για τον host 10.3.3.3.
2. Ο δρομολογητής CE1, χωρίς να έχει διαμορφωθεί με MPLS, προωθεί το πακέτο χωρίς ετικέτα με βάση τη διεύθυνση IP προορισμού, ως συνήθως, χωρίς ετικέτες.
3. Ο MPLS δρομολογητής PE1 λαμβάνει το πακέτο χωρίς ετικέτα και αποφασίζει, ως μέρος της διαδικασίας προώθησης MPLS, να επιβάλει (push) μια νέα ετικέτα (τιμή 22) μέσα στο πακέτο και να προωθήσει πακέτο.
4. Ο MPLS δρομολογητής P1 λαμβάνει το πακέτο με ετικέτα. Ο P1 ανταλλάζει την ετικέτα για μια νέα τιμή ετικέτας (39) και στη συνέχεια προωθεί το πακέτο.
5. Ο MPLS δρομολογητής PE2 λαμβάνει το πακέτο με ετικέτα, αφαιρεί (POP) την ετικέτα, και προωθεί το πακέτο προς CE2.
6. Ο μη MPLS δρομολογητής CE2 προωθεί το πακέτο χωρίς ετικέτα και με βάση τη διεύθυνση IP προορισμού, ως συνήθως.

Ο όρος Router Switch Ετικέτα (LSR) αναφέρεται σε οποιοδήποτε δρομολογητή που έχει επίγνωση των MPLS ετικετών, για παράδειγμα, οι δρομολογητές PE1, P1, και PE2 στην Εικόνα 2.

MPLS Προώθηση χρησιμοποιώντας FIB και LFIB

FORWARDING INFORMATION BASE [FIB]

Χρησιμοποιείται για εισερχόμενα πακέτα χωρίς ετικέτες. Είναι ο πίνακας που δείχνει το καλύτερο ταίριασμα με την IP προορισμού ώστε να προωθήσει το πακέτο. (Εδώ δεν χρησιμοποιούνται ετικέτες)

Π.χ.:

```
AR1#sh ip cef
Prefix              Next Hop            Interface
0.0.0.0/0           drop                Null0 (default route handler entry)
0.0.0.0/8           drop
0.0.0.0/32          receive
10.255.255.5/32     receive
127.0.0.0/8         drop
224.0.0.0/4         drop
224.0.0.0/24        receive
240.0.0.0/4         drop
255.255.255.255/32  receive
```

Εικόνα 3 : FORWARDING INFORMATION BASE πίνακας

LABLE FORWARDING INFOMRATION BASE [LFIB]

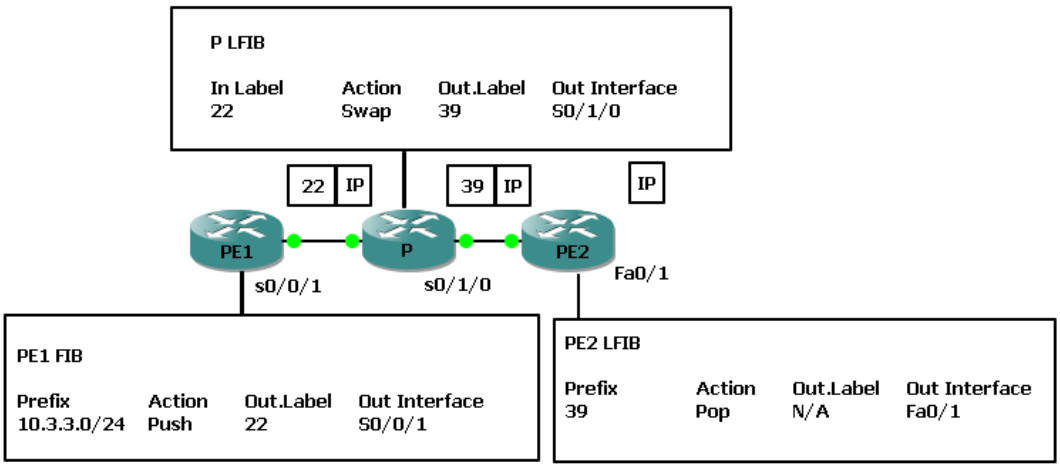
Χρησιμοποιείται για εισερχόμενα πακέτα με ετικέτες. Είναι ο πίνακας όπου ο δρομολογητής χρησιμοποιεί ώστε να προωθήσει πακέτα με ετικέτες στο δίκτυο.

Π.χ.:

```
AR1#sh mpls forwarding-table
Local  Outgoing    Prefix           Bytes tag  Outgoing    Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
17     Pop tag     10.255.255.2/32  0          Se1/2       point2point
20     Pop tag     10.0.0.4/30      0          Se1/2       point2point
21     Pop tag     10.0.0.0/30      0          Se1/2       point2point
       Pop tag     10.0.0.0/30      0          Se1/0       point2point
24     18          10.255.255.7/32  0          Se1/0       point2point
25     21          10.255.255.4/32  0          Se1/2       point2point
26     22          10.255.255.3/32  0          Se1/0       point2point
27     Pop tag     10.255.255.1/32  0          Se1/0       point2point
29     Pop tag     10.8.0.0/30      0          Se1/0       point2point
30     25          10.7.0.0/30      0          Se1/0       point2point
33     Pop tag     10.0.0.12/30     0          Se1/0       point2point
34     32          10.0.0.8/30      0          Se1/2       point2point
       31          10.0.0.8/30      0          Se1/0       point2point
```

Εικόνα 4 : LABLE FORWARDING INFOMRATION BASE πίνακας

Έχοντας σαν βάση το προηγούμενο παράδειγμα (Εικόνα 2) βλέπουμε παρακάτω πως χρησιμοποιούνται οι πίνακες LFIB και FIB



Εικόνα 5 : Χρήση των FIB και LFIB

PE1 -> Όταν το πακέτο φτάνει στον PE1 τότε αυτός χρησιμοποιεί το FIB πίνακα λόγω του ότι το πακέτο είναι χωρίς ετικέτα και ψάχνει να βρει την εγγραφή που ταιριάζει με την διεύθυνση προορισμού του 10.3.3.1 δηλαδή την εγγραφή 10.3.3.0/24 σε αυτή την περίπτωση. Μεταξύ άλλων, η καταχώρηση στο FIB περιλαμβάνει και πληροφορίες ώστε να βάλει την σωστή MPLS ετικέτα μπροστά από το πακέτο.

P1 -> Επειδή ο P1 δέχεται ένα πακέτο με ετικέτα, χρησιμοποιεί τον LFIB πίνακα, βρίσκοντας την τιμή της ετικέτας 22 εκεί και δηλώνοντας ότι πρέπει να ανταλλάξει την τιμή με 39.

PE2 -> Ο PE2 χρησιμοποιεί επίσης τον LFIB επειδή λαμβάνει ένα πακέτο με ετικέτα. Βρίσκει την αντίστοιχη εγγραφή και βλέπει ότι πρέπει να εκτελέσει την διαδικασία αφαίρεσης (pop) της ετικέτας ώστε να προωθήσει ένα πακέτο χωρίς ετικέτα στον CE2 δρομολογητή. (δεν υπάρχει εξωτερική ετικέτα ώστε να κάνει ανταλλαγή όπως ο P1)

MPLS IP Forwarding: Επίπεδο ελέγχου (Control Plane)

Για καθαρά IP δρομολογήσεις που πρέπει να λειτουργήσουν χρησιμοποιώντας FIB, οι δρομολογητές πρέπει να χρησιμοποιήσουν control plane πρωτόκολλα, όπως πρωτόκολλα δρομολόγησης ώστε να συμπληρώσουν πρώτα τον IP πίνακα δρομολόγησης και μετά τον FIB πίνακα. Ομοίως και για το MPLS όπου βασίζεται σε πρωτόκολλα επιπέδου ελέγχου (control plane) για να μάθει ποιες MPLS ετικέτες θα χρησιμοποιήσει ώστε να φτάσει σε κάποια κοντινή διεύθυνση της διεύθυνσης προορισμού (IP prefix) και ακολούθως να συμπληρώσει τόσο τον FIB όσο και τον LFIB με τις σωστές ετικέτες.

Το MPLS υποστηρίζει πολλά πρωτόκολλα επιπέδου ελέγχου. Παρόλο αυτά είναι καθαρά επιλογή του μηχανικού για το ποιο θα επιλέξει, σε σχέση βέβαια με την εφαρμογή MPLS που θα χρησιμοποιηθεί. Για παράδειγμα το MPLS VPNs χρησιμοποιεί 2 πρωτόκολλα επιπέδου ελέγχου: το LDP και το BGP.

Αναφορικά με το MPLS VPN, αναλυτική περιγραφή και εξέταση ακολουθεί σε επόμενο κεφάλαιο 4.2.

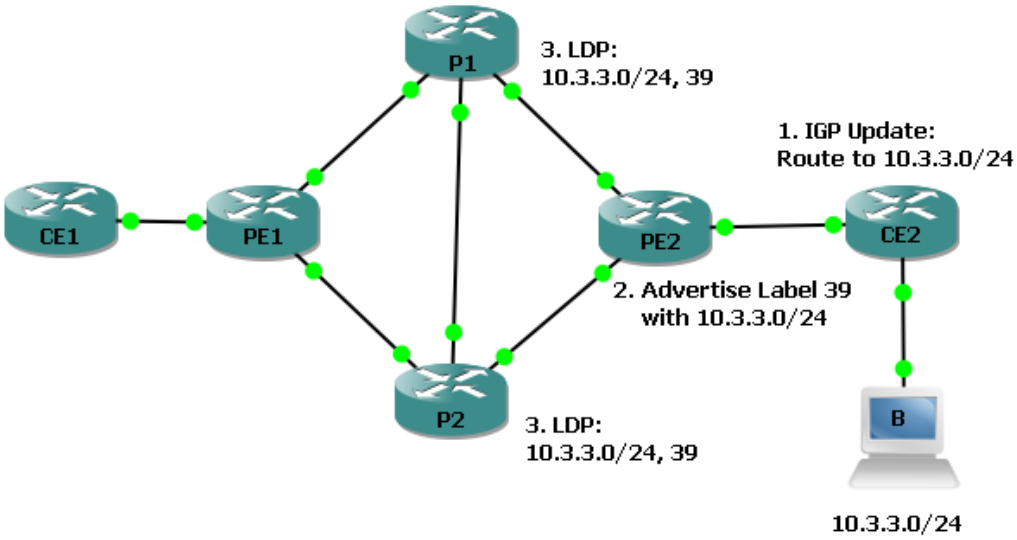
2. MPLS LDP

Είναι ένα πρωτόκολλο στο οποίο οι δρομολογητές μπορούν να ανταλλάσουν πληροφορίες χαρτογράφησης ετικετών. Το LDP χρησιμοποιείται για να χτίσουν και να διατηρήσουν τις βάσεις δεδομένων LSP που χρησιμοποιούνται για να διαβιβάσουν την κυκλοφορία μέσω MPLS δικτύων.

Για unicast IP δρομολόγηση, το LDP απλά διαφημίζει τις ετικέτες για κάθε πρόθεμα (prefix) που υπάρχει στον IP πίνακα δρομολόγησης. Για να γίνει αυτό, οι LSRs χρησιμοποιούν LDP για να στείλουν μηνύματα στους γειτονικούς δρομολογητές, με τις εγγραφές που υπάρχουν με IP προθέματα και τις αντίστοιχες ετικέτες. Διαφημίζοντας ένα IP πρόθεμα και ετικέτα, ο LSR λέει: “Εάν θέλεις να στείλεις πακέτα σε αυτό το πρόθεμα (prefix) στείλε τα σε μένα με την MPLS ετικέτα που περιλαμβάνεται στο LDP update”.

Η LDP διαφήμιση ενεργοποιείται από την εμφάνιση μιας νέας IP διαδρομής στον IP πίνακα δρομολόγησης. Μετά την εκμάθηση της νέας διαδρομής, ο LSR διαθέτει μια ετικέτα που ονομάζεται τοπική ετικέτα. Η τοπική ετικέτα είναι η ετικέτα που, σε αυτό το LSR χρησιμοποιείται για να αντιπροσωπεύσει το IP πρόθεμα που μόλις προστέθηκε στον πίνακα δρομολόγησης.

Παρακάτω μπορούμε να δούμε ένα παράδειγμα για να γίνει πιο κατανοητό αυτό που περιγράφουμε.



Εικόνα 6 : LDP Advertisement

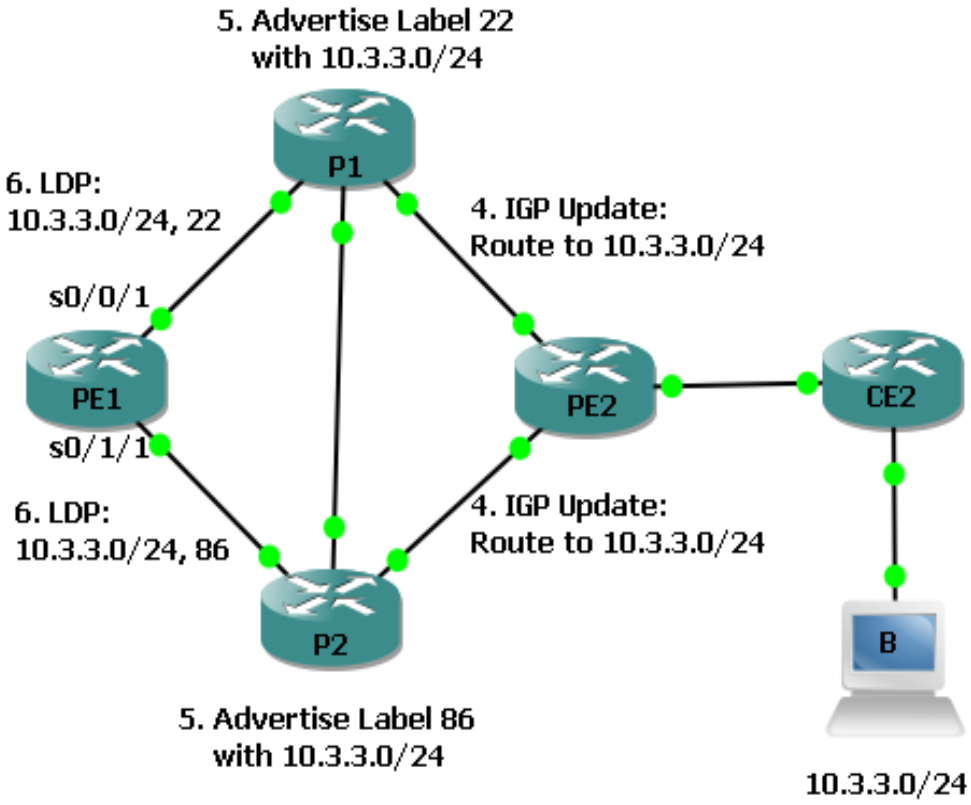
Η τοπολογία στην Εικόνα 6 δείχνει να πραγματοποιούνται τα εξής στον PE2 δρομολογητή:

1. Ο PE2 μαθαίνει μία νέα IP διαδρομή, που εμφανίζεται στον πίνακα δρομολόγησης.
2. Ο PE2 διαθέτει μία καινούρια τοπική ετικέτα, η οποία είναι η ετικέτα που δεν έχει ακόμα διαφημιστεί από τον LSR.
3. Ο PE2 χρησιμοποιεί LDP για να διαφημίσει στους γειτονικούς δρομολογητές την αντιστοιχία μεταξύ του IP προθέματος και της ετικέτας.

Αν και η παραπάνω διαδικασία φαίνεται απλή, είναι σημαντικό να σημειώσουμε πως ο PE2 πρέπει να είναι έτοιμος να διαχειριστεί πακέτα με ετικέτες που φτάνουν με νέα τιμή ετικέτας σε αυτά. Για παράδειγμα στο παραπάνω παράδειγμα ο PE2 πρέπει να είναι έτοιμος να προωθήσει πακέτα που λαμβάνει με ετικέτα 39. Θα προωθήσει τα πακέτα με το ίδιο next-hop και εξωτερικό interface, πληροφορίες που μαθαίνει από το IGP Update στο βήμα 1 που φαίνεται στην Εικόνα 6.

Η παραπάνω διαδικασία περιγράφει μόνο την διαφήμιση από μίας ετικέτας ενός μονοπατιού/διαδρομής (LSP Label switched path). Μια ολοκληρωμένη διαδρομή MPLS (MPLS LSP) είναι συνδυασμός από ετικέτες που χρησιμοποιούνται για να προωθήσουν τα πακέτα σωστά στον προορισμό.

Οι δρομολογητές σε ένα MPLS δίκτυο πρέπει να χρησιμοποιούν κάποια IP routing πρωτόκολλα για να μαθαίνουν τις IP διαδρομές προκειμένου να ενεργοποιηθεί η LDP διαδικασία και να διαφημιστούν οι ετικέτες στο δίκτυο. Τυπικά για το MPLS χρησιμοποιούμε ένα IGP πρωτόκολλο για να μάθουμε όπως αναφέραμε και προηγουμένως όλες τις IP διαδρομές ενεργοποιώντας έτσι τη διαδικασία διαφήμισης των αντίστοιχων ετικετών.



Εικόνα 7 : LDP / IGP Advertisement

Σε συνέχεια λοιπόν του προηγούμενου παραδείγματος έχουμε τα εξής:

4. Ο PE2 χρησιμοποιεί ένα IGP πρωτόκολλο για να διαφημίσει την διαδρομή για το 10.3.3.0/24 τόσο στον P1 όσο και στον P2.
5. Ο P1 αντιδρά στο ότι μαθαίνει μια καινούρια διαδρομή και θέτει μία καινούρια ετικέτα (22) και με τη χρήση του LDP διαφημίζει το δίκτυο με πρόθεμα 10.3.3.0/24 αντιστοιχίζοντας την ετικέτα 22. Σημαντικό να αναφέρουμε είναι ότι ο P1 διαφημίζει την ετικέτα σε όλους τους γείτονές του.
6. Ο P2 επίσης αντιδρά με την προσθήκη της νέας διαδρομής και θέτει μία καινούρια ετικέτα (86) και με τη χρήση του LDP διαφημίζει το δίκτυο με πρόθεμα 10.3.3.0/24 αντιστοιχίζοντας την ετικέτα 86. Σημαντικό να αναφέρουμε είναι ότι ο P2 επίσης διαφημίζει την ετικέτα σε όλους τους γείτονές του όπως προηγουμένως ο P1.

Η ίδια διαδικασία που περιγράφεται παραπάνω συμβαίνει σε κάθε LSR δρομολογητή, για κάθε διαδρομή που υπάρχει στον πίνακα δρομολόγησης του εκάστοτε LSR δρομολογητή. Κάθε φορά λοιπόν που ο LSR δρομολογητής μαθαίνει μια καινούρια διαδρομή, αναθέτει μία καινούρια ετικέτα και διαφημίζει την ετικέτα αυτή μαζί με το πρόθεμα (π.χ. 10.3.3.0/24) σε όλους του γειτονικούς δρομολογητές ακόμα και είναι προφανές ότι η διαφήμιση της ετικέτας αυτής δεν θα είναι χρήσιμη. π.χ. Ο P2 στο παράδειγμά μας διαφημίζει την ετικέτα για το 10.3.3.0/24 πίσω στον PE2 που στην πραγματικότητα δεν είναι χρήσιμο αλλά έτσι λειτουργούν οι MPLS LSRs.

Μόλις όλοι οι δρομολογητές μάθουν το πρόθεμα που χρησιμοποιείται από το IGP πρωτόκολλο και το LDP διαφημίσει όλες τις αντιστοιχίες ετικέτας/προθέματος σε όλους του γειτονικούς LSRs, κάθε LSR έχει αρκετή πληροφορία με την οποία θα επισημάνει τα πακέτα ώστε να μεταβούν από τον εσωτερικό LSR στον εξωτερικό.

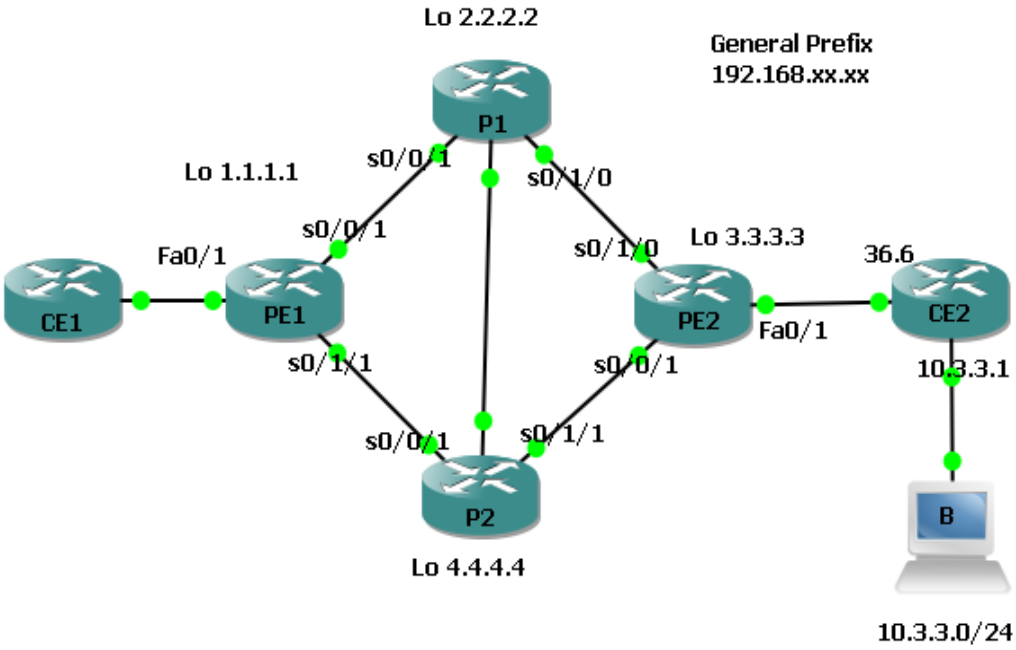
MPLS Label Information Base / Βάση Πληροφοριών Ετικέτας (LIB)

Οι LSRs αποθηκεύουν τις ετικέτες και τις σχετικές πληροφορίες μέσα σε μία δομή δεδομένων που καλείται Βάση Πληροφοριών Ετικέτας (LIB). Η LIB κατέχει ουσιαστικά όλες τις ετικέτες και τις συναφείς πληροφορίες που θα μπορούσαν ενδεχομένως να χρησιμοποιηθούν για να διαβιβάσει τα πακέτα. Ωστόσο, κάθε LSR πρέπει να επιλέξει την καλύτερη ετικέτα και εξερχόμενο interface (διεπαφή) που πραγματικά θα χρησιμοποιηθεί και μετά να συμπληρώσει αυτές τις πληροφορίες μέσα στο FIB και LFIB πίνακα. Ως αποτέλεσμα, το FIB και LFIB περιέχουν ετικέτες μόνο για την επί του παρόντος χρήση καλύτερου LSP μονοπατιού (διαδρομής), ενώ το LIB περιέχει όλες τις ετικέτες που είναι γνωστές στον LSR, είτε η ετικέτα χρησιμοποιείται, αυτή τη στιγμή, για την αποστολή ή όχι.

Για να αποφασιστεί για το ποια ετικέτα είναι καλύτερη να χρησιμοποιηθεί, οι LSRs βασίζονται στην απόφαση των routing πρωτόκολλων για την καλύτερη διαδρομή.

Για κάθε δρομολογητή, στο πίνακα δρομολόγησης, βρίσκει τις αντίστοιχες πληροφορίες ετικέτας στον LIB, βασιζόμενο στην διεπαφή εξόδου (outgoing interface) και στο next-hop δρομολογητή που περιλαμβάνεται στην διαδρομή. Έτσι προσθέτει την αντίστοιχη πληροφορία ετικέτας στον FIB και LFIB.

Ακολουθεί ένα παράδειγμα από ένα πίνακα FIB και LFIB για το δίκτυο 10.3.3.0



FIB

```
PE1# show ip cef 10.3.3.0
10.3.3.0/24, version 65, epoch 0, cached adjacency to Serial0/0/1
0 packets, 0 bytes
  tag information set
    local tag: 24
    fast tag rewrite with Se0/0/1, point2point, tags imposed: {22}
  via 192.168.12.2, Serial0/0/1, 0 dependencies
    next hop 192.168.12.2, Serial0/0/1
    valid cached adjacency
    tag rewrite with Se0/0/1, point2point, tags imposed: {22}
```

Εικόνα 8 : FIB πίνακας για το δίκτυο 10.3.3.0

Ο PE1 λαμβάνει ένα πακέτο χωρίς ετικέτα και προωθεί το πακέτο αυτό στον P1 με την ετικέτα 22.

LFIB

```
P1# show mpls forwarding-table 10.3.3.0/24
Local  Outgoing    Prefix           Bytes tag  Outgoing    Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
22     39          10.3.3.0/24      0          Se0/1/0     point2point
P1# show mpls ldp bindings 10.3.3.0/24
  tib entry: 10.3.3.0/24, rev 30
        local binding:  tag: 22
        remote binding: tsr: 1.1.1.1:0, tag: 24
        remote binding: tsr: 4.4.4.4:0, tag: 86
        remote binding: tsr: 3.3.3.3:0, tag: 39
```

Εικόνα 9 : LFIB πίνακας για το δίκτυο 10.3.3.0

Παραπάνω βλέπουμε πώς ο P1 ανταλλάσει (swap) την εισερχόμενη ετικέτα 22 με την εξερχόμενη ετικέτα 39 και στην δεύτερη εντολή (show mpls ldp bindings 10.3.3.0/24) βλέπουμε πάλι τις εγγραφές του LIB πίνακα για την διαδρομή προς το 10.3.3.0/24.

Σημαντικό επίσης θα είναι να ελέγξουμε την λειτουργία της αφαίρεσης ετικέτας (pop). Έχοντας πάλι σαν βάση την παραπάνω τοπολογία ας εστιάσουμε στον PE2. Όταν λαμβάνει ένα πακέτα με ετικέτα από τον P1 (39) τότε ο PE2 θα προσπαθήσει να χρησιμοποιήσει τον δικό του LFIB για να προωθήσει το πακέτο. Τότε ο PE2 αντιλαμβάνεται εύκολα ότι πρέπει να αφαιρέσει (pop) την ετικέτα και να προωθήσει το πακέτο χωρίς ετικέτα από την διεπαφή (interface) Fa0/1. Αυτό γίνεται γιατί ο PE2 δεν έχει ενεργοποιήσει τη λειτουργία MPLS στην διεπαφή Fa0/1 και επίσης δεν είχε μάθει καμία ετικέτα από τον CE2.

Όπως βλέπουμε και παρακάτω σαν outgoing η τιμή είναι Untagged που σημαίνει πως δεν υπάρχει κάποια ετικέτα που θα τοποθετηθεί στο πακέτο αυτό από αυτόν τον δρομολογητή κατά την προώθησή του.

```
PE2# show mpls forwarding-table 10.3.3.0/24
Local  Outgoing    Prefix           Bytes tag  Outgoing    Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
39     Untagged    10.3.3.0/24      0          Fa0/1       192.168.36.6
```

Εικόνα 10 : MPLS πίνακας δρομολόγησης

3. VPN Τεχνολογία

Τα Ιδεατά Ιδιωτικά Δίκτυα (Virtual Private Networks – VPNs) που βασίζονται στο Internet Πρωτόκολλο (IP) έχουν αναδυθεί σαν μια από τις ταχύτερα αναπτυσσόμενες και πιο δημοφιλείς υπηρεσίες για τις επικοινωνίες των επιχειρήσεων. Η εμφάνιση των IP VPNs μπορεί να αποδοθεί σε δύο παράγοντες: συνθήκες αγοράς και τεχνική ανάπτυξη.

Οι συνθήκες της αγοράς επιβάλλουν μια ανάγκη για λύσεις Δικτύων Ευρείας Περιοχής (Wide Area Networks – WAN) που επιτρέπουν στους υπαλλήλους που βρίσκονται διασπαρμένοι σε όλο τον κόσμο να επικοινωνούν σα να βρίσκονταν στο ίδιο γραφείο. Ταυτόχρονα, όμως, οι υπάρχουσες WAN τεχνολογίες ανάμεσα στα κέντρα των επιχειρήσεων και στα γραφεία των διακλαδώσεων είναι κάπως περιορισμένες.

Η εμφάνιση της VPN τεχνολογίας σε ένα τέτοιο περιβάλλον παρουσιάζεται σαν την καλύτερη λύση. Η χρονική στιγμή είναι η ιδανική μια και το Internet πρωτόκολλο αποτελεί τη βάση για πολλές υπηρεσίες στις οποίες βασίζονται οι σημερινές επιχειρήσεις. Χωρίς να βασίζονται σε ένα δίκτυο με ακριβές μισθωμένες γραμμές, ή μόνιμα ιδεατά κυκλώματα (Permanent Virtual Circuits – PVCs), τα VPNs επιτρέπουν μια χαμηλού κόστους επικοινωνία και χρησιμοποιούν νέες web-based εφαρμογές για αποδοτικότερη λειτουργία.

Τα σημερινά VPNs υλοποιούνται βάση ενός μοντέλου στο οποίο ο παροχέας υπηρεσιών δίνει σε έναν πελάτη της εταιρείας τη δυνατότητα σύνδεσης πολλών τοποθεσιών χρησιμοποιώντας ένα ιδιωτικό WAN IP δίκτυο. Προς το παρόν, τα IP δίκτυα των επιχειρήσεων τοποθετούνται στην κορυφή του δικτύου κορμού του παροχέα υπηρεσιών. Το δίκτυο της επιχείρησης είναι το υψηλότερο επίπεδο (επίπεδο δικτύου) ενώ το δίκτυο κορμού είναι το χαμηλότερο επίπεδο (επίπεδο διασύνδεσης δεδομένων). Και τα δύο δίκτυα υπάρχουν, αλλά ανεξάρτητα το ένα από το άλλο. Η επιχείρηση εγκαθιστά την επικοινωνία μεταξύ των δρομολογητών

χρησιμοποιώντας κάποιο IGP και ο παροχέας υπηρεσιών αντιμετωπίζει την πληροφορία δρομολόγησης σαν απλά επιπλέον δεδομένα.

Ένας από τους παράγοντες κλειδιά που συνέβαλαν στην εξάπλωση των VPNs και των υπηρεσιών που βασίζονται σε IP είναι η πρωτοφανής ζήτηση για εύρος ζώνης. Καθώς όλο και περισσότερο εύρος ζώνης γίνεται διαθέσιμο, δημιουργούνται όλο και περισσότερες εφαρμογές που απαιτούν αυξημένο εύρος ζώνης. Η ζήτηση για αυτές τις εφαρμογές αυξάνει περαιτέρω την ανάγκη για περισσότερο εύρος ζώνης. Καθώς το εύρος ζώνης γίνεται όλο και πιο άφθονο, νέες τεχνολογίες που βασίζονται στη διαθεσιμότητά του, όπως οι IP εφαρμογές και τα VPNs, κάνουν την εμφάνισή τους.

Η νέα τεχνολογία που αντιπροσωπεύεται από τα VPNs προσπαθεί να εφαρμόσει τεχνικές κρυπτογραφίας, κατηγοριοποίησης των πληροφοριών και κατανομής υπηρεσιών σε κατηγορίες χρηστών με τέτοιο τρόπο ώστε να αντιμετωπίζει ως ένα βαθμό τα προβλήματα της υποδομής η οποία τελικά αναλαμβάνει την μεταφορά της πληροφορίας. Τα VPNs προσφέρουν ένα χαμηλού κόστους, κλιμακώμενο και διαχειρίσιμο τρόπο για δημιουργία ιδιωτικών δικτύων πάνω από μια δημόσια υποδομή όπως είναι το Internet ή πάνω από το Frame Relay, ATM ή IP δίκτυο ενός παροχέα υπηρεσιών. Ωστόσο, δε θα αποτελούν μια βιώσιμη λύση εκτός κι αν μπορούν να εγγυηθούν ένα προβλέψιμο εύρος ζώνης, αξιοπιστία και ασφάλεια στους χρήστες.

4. Εφαρμογές του MPLS

Οι βασικές εφαρμογές του MPLS είναι οι εξής:

- Traffic Engineering
- MPLS VPNs
- Quality of Service (QoS)

4.1 MPLS Traffic Engineering

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

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

Υπάρχουν πολλοί λόγοι γιατί οι διαχειριστές δικτύων επιθυμούν να επηρεάζουν τα χαρακτηριστικά ενός μονοπατιού, ένας από τους οποίους είναι η βελτιστοποίηση της χρήσης των δικτυακών πόρων. Ο σκοπός είναι απλός: **αποφυγή της κατάστασης όπου ορισμένα τμήματα του δικτύου παρουσιάζουν συμφόρηση όταν άλλα υπό-χρησιμοποιούνται**. Άλλοι σημαντικοί λόγοι είναι το μονοπάτι να

διαθέτει ορισμένους περιορισμούς – constraints (παράδειγμα να μην κάνει χρήση συνδέσμων μεγάλης καθυστέρησης), ώστε σε περιπτώσεις κατάρρευσης γραμμής να εξασφαλίζεται δίκαιη προτεραιότητα κατά τη διανομή της κίνησης. Μέσα από τη διαδικασία αυτή του Traffic Engineering προσφέρονται νέες υπηρεσίες με εκτεταμένες εγγυήσεις ποιότητας υπηρεσιών, ενώ μειώνονται οι επενδύσεις σε νέους δικτυακούς πόρους, όπως εύρος ζώνης, μέσω της βελτιστοποίησης της χρήσης ήδη υπαρχόντων. Έχει αποδειχθεί στη πράξη ότι η τεχνολογία του MPLS, και κατ'επέκτασιν ο διάδοχος του το Generalized, προσφέρουν την απαιτούμενη επιχειρησιακή ευελιξία ταυτόχρονα με την απλότητα για την υλοποίηση πολύπλοκων πολιτικών ΤΕ.

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

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

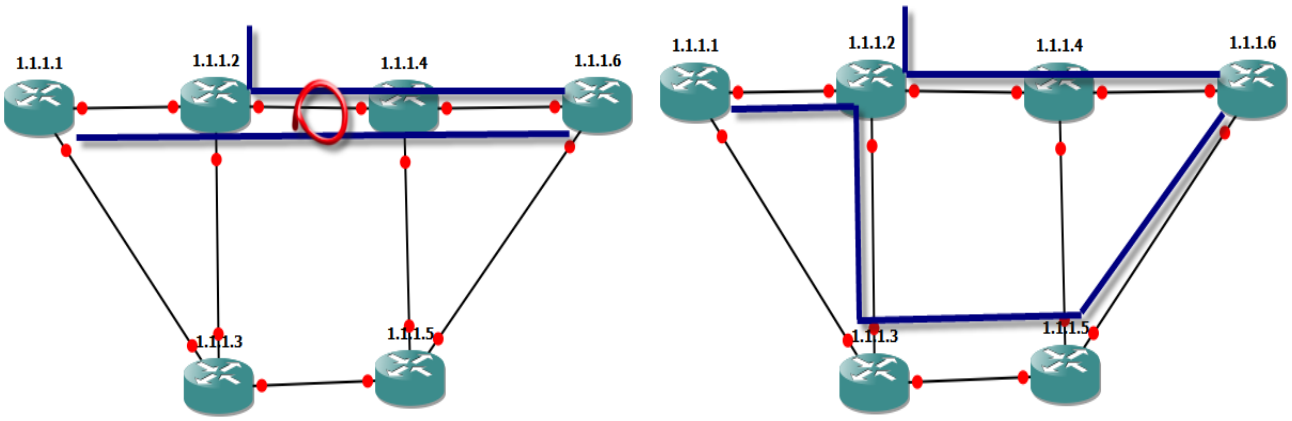
Όσον αφορά τις προτεραιότητες των LSPs το MPLS-TE καθορίζει 8 επίπεδα, με το 0 ως το βέλτιστο και το 7 ως το χειρότερης προτεραιότητας. Ένα LSP διαθέτει δύο priorities: το **setup priority** και το **hold priority**. Ο πρώτος τύπος προτεραιότητας είναι υπεύθυνος για τον έλεγχο των πόρων τη στιγμή που ένα

μονοπάτι εγκαθιδρύεται, ενώ ο δεύτερος πραγματοποιεί έλεγχο της πρόσβασης στους πόρους σε ένα LSP που έχει ήδη εγκαθιδρυθεί. Όταν ένα μονοπάτι αρχικοποιείται εάν δεν υπάρχουν διαθέσιμα αρκετά resources, το setup priority του νέου LSP συγκρίνεται με το hold priority των ήδη υπαρχόντων μονοπατιών που κάνουν χρήση των πόρων στο δίκτυο, ώστε να διαπιστωθεί αν πράγματι μπορεί να κάνει preempt τα υπάρχοντα LSPs και να πάρει τους πόρους τους. Εάν κάτι τέτοιο επιτευχθεί τα υπόλοιπα LSPs αποτρέπονται. Έχει αποδειχθεί μάλιστα ότι αναθέτοντας ένα σημαντικό hold priority, έστω 0, και ένα λιγότερο σημαντικό setup priority, έστω 7, σε ένα LSP, κάτι τέτοιο εξασφαλίζει δικτυακή σταθερότητα. Αυτό είναι το αποτέλεσμα του ανταγωνισμού των μονοπατιών για πόρους σε ένα δικτυακό περιβάλλον, ιδιαίτερα μάλιστα ύστερα από περιπτώσεις αστοχίας όπως κατάρρευση γραμμής.

Όπως αναφέρθηκε και σε προηγούμενες ενότητες στο IGP(Interior Gateway Protocol) σύνολο πρωτοκόλλων, όπως στο **OSPF(Open Shortest Path First)** ή **IS–IS (Intermediate System to Intermediate System)**, ένα μονοπάτι επιλέγεται με τέτοιο τρόπο ώστε το άθροισμα του συνολικού κόστους που κατανέμεται σε κάθε σύνδεσμο να είναι το ελάχιστο. Το μονοπάτι αυτό δεν αλλάζει ακόμη και όταν οι συνθήκες κίνησης στο δίκτυο αλλάξουν, και τα πακέτα μεταφέρονται κατά μήκος του ακόμη και με τη παρουσία συμφόρησης.

Στην παρακάτω εικόνα (Εικόνα 11) διακρίνουμε ένα παράδειγμα όπου κίνηση από τον δρομολογητή 1. 1. 1. 2 στον δρομολογητή 1. 1. 1. 6, και αντίστοιχα από τον 1. 1. 1. 1 στον 1. 1. 1. 6, συγκρούονται, δημιουργώντας συμφόρηση. Σε αυτή τη περίπτωση είναι εφικτό να αποφύγουμε τη δημιουργία αυτής της συμφόρησης με το να αλλάξουμε το μονοπάτι από τον 1. 1. 1. 1 router στον 1. 1. 1. 6 όπως φαίνεται στην εικόνα (Εικόνα 12). Επειδή ωστόσο η δρομολόγηση στα IGP πρωτόκολλα καθορίζεται από τη διεύθυνση προορισμού των πακέτων, είναι αδύνατον να αλλάξουμε το μονοπάτι των πακέτων με την ίδια διεύθυνση παραλήπτη. Στο IGP δεν υπάρχει καμία λειτουργικότητα να γίνεται αλλαγή της πορείας του μονοπατιού δυναμικά σε εξάρτηση με τις συνθήκες κίνησης στο δίκτυο, ακόμη και όταν υπάρχει συμφόρηση σε ένα σύνδεσμο και τα πακέτα ακολουθούν

το συντομότερο μονοπάτι. Έτσι η διαδικασία της μεταγωγής μονοπατιού ώστε να λαμβάνονται υπόψιν οι συγκυρίες κυκλοφορίας στο δίκτυο, τεχνική που καλείται όπως είπαμε Traffic Engineering, είναι αδύνατη στο συγκεκριμένο πρωτόκολλο.



Εικόνα 11-12 : IGP και Traffic Engineering δρομολόγηση

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

Η τεχνική του Source Routing έγκειται στην εγκατάσταση ενός LSP πάνω σε ένα προκαθορισμένο μονοπάτι στο MPLS για την αποφυγή συμφόρησης. Η εγκαθίδρυση του LSP πάνω σε ένα μονοπάτι μπορεί να γίνει είτε λαμβάνοντας κάποιες μετρήσεις – συμβάσεις στον κόμβο προέλευσης **(source routing)**, είτε με τον καθορισμό της πληροφορίας δρομολόγησης μέσω μηνυμάτων σηματοδοσίας **(explicit route –ER)**.

4.2 MPLS VPNs

Μία από τις πιο διάσημες MPLS εφαρμογές όπως έχουμε αναφέρει και στην αρχή είναι η MPLS VPN (virtual private networks).Με τον όρο VPN εννοούμε το δίκτυο εκείνο το οποίο χρησιμοποιεί μια υπάρχουσα τηλεπικοινωνιακή υποδομή όπως το διαδίκτυο για να παρέχει ασφαλή διασύνδεση μεταξύ απομακρυσμένων τοποθεσιών και/ή χρηστών.
Τα οφέλη από τη χρήση VPNs συνοψίζονται στα εξής:

- Παρέχουν ασφαλή μετάδοση δεδομένων
- Είναι εύκολα επεκτάσιμα
- Το κόστος λειτουργία τους είναι κατά πολύ μικρότερο από τις παραδοσιακές μισθωμένες γραμμές

Η MPLS VPN εφαρμογή επιτρέπει στον service provider να προσφέρει υπηρεσίες Layer 3 VPN. Ειδικότερα οι service providers αντικαθιστούν παλαιότερες Layer 2 WAN υπηρεσίες όπως Frame Relay και ATM με μία υπηρεσία MPLS VPN. Οι MPLS VPN υπηρεσίες δίνουν την δυνατότητα στους service providers να παρέχουν ένα ευρύ φάσμα από επιπρόσθετες υπηρεσίες στους πελάτες τους επειδή είναι ενήμερες (MPLS VPNs υπηρεσίες) για τις Layer 3 διευθύνσεις στα σημεία / τοποθεσίες των πελατών. Επιπρόσθετα μπορούν να εξακολουθούν να παρέχουν την προστασία προσωπικών δεδομένων που υπάρχουν στις Layer 2 WAN υπηρεσίες.

Τα ιδιωτικά ιδεατά δίκτυα τυπικά κατασκευάζονται με χρήση τεσσάρων βασικών δομικών τμημάτων:

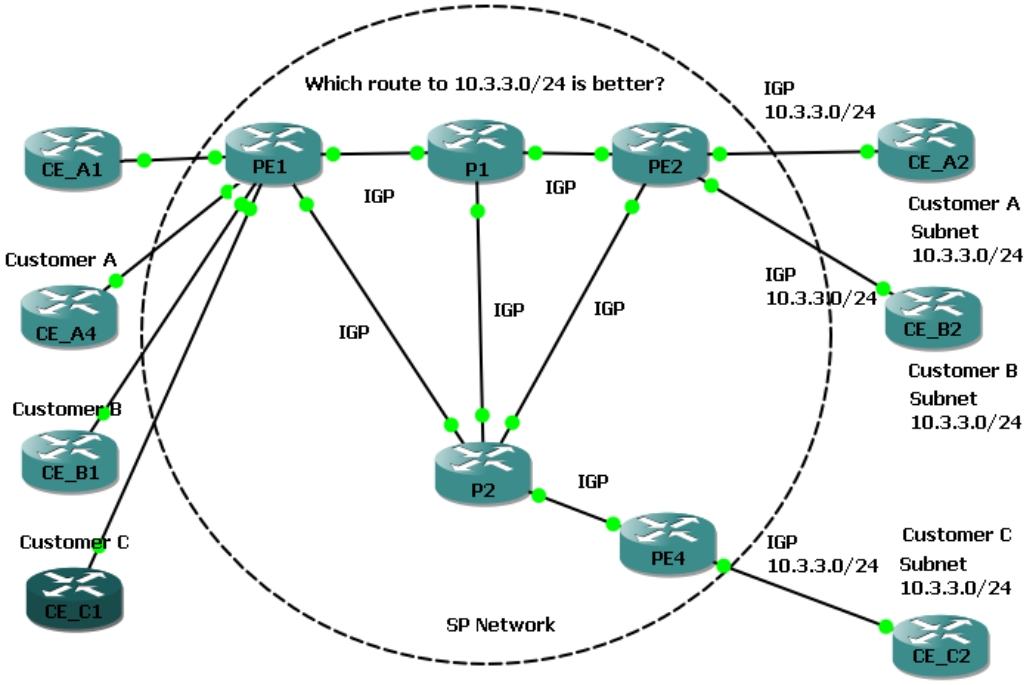
1. Τοίχους προστασίας (Firewalls) για την προστασία του δικτυακού τόπου κάθε πελάτη και την παροχή ασφαλούς τρόπου διασύνδεσης με το διαδίκτυο.

2. Πιστοποίηση για την επαλήθευση του γεγονότος ότι ο δικτυακός τόπος ενός πελάτη ανταλλάσσει δεδομένα μόνο με εξουσιοδοτημένους απομακρυσμένους τόπους.
3. Κρυπτογράφηση για την προστασία δεδομένων από υποκλοπή ή παρακολούθηση κατά τη μεταφορά τους κατά μήκος του διαδικτύου.
4. Tunneling encapsulation για την παροχή υπηρεσίας μεταφοράς πολλαπλών πρωτοκόλλων και την δυνατότητα χρήσης ιδιωτικού χώρου IP διευθύνσεων μέσα σε ένα VPN.

Το πρόβλημα που ακούει στο όνομα Διπλές περιοχές διευθύνσεων πελατών (Duplicate Customer Address Ranges)

Όταν ο Service Provider συνδέεται σε ένα ευρύ φάσμα από πελάτες χρησιμοποιώντας Layer 2 WAN υπηρεσίες όπως Frame Relay ή ATM, δεν ενδιαφέρεται για τις IP διευθύνσεις και για τα υποδίκτυα που χρησιμοποιούνται από τους πελάτες. Παρόλο αυτά προκειμένου να μεταναστεύσουν αυτοί οι πελάτες σε Layer 3 WAN υπηρεσίες, ο SP (service provider) πρέπει να μάθει τις περιοχές διευθύνσεων από τους διάφορους πελάτες και μετά να διαφημίσει αυτά τα δρομολόγια / διαδρομές στο δίκτυο του SP. Ωστόσο ακόμα και αν ο SP ήθελε να ξέρει για όλα τα υποδίκτυα από όλους τους πελάτες του, πολλές εταιρίες χρησιμοποιούν το ίδιο εύρος διευθύνσεων, δηλαδή τις ιδιωτικές IP διευθύνσεις, συμπεριλαμβανομένου και του ολοένα και πιο δημοφιλούς δικτύου 10.0.0.0.

Ας δούμε το παρακάτω παράδειγμα για να παρουσιάσουμε καλύτερα το πρόβλημα.



Εικόνα 13 : MPLS VPN

Ο πρώτος και πιο βασικός στόχος για την Layer 3 VPN υπηρεσία είναι να επιτρέπει στους πελάτες “Customer A” να επικοινωνούν μόνο μεταξύ τους. Παρόλο αυτά στην τοπολογία που βλέπουμε παραπάνω αυτός ο στόχος αποτυγχάνει για πολλούς λόγους. Λόγω της επικάλυψης των χώρων διευθύνσεων πολλοί δρομολογητές θα βρεθούν αντιμέτωποι με το δίλημμα της επιλογής μιας διαδρομής προς το δίκτυο 10.3.3.0/24 ως την καλύτερη διαδρομή και να αγνοήσουν την διαδρομή προς το ίδιο δίκτυο που έχουν μάθει από κάποιον άλλο πελάτη. Για παράδειγμα, ο PE2 θα μάθει από δύο διαφορετικούς πελάτες το ίδιο δίκτυο (πρόθεμα), 10.3.3.0/24. Εάν ο PE2 επιλέξει μία από τις δύο πιθανές διαδρομές, για παράδειγμα την διαδρομή για τον CE-A2 ως την καλύτερη διαδρομή, τότε ο PE2 δεν θα μπορεί να προωθήσει πακέτα στον πελάτη B με δίκτυο 10.3.3.0/24 του CE-B2 δρομολογητή. Επίσης, η χειρότερη ενδεχομένως επίδραση είναι ότι οι χρήστες (hosts) από την μία πλευρά ενός πελάτη να μπορούν να αποστέλλουν και να λαμβάνουν πακέτα, με χρήστες (hosts) σε δίκτυο άλλου πελάτη. Μετά από αυτό το παράδειγμα οι χρήστες των πελατών B και C θα μπορούσαν να προωθήσουν

πακέτα στο υποδίκτυο 10.3.3.0/24, και οι δρομολογητές να προωθήσουν αυτά τα πακέτα στον δρομολογητή CE-A2 του πελάτη Α.

Η λύση στο παραπάνω πρόβλημα έρχεται να δοθεί με το **MPLS VPN.** Τα πρότυπα που ορίζονται από το MPLS VPN επιλύουν τα προβλήματα που είδαμε παραπάνω και παρέχουν ακόμα ένα μεγάλο σύνολο χαρακτηριστικών. Ειδικότερα ορίζουν την έννοια της χρησιμοποίησης πολλαπλών πινάκων δρομολόγησης που ονομάζονται Virtual Routing and Forwarding tables (VRF tables), οι οποίοι διαχωρίζουν τις διαδρομές ανά πελάτη ούτως ώστε να αποφευχθεί το θέμα των διπλών περιοχών (διπλού εύρους) διευθύνσεων.

Τρία διαφορετικά είδη δρομολογητών συναντάμε στα MPLS VPNs:

- **Δρομολογητές CE (customer edge)**. Είναι οι δρομολογητές που τους διαχειρίζεται ο πελάτης και ανήκουν συνήθως σε αυτόν.

- **Δρομολογητές PE (provider edge)**. Είναι οι δρομολογητές που αποτελούν τα σημεία εισόδου και εξόδου των VPNs. Ανήκουν διαχειριστικά στον ISP. Αποτελούν το πιο σημαντικό τμήμα στη «λογική» των MPLS VPNs.

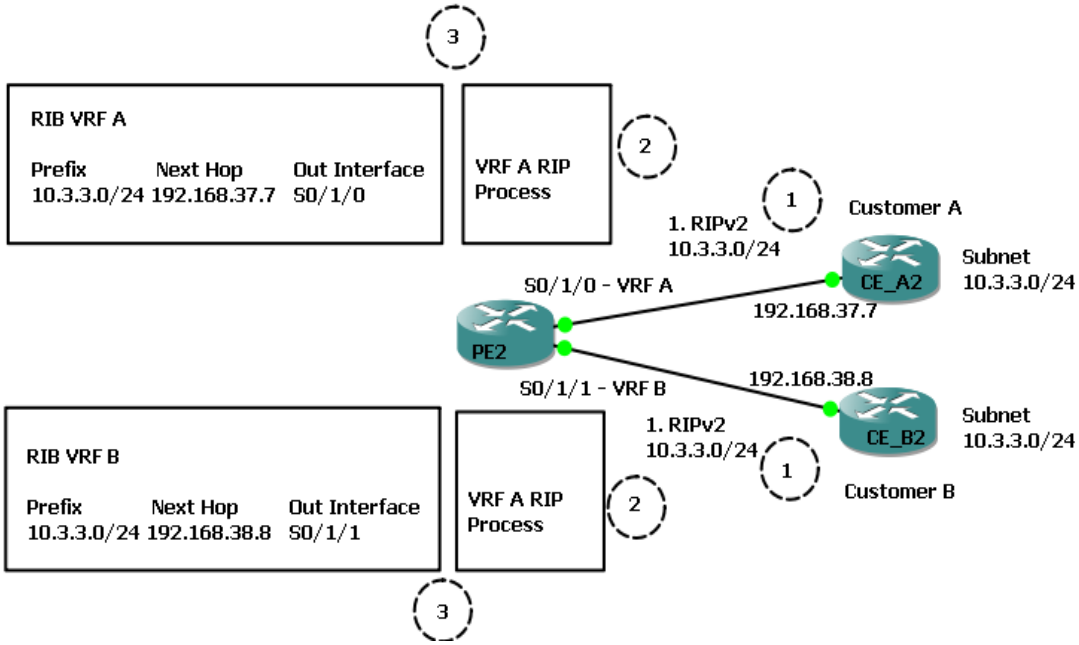
- **Δρομολογητές P (provider)**. Είναι οι δρομολογητές που αποτελούν το δίκτυο κορμού του ISP και ανήκουν και αυτοί διαχειριστικά σε αυτόν. Δεν συμμετέχουν στη λογική VPN - ο κύριος σκοπός τους είναι η προώθηση των MPLS ετικετών προς τους PE routers.

Το κλειδί για την κατανόηση της γενικής ιδέας για το πώς το MPLS VPN λειτουργεί είναι στο να εστιάσουμε στο επίπεδο ελέγχου μεταξύ των δρομολογητών PEs και Ps. Τόσο οι PEs όσο και οι Ps χρησιμοποιούν LDP και κάποιο IGP πρωτόκολλο για την υποστήριξη IP δρομολόγησης. Παρόλο αυτά το IGP διαφημίζει διαδρομές μόνο από υποδίκτυα μέσα στο MPLS δίκτυο χωρίς να περιλαμβάνει διαδρομές που βρίσκονται σε επίπεδο πελατών. Ως εκ τούτου οι δρομολογητές P και PE μπορούν

μαζί να προωθούν πακέτα από τον εσωτερικό PE στον εξωτερικό PE (ingress PE to egress PE).

Οι PEs έχουν αρκετά άλλα καθήκοντα, καθώς, όλοι προσανατολίζονται προς το θέμα της μάθησης των διαδρομών των πελατών και την παρακολούθηση για το ποιες διαδρομές ανήκουν σε ποιους πελάτες. Οι PEs ανταλλάσουν διαδρομές με τους συνδεδεμένους δρομολογητές CE διαφόρων πελατών χρησιμοποιώντας είτε EBGP, RIPv2, OSPF σημειώνοντας το ποια διαδρομή έχουν μάθει από ποιόν πελάτη. Για την αποφυγή των επικαλυπτόμενων δικτύων (προθεμάτων / prefixes),όπως αναφέραμε παραπάνω οι PEs δρομολογητές δεν καταχωρούν τις διαδρομές στον κανονικό πίνακα δρομολόγησης, αλλά, τις αποθηκεύουν σε ξεχωριστούς ανά πελάτη πίνακες δρομολόγησης που ονομάζονται VRFs. Στη συνέχεια διαφημίζουν αυτές τις διαδρομές και στους υπόλοιπους PEs δρομολογητές αλλά ποτέ προς του Ps δρομολογητές.

Ας δούμε το παρακάτω παράδειγμα για να καταλάβουμε την έννοια των VRFs.



* RIB = IP Routing table

Εικόνα 14 : MPLS VRF

Στο παραπάνω κομμάτι δικτύου έχουμε τον PE2 να χρησιμοποιεί RIPv2 ως IGP πρωτόκολλο και για τους δύο πελάτες (CE-A2 και CE-B2).
Τα βήματα που σημειώνονται περιγράφονται παρακάτω:

1. Ο CE δρομολογητής ο οποίος δεν έχει καθόλου γνώση για MPLS διαφημίζει την διαδρομή για το δίκτυο 10.3.3.0/24, με RIPv2 όπως αναφέραμε παραπάνω.
2. Η RIPv2 ενημέρωση φτάνει στην διεπαφή (interface) S0/1/0 του PE2 η οποία έχει ανατεθεί στον VRF του πελάτη A, VRF-A. Ο PE2 χρησιμοποιεί ξεχωριστή RIP διαδικασία για κάθε VRF. Ομοίως για το VRF-B αναλύει την ενημέρωση που λαμβάνει από τον CE-B2 στην διεπαφή S0/1/1.
3. Στο στάδιο 3 η διαδικασία του VRF-A RIP προσθέτει μια καταχώρηση για το δίκτυο 10.3.3.0/24 στον RIB για το VRF-A. Ομοίως και για το VRF-B

4.2.1 L3VPNs

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

- VPN Routing και Forwarding Tabled (VRFs)
- Διανομή διαδρομών με τη χρήση του BGP
- Route Distinguisher (RD)
- Route Targets (RT)
- Προώθηση επισημασμένων πακέτων

VPN Routing και Forwarding Tabled (VRFs)

Τη λειτουργία των VRFs την είδαμε και παραπάνω πιο αναλυτικά και με παράδειγμα.

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.

Διανομή διαδρομών με τη χρήση του BGP

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

- Υποστηρίζει φιλτράρισμα διαδρομών. Δηλαδή μπορεί να κάνει περιορισμένη διανομή των πληροφοριών δρομολόγησης.
- Έχει τη δυνατότητα να μεταφέρει ένα μεγάλο πλήθος διαδρομών και έτσι να 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 δρομολογητών.
- Είναι ικανό να μεταφέρει ετικέτες σύμφωνα με τις διαδρομές.

Route Distinguisher (RD)

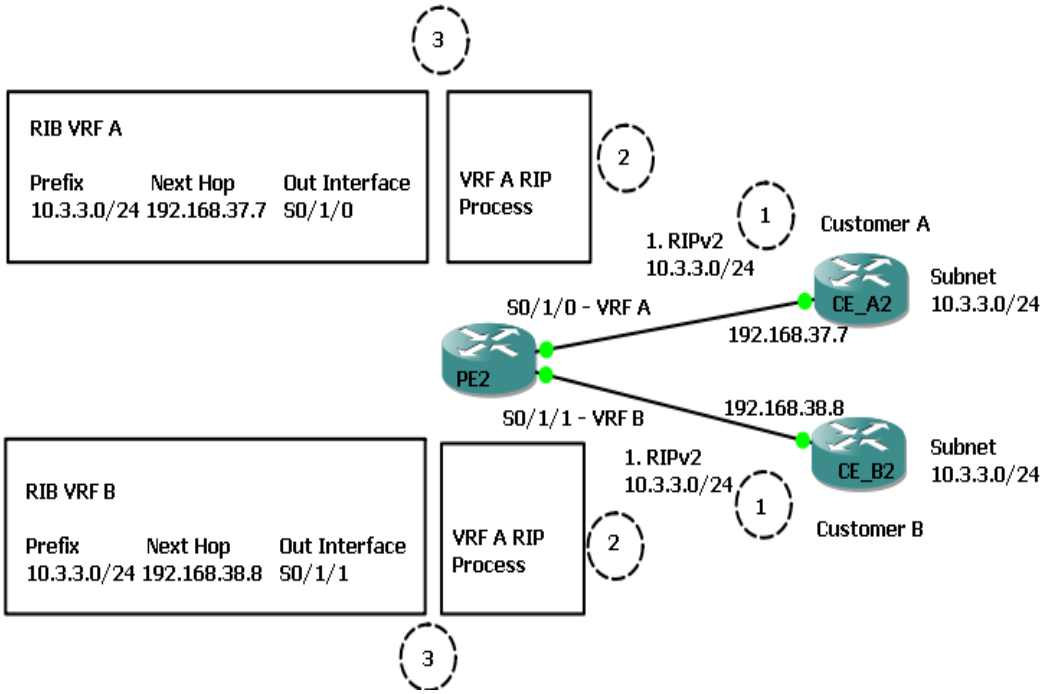
Όπως αναφέραμε και στην αρχή της ενότητας του MPLS VPN, το ίδιο σου δίνει την δυνατότητα να χρησιμοποιήσεις το ίδιο MPLS backbone για διάφορους πελάτες ή υπηρεσίες χωρίς το καθένα να αλληλεπιδρά με το άλλο. Είναι πολύ συνηθισμένο να βρεις διαφορετικούς πελάτες να χρησιμοποιούν το ίδιο εύρος ιδιωτικών IP διευθύνσεων. Εδώ λοιπόν έρχεται το πρώτο απαραίτητο στοιχείο:

“Οι διευθύνσεις από κάθε τοποθεσία πρέπει να είναι μοναδικές μέσα στο δίκτυο που ανήκουν.”

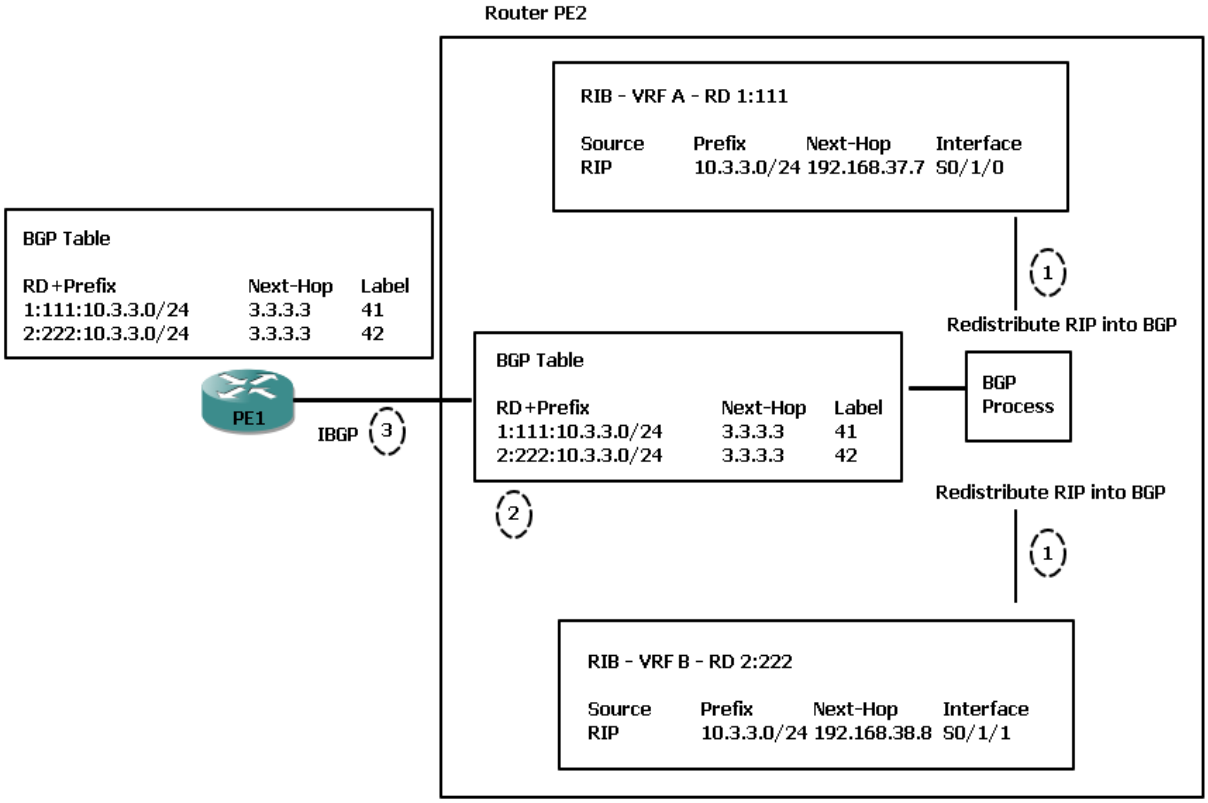
Δύο πελάτες μπορεί να χρησιμοποιούν τι ίδιο εύρος ιδιωτικών διευθύνσεων, έτσι πρέπει να προσθέσουμε κάτι σε κάθε διεύθυνση ώστε να την κάνουμε μοναδική από τις υπόλοιπες. Η λύση σε αυτό είναι η χρήση του Route Distinguisher (RD).

Με τον Route Distinguisher (RD) μετατρέπουμε μια διεύθυνση 32bits σε μία των 96bits μοναδική στο δίκτυο με αποτέλεσμα οι PEs δρομολογητές να μην ανακοινώνουν 32bit διευθύνσεις αλλά 96bits.

Στην συνέχεια βλέπουμε πρακτικά την λειτουργία του Route Distinguisher (RD)



Εικόνα 15 : Route Distinguisher (1)



Εικόνα 16 : Route Distinguisher (2)

1. Ο PE2 δρομολογητής διανέμει κάθε VRF στο BGP.
2. Κατά τη διαδικασία της διανομής παίρνει το RD από το αντίστοιχο VRF και περιλαμβάνει αυτό το RD με όλες τις διαδρομές που διαφημίστηκαν από τον VRF πίνακα δρομολόγησης.
3. Ο PE2 χρησιμοποιεί IBGP για να διαφημίσει αυτές τις διαδρομές στον PE1 προκαλώντας στον PE1 να γνωρίζει και τις δύο διαδρομές για το 10.3.3.0/24, καθεμιά με διαφορετική τιμή RD.

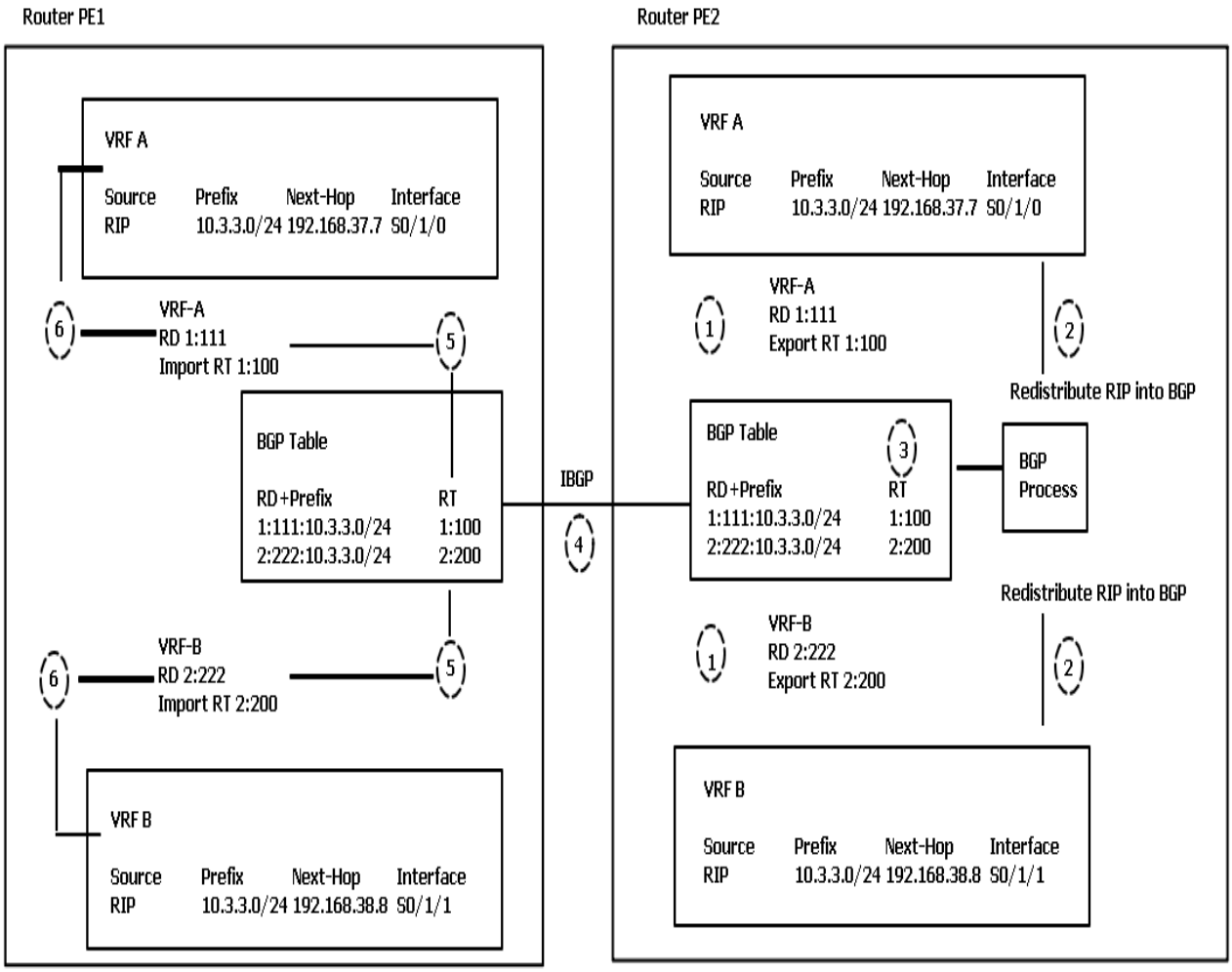
Route Targets (RT)

Τα MPLS RTs ενεργοποιούν την δυνατότητα να επιτρέπει σε μερικές τοποθεσίες να είναι προσβάσιμες από πολλαπλά VPNs. Ελέγχει δηλαδή την επικοινωνία μεταξύ διαφορετικών περιοχών VPN.

Ένας γενικός ορισμός του σκοπού των RTs είναι ότι:

"Το MPLS χρησιμοποιεί Route Targets για να καθορίσει σε ποια VRFs ένας PE δρομολογητής θα τοποθετήσει τις διαδρομές που έμαθε από το IBGP (internal BGP)"

Η παρακάτω εικόνα (Εικόνα 17) δείχνει το πώς οι PEs δρομολογητές χρησιμοποιούν τα RTs για να καθορίσουν σε ποια VRFs μια διαδρομή προστέθηκε. Στην περίπτωση αυτή δείχνει ένα export RT με διαφορετική τιμή για κάθε VRF του PE2 (VRF-A & VRF-B). Στον PE1 βλέπουμε το import RT για κάθε VRF το οποίο επιτρέπει στον PE1 να επιλέξει ποιες εγγραφές του BGP πίνακα πηγαίνουν στο κάθε VRF του.



Εικόνα 17 : Route Target

Αναλυτικά έχουμε τα εξής :

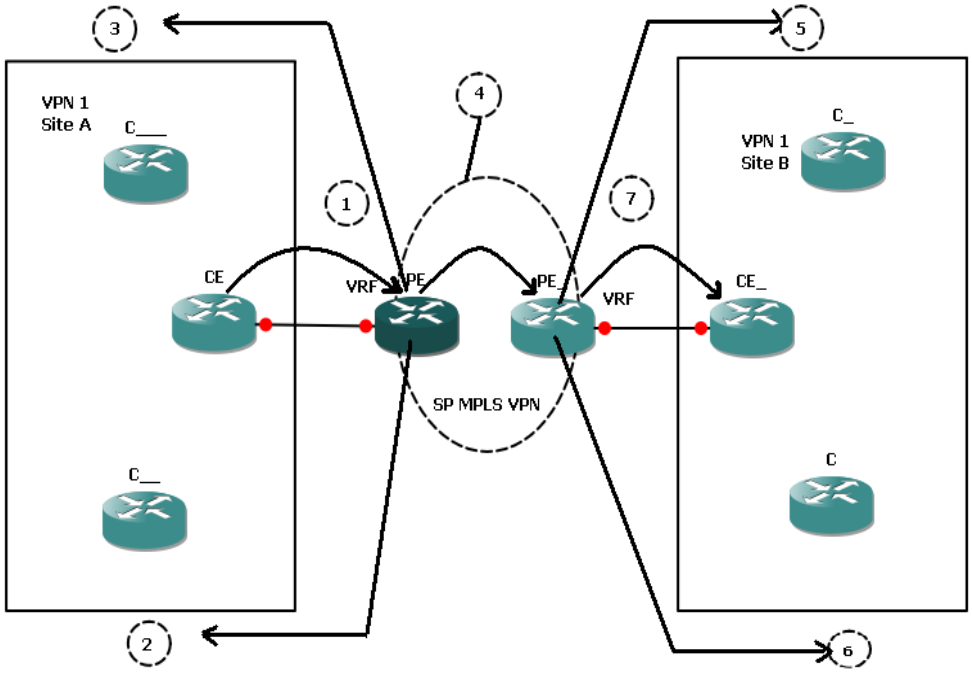
1. Οι δύο VRFs στον PE2 έχουν διαμορφωθεί με μία RT τιμή.
2. Διανέμονται στο BGP τα VRFs
3. Κατά την διαδικασία την διανομής στο BGP θέτονται οι κατάλληλες τιμές RT.
4. Ο PE2 διαφημίζει τις διαδρομές με IBGP
5. Ο PE1 εξετάζει τις καινούριες εγγραφές του BGP πίνακα και συγκρίνει τις RT τιμές με τις καθορισμένες τιμές RT που έχουν εισαχθεί, όπου προσδιορίζεται ποιες εγγραφές από τον BGP πίνακα πρέπει να πάνε σε ποιο VRF.
6. Ο PE1 διανέμει τις διαδρομές στα αντίστοιχα VRFs, ειδικά τις διαδρομές των οποίων τα RT ταιριάζουν με τα καθορισμένα RT στα VRFs (import RT).

Προώθηση επισημασμένων πακέτων
Διάδοση Διαδρομών σε ένα MPLS VPN

Οι VRF πίνακες διαχωρίζουν τις διαδρομές των πελατών στους PE δρομολογητές. Η προσθήκη του RD που αναλύσαμε παραπάνω συντελεί στην ασφαλή μεταφορά των διαδρομών μέσω του MPLS VPN δικτύου.

Ένας PE δρομολογητής λαμβάνει τις διαδρομές από έναν CE δρομολογητή μέσω ενός IGP. Αυτές οι διαδρομές από την VPN περιοχή τοποθετούνται στον VRF πίνακα δρομολόγησης. Ο VRF που θα χρησιμοποιηθεί για μια συγκεκριμένη περιοχή εξαρτάται από τις ρυθμίσεις που έχουν γίνει στον PE δρομολογητή. Στις διαδρομές ενός VRF προστίθεται και το RD που έχει ρυθμιστεί για αυτόν τον πίνακα και σχηματίζονται οι VPN διαδρομές οι οποίες διαφημίζονται με το BGP στους υπόλοιπους PE δρομολογητές του MPLS VPN δικτύου.

Η όλη διαδικασία περιγράφεται και φαίνεται πιο αναλυτικά στην παρακάτω τοπολογία (Εικόνα 18):



Εικόνα 18 : Διάδοση Διαδρομών σε ένα MPLS VPN

1. Ο CE δρομολογητής διαφημίζει στον PE μέσω IGP τις διαδρομές του.
2. Οι διαδρομές αυτές καταχωρούνται στον VRF πίνακα δρομολόγησης του PE.
3. Στη συνέχεια διανέμονται εκ νέου μέσα στο BGP. Ένα RD προστίθεται στις διαδρομές για να τις κάνει διαδρομές VPN. Επίσης προστίθεται και ένα RT.
4. Το BGP διαφημίζει τις VPN διαδρομές με μία MPLS ετικέτα και με RT.
5. Τα RT υποδεικνύουν σε ποιο VRF οι διαδρομές εισάγονται. Το RD αφαιρείται από τις VPN διαδρομές.
6. Οι IP διαδρομές εισάγονται στον VRF πίνακα δρομολόγησης.
7. Το IGP διαφημίζει τις IP διαδρομές.

Η προώθηση πακέτων εντός του MPLS VPN είναι βασισμένη στις ετικέτες. Οι P δρομολογητές χρειάζονται μόνο την κατάλληλη πληροφορία για την αντικατάσταση των ετικετών για να προωθήσουν τα πακέτα. Ο πιο συνηθισμένος τρόπος για να γίνει αυτό είναι να ρυθμιστεί το LDP μεταξύ των LSRs και των PEs

δρομολογητών έτσι ώστε όλη η κίνηση να γίνεται βασισμένη στις ετικέτες. Τα πακέτα προωθούνται στον κορμό δικτύου με μία ετικέτα που ορίζει το LSP από τον ingress PE στον egress PE δρομολογητή. Κάθε ενδιάμεσος LSR δε χρειάζεται ποτέ να κάνει κάποια αναζήτηση σχετικά με τη διεύθυνση δικτύου. Αυτός είναι ο τρόπος με τον οποίο γίνεται η μεταγωγή των πακέτων από τον ingress PE δρομολογητή στον egress PE δρομολογητή. Η παραπάνω ετικέτα ονομάζεται IGP ετικέτα γιατί σχετίζεται με κάποιο IP πρόθεμα στον γενικό πίνακα δρομολόγησης των P και PE δρομολογητών.

Ο τρόπος με τον οποίο ο egress PE δρομολογητής καταλαβαίνει σε ποιόν VRF ανήκει το πακέτο, δε βρίσκεται στην IP κεφαλίδα του πακέτου αλλά ούτε προκύπτει από την IGP ετικέτα, η οποία χρησιμοποιείται μόνο για την προώθηση του πακέτου στο δίκτυο. Η λύση είναι η πρόσθεση άλλης μίας ετικέτας στην στοίβα ετικετών του MPLS. Αυτή η ετικέτα προσδιορίζει σε ποιόν VRF πίνακα ανήκει το πακέτο. Έτσι λοιπόν κάθε πακέτο ενός πελάτη προωθείται με δύο ετικέτες: την IGP ετικέτα και την VPN ετικέτα. Η VPN ετικέτα πρέπει να εισαχθεί από τον ingress PE για να μπορέσει ο egress PE να αντιστοιχίσει το πακέτο με ένα VRF πίνακα. Το BGP εκτός από τα VPN προθέματα διαφημίζει επίσης και την VPN ετικέτα που σχετίζεται με το συγκεκριμένο VPN πρόθεμα. Έτσι ο ingress PE γνωρίζει ποια ετικέτα πρέπει να χρησιμοποιήσει.

Πιο συνοπτικά λοιπόν έχουμε:

Για την κίνηση μεταξύ των VRF κάθε πακέτο έχει 2 ετικέτες στο MPLS VPN δίκτυο. Την IGP που διανέμεται με LDP μεταξύ όλων των PE και P δρομολογητών και την VPN που διανέμεται από τον έναν PE στον άλλο. Οι P δρομολογητές χρησιμοποιούν την IGP για να προωθήσουν το πακέτο στον κατάλληλο egress PE δρομολογητή και οι egress PE χρησιμοποιούν την VPN ετικέτα για να προωθήσουν το πακέτο στον κατάλληλο CE δρομολογητή.

4.2.2 L2VPNs

Τα Layer 2 VPN σε αντίθεση με τα Layer 3 VPN, που υποστηρίζουν μόνο IP είναι ικανά να μεταφέρουν οποιοδήποτε πρωτόκολλο μέσω της δικτυακής υποδομής. Επίσης στα Layer 2 VPN δεν υπάρχει η ανάγκη ύπαρξης πινάκων δρομολόγησης στους PE για κάθε συνδεδεμένο VPN διότι δεν αποθηκεύονται πίνακες δρομολόγησης των πελατών στους δρομολογητές του παροχέα υπηρεσιών.

Στο επίπεδο αυτό μιλάμε για μετάδοση πλαισίων επιπέδου 2 (layer 2 frames) πάνω από MPLS. Για να επιτευχθεί αυτό, βασίζεται στην δυνατότητα για **ενθυλάκωση** (encapsulation) και **μεταφορά** (transport) της πληροφορίας για διάφορα πρωτόκολλα επιπέδου 2 πάνω από ένα MPLS δίκτυο.

Υπάρχουν 3 επίπεδα ενθυλάκωσης:

- **Η επικεφαλίδα του τούνελ (tunnel header),** που περιέχει τις πληροφορίες που απαιτούνται για τη μετάδοση της πληροφορίας πάνω από το IP ή το MPLS δίκτυο. Αυτή η επικεφαλίδα καθορίζεται από το πρωτόκολλο που χρησιμοποιείται για το μηχανισμό των τούνελ, π.χ. MPLS.

- **Το πεδίο αποπολυπλεξίας (demultiplexer field),** που χρησιμοποιείται για τον διαχωρισμό των ξεχωριστών εξομοιούμενων εικονικών κυκλωμάτων (Virtual Circuit) μέσα σε ένα τούνελ. Το πεδίο αυτό πρέπει, επίσης, να γίνεται

κατανοητό από το πρωτόκολλο που χρησιμοποιείται για το μηχανισμό των τούνελ, π.χ. μπορεί να είναι μία MPLS ετικέτα (MPLS label).

- **Η ενθυλάκωση του εξομοιούμενου εικονικού κυκλώματος (emulated VC encapsulation),** που περιέχει πληροφορία για την ενθυλακωμένη πληροφορία και η οποία είναι απαραίτητη για την σωστή εξομοίωση του αντίστοιχου πρωτοκόλλου του επιπέδου 2.

Για την **μετάδοση** των πλαισίων από ένα ingress router σε ένα egress router θα πρέπει να δημιουργηθεί ένα LSP. Τοποθετώντας ένα tunnel label μεταφέρεται το πακέτο από τον ingress στον egress router. Η διαδρομή ονομάζεται LSP tunnel. Ο egress δεν καταλαβαίνει το tunnel label και δε μπορεί να αποφασίσει τι θα το κάνει. Έτσι στη αρχή της διαδρομής τοποθετείται ένα label το οποίο ονομάζεται VC Label και το οποίο δεν είναι αντιληπτό μέσα από το δίκτυο MPLS.

Πλεονεκτήματα για τα Layer 2 MPLS VPNs

- Έμφυτη δυνατότητα κλιμάκωσης
- Διαχωρισμός διαχειριστικών αρμοδιοτήτων
- Μυστικότητα πληροφοριών δρομολόγησης
- Ευκολία ρύθμισης
- Ανεξαρτησία από το πρωτόκολλο του επιπέδου 3
- Πραγματικά end-to-end connectivity (ακόμα και για Ethernet επίπεδο διασύνδεσης δεδομένων)

Μειονεκτήματα

- Κάθε δρομολογητής πρέπει να καταλαβαίνει το MPLS
- Πολυπλοκότητα δρομολόγησης για τους πελάτες

4.3 Quality of Service (QoS)

4.3.1 Η αρχιτεκτονική IntServ

Ο όρος ολοκληρωμένες υπηρεσίες ή Integrated Services(IntServ), αναφέρεται σε μια συνολική αρχιτεκτονική QoS, που προτάθηκε από την IETF στα μέσα της δεκαετίας του ’90. Ο σκοπός αυτής της αρχιτεκτονικής είναι η εγγυημένη παροχή του ζητούμενου από τις εφαρμογές επιπέδου ποιότητας υπηρεσίας από άκρη σε άκρη του δικτύου. Για την ικανοποίηση των απαιτήσεων που έχουν οι διάφορες εφαρμογές, αναπτύχθηκε το πρωτόκολλο RSVP, το οποίο λειτουργεί ως μεταφορικό μέσο των αιτήσεων των εφαρμογών για τη παροχή του ζητούμενου επιπέδου QoS.

Για τη σωστή λειτουργία της αρχιτεκτονικής IntServ, απαιτείται η ύπαρξη των κατάλληλων συσκευών δικτύου όπως οι δρομολογητές και οι μεταγωγείς, οι οποίες εκτός από την υποστήριξη του πρωτοκόλλου RSVP, οφείλουν να εκτελούν και τις ακόλουθες λειτουργίες :

-Τη λειτουργία επόπτευσης(Policing).

Η λειτουργία αυτή επιβεβαιώνει ότι η κίνηση δεδομένων πραγματοποιείται σύμφωνα με τις επιταγές που ορίζουν οι προδιαγραφές κίνησης (Traffic Specifications) στα μηνύματα RSVP ενώ σε αντίθετη περίπτωση απορρίπτει τα πακέτα δεδομένων.

-Τον έλεγχο επίτρεψης εισόδου(Admission Control)

Με τη λειτουργία αυτή πραγματοποιείται έλεγχος για το εάν υπάρχουν οι απαιτούμενοι πόροι για το ζητούμενο επίπεδο QoS. Στη περίπτωση που αυτοί δεν υπάρχουν δεν επιτρέπεται η πρόσβαση.

-Την ταξινόμηση των πακέτων(Packet Classification).

Με τη λειτουργία της ταξινόμησης τα πακέτα κατηγοριοποιούνται ανάλογα με το ζητούμενο επίπεδο QoS.

-Τη τοποθέτηση σε ουρές αναμονής και το χρονικό προγραμματισμό εξυπηρέτησης(Packet Queuing & Scheduling)

Με τις λειτουργίες αυτές τα πακέτα τοποθετούνται σε κατάλληλες ουρές αναμονής περιμένοντας εξυπηρέτηση τη κατάλληλη χρονική στιγμή.

Το βασικό χαρακτηριστικό της αρχιτεκτονικής IntServ είναι ότι οι εφαρμογές θα πρέπει να δεσμεύουν τους απαιτούμενους πόρους πριν αποστείλουν τα δεδομένα τους. Αυτό σημαίνει ότι όλες οι συσκευές στη διαδρομή προς το προορισμό, θα πρέπει να τους έχουν δεσμεύσει και να τους διατηρούν δεσμευμένους καθ'όλη τη διάρκεια της συνόδου επικοινωνίας. Συνεπώς σε κάθε συσκευή που μετέχει στη σύνοδο επικοινωνίας θα πρέπει να διατηρείται και το αντίστοιχο διάγραμμα κατάστασης(state flow diagram) για αυτή. Τα παραπάνω αποτελούν μια δραματική αλλαγή στη μέχρι σήμερα ακολουθούμενη πορεία στην αρχιτεκτονική του διαδικτύου, η οποία βασίζεται στη λογική διατήρησης της απλότητας στην υλοποίηση. Με τη μέχρι σήμερα προσέγγιση η πληροφορία που σχετίζεται με τη διατήρηση της κατάστασης της ροής των δεδομένων βρίσκεται μόνο στα τελικά συστήματα. Οι ενδιάμεσοι κόμβοι απλώς προωθούν τα πακέτα προς το τελικό προορισμό.

Η εισαγωγή της αρχιτεκτονικής IntServ αποτελεί μια μεγάλη αλλαγή μιας και η πολυπλοκότητα που θα επιφέρει στα δίκτυα κορμού των παροχέων είναι μεγάλη. Η λύση που προτείνει είναι μέχρι σήμερα αρκετά ακριβή σε κόστος υλοποίησης αλλά και απαιτητική όσον αφορά την υπολογιστική ισχύ που ζητείται από τα στοιχεία του δικτύου. Η άλλη μεγάλη πρόκληση είναι ότι θα πρέπει ταυτόχρονα να αναπτυχθούν και οι αντίστοιχες εφαρμογές που να υποστηρίζουν την αρχιτεκτονική IntServ και να γίνουν αποδεκτές από το ευρύ κοινό.

Στα μειονεκτήματα της αρχιτεκτονικής IntServ θα πρέπει να σημειωθούν τα εξής :

- Το ποσό της πληροφορίας που σχετίζεται με τη κατάσταση των συνόδων επικοινωνίας ,είναι ανάλογο με τον αριθμό των ροών δεδομένων. Αυτό έχει

ως συνέπεια να απαιτείται μεγάλος αποθηκευτικός χώρος(μνήμη) αλλά και αυξημένη υπολογιστική ισχύς στις συσκευές του δικτύου κορμού.

- Για να υπάρχει εγγυημένο επίπεδο QoS από άκρη σε άκρη του δικτύου θα πρέπει όλοι οι δρομολογητές του δικτύου να διαθέτουν τα στοιχεία της αρχιτεκτονικής IntServ(RSVP, Admission Control, Packet Classifier, Packet Scheduler). Αυτό δεν ισχύει μόνο για το δίκτυο ενός παροχέα, αλλά και για τα δίκτυα των υπόλοιπων παροχέων διαμέσου των οποίων μεταφέρεται η πληροφορία στον τελικό προορισμό. Αυτό από μόνο του αποτελεί ένα δύσκολο σημείο στη σχεδίαση, λόγω των συμφωνιών επιπέδου υπηρεσίας(SLAs) που πρέπει να τηρούνται μεταξύ των παροχέων.
- Τέλος απαιτείται η αδιάκοπη και συνεχής ανάπτυξη του δικτύου για την παροχή της εγγυημένης υπηρεσίας, με χρήση πιο ισχυρών υπολογιστικών συστημάτων και πιο αποτελεσματικών τεχνικών δρομολόγησης. Παρά την πολυπλοκότητά της φαίνεται ότι η αρχιτεκτονική IntServ δείχνει το μέλλον για την ανάπτυξη του διαδικτύου και τη μετατροπή του σε ένα δίκτυο παροχής εξελιγμένων υπηρεσιών.

Τάξεις υπηρεσίας στην αρχιτεκτονική IntServ

Στην αρχιτεκτονική IntServ έχουν οριστεί δυο τάξεις υπηρεσίας(Classes of Service):
-Η εγγυημένη υπηρεσία (guaranteed service)
-Η υπηρεσία ελεγχόμενου φορτίου(controled load)

Οι εφαρμογές μπορούν να επιλέξουν οποιονδήποτε τύπο από τις παραπάνω υπηρεσίες ανάλογα με το ποια από τις δυο ικανοποιεί τις απαιτήσεις τους και υποστηρίζεται από το δίκτυο του παροχέα.

Η εγγυημένη υπηρεσία

Η εγγυημένη υπηρεσία εξυπηρετεί τις ανάγκες εφαρμογών που απαιτούν αυστηρές εγγυήσεις από το δίκτυο όσον αφορά το διαθέσιμο εύρος ζώνης και την καθυστέρησης μετάδοσης. Η υπηρεσία αυτή εγγυάται ότι τα πακέτα δεδομένων θα

φτάσουν στο προορισμό τους μέσα σε συγκεκριμένο χρονικό διάστημα και δεν θα απορριφθούν στο δίκτυο λόγω υπερχειλίσεων στις ουρές αναμονής και τους καταχωρητές ενδιάμεσης αποθήκευσης. Η υπηρεσία ενεργοποιείται από την εφαρμογή μέσω της αποστολής των κατάλληλων μηνυμάτων RSVP. Στη συνέχεια υπολογίζεται η μέγιστη καθυστέρηση που αναμένεται για τη μετάδοση ενός πακέτου, ενώ πραγματοποιείται και η απαραίτητη δέσμευση των πόρων σύμφωνα με έναν αλγόριθμο τύπου tocken bucket. Η εγγυημένη υπηρεσία έχει αυξημένο κόστος υλοποίησης γιατί απαιτείται από κάθε ροή δεδομένων που τη χρησιμοποιεί, να τοποθετείται σε ξεχωριστή ουρά εξυπηρέτησης. Αυτό οδηγεί σε αύξηση της χρησιμοποίησης των πόρων του δικτύου. Επιπλέον στην εγγυημένη υπηρεσία δεν πρέπει να πραγματοποιείται τμηματοποίηση (fragmentation) των πακέτων.

Η υπηρεσία ελεγχόμενου φορτίου-Controlled Load

Η υπηρεσία ελεγχόμενου φορτίου από την άλλη, χρησιμοποιείται κυρίως από τις εφαρμογές πραγματικού χρόνου που έχουν τη δυνατότητα να προσαρμόζουν τη ροή των δεδομένων τους στις διάφορες συνθήκες του δικτύου (αυξημένη κίνηση, ένα υπερφόρτιση και συμφόρηση) και αποτελεί ακόμα αντικείμενο εκτεταμένης έρευνας. Έχει αποδειχθεί ότι οι εφαρμογές αυτές λειτουργούν καλά σε περιβάλλοντα δικτύων χωρίς ιδιαίτερη φόρτιση, ενώ η απόδοσή τους μειώνεται σημαντικά σε συνθήκες υπερφόρτισης. Το επίπεδο ποιότητας υπηρεσίας που προσφέρει η υπηρεσία ελεγχόμενου φορτίου είναι αντίστοιχο του επιπέδου που προσφέρεται σε ένα σημερινό δίκτυο, όταν μεταφέρει μόνο αυτό το είδος κίνησης. Τυπικά προσεγγίζει τον παραδοσιακό τρόπο εξυπηρέτησης μέγιστης δυνατής προσπάθειας (best-effort) σε ένα δίκτυο χωρίς όμως την ύπαρξη άλλου φόρτου κίνησης. Σκοπός είναι η μέγιστη δυνατή χρησιμοποίηση των πόρων του δικτύου ,όσο το δυνατό πλησιέστερα προς το ιδανικό. Και στην υπηρεσία ελεγχόμενου φορτίου δεν πραγματοποιείται η τμηματοποίηση των πακέτων. Απλά τα δεδομένα δεν πρέπει να ξεπερνούν το μέγιστο MTU του δικτύου.

4.3.2 DiffServ στο MPLS

Το MPLS είναι συμβατό με την αρχιτεκτονική DiffServ στο ότι και αυτό μαρκάρει την κίνηση στους δρομολογητές εισόδου του δικτύου και αφαιρεί το μαρκάρισμα στους δρομολογητές εξόδου. Παρόλο που μπορεί σε κάθε δρομολογητή να καθορίζει την ποιότητα υπηρεσίας με βάση το μαρκάρισμα της κίνησης, η κύρια χρησιμότητα του μαρκαρίσματος για το πρωτόκολλο MPLS είναι η μεταγωγή της κίνησης. Για το λόγο αυτό το πρωτόκολλο MPLS χαρακτηρίζεται πιο πολύ ως ένα πρωτόκολλο διαχείρισης κίνησης και λιγότερο ως ένα πρωτόκολλο για την παροχή ποιότητας υπηρεσίας. Η χρησιμοποίηση της αρχιτεκτονικής DiffServ για την παροχή ποιότητας υπηρεσίας και του πρωτοκόλλου MPLS για την διαχείριση της κίνησης σε ένα δίκτυο IP προσφέρει πολλά πλεονεκτήματα:

(i) Καθορίζοντας LSP βάσει κριτηρίων ποιότητας υπηρεσίας και δρομολογώντας την ομαδοποιημένη κίνηση μιας κλάσης ποιότητας υπηρεσίας DiffServ μέσα από αυτά ελέγχεται η ροή της κυκλοφορίας της κλάσης ποιότητας υπηρεσίας στο δίκτυο, διαφοροποιείται από την υπόλοιπη κυκλοφορία και παρέχονται εγγυήσεις για την ποιότητα υπηρεσίας κατά μήκος των LSP.

(ii) Μπορούμε να διαχειριστούμε την κίνηση κάθε κλάσης ποιότητας υπηρεσίας κατάλληλα, ώστε να χρησιμοποιούμε αποδοτικά τους πόρους του δικτύου.

(iii) Παρέχεται η δυνατότητα για δημιουργία βοηθητικών LSP στα οποία εισάγεται η κίνηση κλάσεων ποιότητας υπηρεσίας με υψηλές εγγυήσεις για ποιότητα υπηρεσίας, σε περίπτωση καταστροφής των αρχικών LSP στα οποία δρομολογείται.

(iv) Η συνολική αρχιτεκτονική είναι πολύ επεκτάσιμη, αφού ο επιπλέον φόρτος που εισάγεται στο δίκτυο είναι μικρός. Επίσης, παρέχει διαλειτουργικότητα με δίκτυα που υποστηρίζουν μόνο την αρχιτεκτονική DiffServ.

Τα προβλήματα που έπρεπε να αντιμετωπιστούν για την υποστήριξη DiffServ από MPLS δίκτυα ήταν δύο.

Το πρώτο είναι το γεγονός ότι η DSCP τιμή (Differentiated Services Code Point - είναι ένα πεδίο σε ένα πακέτο IP που επιτρέπει διαφορετικά επίπεδα υπηρεσιών που θα διατεθούν για την κυκλοφορία του δικτύου) αναγράφεται στην IP επικεφαλίδα, ενώ οι LSRs εξετάζουν μόνο τα labels του MPLS.

Δεύτερο, είναι ότι η DSCP τιμή καταλαμβάνει 6 bits, ενώ η EXP τιμή είναι μόνο 3 bits. Για την αντιμετώπιση των προβλημάτων αυτών, έχουν προταθεί δύο λύσεις.

1. Η πρώτη λύση ονομάζεται EXP-Inferred-PSC LSP (E-LSP). Σύμφωνα με αυτή, η πληροφορία που σχετίζεται με το DSCP περικλείεται στο πεδίο EXP της επικεφαλίδας του πακέτου MPLS. Έτσι, ένα E-LSP μπορεί να χρησιμοποιηθεί για την υποστήριξη το πολύ οκτώ διαφορετικών ενοποιημένων ροών της ίδιας ισοδύναμης κλάσης προώθησης (Forwarding Equivalence Class – FEC). Η τιμή του πεδίου EXP αντιστοιχεί σε μια PHB (Per Hop Behavior) του δρομολογητή. Η ακριβής αντιστοιχία μεταξύ EXP και PHB είναι είτε στατικά προκαθορισμένη, είτε καθορίζεται με τη σηματοδοσία για την κατασκευή του E-LSP.

2. Η δεύτερη λύση ονομάζεται Label-Only-Inferred-PSC LSP (L-LSP). Σύμφωνα με αυτή η PHB Scheduling Class (PSC) για ένα πακέτο σε ένα δρομολογητή του δικτύου MPLS καθορίζεται ταυτόχρονα με τη διάδοση των ετικετών για ένα LSP. Έτσι, μετά τη δημιουργία του L-LSP η PSC συμπεραίνεται από την ετικέτα της επικεφαλίδας ενός πακέτου MPLS σε κάθε δρομολογητή. Η προτεραιότητα απόρριψης ενός πακέτου καθορίζεται από το πεδίο EXP της επικεφαλίδας του MPLS πακέτου. Το ζεύγος τιμών ετικέτας και πεδίου EXP καθορίζουν μοναδικά τη PHB που θα έχει ένα πακέτο σε ένα δρομολογητή.

Σε ένα δίκτυο MPLS που υποστηρίζει DiffServ μπορούν να χρησιμοποιηθούν κανένα ή πολλά E-LSP και κανένα ή πολλά L-LSP. Είναι αρμοδιότητα του διαχειριστή του δικτύου να διαλέξει το συνδυασμό των LSP που θα κατασκευάσει στο δίκτυο και το πώς θα μοιράσει την κίνηση των ομαδοποιημένων ροών κίνησης σε αυτά, προκειμένου να εξυπηρετήσει καλύτερα τα συμφέροντα του δικτύου του, όσον αφορά την υποστήριξη υπηρεσιών DiffServ, τη διαχείριση κυκλοφορίας και τη γρήγορη αποκατάσταση βλάβης.

5. Πλεονεκτήματα του MPLS

Συνολικά η τεχνολογία MPLS προσφέρει σημαντικά πλεονεκτήματα. Καταρχήν, η προώθηση πακέτων από τους δρομολογητές όπως έχουμε αναφέρει γίνεται πιο απλά και πιο γρήγορα σε σχέση με τη μέθοδο προώθησης στα παραδοσιακά δίκτυα IP. Αυτό συμβαίνει διότι στο εσωτερικό του δικτύου MPLS γίνεται μεταγωγή (switching) και όχι δρομολόγηση (routing).

Επιπλέον παρέχει ένα αποδοτικό μηχανισμό για σαφή καθορισμό της διαδρομής των πακέτων. Πιο συγκεκριμένα η διαδρομή που ακολουθεί το πακέτο καθορίζεται από την ετικέτα η οποία έχει μικρό μέγεθος. Αντίθετα στα παραδοσιακά δίκτυα IP, ο ορισμός κάποιας συγκεκριμένης διαδρομής για να πακέτο (source routing) απαιτεί το πακέτο να φέρει κωδικοποίηση της πλήρους διαδρομής, δηλαδή τις διευθύνσεις όλων των ενδιάμεσων δρομολογητών. Η τεχνική αυτή δεν είναι αποδοτική και για τον λόγο αυτό δε χρησιμοποιήθηκε στη πράξη.

Επιπρόσθετα, το MPLS μπορεί να υποστηριχτεί και από μεταγωγείς οι οποίοι έχουν δυνατότητες αναζήτησης και αντικατάστασης επικεφαλίδας αλλά δεν έχουν τη δυνατότητα ανάλυσης επικεφαλίδων επιπέδου δικτύου (όπως μεταγωγείς ATM και Frame Relay). Σε αυτές τις περιπτώσεις η ετικέτα είναι η επικεφαλίδα επιπέδου 2. Επομένως δεν υπάρχει κόστος για τη μεταφορά της ετικέτας.

Επίσης, όπως αναφέρθηκε προηγούμενα το MPLS μπορεί να χρησιμοποιηθεί σαν ένας μηχανισμός διαχείρισης κυκλοφορίας. Τα παραδοσιακά πρωτόκολλα δρομολόγησης που χρησιμοποιούνται σε δίκτυα IP, επιλέγουν πάντα το συντομότερο μονοπάτι για να προωθήσουν την κίνηση. Το γεγονός αυτό μπορεί να οδηγήσει σε προβληματικά φαινόμενα, όπως ορισμένοι σύνδεσμοι να παρουσιάζουν συμφόρηση ενώ άλλοι να παραμένουν ουσιαστικά ανενεργοί. Το φαινόμενο αυτό παρουσιάζεται και στο πρωτόκολλο LDP το οποίο επιλέγει μονοπάτια με βάση τη πληροφορία που παρέχεται από τα πρωτόκολλα δρομολόγησης IP. Όμως η κατασκευή LSPs τα οποία δε χρησιμοποιούν απαραίτητα

το συντομότερο μονοπάτι μπορεί να οδηγήσει στην εξάλειψη τέτοιων φαινομένων με χρήση κατάλληλων αλγορίθμων διαμοίρασης φορτίου (load balancing).

Τέλος, το MPLS μπορεί να χρησιμοποιηθεί για την παροχή σύγχρονών υπηρεσιών, όπως τα Ιδεατά Ιδιωτικά Δίκτυα (Virtual Private Networks - VPN)

Πιο συγκεκριμένα λοιπόν έχουμε τα παρακάτω πλεονεκτήματα:

1. **Επεκτασιμότητα:**

   Καθώς οι επιχειρήσεις αυξάνονται συνεχώς και προσεγγίζουν όλο και περισσότερους προορισμούς, η ανάγκη τους να συνδεθούν με άλλες τοποθεσίες μεγαλώνει. Η επέκταση αυτή μπορεί να εισάγει δυσκολίες για τους οργανισμούς, καθώς επίσης και για τους φορείς παροχής υπηρεσιών. Όταν ο αριθμός των τοποθεσιών που συνδέονται μεταξύ τους ολοένα και αυξάνει, γίνεται πολύ δύσκολο να διαχειριστεί. Οι πάροχοι υπηρεσιών αντιμετωπίζουν περισσότερα προβλήματα, διότι πρέπει να εξυπηρετούν πολλαπλούς πελάτες και όλοι προσπαθούν να προσεγγίσουν ολοένα και περισσότερες περιοχές. Άλλο ένα πρόβλημα είναι ότι ο ανταγωνισμός στην αγορά έχει επίσης μεγαλώσει σημαντικά, γεγονός που αναγκάζει τους παρόχους υπηρεσιών να προσφέρουν οικονομικά αποδοτικές και εύκολα διαχειρίσιμες λύσεις στους πελάτες τους. Το MPLS είναι μια απάντηση σε όλα αυτά τα ζητήματα. Δίνει την ικανότητα στους παρόχους υπηρεσιών να αναβαθμίσουν πολύ εύκολα και χωρίς δυσκολία. Κατά τις πρώτες ημέρες της Διαδικτύωσης, ένας πάροχος υπηρεσιών έπρεπε να διαχειριστεί πολλά εικονικά κυκλώματα και να ασχολείται με διαφορετικές τεχνολογίες. Με τις δυνατότητες του MPLS έχει γίνει πολύ εύκολο για αυτούς να διαχειριστούν τέτοιες καταστάσεις. Επιπλέον, μπορούν να φτάσουν σε άλλες αναπτυσσόμενες αγορές - ακόμη και σε αγορές στις οποίες δεν έχουν φυσική παρουσία.

   Όσο αναφορά τους πελάτες, μπορούν να επεκτείνουν τις δραστηριότητές τους, χωρίς να χρειάζεται να ανησυχούν για τα θέματα συνδεσιμότητας. Δεδομένου ότι ο πάροχος υπηρεσιών μπορεί να συμμετέχει στη συνδεσιμότητας γι 'αυτούς,

δεν έχουν να αντιμετωπίσουν θέματα, όπως η διαχείριση των δικών τους δρομολογήσεων.

2. Εξοικονόμηση κόστους.

Οι MPLS-based υπηρεσίες μπορούν να μειώσουν το κόστος κατά 10% έως 25% σε σχέση με συγκρίσιμες υπηρεσίες (Frame Relay και ATM). Καθώς οι εταιρείες προσθέτουν κίνηση φωνής και βίντεο, η εξοικονόμηση κόστους μπορεί να ανέλθει έως και το 40%.

3. Quality of Service (QOS).

Με τις εφαρμογές πολυμέσων να κερδίζουν τη δημοτικότητα είναι πλέον απαραίτητο να υπάρχει QoS. Οι υπηρεσίες φωνής θα πρέπει να έχουν μεγαλύτερη προτεραιότητα, καθώς είναι πολύ ευαίσθητες στην καθυστέρηση. Επίσης, όλο και περισσότερες εφαρμογές βίντεο βρίσκουν τη θέση της σε εταιρικά δίκτυα, όπως λύσεις Τηλεδιάσκεψης, που μπορούν να μειώσουν το κόστος των ταξιδιών αλλά και της εξοικονόμησης χρόνου. Για τις εφαρμογές αυτές θα πρέπει επίσης να δοθεί προτεραιότητα.

Η MPLS ετικέτα έχει ένα 3 bit πεδίο που ονομάζεται Traffic Class (TC), η οποία ήταν παλαιότερα γνωστή ως EXP (Experimental) πεδίο. Οι δρομολογητές πυρήνα μπορούν να παρέχουν διαφορετική μεταχείριση για κάθε πλαίσιο MPLS με βάση την αξία του TC.

4. Ευελιξία

Ως τεχνολογία, το MPLS επιβάλλει ορισμένους περιορισμούς σχετικά με τη διαλειτουργικότητα με άλλες τεχνολογίες. Ας υποθέσουμε, έναν πελάτη ο οποίος θέλει να συνδέσει διάφορες υπηρεσίες του σε όλη την υδρόγειο. Οι φορείς παροχής υπηρεσιών στη Βόρεια Αμερική προσφέρουν διαφορετικές τεχνολογίες σε σχέση με αυτούς της Ευρώπης ή της Ασίας. Σε τέτοιες περιπτώσεις, γίνεται πονοκέφαλος στο πως να κάνεις όλες αυτές οι τεχνολογίες να συνεργαστούν χρησιμοποιώντας απλό VPN IP. Διαφορετικές τεχνολογίες μπορεί να χρειαστούν περισσότερες κεφαλαιουχικές δαπάνες. Αλλά το MPLS κάνει αυτό το εύκολο. Το MPLS μπορεί να συνεργάζεται διάφορες τεχνολογίες.

Με οποιαδήποτε κίνηση πάνω από το MPLS ο Πάροχος Υπηρεσιών μπορεί να μεταφέρει Layer 2 πλαίσια πάνω από το MPLS backbone. Αυτό καθιστά τη ζωή ευκολότερη για τους πελάτες και τους προμηθευτές.

Εκτός από την ευελιξία με την ίδια την τεχνολογία, ο Πάροχος Υπηρεσιών μπορεί να προσφέρει τόσο Layer 2 και Layer 3 VPNs στην ίδια πλατφόρμα. Οι πελάτες που θέλουν να διαχειρίζονται τις δρομολογήσεις τους μπορούν να το κάνουν οι ίδιοι με Layer 2 VPN και άλλοι μπορούν να χρησιμοποιήσουν Layer 3 VPN.

5. Traffic Engineering

Αυτό είναι ένα χαρακτηριστικό που κάθε πάροχος υπηρεσιών θα ήθελε να χρησιμοποιείται. Κυρίως, οι πάροχοι υπηρεσιών θα πρέπει να έχουν περισσότερους από ένα σύνδεσμο μεταξύ των διαφόρων δρομολογητών, τόσο για εφεδρικό (redundancy) όσο και για την ικανοποίηση των απαιτήσεων των πελατών. Το πρόβλημα προκύπτει, όταν το εύρος ζώνης αυτών των συνδέσεων είναι διαφορετικό. Οι πάροχοι υπηρεσιών μπορούν να ρυθμίσουν την κατανομή του φορτίου μεταξύ αυτών των συνδέσεων χρησιμοποιώντας διάφορα χαρακτηριστικά IGP, αλλά αυτό μπορεί να αποδειχθεί πολύ δύσκολο και το μοντέλο αυτό από μόνο του δεν είναι επεκτάσιμο. Το MPLS TE μπορεί να αντιμετωπίσει τέτοιες καταστάσεις. Η χρήση του μαζί με IGP πρωτόκολλα μπορούν να παρέχουν πολύ καλύτερες λύσεις.

Το MPLS είναι περισσότερο προσανατολισμένο προς του παρόχους υπηρεσιών. Ένας πελάτης του δικτύου δε χρειάζεται να γνωρίζει το MPLS και για τις περισσότερες συνδέσεις η προκαθορισμένη διαδρομή από τον δρομολογητή του πελάτη προς το δρομολογητή του παρόχου είναι αρκετή.

6. Βελτιωμένη απόδοση.

Λόγω της φύσης των MPLS υπηρεσιών, οι σχεδιαστές του δικτύου μπορούν να μειώσουν τον αριθμό των "hops" μεταξύ των σημείων του δικτύου, το οποίο μεταφράζεται άμεσα σε αυξημένο χρόνο απόκρισης και βελτιωμένη απόδοση εφαρμογής.

7. Αποκατάσταση μετά από καταστροφή.

Οι MPLS υπηρεσίες βελτιώνουν την αποκατάσταση μετά από καταστροφή με ποικίλους τρόπους. Πρώτο και κυριότερο είναι ότι, data centers αλλά και άλλες βασικές περιοχές μπορούν να συνδεθούν με πολλαπλούς τρόπους σε cloud (συνήθως internet) (και ως εκ τούτου σε άλλους δικτυακούς τόπους στο δίκτυο). Δεύτερον, απομακρυσμένες περιοχές μπορούν γρήγορα και εύκολα να επανασυνδεθούν σε backup περιοχές εάν χρειαστεί.

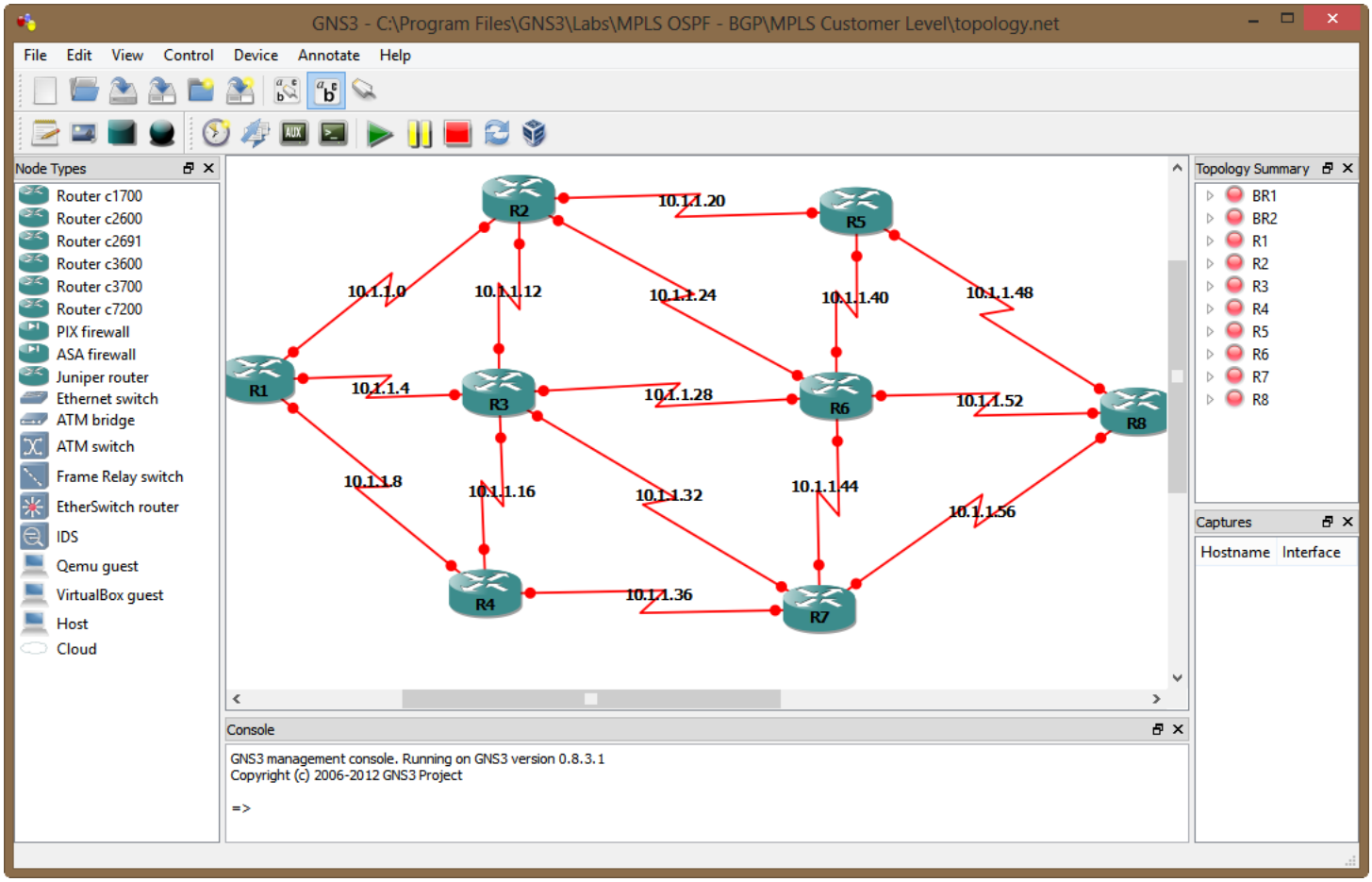
6. Παρουσίαση του GNS3 Εξομοιωτή

Στα πλαίσια της παρούσας διπλωματικής εργασίας χρησιμοποιήθηκε ο εξομοιωτής GNS3 για την μελέτη του MPLS μηχανισμού και την αλληλεπίδρασή του με πρωτόκολλα όπως OSPF , EIGRP , RIPv2, BGP, CSPF (OSPF-TE) και χρήση VPN τεχνολογίας.

Ο GNS3 είναι ένας Γραφικός Εξομοιωτής Δικτύου που επιτρέπει την εξομοίωση πολύπλοκων δικτύων. Είναι ένα γραφικό περιβάλλον για ένα προϊόν που ονομάζεται Dynagen, το οποίο τρέχει πάνω από το πρόγραμμα Dynamips.

Το Dynagen όπως αναφέραμε παραπάνω τρέχει πάνω από το Dynamips για να δημιουργήσει ένα πιο φιλικό προς το χρήστη περιβάλλον (χρησιμοποιώντας απλά αρχεία windows .ini).

Το GNS3 χρησιμοποιεί το παραπάνω και προχωράει ένα βήμα πιο πέρα παρέχοντας ένα γραφικό περιβάλλον με δυνατότητα δημιουργίας πλήρους εικονικού δικτύου, προσθέτοντας πολλά επιπλέον χαρακτηριστικά και το πιο σημαντικό είναι ότι εύκολο να δημιουργήσετε, να αλλάξετε και να αποθηκεύσετε τη δικτυακή σας τοπολογία.



Εικόνα 19 : Περιβάλλον GNS3

Οδηγίες λήψης του προγράμματος, εγκατάστασης, παραμετροποίησης και βασικών λειτουργιών ανατρέξτε στο Παράρτημα Α.

7. Μελέτη σεναρίων υλοποίησης MPLS με τη χρήση του GNS3

Κατά την εκπόνηση της παρούσης διπλωματικής εργασίας αναπτύχθηκαν εξολοκλήρου και μελετήθηκαν τα ακόλουθα σενάρια:

Σενάριο 1. MPLS - OSPF

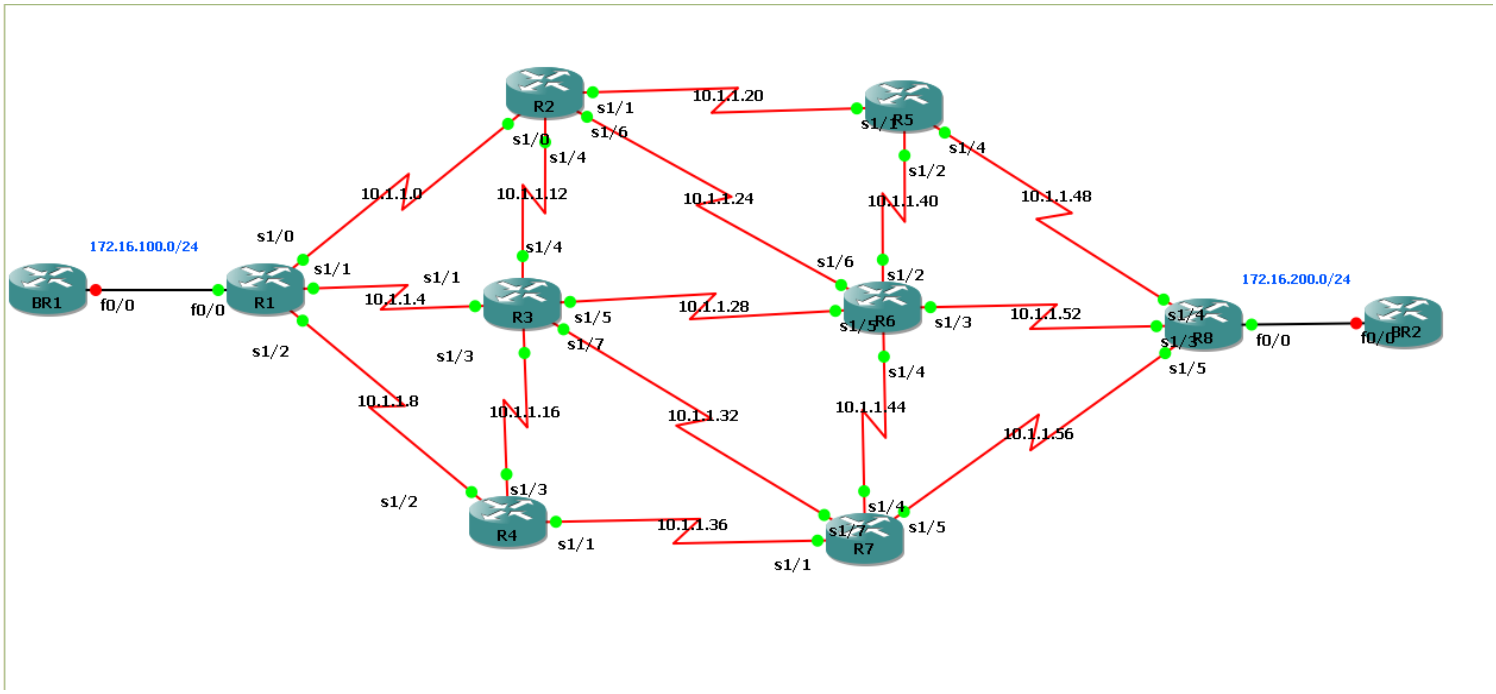
Σενάριο 2. MPLS - EIGRP

Σενάριο 3. MPLS - RIPv2

Σενάριο 4. MPLS - VPN

Σενάριο 5. MPLS TE - CSPF (OSPF-TE) / Constraint-Based Routing

Η τοπολογία που σχεδιάσθηκε και υλοποιήθηκε για τις ανάγκες των σεναρίων είναι:



Εικόνα 20 : MPLS – OSPF

Για λεπτομέρειες σχετικά με τη δημιουργία των εν λόγω σεναρίων ανατρέξτε στο Παράρτημα Β.

7.1 Σενάριο 1. MPLS – OSPF

Για το εν λόγω σενάριο χρησιμοποιείται η τοπολογία που απεικονίζεται στην Εικόνα 20. Θα δούμε μέρος από το configuration που χρειάζονται οι δρομολογητές ούτως ώστε να επιτύχουμε την επικοινωνία σε όλο το δίκτυο μέσα από τη χρήση του MPLS μηχανισμού και του OSPF πρωτοκόλλου όπως επίσης και πώς μπορούμε να παρέμβουμε ώστε να έχουμε Load Balancing και Re-Routing (αναδρομολόγηση κίνησης).

Το OSPF πρωτόκολλο ως ένα Link State Πρωτόκολλο βασίζεται στη λογική του Shortest Path First χρησιμοποιώντας την παράμετρο του κόστους της κάθε ζεύξης ώστε να υπολογίζει τη διαδρομή για το κάθε δίκτυο με το οποίο επικοινωνεί. Έτσι παραμετροποιώντας το κόστος της κάθε σύνδεσης επιτυγχάνουμε τα παραπάνω.

Εξ ορισμού το OSPF κάνει load balancing, όμως για να επιτύχουμε στοχευόμενο load balancing ή να ορίσουμε συγκεκριμένο μονοπάτι στην κίνηση πρέπει να παρέμβουμε στην επεξεργασία του.

Πιο συγκεκριμένα στο σενάριο αυτό έχουμε επιλέξει να πραγματοποιείται Load balancing στέλνοντας πακέτα από τον R1 -> Lo int R8 από τα παρακάτω μονοπάτια:

- R1 - R2 - R5 - R8
- R1 - R3 - R6 - R8
- R1 - R4 - R7 - R8

Για να το επιτύχουμε αυτό έχουμε τροποποιήσει τα κόστη των links των παραπάνω διαδρομών να είναι μικρότερα από το εξ ορισμού κόστος που έχει το OSPF (64).

- R1(cost 64) - R2 (cost 2) R2 - R5 (cost 2)
- R1(cost 64) - R3 (cost 2) R3 - R6 (cost 2)
- R1(cost 64) - R4 (cost 2) R4 - R7 (cost 2)

Αποτέλεσμα του παραπάνω είναι τα μονοπάτια αυτά να έχουν συνολικό κόστος 68 από την πηγή (R1) στον προορισμό (R8), με αποτέλεσμα το Load Balancing από τον R1 στον R8 να γίνεται μόνο από τα συγκεκριμένα μονοπάτια και όχι από κάποιο άλλο μονοπάτι όπως πριν από την παραπάνω επεξεργασία (π.χ. R1-R3-R7-R8).

- R1(cost 64) - R2(cost 2) - R5(cost 2) - R8 = **68 cost**
- R1 (cost 64)- R3(cost 64) - R7(cost 64) - R8 = 192 cost

Μέρος Διαμόρφωσης δρομολογητή R7

hostname R7 – Ορίζουμε το όνομα του δρομολογητή

interface Serial1/1 – Θέτουμε την Ip διεύθυνση και μάσκα στο interface S1/1

ip address 10.1.1.38 255.255.255.252 (αντίστοιχα ορίζουμε και τα υπόλοιπα inmterfaces)

ip ospf cost 2 – Θέτουμε το κόστος της σύνδεσης R7 – R4 σε 2 ώστε να κατευθύνουμε την κίνηση

mpls ip – Ορίζουμε το interface να τρέχει σε mpls λειτουργία

router ospf 100 – Θέτουμε τον δρομολογητή να τρέχει σε OSPF πρωτόκολλο και διαφημίζει στους γειτονικούς δρομολογητές τα δίκτυα που έχει συνδεδεμένα πάνω του.

network 10.1.1.32 0.0.0.3 area 0 – Η διαφήμιση του δικτύου γίνεται με την IP wildcard mask (η μάσκα είναι η 255.255.255.252) *area* area-id

network 10.1.1.36 0.0.0.3 area 0

network 10.1.1.44 0.0.0.3 area 0

network 10.1.1.56 0.0.0.3 area 0

Παρακάτω βλέπουμε το routing table του R1 που θα είναι η πηγή αποστολής πακέτων για το παράδειγμά μας.

Show Routing Table of R1

```
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/30 is subnetted, 15 subnets
C       10.1.1.8 is directly connected, Serial1/2
O       10.1.1.12 [110/66] via 10.1.1.6, 00:23:23, Serial1/1
                  [110/66] via 10.1.1.2, 00:23:43, Serial1/0
C       10.1.1.0 is directly connected, Serial1/0
C       10.1.1.4 is directly connected, Serial1/1
O       10.1.1.24 [110/66] via 10.1.1.2, 00:18:41, Serial1/0
O       10.1.1.28 [110/4] via 10.1.1.6, 00:18:31, Serial1/1
O       10.1.1.16 [110/66] via 10.1.1.10, 00:23:43, Serial1/2
                  [110/66] via 10.1.1.6, 00:23:23, Serial1/1
O       10.1.1.20 [110/4] via 10.1.1.2, 00:23:43, Serial1/0
O       10.1.1.40 [110/68] via 10.1.1.6, 00:18:21, Serial1/1
                  [110/68] via 10.1.1.2, 00:18:31, Serial1/0
O       10.1.1.44 [110/68] via 10.1.1.10, 00:18:23, Serial1/2
                  [110/68] via 10.1.1.6, 00:18:23, Serial1/1
O       10.1.1.32 [110/66] via 10.1.1.6, 00:18:33, Serial1/1
O       10.1.1.36 [110/4] via 10.1.1.10, 00:18:43, Serial1/2
O       10.1.1.56 [110/68] via 10.1.1.10, 00:18:23, Serial1/2
O       10.1.1.48 [110/68] via 10.1.1.2, 00:20:07, Serial1/0
O       10.1.1.52 [110/68] via 10.1.1.6, 00:18:23, Serial1/1
     192.168.1.0/32 is subnetted, 1 subnets
O       192.168.1.1 [110/69] via 10.1.1.10, 00:18:23, Serial1/2
                    [110/69] via 10.1.1.6, 00:18:23, Serial1/1
                    [110/69] via 10.1.1.2, 00:18:43, Serial1/0
R1#
```

Εικόνα 21 : Πίνακας δρομολόγησης R1

O 10.1.1.48 [110/68] via 10.1.1.2 , 00:20:07, Serial 1/0

***O** = OSPF*

***10.1.1.48 [110/68]** = Δίκτυο Προορισμού [Admin Distance / Cost]*

***10.1.1.2** = Επόμενο hop (R2)*

***00:20:07** = Τελευταία ενημέρωση για αυτόν τον προορισμό πριν από 20'*

***Serial 1/0** = Interface μέσω του οποίου θα ξεκινήσει η κίνηση προς το 10.1.1.48 δίκτυο.*

Όπως βλέπουμε στον πίνακα δρομολόγησης του R1 για την τελευταία IP προορισμού που είναι η 192.168.1.1 υπάρχουν 3 διαθέσιμα μονοπάτια.

Η διεύθυνση αυτή είναι που έχει ανατεθεί στο Loopback interface του R8.

Μέσα από αυτή τη πληροφορία μπορούμε να διαπιστώσουμε ότι το Load Balancing θα πραγματοποιηθεί κατά την αποστολή κάποιων πακέτων.

Αντίστοιχα με τον πίνακα δρομολόγησης που είδαμε παραπάνω μπορούμε να δούμε πως η πληροφορία διαμοιράζεται στο δίκτυο μέσω του MPLS. Ποιες ετικέτες ανατίθενται για ποια δίκτυα και μέσω ποιού interface ξεκινάει η κίνηση.

Show mpls table of R1

```
R1#sh mpls forwarding-table
Local  Outgoing      Prefix           Bytes Label   Outgoing   Next Hop
Label  Label or VC   or Tunnel Id     Switched      interface
16     Pop Label     10.1.1.16/30     0             Se1/1      point2point
       Pop Label     10.1.1.16/30     0             Se1/2      point2point
17     Pop Label     10.1.1.36/30     0             Se1/2      point2point
18     Pop Label     10.1.1.12/30     0             Se1/0      point2point
       Pop Label     10.1.1.12/30     0             Se1/1      point2point
19     Pop Label     10.1.1.28/30     0             Se1/1      point2point
20     Pop Label     10.1.1.24/30     0             Se1/0      point2point
21     Pop Label     10.1.1.20/30     0             Se1/0      point2point
22     20            10.1.1.40/30     1026          Se1/0      point2point
       20            10.1.1.40/30     0             Se1/1      point2point
23     21            10.1.1.48/30     1008          Se1/0      point2point
24     Pop Label     10.1.1.32/30     0             Se1/1      point2point
25     23            10.1.1.52/30     0             Se1/1      point2point
26     24            10.1.1.44/30     0             Se1/1      point2point
       26            10.1.1.44/30     0             Se1/2      point2point
27     27            192.168.1.1/32   0             Se1/0      point2point
       25            192.168.1.1/32   0             Se1/1      point2point
       27            192.168.1.1/32   0             Se1/2      point2point
28     28            10.1.1.56/30     1140          Se1/2      point2point
R1#
```

Εικόνα 22 : MPLS πίνακας δρομολόγησης R1

23 21 10.1.1.48/30 0 Se1/0

23 = *Τοπική ετικέτα*

21 = *Ετικέτα εξόδου*

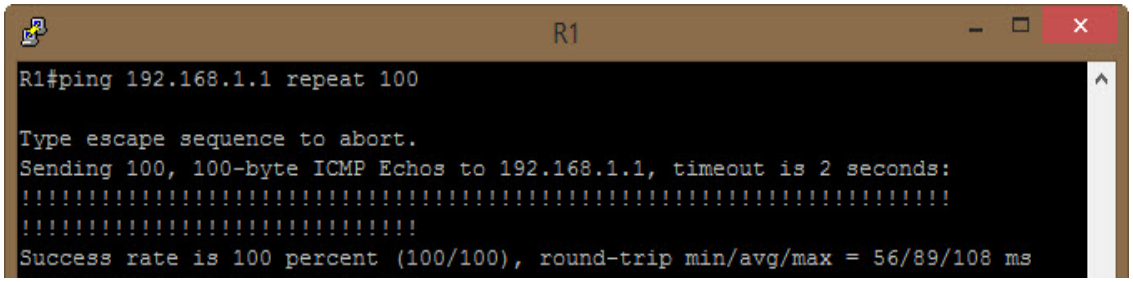
10.1.1.48/30 = *Δίκτυο Προορισμού*

Se1/0 = *Interface μέσω του οποίου θα ξεκινήσει η κίνηση προς το 10.1.1.48 δίκτυο*

Σημείωση: *Το Pop Label σημαίνει πως έχει φτάσει στον προορισμό και αφαιρείται η ετικέτα MPLS για να παραδοθεί το πακέτο*

Έλεγχος επικοινωνίας R1 – R8 με την εντολή ping

Ping from R1 to loopback interface of R8



Εικόνα 23 : Ping R1 -> R8

Όπως είδαμε και προηγουμένως στον πίνακα δρομολόγησης του R1 για την διεύθυνση 192.168.1.1 υπάρχουνε 3 πιθανά μονοπάτια ισοδύναμα μεταξύ τους.(**Load Balancing**).

Για να το δούμε και στην πράξη αυτό εκτελούμε extended ping command από τον R1 στο Loopback interface του R8.

Αναλύοντας την παρακάτω εντολή με τα αποτελέσματα βλέπουμε ότι τα πακέτα που αποστέλλονται τηρούν το load balancing και έτσι και στα 3 διαθέσιμα μονοπάτια έχουμε αποστολή των πακέτων.

- **10.1.1.1 - 10.1.1.21 - 10.1.1.49 - 192.168.1.1 (**R1 - R2 - R5 - R8**)**
- **10.1.1.9 - 10.1.1.37 - 10.1.1.57 - 192.168.1.1 (**R1 - R4 - R7 - R8**)**
- **10.1.1.5 - 10.1.1.29 - 10.1.1.53 - 192.168.1.1 (**R1 - R3 - R6 - R8**)**

```
R1#ping
Protocol [ip]:
Target IP address: 192.168.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]: R
Number of hops [ 9 ]:
Loose, Strict, Record, Timestamp, Verbose[RV]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
Packet has IP options:  Total option bytes= 39, padded length=40
 Record route: <*>
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)

Reply to request 0 (824 ms).  Received packet has options
 Total option bytes= 40, padded length=40
 Record route:
    (10.1.1.1)
    (10.1.1.21)
    (10.1.1.49)
    (192.168.1.1)
    (10.1.1.50)
    (10.1.1.22)
    (10.1.1.2)
    (10.1.1.1) <*>
    (0.0.0.0)
 End of list

Reply to request 1 (356 ms).  Received packet has options
 Total option bytes= 40, padded length=40
 Record route:
    (10.1.1.9)
    (10.1.1.37)
    (10.1.1.57)
    (192.168.1.1)
    (10.1.1.58)
    (10.1.1.38)
    (10.1.1.10)
    (10.1.1.9) <*>
    (0.0.0.0)
 End of list

Reply to request 2 (608 ms).  Received packet has options
 Total option bytes= 40, padded length=40
 Record route:
    (10.1.1.5)
    (10.1.1.29)
    (10.1.1.53)
    (192.168.1.1)
    (10.1.1.54)
    (10.1.1.30)
    (10.1.1.6)
    (10.1.1.5) <*>
    (0.0.0.0)
 End of list

Reply to request 3 (200 ms).  Received packet has options
 Total option bytes= 40, padded length=40
 Record route:
    (10.1.1.1)
    (10.1.1.21)
    (10.1.1.49)
    (192.168.1.1)
    (10.1.1.50)
    (10.1.1.22)
    (10.1.1.2)
    (10.1.1.1) <*>
    (0.0.0.0)
 End of list

Reply to request 4 (388 ms).  Received packet has options
 Total option bytes= 40, padded length=40
 Record route:
    (10.1.1.9)
    (10.1.1.37)
    (10.1.1.57)
    (192.168.1.1)
    (10.1.1.58)
    (10.1.1.38)
    (10.1.1.10)
    (10.1.1.9) <*>
    (0.0.0.0)
 End of list

Success rate is 100 percent (5/5), round-trip min/avg/max = 200/475/824 ms
R1#
```

Εικόνα 24 : Extended Ping R1 ->Lo R8

Εκτελώντας Traceroute R1 –> Lo int R8

Με την εντολή traceroute “ip” μπορούμε να δούμε τις ετικέτες του mpls κατά την διαδρομή από τον R1 στο Lo interface του R8. Διαπιστώνουμε πως και εδώ φαίνεται το load balancing σε 3 διαθέσιμα μονοπάτια / διαδρομές.

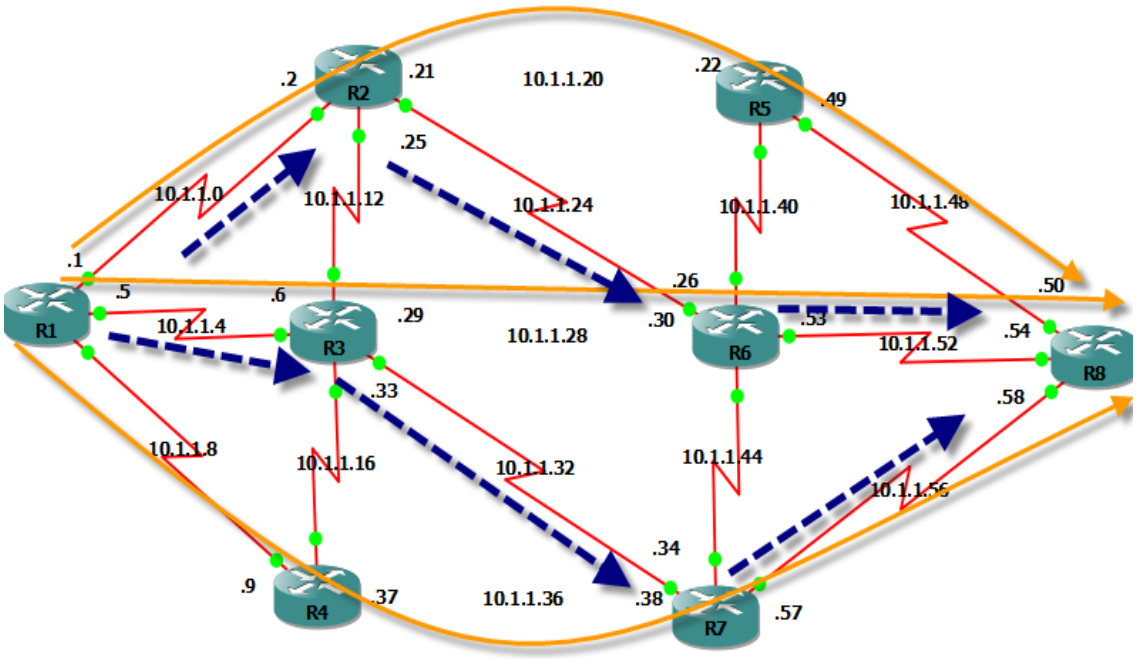
```
R1#traceroute 192.168.1.1

Type escape sequence to abort.
Tracing the route to 192.168.1.1

  1 10.1.1.2 [MPLS: Label 27 Exp 0] 372 msec
    10.1.1.6 [MPLS: Label 25 Exp 0] 332 msec
    10.1.1.10 [MPLS: Label 27 Exp 0] 424 msec
  2 10.1.1.22 [MPLS: Label 27 Exp 0] 364 msec
    10.1.1.30 [MPLS: Label 25 Exp 0] 388 msec
    10.1.1.38 [MPLS: Label 16 Exp 0] 272 msec
  3 10.1.1.50 340 msec
    10.1.1.54 880 msec
    10.1.1.58 312 msec
R1#
```

Εικόνα 25 : traceroute – Έλεγχος load balancing

Re-routing (Αναδρομολόγηση κίνησης)

Για να ελέγξουμε ότι πραγματοποιείται rerouting της κίνησης στέλνουμε συνεχόμενα πακέτα από μια πηγή σε κάποιο προορισμό και ρίχνοντας τις ζεύξεις που έχει επιλέξει ο πίνακας δρομολόγησης για την αποστολή των πακέτων προς αυτό το δίκτυο παρακολουθούμε την κίνηση πριν και μετά τη πτώση των ζεύξεων.

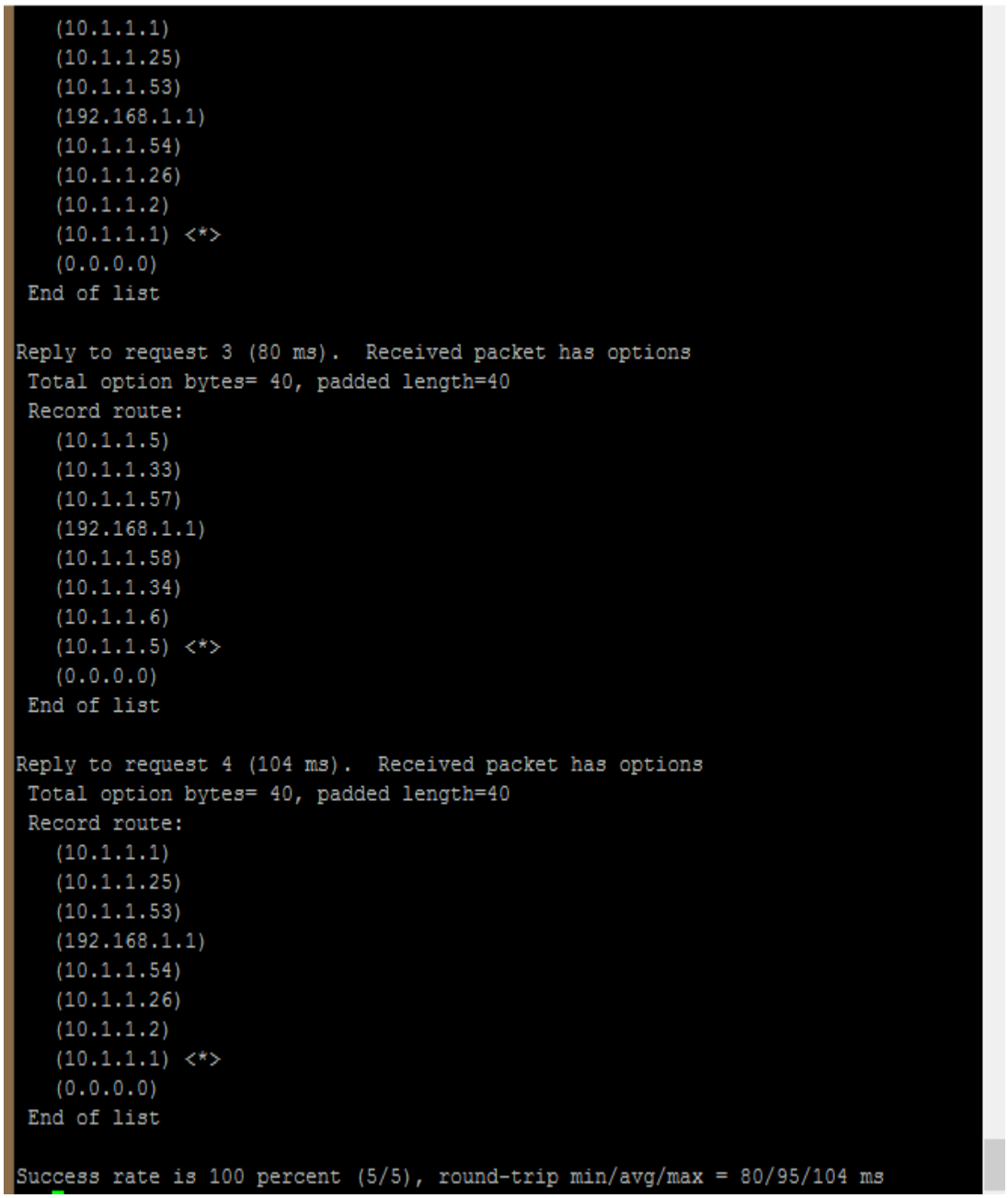
Όπως είδαμε και στην **Εικόνα 21** ο R1 κάνει load balancing για την αποστολή πακέτων προς το 192.168.1.1 δίκτυο. Για να δούμε ότι όντως γίνεται αναδρομολόγηση της κίνησης ρίχνουμε τα μονοπάτια που έχει επιλέξει.



Εικόνα 26 : Διαδρομή κίνησης πριν και μετά την πτώση των ζεύξεων

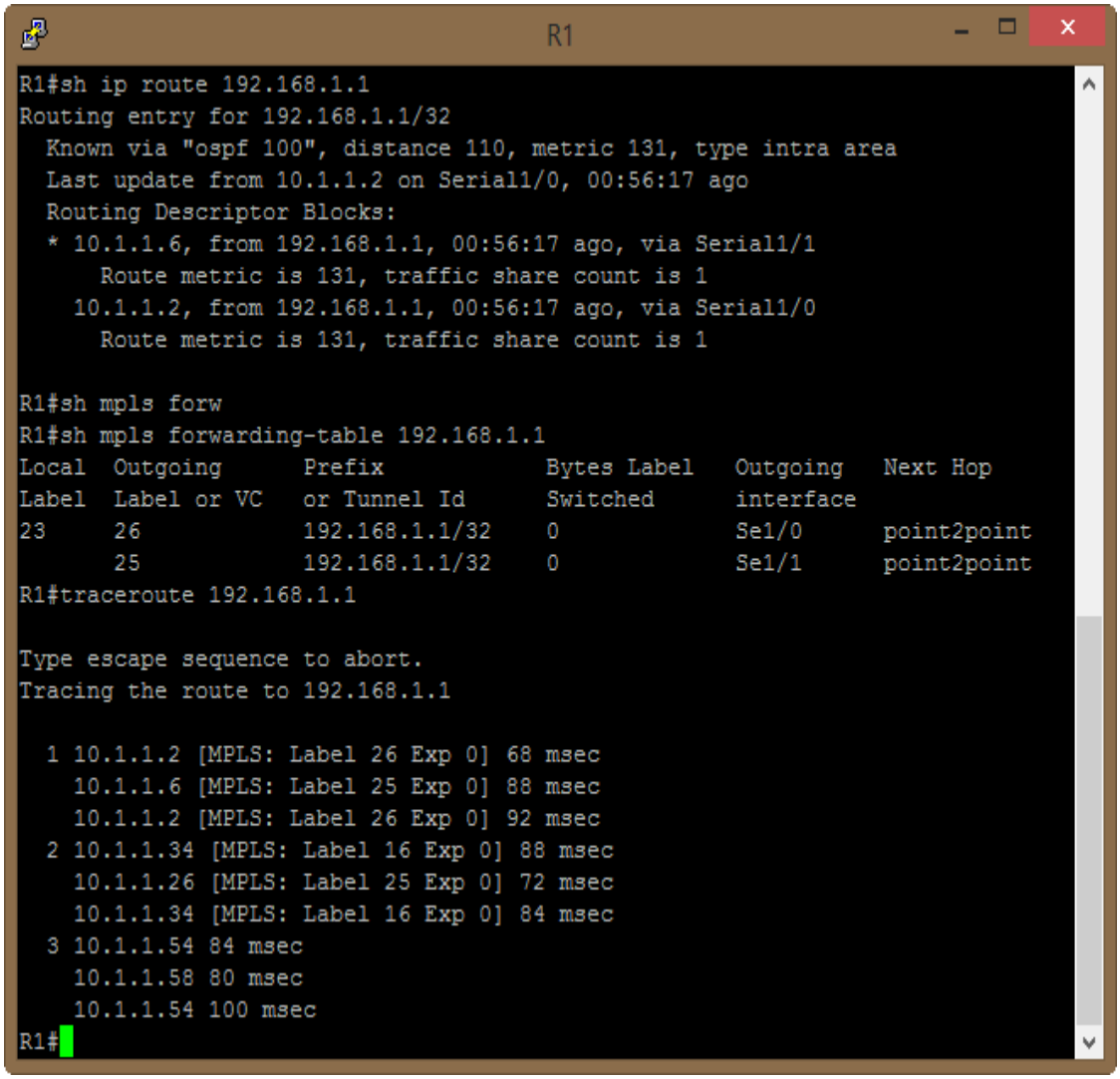
Όπως βλέπουμε παραπάνω οι πορτοκαλί διαδρομές είναι οι επιλεγμένες διαδρομές πριν από την πτώση οποιασδήποτε ζεύξης και οι μπλε διαδρομές είναι αυτές που επιλέγονται μετά την πτώση των ζεύξεων από τις οποίες ο R1 είχε επιλέξει να αποστέλλει την κίνηση των πακέτων.

Αυτό επιβεβαιώνεται και με το παρακάτω



Εικόνα 27 : Αναδρομολόγηση κίνησης OSPF

Παραπάνω βλέπουμε ότι η πρώτη διαδρομή που επιλέγεται για την αποστολή των πακέτων είναι η πάνω “πορτοκαλί” διαδρομή (πριν από την πτώση κάποιας ζεύξης) και στην συνέχεια λόγω την πτώση των ζεύξεων γίνεται υπολογισμός καινούριων διαδρομών προς το προορισμό και αναδρομολόγηση της κίνησης μέσω των καινούριων διαδρομών (μπλε).



Εικόνα 28 : Πίνακας δρομολόγησης R1->Lo R8 / MPLS πίνακας R1-Lo R8 / traceroute R1-Lo R8 μετά την πτώση των ζεύξεων

7.2 Σενάριο 2. MPLS – EIGRP

Το EIGRP είναι ένα πρωτόκολλο που χαρακτηρίζεται ως Advanced Distance Vector. Το κυριότερο χαρακτηριστικό του είναι ότι έχει κατασκευαστεί από την Cisco. Είναι εύκολο στην υλοποίησή του, αλλά δεν είναι προτείνεται για μεγάλα δίκτυα όπως το OSPF και επίσης δεν υποστηρίζει TE (Traffic engineering). Για να υπολογίζει τις διαδρομές για τον πίνακα δρομολόγησής του, βασίζεται σε μία formula που χρησιμοποιεί τόσο το bandwidth της κάθε γραμμής όσο και το delay προς τα δίκτυα που επικοινωνεί.

Αντίστοιχα με το σενάριο που χρησιμοποιήσαμε το OSPF με MPLS θα δούμε πως μπορούμε μέσω MPLS – EIGRP να επιτύχουμε Load Balancing και αναδρομολόγηση της κίνησης.

Με βάση λοιπόν τα παραπάνω θα πρέπει να τροποποιήσουμε το bandwidth των γραμμών (συνδέσεων) που επιθυμούμε ώστε να κατευθύνουμε την κίνηση.

Όπως λοιπόν και στο πρώτο σενάριο έχουμε επιλέξει να πραγματοποιείται Load balancing στέλνοντας πακέτα από τον R1 -> Lo int R8 από τα παρακάτω μονοπάτια:

- R1 - R2 - R5 - R8
- R1 - R3 - R6 - R8
- R1 - R4 - R7 - R8

Τροποποιούμε λοιπόν το bandwidth των παραπάνω διαδρομών να είναι μεγαλύτερο από το εξ ορισμού bandwidth της γραμμής (serial interface = 1544Kbit).

- R1(bandwith 2000kbit) - R2 (bandwith 2000kbit) R2 - R5 (bandwith 2000kbit)
- R1(bandwith 2000kbit) - R3 (bandwith 2000kbit) R3 - R6 (bandwith 2000kbit)
- R1(bandwith 2000kbit) - R4 (bandwith 2000kbit) R4 - R7 (bandwith 2000kbit)

Με τον τρόπο αυτό επιτυγχάνουμε να έχουμε μικρότερο metric για την επιλογή της διαδρομής όπου είναι και το κριτήριο του EIGRP.

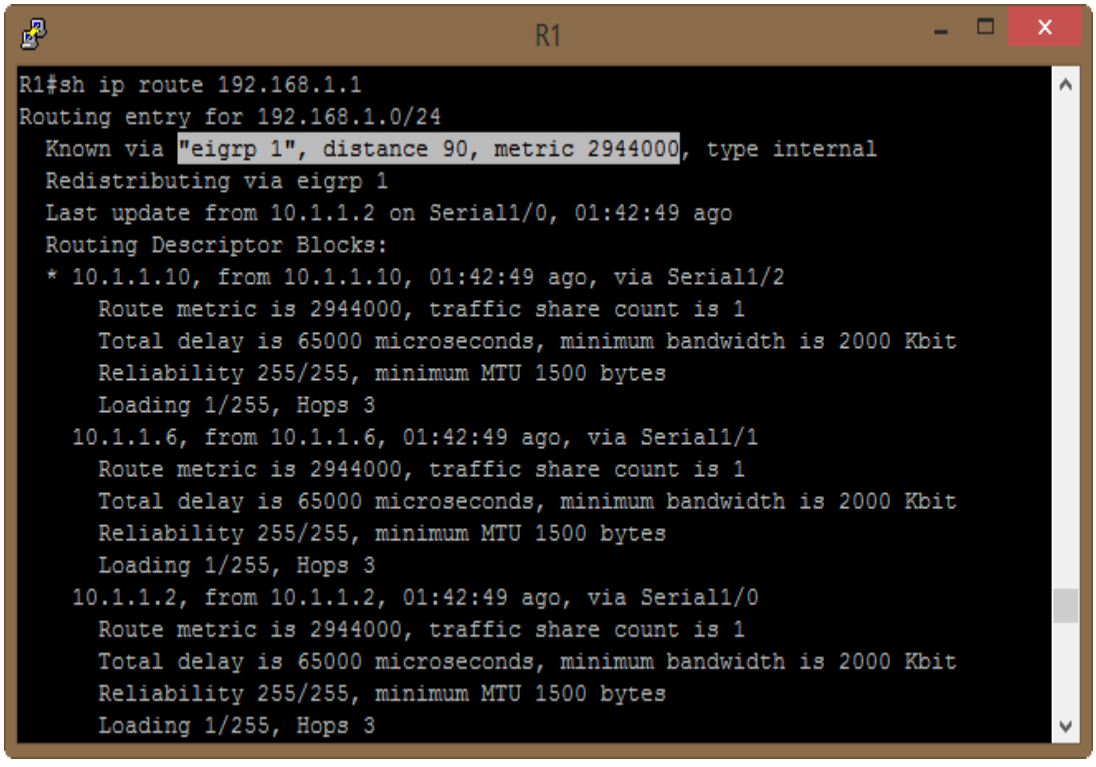
Το metric της διαδρομής υπολογίζεται από το παρακάτω τύπο:

Metric Value = ((10^7 / link bw kbit) + delay msec) * 256

Στη προκειμένη περίπτωση το link bw είναι ίσο με 2000kbit και το delay μπορούμε να το βρούμε ελέγχοντας τις λεπτομέρειες της κάθε διαδρομής από μία πηγή σε κάποιο προορισμό.

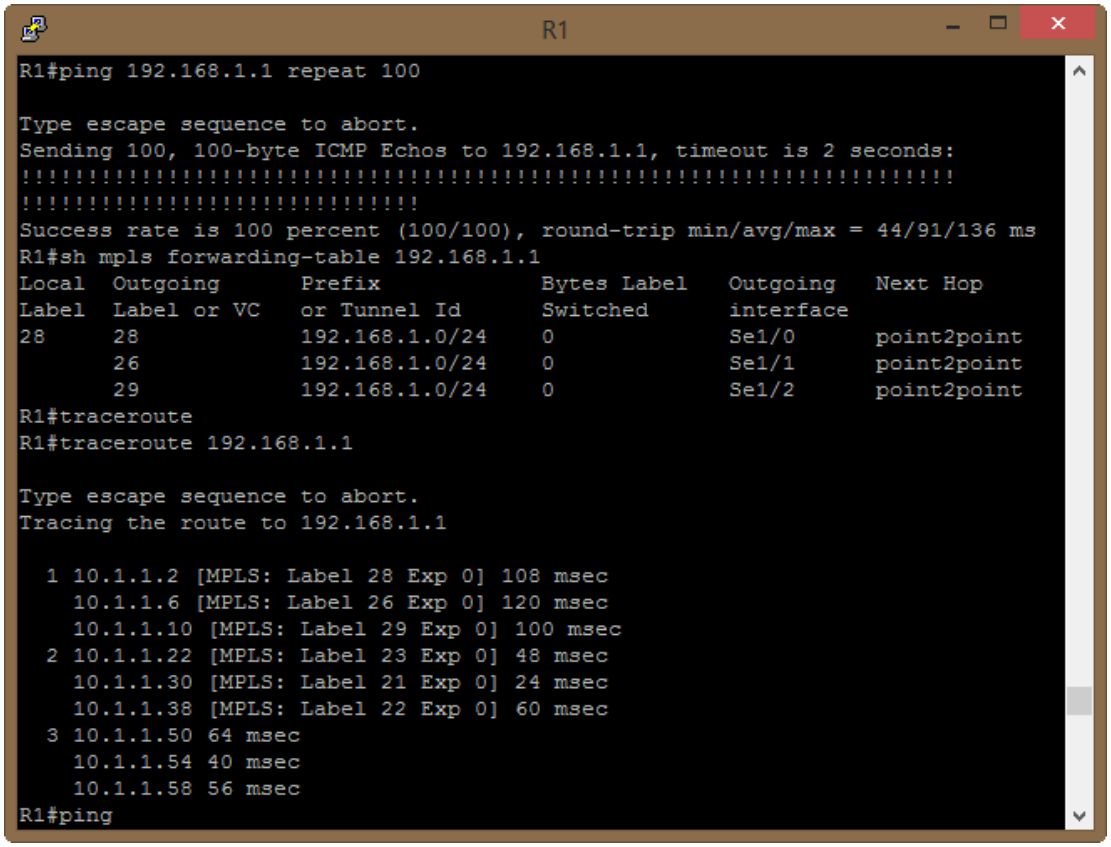
Όπως βλέπουμε στη παρακάτω εικόνα το Total Delay από τον R1 στο Lo int R8 είναι 65000 microseconds (6500 msec).

Άρα έχουμε : (10^7 / (2000 + 6500))*256 = **2944000 metric με administrative distance 90 που είναι η εξ ορισμού τιμή για το EIGRP πρωτόκολλο.**



Εικόνα 29 : Eigrp Route metric (R1 – Lo int R8)

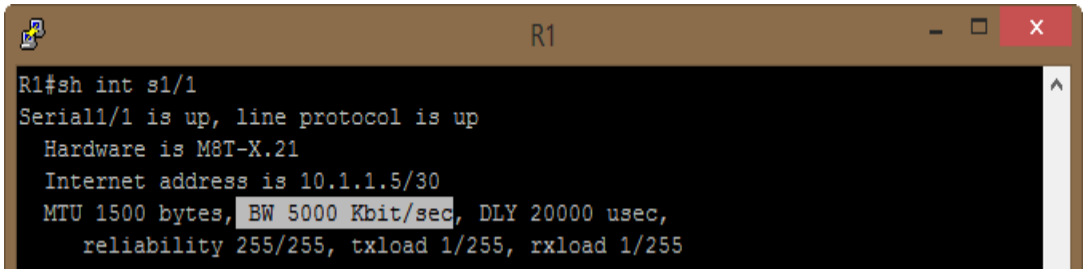
Πραγματοποιώντας τις παραπάνω αλλαγές στο bandwidth των συνδέσεων που μας ενδιαφέρουν να κατευθύνουμε την κίνηση έχουμε πετύχει Load Balancing στις προαναφερθείσες διαδρομές.



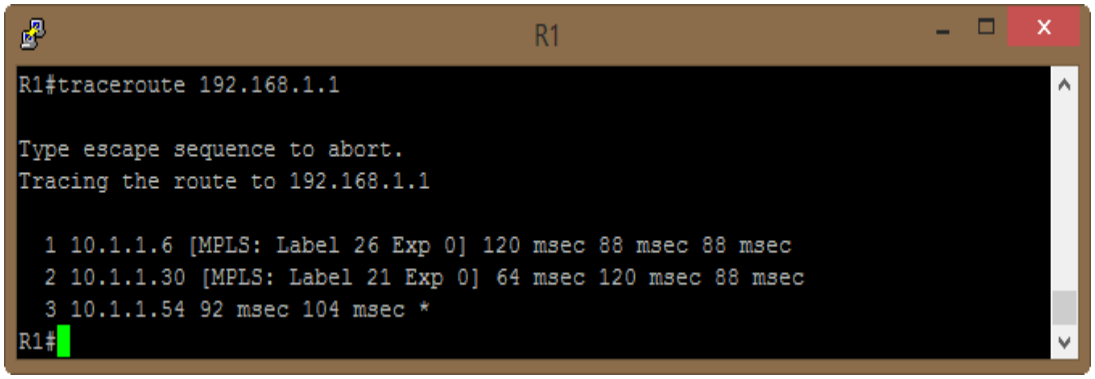
Εικόνα 30 : Load Balancing μέσω EIGRP

Στην παραπάνω εικόνα βλέπουμε ότι η διαδρομές που επιλέγονται για την αποστολή των πακέτων από τον R1 – Lo int R8 είναι οι διαδρομές που έχουμε στοχευόμενα επηρεάσει να είναι προς επιλογή.

Στη συνέχεια καθορίζουμε έτσι το bandwidth ώστε να επιλέγεται μόνο μία διαδρομή από τον R1 στον R8 για να ελέγξουμε την αναδρομολόγηση της κίνησης. Η επιλογή της διαδρομής είναι η R1-R3-R6-R8 όπως φαίνεται και παρακάτω.

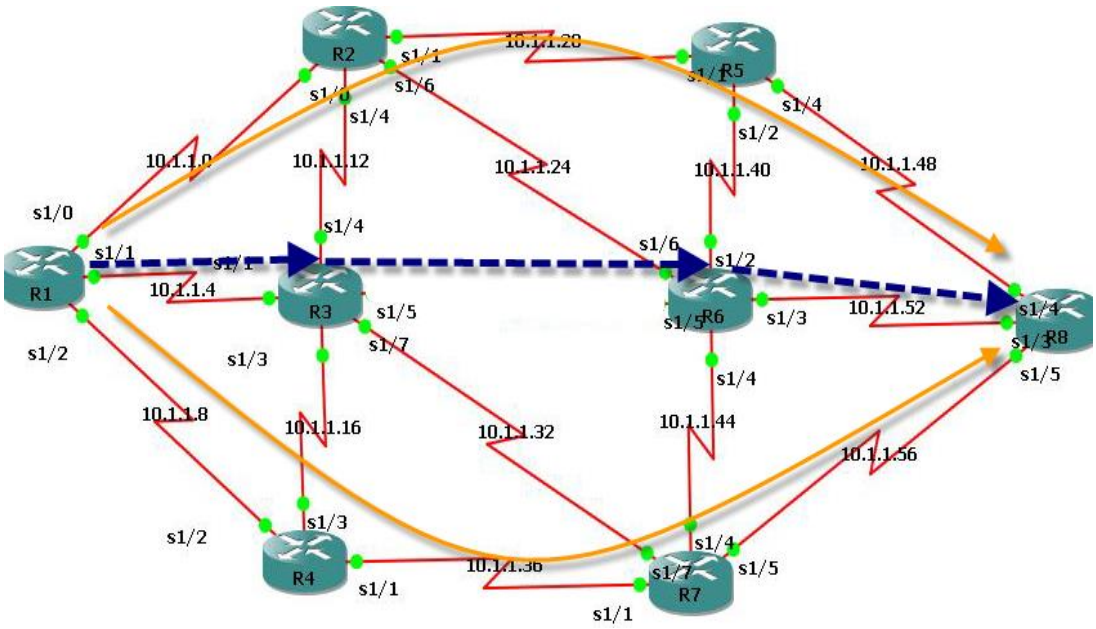


Εικόνα 31 : Καθορισμός Bandwidth



Εικόνα 32 : Επιλογή καινούριας διαδρομής

Ρίχνοντας λοιπόν κάποια ζεύξη από την επιλεγμένη διαδρομή R3-R6 βλέπουμε πως γίνεται αναδρομολόγηση της κίνησης μέσω των δύο εναλλακτικών διαδρομών (πορτοκαλί) λόγω του ότι έχουν το αμέσως μικρότερο bandwidth (2000Kbit)



Εικόνα 33 : Αναδρομολόγηση μέσω EIGRP (1)

Εικόνα 34 : Αναδρομολόγηση μέσω EIGRP (2)

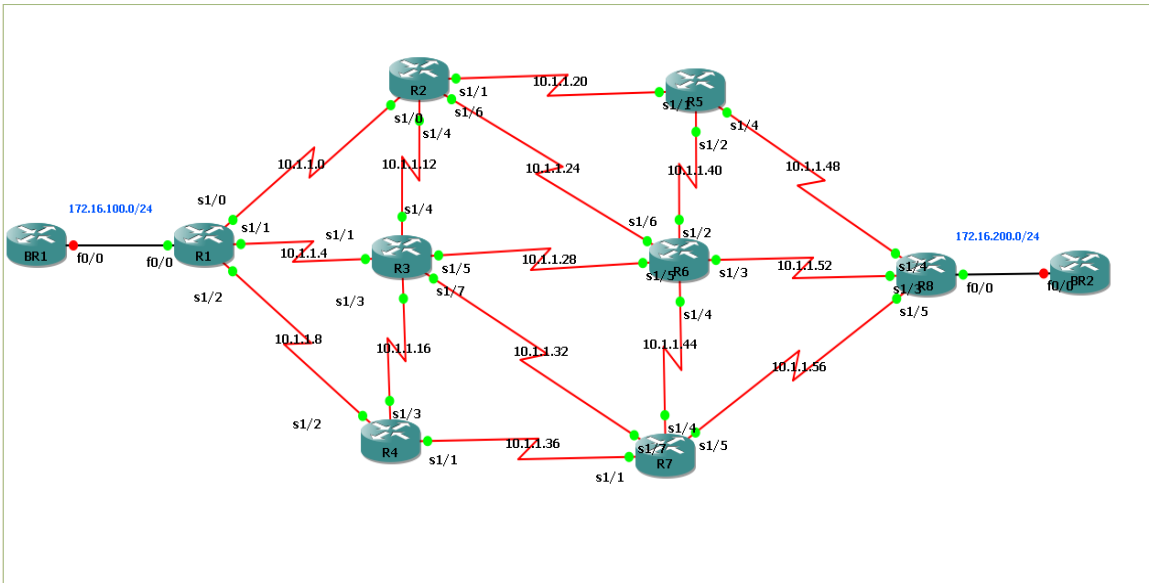
7.3 Σενάριο 3. MPLS - RIPv2

Το RIPv2 χαρακτηρίζεται ως ένα Distance Vector Routing Protocol το οποίο χρησιμοποιεί το hop count ως μέτρο για να υπολογίζει τις διαδρομές προς τους υπόλοιπους δρομολογητές του δικτύου. Το κύριο μειονέκτημά του είναι ο περιορισμός των hops που μπορεί να διαδώσει μία πληροφορία μέσα στο δίκτυο που είναι μέγιστο 15 hops. Όπως είναι κατανοητό, το RIP δεν μπορεί να εφαρμοστεί σε πολύ μεγάλα δίκτυα.

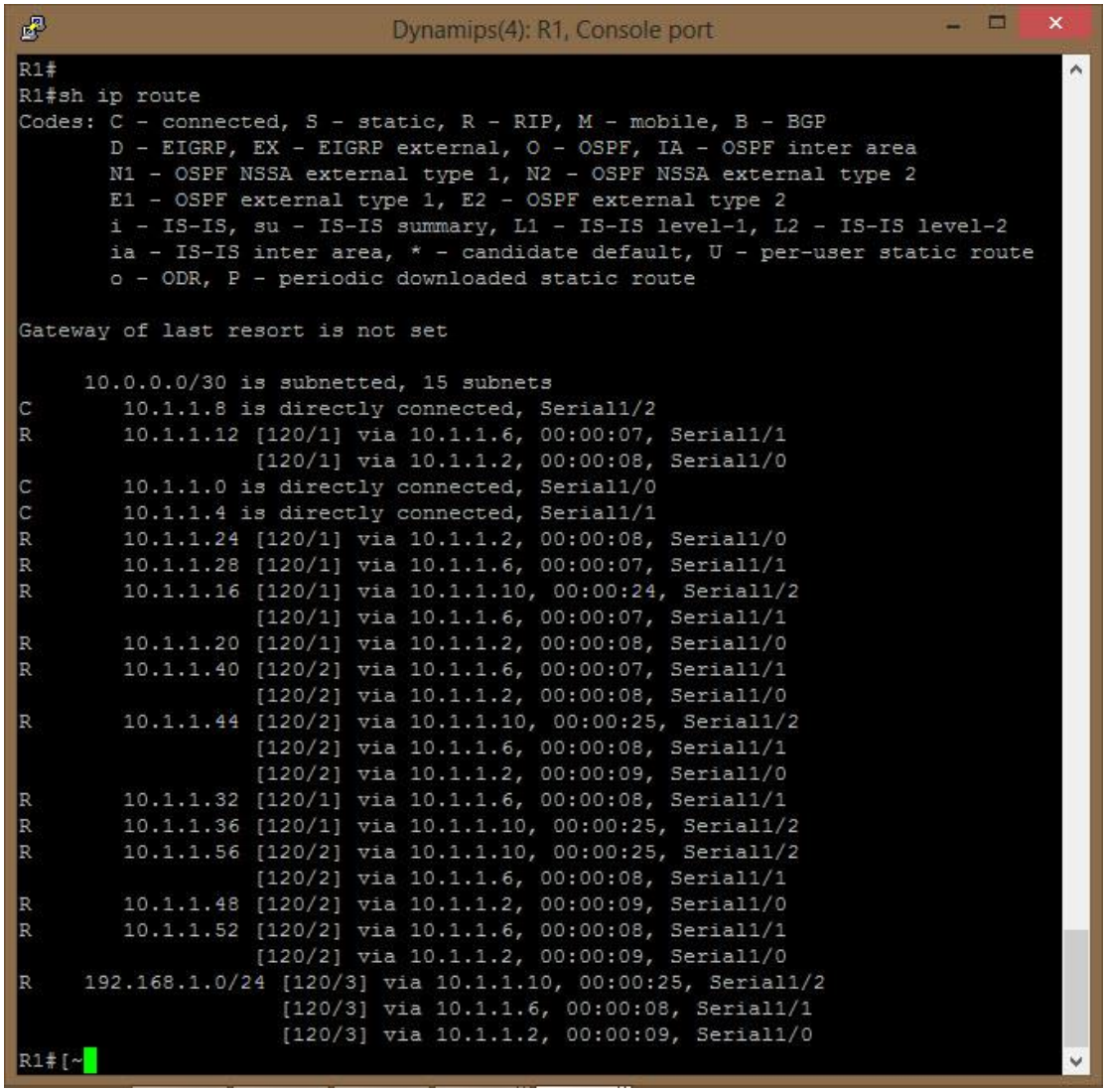
Στο συγκεκριμένο δίκτυο που μελετάμε η υλοποίηση του RIPv2 είναι εφικτή μιας και το δίκτυό μας δεν φτάνει ποτέ στα 15 hops από μια οποιαδήποτε πηγή σε ένα οποιονδήποτε προορισμό.

Αντίστοιχα με τα παραπάνω σενάρια θα δούμε πως το RIPv2 κάνει load balancing και αναδρομολόγηση της αρχικής διαδρομής που είχε υπολογιστεί στον πίνακα δρομολόγησης σε περίπτωση πτώσης κάποιας ζεύξης.

Όπως μπορούμε να δούμε στη τοπολογία που χρησιμοποιούμε υπάρχουν πολλές διαδρομές από τον R1 στον R8 με ίδια hops



1. R1 – R2 – R5 – R8 = 3 hops
2. R1 – R2 – R6 – R8 = 3 hops
3. R1 – R3 – R6 – R8 = 3 hops
4. R1 – R3 – R7 – R8 = 3 hops
5. R1 – R4 – R7 – R8 = 3 hops



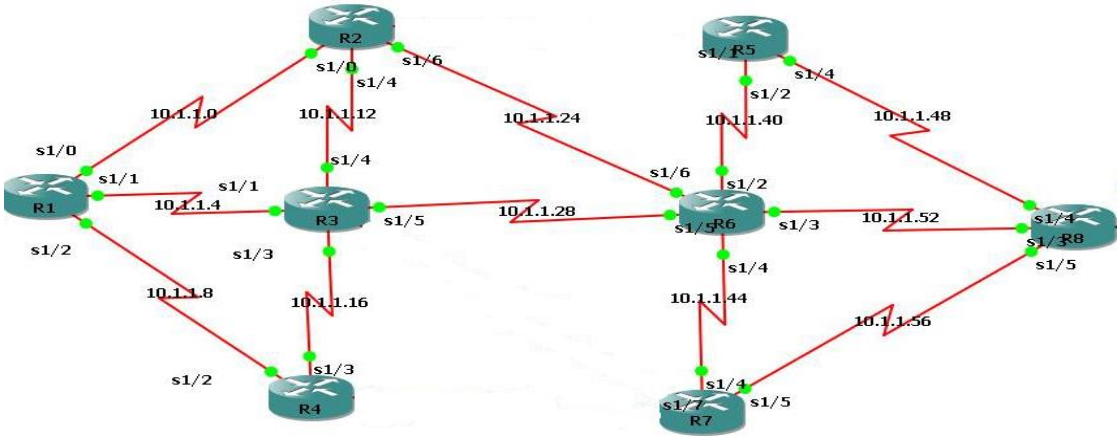
Εικόνα 35 : Πίνακας δρομολόγησης R1 με RIPv2 πρωτόκολλο

Όπως βλέπουμε και παραπάνω οι διαδρομές από τον R1 προς το Lo interface του R8 είναι 3 με metric 3 μέσω του R2 R3 και R4. Αναλυτικότερα φαίνεται στη παρακάτω εικόνα όπου φαίνονται οι συνολικές διαδρομές από τον R1 στον R8

```
R1#ping
Protocol [ip]:
Target IP address: 192.168.1.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface:
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]: r
Number of hops [ 9 ]:
Loose, Strict, Record, Timestamp, Verbose[RV]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
Packet has IP options:  Total option bytes= 39, padded length=40
 Record route: <*>
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)

Reply to request 0 (152 ms).  Received packet has options
 Total option bytes= 40, padded length=40
 Record route:
    (10.1.1.1)
    (10.1.1.21)
    (10.1.1.49)
    (192.168.1.1)
    (10.1.1.54)
    (10.1.1.26)
    (10.1.1.2)
    (10.1.1.1) <*>
    (0.0.0.0)
 End of list

Reply to request 1 (132 ms).  Received packet has options
 Total option bytes= 40, padded length=40
 Record route:
    (10.1.1.9)
    (10.1.1.37)
    (10.1.1.57)
    (192.168.1.1)
    (10.1.1.58)
    (10.1.1.38)
    (10.1.1.10)
    (10.1.1.9) <*>
    (0.0.0.0)
 End of list

Reply to request 2 (116 ms).  Received packet has options
 Total option bytes= 40, padded length=40
 Record route:
    (10.1.1.5)
    (10.1.1.33)
    (10.1.1.57)
    (192.168.1.1)
    (10.1.1.54)
    (10.1.1.30)
    (10.1.1.6)
    (10.1.1.5) <*>
    (0.0.0.0)
 End of list

Reply to request 3 (124 ms).  Received packet has options
 Total option bytes= 40, padded length=40
 Record route:
    (10.1.1.1)
    (10.1.1.25)
    (10.1.1.53)
    (192.168.1.1)
    (10.1.1.50)
    (10.1.1.22)
    (10.1.1.2)
    (10.1.1.1) <*>
    (0.0.0.0)
 End of list

Reply to request 4 (84 ms).  Received packet has options
 Total option bytes= 40, padded length=40
 Record route:
    (10.1.1.9)
    (10.1.1.37)
    (10.1.1.57)
    (192.168.1.1)
    (10.1.1.58)
    (10.1.1.38)
    (10.1.1.10)
    (10.1.1.9) <*>
    (0.0.0.0)
 End of list

Success rate is 100 percent (5/5), round-trip min/avg/max = 84/121/152 ms
```

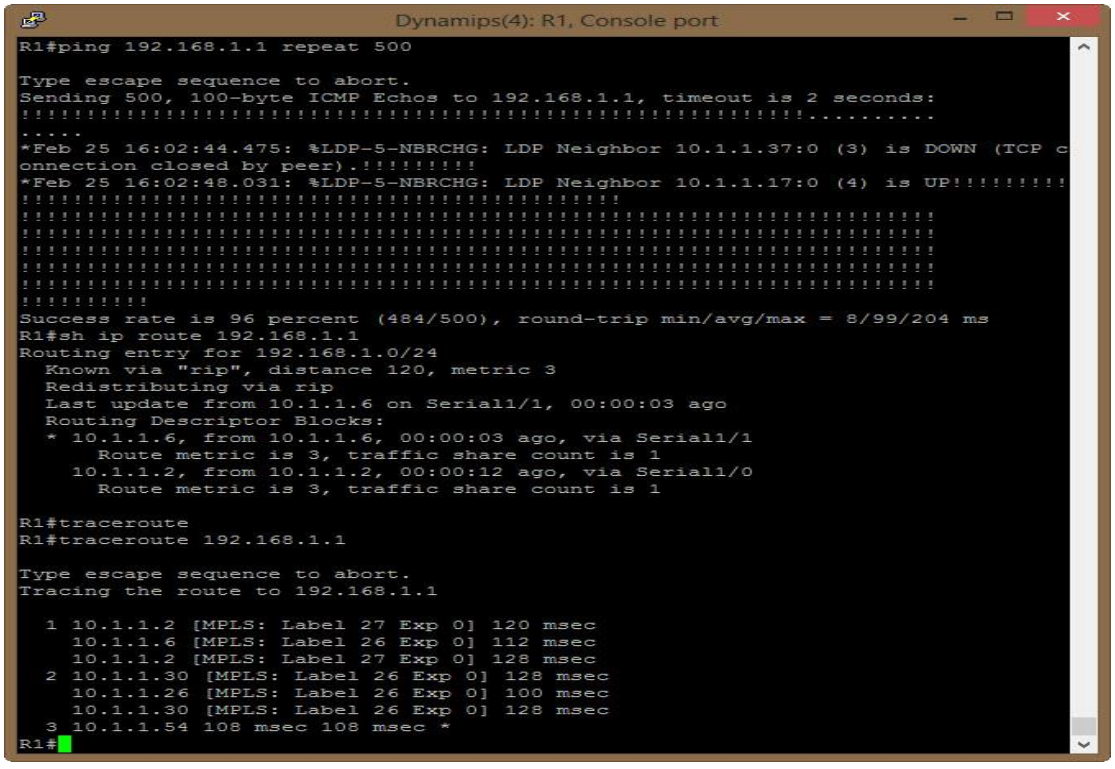
Εικόνα 36 : Διαδρομές από R1-Lo int R8 (extended ping command)

Στη συνέχεια ρίχνουμε κάποιες από τις συνδέσεις της τοπολογίας μας για να δούμε ότι οι διαδρομές υπολογίζονται εκ νέου και έτσι έχουμε αναδρομολόγηση της κίνησης



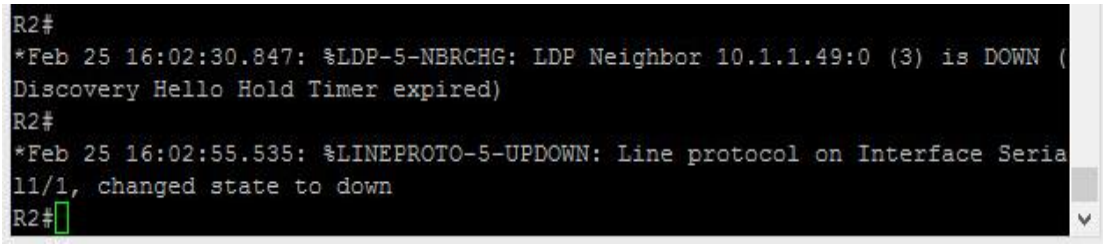
Εικόνα 37 : Πτώση ζεύξεων RIP

Σύμφωνα λοιπόν με το παραπάνω κατευθύνουμε την κίνηση μόνο σε 2 μονοπάτια και έχοντας εκτελέσει ένα ping command νωρίτερα περιμένουμε να δούμε κάποιες απώλειες πακέτων και στη συνέχεια μετά τον υπολογισμό των καινούριων διαδρομών να έχουμε και πάλι επιτυχημένες αποστολές.

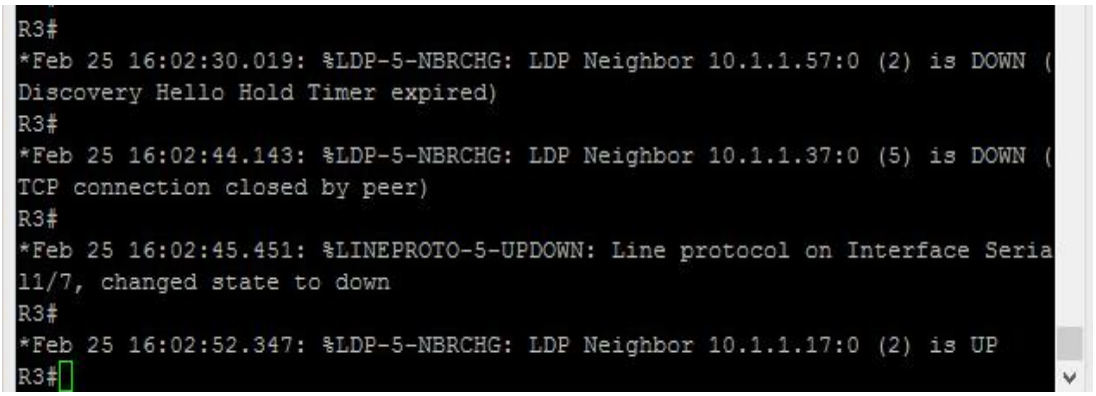


Εικόνα 38 : Απώλειες πακέτων και αναδρομολόγηση κίνησης

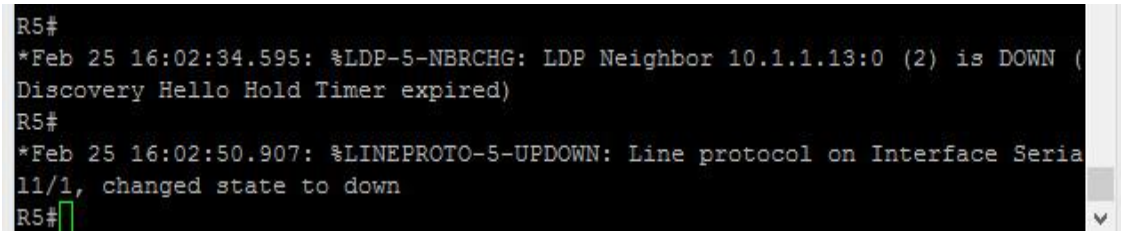
Κατά την εκτέλεση του παραπάνω ping και ρίχνοντας τις συνδέσεις μεταξύ των R2-R5 R3-R7 και R4-R7 βλέπουμε την κατάσταση που επικρατεί στους δρομολογητές που επηρεάζονται. Τα δίκτυα που πέφτουν και ποιο interface



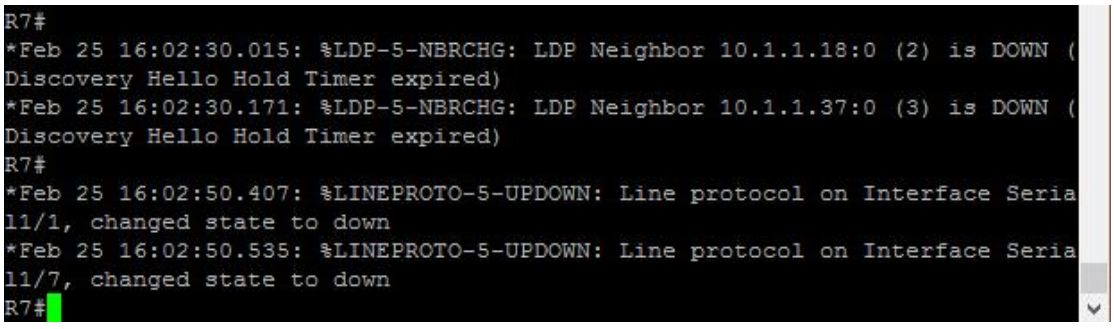
Εικόνα 39 : Router 2 – Πτώση S1/1



Εικόνα 40 : Router 3 – Πτώση S1/7



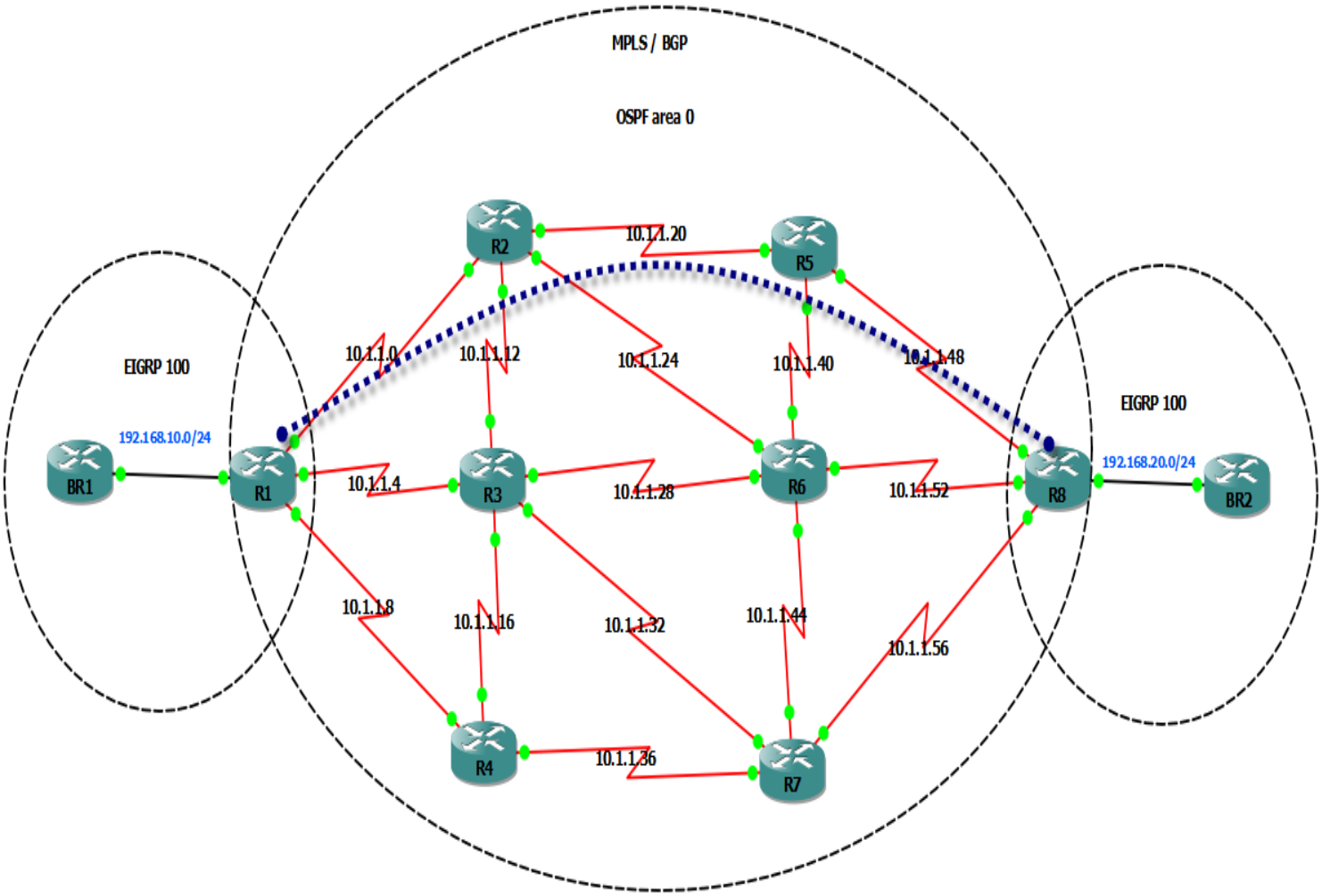
Εικόνα 41 : Router 5 – Πτώση S1/1



Εικόνα 42 : Router 7 – Πτώση S1/1 , S1/7

7.4 Σενάριο 4. MPLS - VPN

Στο συγκεκριμένο σενάριο φτιάχνουμε ένα δίκτυο MPLS και προσπαθούμε να επιτύχουμε επικοινωνία εκτός του MPLS δικτύου, αλλά μέσω αυτού. Πιο αναλυτικά έχουμε το MPLS δίκτυο που χρησιμοποιήσαμε και στα προηγούμενα σενάρια, (βλέπε επίσης Εικόνα 43) με την προσθήκη δρομολογητών έξω από τα άκρα του MPLS δικτύου και μέσω MPLS VPN επιτυγχάνουμε επικοινωνία. Για να γίνει αυτό χρησιμοποιούμε επίσης το πρωτόκολλο BGP στο δίκτυο του MPLS ούτως ώστε να διαφημίσει το VPN που θέλουμε ώστε να επιτευχθεί η επικοινωνία. Επιπρόσθετα εσωτερικά του MPLS δικτύου έχουμε υλοποιήσει το OSPF πρωτόκολλο για την επικοινωνία των δρομολογητών εντός του MPLS δικτύου. Για την επικοινωνία των δρομολογητών εκτός του MPLS με τους ακραίους δρομολογητές του MPLS έχουμε πραγματοποιήσει ένα EIGRP δίκτυο. Για να επιτύχουμε όλα τα παραπάνω πρέπει επίσης να υλοποιηθούν VRF και στους δύο ακραίους δρομολογητές, όπου σαν παραμέτρους ορίζουμε το RD (route distinguisher), που στην ουσία κάνει μοναδικές τις διευθύνσεις που θα διαφημιστούν μέσω του VPN, και το RT (route target) το οποίο είναι αυτό που δημιουργεί το VPN.



Εικόνα 43 : MPLS VPN

Επιβεβαιώνοντας λοιπόν τα παραπάνω βλέπουμε στη Εικόνα 44 την υλοποίηση EIGRP 100 μεταξύ των BR1 – R1 και BR2 – R8 όπου στους δρομολογητές εκτός MPLS δικτύου διαφημίζουμε μέσω EIGRP 100 τα δίκτυα και τις Loopback διευθύνσεις τους.

BR1

```
!
!
!
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 192.168.10.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
router eigrp 100
 network 1.0.0.0
 network 192.168.10.0
 no auto-summary
!
```

BR2

```
!
!
!
!
interface Loopback0
 ip address 3.3.3.3 255.255.255.0
!
interface FastEthernet0/0
 ip address 192.168.20.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
router eigrp 100
 network 3.0.0.0
 network 192.168.20.0
 no auto-summary
```

Εικόνα 44 : EIGRP 100

Στη συνέχεια προχωρούμε με την υλοποίηση της διαμόρφωσης των ακραίων MPLS δρομολογητών που θα κάνουν όλη τη διαχείριση για τη μετάδοση των πληροφοριών και τη δημιουργία του MPLS VPN.

Στην αρχή δημιουργούμε το VRF, το οποίο είναι σαν ένα «**virtual routing table**» και όπως αναφέραμε και στο θεωρητικό μέρος, διαχωρίζουν τις διαδρομές ανά πελάτη ούτως ώστε να αποφευχθεί το θέμα των διπλών περιοχών (διπλού εύρους) διευθύνσεων. Για την ολοκλήρωση της δημιουργίας του VRF, χρειαζόμαστε την εγκατάσταση του RD (route distinguisher) και τη ρύθμιση του RT (route target). Το RD είναι απαραίτητο για να κάνει τα προθέματα των πελατών (BR1 , BR2) μοναδικά στην εγκατάσταση του MPLS VPN. Με τον Route Distinguisher (RD) μετατρέπουμε μια διεύθυνση 32bits σε μία των 96bits μοναδική στο δίκτυο με αποτέλεσμα οι PEs δρομολογητές να μην ανακοινώνουν 32bit διευθύνσεις αλλά 96bits. Το RT είναι αυτό που «δημιουργεί» το VPN, και ρυθμίζει τις παραμέτρους για την σωστή διαδρομή. Ακόμα, πρέπει να προσθέσουμε στις διεπαφές που είναι στραμμένες προς τον πελάτη, το σωστό VRF.

Εφόσον δημιουργήσουμε το VPN και στα δύο άκρα που θέλουμε να ενώσουμε, και ενώ έχουμε ήδη διαμορφώσει τους δρομολογητές εκτός του MPLS δικτύου να τρέχουν κάτω από eigrp πρωτόκολλο, πρέπει να διαφημίσουμε μέσω BGP όλη την πληροφορία του VRF και του EIGRP στο απέναντι άκρο.

Ότι περιγράφεται παραπάνω φαίνεται με την Εικόνα 45 για τον δρομολογητή R1. Αντίστοιχη υλοποίηση έχει γίνει και για τον R8.

```
ip vrf CLIENT
 rd 100:1
 route-target export 1:100
 route-target import 1:100
```

```
interface FastEthernet0/0
 ip vrf forwarding CLIENT
 ip address 192.168.10.254 255.255.255.0
```

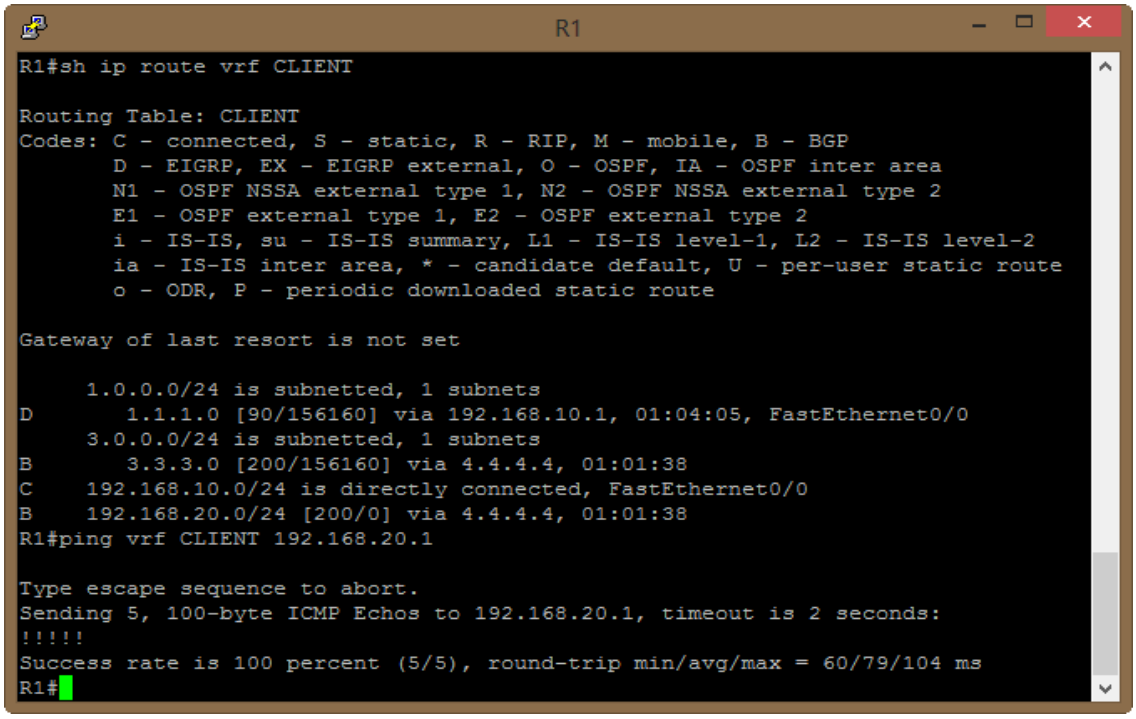
```
interface Serial1/0
 ip address 10.1.1.1 255.255.255.252
 mpls ip
 serial restart-delay 0
```

```
router eigrp 1
 auto-summary
 !
 address-family ipv4 vrf CLIENT
  redistribute bgp 1 metric 1500 4000 200 10 1500
  network 192.168.10.0
  no auto-summary
  autonomous-system 100
 exit-address-family
!
router ospf 1
 log-adjacency-changes
 network 2.2.2.0 0.0.0.255 area 0
 network 10.1.1.0 0.0.0.3 area 0
 network 10.1.1.4 0.0.0.3 area 0
 network 10.1.1.8 0.0.0.3 area 0
!
router bgp 1
 no synchronization
 bgp log-neighbor-changes
 neighbor 4.4.4.4 remote-as 1
 neighbor 4.4.4.4 update-source Loopback0
 no auto-summary
 !
 address-family vpnv4
  neighbor 4.4.4.4 activate
  neighbor 4.4.4.4 send-community both
 exit-address-family
 !
 address-family ipv4 vrf CLIENT
  redistribute eigrp 100
  no synchronization
 exit-address-family
```

Εικόνα 45 : Διαμόρφωση R1 δρομολογητή / VRF – OSPF – EIGRP - BGP

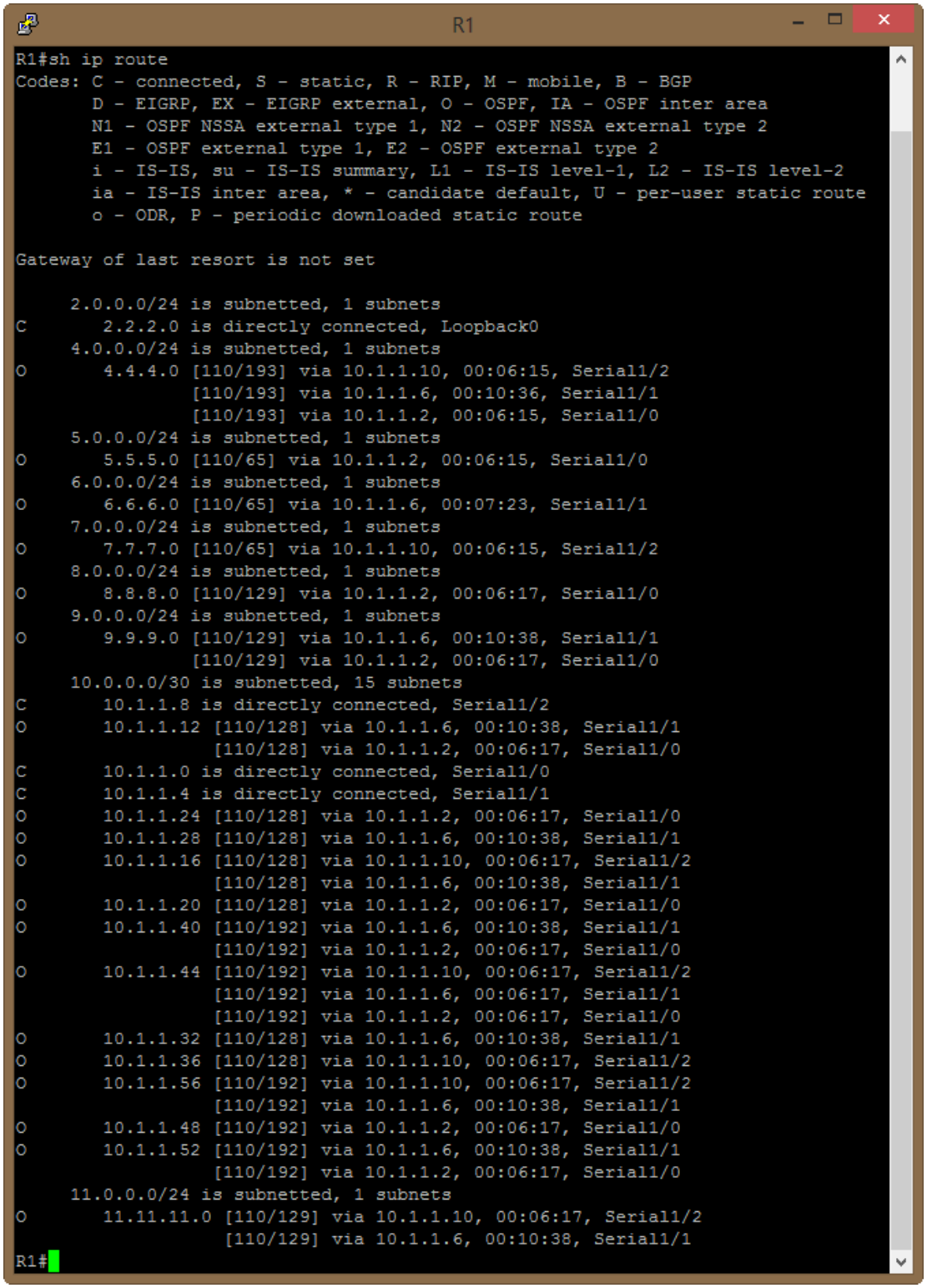
Λόγω του ότι δημιουργούμε ξεχωριστό πίνακα δρομολόγησης για την επικοινωνία του R1-BR2 και R8-BR1 με απλό ping command δεν θα δούμε επιτυχημένη επικοινωνία. Αντιθέτως πρέπει να εκτελέσουμε ping μέσω του vrf που έχουμε δημιουργήσει γιατί ο δρομολογητής με απλό ping κοιτάει τον εξ ορισμού πίνακα

δρομολόγησής του. Στην παρακάτω εικόνα 45, βλέπουμε τον vrf πίνακα δρομολόγησης του R1 καθώς και ένα επιτυχημένο ping vrf command προς τον BR2. Όπως παρατηρούμε ο vrf πίνακας δρομολόγησης δεν έχει κάτι άλλο παρά τη Lo διεύθυνση του BR1 που την μαθαίνει μέσω eigrp (D) και την Lo διεύθυνση καθώς και το δίκτυο που ανήκει ο BR2 που γνωστοποιείται μέσω BGP (B).



Εικόνα 46 : VRF πίνακας δρομολόγησης R1 – ping vrf command

Ενώ ο κανονικό πίνακας δρομολόγησης του R1 περιέχει όλα τα δίκτυα που συμμετέχουν στο MPLS και έχουν διαφημιστεί μέσω OSPF όπως είπαμε και νωρίτερα. Εννοείται ότι δεν περιέχονται τα δίκτυα που είναι εκτός MPLS τα οποία βρίσκονται στον vrf πίνακα.



Εικόνα 47 : Πίνακας δρομολόγησης R1

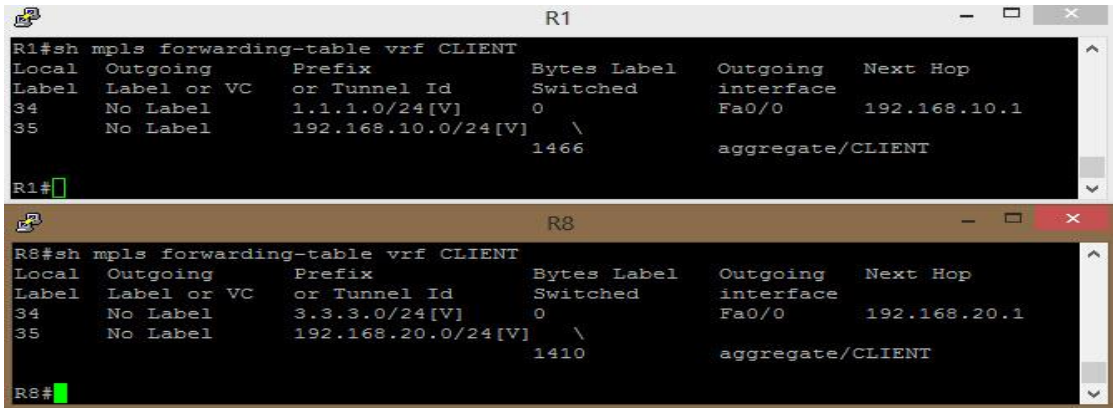
Τελειώνοντας λοιπόν την διαμόρφωση όλων των δρομολογητών ελέγχουμε την επικοινωνία αυτών εκτός του MPLS δικτύου. Βλέπουμε ότι (Εικόνα 48) σωστά επικοινωνούν μέσω του VPN και αυτό φαίνεται στο ότι δεν μεσολαβούν κάποιοι

κόμβοι στην επικοινωνία. Στην πραγματικότητα αυτό είναι εικονικό διότι για την όλη επικοινωνία χρειάζονται οι μεζάζωντες δρομολογητές για να μεταφερθεί η κίνηση.

```
BR1#ping
Protocol [ip]:
Target IP address: 192.168.20.1
Repeat count [5]: 3
Extended commands [n]: y
Loose, Strict, Record, Timestamp, Verbose[none]: r
Type escape sequence to abort.
Sending 3, 100-byte ICMP Echos to 192.168.20.1, timeout is 2 seconds:
Packet has IP options:  Total option bytes= 39, padded length=40
 Record route: <*>
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)

Reply to request 0 (104 ms).  Received packet has options
 Total option bytes= 40, padded length=40
 Record route:
    (192.168.10.1)
    (192.168.20.1)
    (192.168.20.1)
    (192.168.10.1) <*>
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
 End of list

Reply to request 1 (124 ms).  Received packet has options
 Total option bytes= 40, padded length=40
 Record route:
    (192.168.10.1)
    (192.168.20.1)
    (192.168.20.1)
    (192.168.10.1) <*>
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
 End of list

Reply to request 2 (132 ms).  Received packet has options
 Total option bytes= 40, padded length=40
 Record route:
    (192.168.10.1)
    (192.168.20.1)
    (192.168.20.1)
    (192.168.10.1) <*>
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
    (0.0.0.0)
 End of list

Success rate is 100 percent (3/3), round-trip min/avg/max = 104/120/132 ms
```

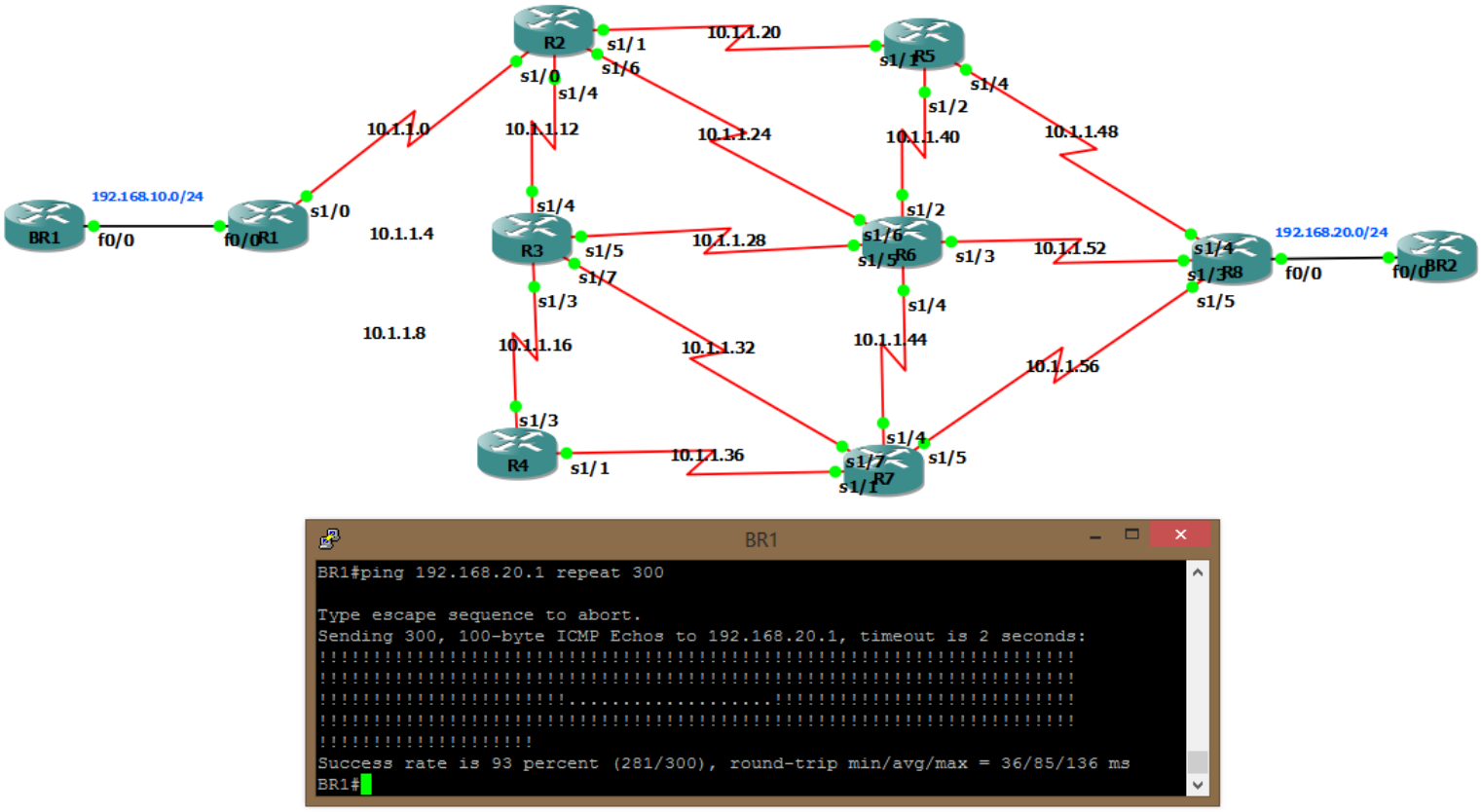
Εικόνα 48 : Επικοινωνία μέσω VPN

Στην συνέχεια βλέπουμε το mpls table του R1 και R8 για το vrf που έχουμε δημιουργήσει. Όπως φαίνεται παρακάτω για να προωθηθεί η πληροφορία στον BR1 και BR2 αντίστοιχα δεν χρειάζεται mpls label, λόγω του ότι οι τελευταίοι δεν ανήκουν στον MPLS μέρος.



Εικόνα 49 : MPLS table R1,R8

Τέλος στην εικόνα 50 βλέπουμε πως παρόλο που έχουμε δημιουργήσει ένα εικονικό δίκτυο από μία άκρη στην άλλη, αν έχουμε πτώση κάποιων ενδιάμεσων ζεύξεων έχουμε κάποιες μερικές απώλειων



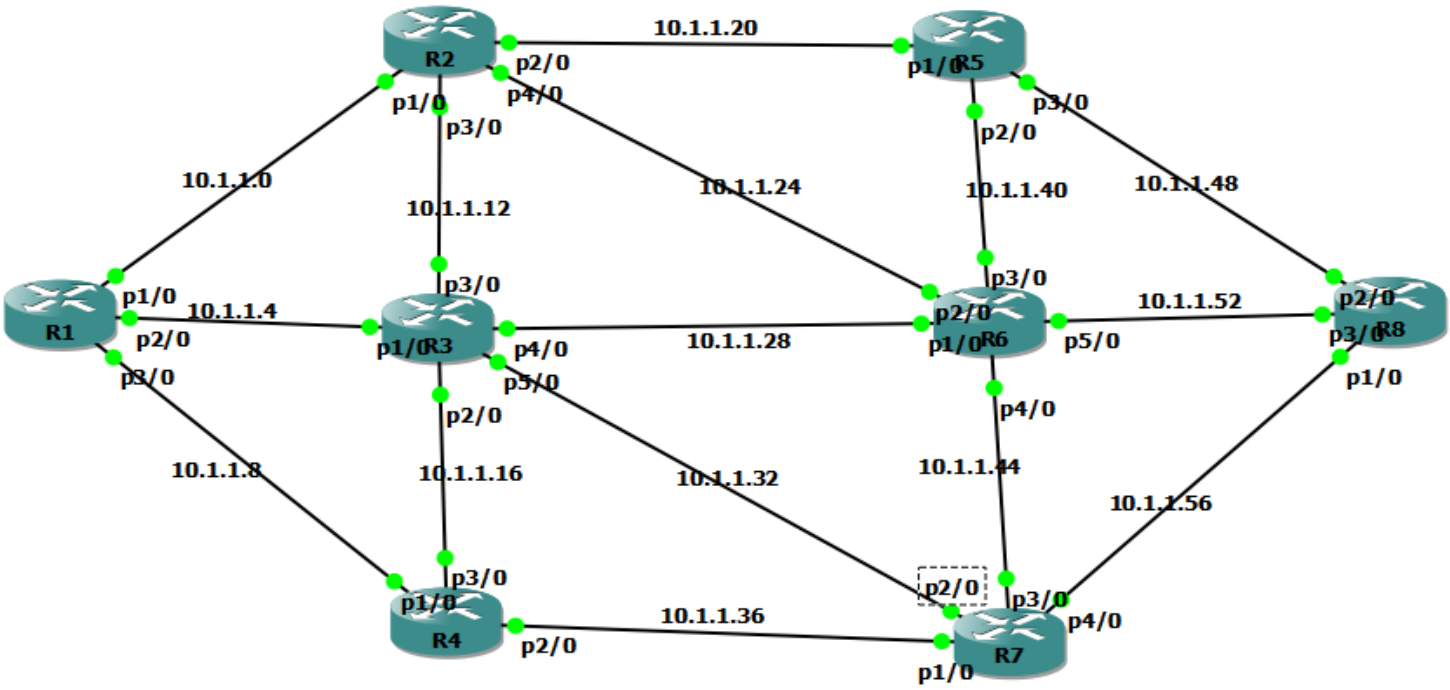
Εικόνα 50 : Απώλειες πακέτων με την πτώση ζεύξεων

7.5 Σενάριο 5. MPLS TE - CSPF (OSPF-TE) / Constraint-Based Routing

Όπως αναφέραμε και στο θεωρητικό μέρος οι αλγόριθμοι δρομολόγησης, που χρησιμοποιούνται στα πρωτόκολλα δρομολόγησης όπως OSPF , RIP κλπ. επιτρέπουν πολύ μικρό έλεγχο του χρήστη πάνω στην επιλογή του μονοπατιού. Επιστρέφουν μόνο συντομότερα μονοπάτια, ενώ για τον χρήστη σημασία μπορεί να έχουν κάποια paths τα οποία αποφεύγουν εσκεμμένα ορισμένους κόμβους και ακμές είτε λόγω των επιλεγμένων πολιτικών τοπολογίας, είτε επειδή κάποιες από αυτές ενδεχομένως έχουν υποστεί βλάβη. Επίσης συνδέσεις μπορεί να μην έχουν επαρκείς πόρους να μεταφέρουν την κίνηση ανάμεσα σε διαδοχικούς κόμβους. Έτσι λοιπόν υπάρχει η ανάγκη για constraint–based αλγορίθμους καθορισμού μονοπατιού, οι οποίοι επιτρέπουν σε έννοιες όπως διαθέσιμο εύρος ζώνης γραμμής, ικανότητες προστασίας σύνδεσης, και διαθέσιμοι πόροι να λαμβάνονται σημαντικά υπόψη κατά την επιλογή του μονοπατιού.

Σε αυτό το σενάριο γίνεται υλοποίηση του MPLS TE (Traffic engineering) σε συνδυασμό με το πρωτόκολλο δρομολόγησης OSFP. Έτσι έχουμε το λεγόμενο CSPF (Constrained Shortest Path First). Είναι μια επέκταση των αλγορίθμων συντομότερης διαδρομής. Η διαδρομή που υπολογίζεται με CSPF είναι μια συντομότερη διαδρομή που πληροί μια σειρά από περιορισμούς.

Η τοπολογία είναι ίδια με των προηγούμενων σεναρίων και αυτή φαίνεται παρακάτω στην εικόνα 51.



Εικόνα 51 : MPLS TE – CSPF τοπολογία

Για την επίτευξη του MPLS TE πρέπει όλα τα interfaces να ρυθμιστούν ώστε να υποστηρίζουν traffic engineering. Επίσης κατά τη διαμόρφωση των δρομολογητών πρέπει να προστεθεί και η κατάλληλη ρύθμιση για να υποστηρίζουν OSPF TE. Τέλος οι ροές κυκλοφορίας αντιστοιχίζονται σε tunnels που έχουμε δημιουργήσει ανάλογα με τον προορισμό τους.

Πιο συγκεκριμένα έχουμε δημιουργήσει δύο tunnels (tunnel0 , tunnel1) στον R1 με προορισμό το Lo interface του R8.

Το tunnel0 έχει ως περιορισμό το bandwidth. Έχουμε θέσει λοιπόν να υπάρχει διαθεσιμότητα σε bandwidth 500Kbps σε όλη τη πορεία της κίνησης προς τον προορισμό. Για να κατευθύνουμε λοιπόν την κίνηση πρέπει να ρυθμίσουμε ανάλογα τα interfaces του κάθε δρομολογητή. Εξ ορισμού ένα Packet over Sonet interface, όπου χρησιμοποιούμε για τις ανάγκες του συγκεκριμένου σεναρίου, έχει φυσικό bandwidth 155000 Kbps. Έχουμε θέσει λοιπόν τα παρακάτω:

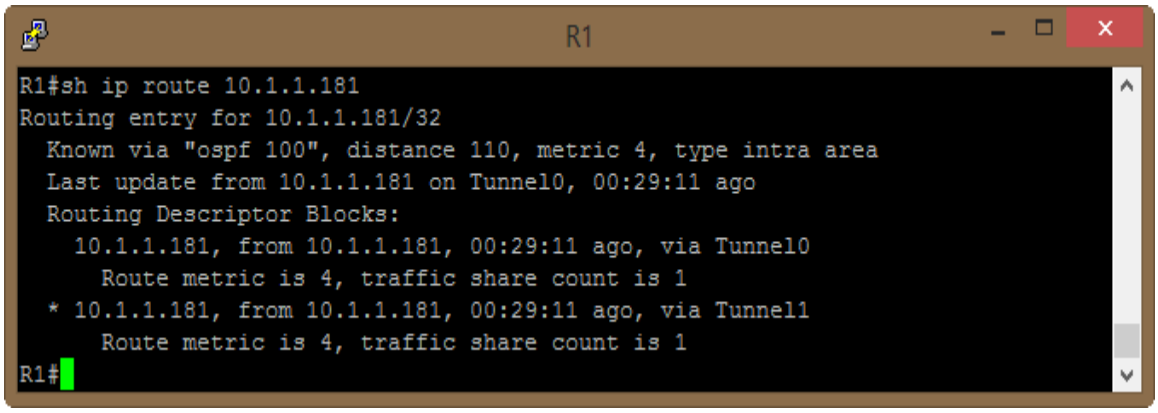
- Δεσμευμένο bandwidth 200 Kbps για τις συνδέσεις R1-R4 , R4-R7 , R7-R8
- Δεσμευμένο bandwidth 800 Kbps για τις συνδέσεις R1-R2 , R2-R5 , R5-R8
- Δεσμευμένο bandwidth 600 Kbps για τις συνδέσεις R1-R3 , R3-R6 , R6-R8

Τα αποτελέσματα των παραπάνω ρυθμίσεων θα τα δούμε στη συνέχεια πιο αναλυτικά.

Το δεύτερο tunnel (tunnel1) έχει ως περιορισμό, ένα συγκεκριμένο μονοπάτι. Δηλαδή η κίνηση θα περάσει από συγκεκριμένους δρομολογητές τους οποίους έχουμε ορίσει στην επεξεργασία της δημιουργίας του tunnel1.

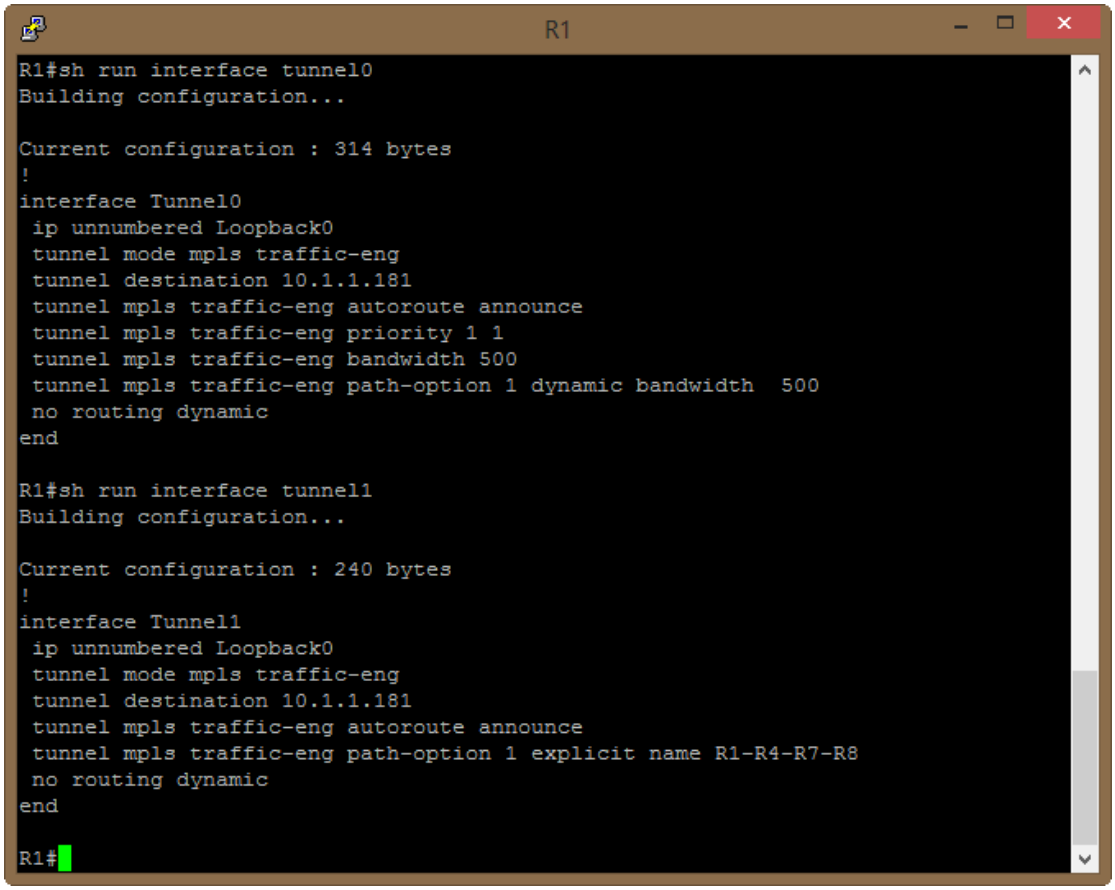
Η διαδρομή που έχει οριστεί είναι η:
R1 - R4 - R7 - R8

Επιβεβαιώνοντας όλα τα παραπάνω βλέπουμε στην Εικόνα 52 πως η κίνηση για το Lo interface του R8 είναι μέσα από τα tunnel0 και tunnel1



Εικόνα 52 : Δρομολόγηση μέσω tunnel – MPLS TE

Στη συνέχεια φαίνονται οι απαραίτητες ρυθμίσεις για τις οποίες έγινε αναφορά προηγουμένως για την δημιουργία των tunnels.

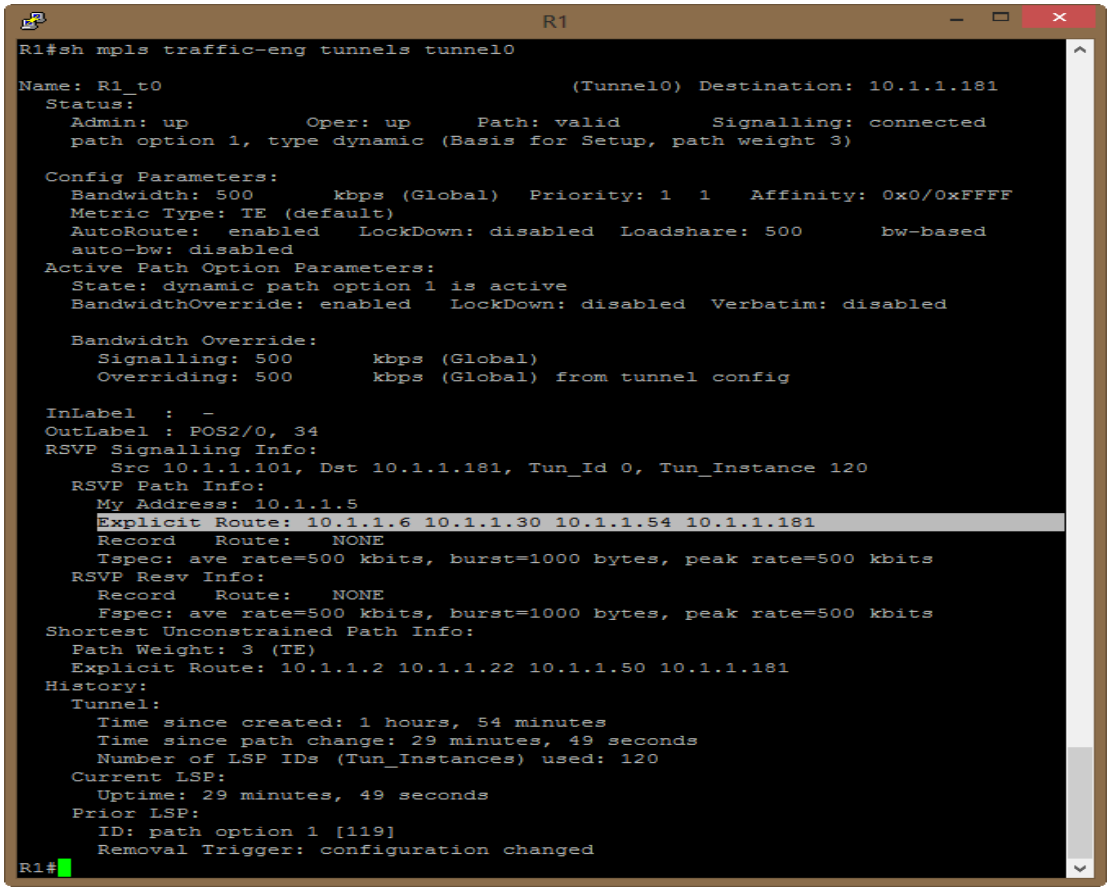


Εικόνα 53 : Δημιουργία Tunnels

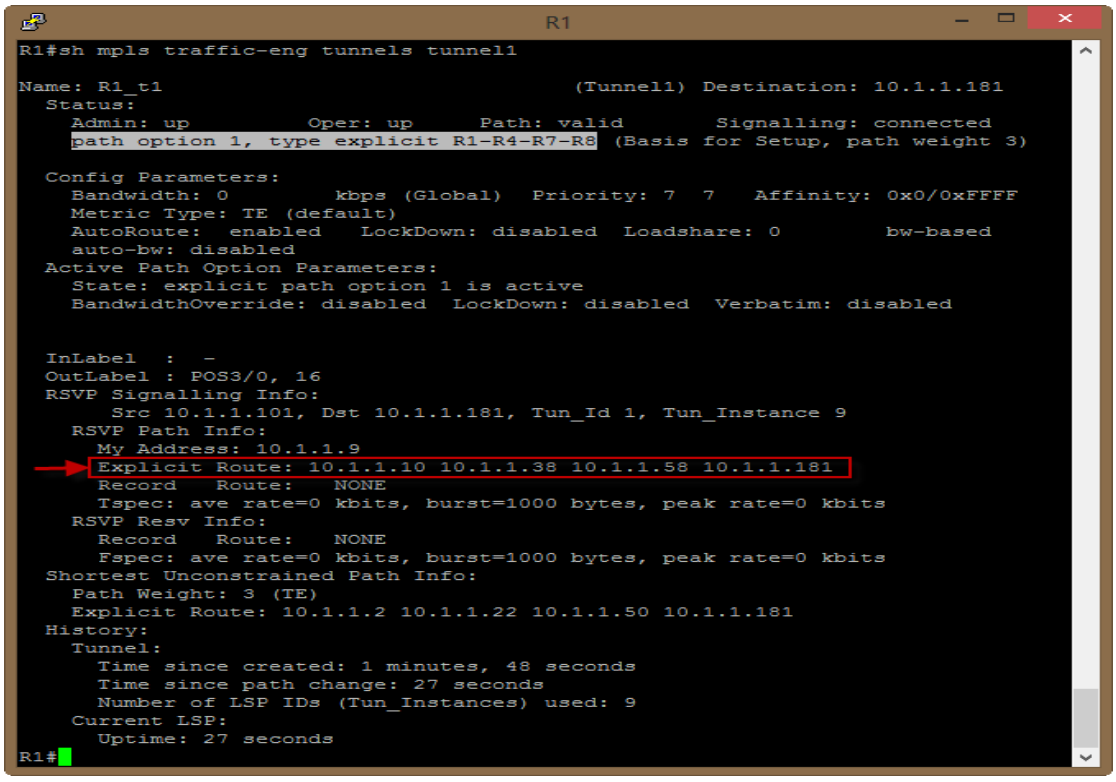
Αποτέλεσμα των παραπάνω είναι να οδηγήσουμε την κίνηση προς τον προορισμό με βάση τους περιορισμούς που έχουμε θέσει εμείς σαν χρήστες.

Στην Εικόνα 54 και 55 φαίνονται τα χαρακτηριστικά των δύο tunnels που έχουμε φτιάξει.

Το Explicit route που έχουμε υπογραμμίσει είναι το μονοπάτι που χρησιμοποιεί το κάθε tunnel



Εικόνα 54 : Tunnel 0



Εικόνα 55 : Tunnel 1

Τέλος βλέπουμε με βάση όσα έχουν προηγηθεί την επικοινωνία του R1 με τον R8 μέσω ενός traceroute και ενός ping command. Επιπρόσθετα προκαλούμε την πτώση μιάς ζεύξης για να δούμε αν υπάρχουν απώλειες και αν η κυκλοφορία των πακέτων συνεχίζεται από το 2^{o} μονοπάτι, καθώς έχουμε δημιουργήσει load balancing μέσω των 2 tunnels.

```
R1
R1#traceroute 10.1.1.181
Type escape sequence to abort.
Tracing the route to 10.1.1.181
VRF info: (vrf in name/id, vrf out name/id)
  1 10.1.1.6 [MPLS: Label 34 Exp 0] 48 msec
    10.1.1.10 [MPLS: Label 35 Exp 0] 40 msec
    10.1.1.6 [MPLS: Label 34 Exp 0] 44 msec
  2 10.1.1.38 [MPLS: Label 34 Exp 0] 48 msec
    10.1.1.30 [MPLS: Label 33 Exp 0] 44 msec
    10.1.1.38 [MPLS: Label 34 Exp 0] 64 msec
  3 10.1.1.54 60 msec
    10.1.1.58 44 msec
    10.1.1.54 28 msec
R1#
```

Εικόνα 56 : Traceroute R1 – Lo R8

```
R1
R1#ping 10.1.1.181 repeat 300
Type escape sequence to abort.
Sending 300, 100-byte ICMP Echos to 10.1.1.181, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!........
*Apr  7 15:08:30.555: %LDP-5-NBRCHG: LDP Neighbor 10.1.1.141:0 (5) is DOWN (Disc
overy Hello Hold Timer expired).........
*Apr  7 15:08:48.883: %LINEPROTO-5-UPDOWN: Line protocol on Interface POS3/0, ch
anged state to down
*Apr  7 15:08:48.915: %OSPF-5-ADJCHG: Process 100, Nbr 10.1.1.141 on POS3/0 from
 FULL to DOWN, Neighbor Down: Interface down or detached..
.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 93 percent (280/300), round-trip min/avg/max = 28/48/248 ms
R1#
*Apr  7 15:09:07.883: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel1, c
hanged state to down
R1#
```

Εικόνα 57 : Ping R1 – Lo R8

8. Συμπεράσματα

Η παρούσα διπλωματική εργασία είχε ως στόχο τη μελέτη της MPLS τεχνολογίας τόσο σε θεωρητικό, όσο και σε πρακτικό επίπεδο. Παρουσιάστηκαν εφαρμογές, μηχανισμοί και η λειτουργία της εν λόγω τεχνολογίας καθώς επίσης και σενάρια MPLS, στο πρακτικό μέρος, με την αλληλεπίδραση πρωτοκόλλων δρομολόγησης και λειτουργιών όπως MPLS VPN και MPLS TE. Η δημιουργία των σεναρίων έγινε με σκοπό την εφαρμογή όσων αναφέρθηκαν στο θεωρητικό μέρος καθώς επίσης και την επίτευξη λειτουργίας εξισορρόπησης φορτίου (Load Balancing) και αναδρομολόγησης της κίνησης (Re-routing).

Συμπερασματικά, το MPLS είναι ένας μηχανισμός που μπορεί να αποφέρει πολλά πλεονεκτήματα στην αγορά, δίνοντας λύση σε ζητήματα που αφορούν την καθημερινότητα, όπως εξοικονόμηση κόστους, ποιότητα υπηρεσίας, επεκτασιμότητα και διαχείριση εύρους ζώνης. Μερικά, λοιπόν, από τα προαναφερθέντα οφέλη του MPLS, μελετήθηκαν μέσω των λειτουργιών του Traffic Engineering και MPLS – VPN, στο πρακτικό μέρος της εν λόγω εργασίας. Παράλληλα, το γεγονός ότι το MPLS μπορεί να συνυπάρξει με πολλά από τα πρωτόκολλα δρομολόγησης, που έχουν ήδη διαδοθεί στην αγορά, δίνει πρόσφορο έδαφος στη διάδοσή του. Μερικά από τα πρωτόκολλα αυτά μελετήθηκαν στη παρούσα εργασία επιβεβαιώνοντας ότι το MPLS είναι επιπροσθέτως ένας ευέλικτος μηχανισμός.

Βιβλιογραφία

1. Andrew S. Tanenbaum - Computer networks Prentice Hall PTR, 2003
2. Rick Graziani , Allan Johnson - Routing Protocols and Concepts
3. Mark A.Dye , Rick McDonald , Antoon W. Rufi – Network Fundamentals
4. Rob Vachon , Rick Graziani - Accessing the WAN
5. MPLS Traffic Engineering Path Calculation and Setup Configuration Guide, Cisco IOS Release 15.0M
6. MPLS Traffic Engineering Path, Link, and Node Protection Configuration Guide, Cisco IOS Release 15.0M
7. Wendell Odom , Rus Healy , Denise Donohue – CCIE Routing and Switching
8. Presentation Henning Peters – Fast Reroute in MPLS
9. Luc De Ghein - MPLS Fundamentals
10. Cisco Presentation - TROUBLESHOOTING MPLS NETWORKS
11. www.nortel.com - Troubleshooting – MPLS
12. http://searchenterprisewan.techtarget.com/tutorial/MPLS-VPN-basics
13. http://fengnet.com/book/ios_mpls/ch09lev1sec4.html
14. http://www.cisco.com/en/US/tech/tk436/tk428/technologies_configuration_example09186a0080093fd0.shtml
15. http://www.ciscopress.com/articles/article.asp?p=426640&seqNum=3

16. http://gns3vault.com/Labs/MPLS/

17. http://blog.ipexpert.com/2009/04/15/mpls-te-%E2%80%93-load-sharing/

18. http://iwing.wordpress.com/black-box/belajar-mengkonfigurasi-mpls-te-unequal-cost-load-sharing/

19. http://www.gompls.net/2009/08/what-is-mpls-and-why-do-we-need-it.html

20. http://www.ee.ucl.ac.uk/lcs/previous/LCS2004/9.pdf

21. https://learningnetwork.cisco.com/thread/42549

22. http://www.ciscopress.com/articles/article.asp?p=426640&seqNum=5

23. http://www.cathayschool.com/MPLS-Traffic-Engineering-with-Autoroute-a285.html

24. https://sites.google.com/site/amitsciscozone/home/important-tips/traffic-engineering/mpls-te-basics

25. http://www.cisco.com/en/US/tech/tk436/tk428/technologies_configuration_example09186a0080093f23.shtml

26. http://www.ccie18473.net/dynamips/dynamips.htm#mpls-te

27. http://www.cisco.com/en/US/docs/ios/12_0s/feature/guide/pplb.html#wp1028971

28. http://www.gns3.net/

29. http://www.gns3.net/documentation/

30. http://forum.gns3.net/

31. http://www.iptut.com/ccip-knowledge/practice-ccip-gns3-lab/simple-mpls-gns3-lab

32. http://rednectar.net/2011/03/27/excellent-mpls-configuration-example/

33. http://blog.ipexpert.com/2009/05/27/mpls-te-bandwidth-and-priority/

34. http://www.cisco.com/en/US/docs/switches/datacenter/sw/5_x/nx-os/mpls/configuration/guide/mpls_qos.html#wp1097336

35. http://en.wikipedia.org/wiki/Wiki

36. RFC 3031 - MPLS Architecture

37. RFC 2547 - BGP/MPLS VPNs

38. RFC 4659 - BGP-MPLS IP VPN Extension for IPv6 VPN

39. RFC 2702 - MPLS Traffic Engineering

40. RFC 4577 - OSPF for BGP/MPLS IP VPNs

Παράρτημα Α

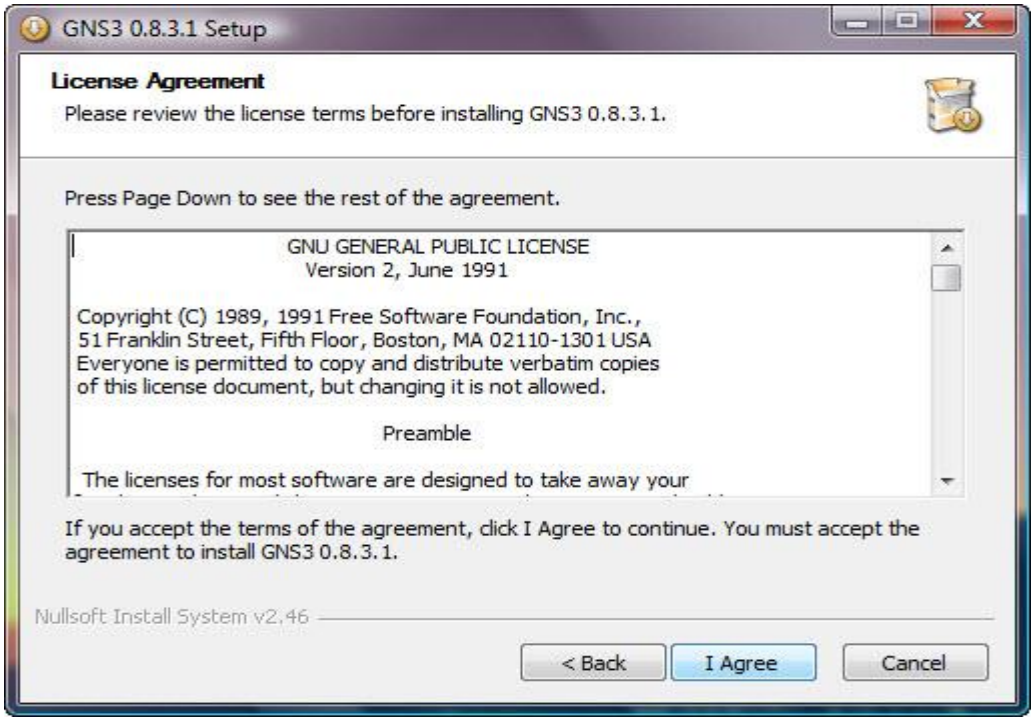
1. Λήψη και εγκατάσταση GNS3

Η τελευταία έκδοση του εργαλείου GNS3 είναι διαθέσιμη για μεταφόρτωση από το σύνδεσμο http://www.gns3.net/download/ . Η τελευταία έκδοση του εργαλείου είναι διαθέσιμη για λειτουργικά συστήματα Windows XP, Vista, Windows 7 και Windows 8 καθώς επίσης και για εκδόσεις LINUX και Mac OS. Η εγκατάσταση πρέπει να γίνει από λογαριασμό όπου διαθέτει προνόμια διαχειριστή αλλιώς ενδέχεται να προκληθούν σφάλματα του τύπου “Access Denied”.

Σημείωση: Απαιτείται 50MB ελεύθερος χώρος μόνο για το αρχείο .exe

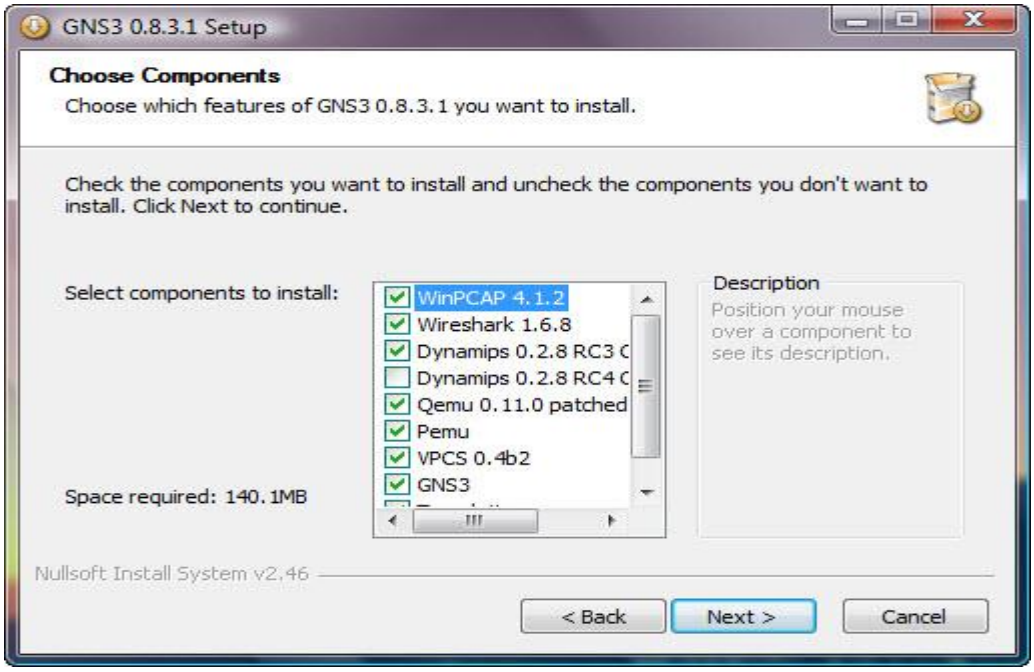
Εικόνα 1 : Εγκατάσταση της εφαρμογής GNS3

Κατά τη διάρκεια της εγκατάστασης ο χρήστης θα πρέπει να παρέχει κάποιες βασικές πληροφορίες στο παράθυρο αλληλεπίδρασης και να αποδεχτεί την άδεια χρήσης ώστε να ξεκινήσει η εγκατάσταση.



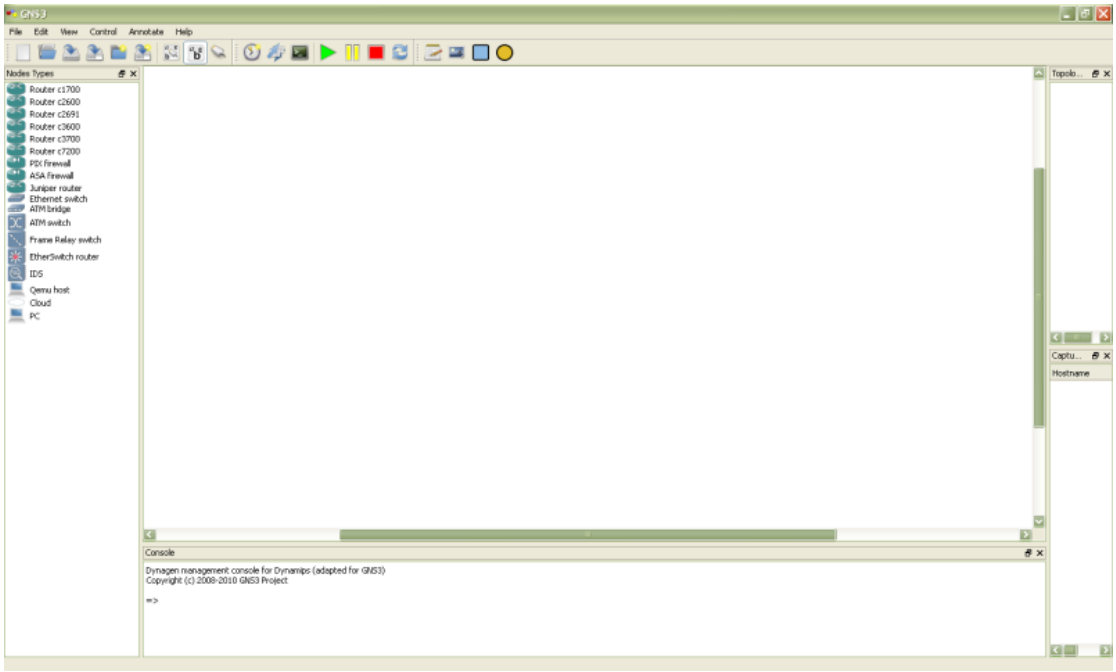
Εικόνα 2 : Άδεια χρήσης του GNS3

Μετά την αποδοχή των όρων για εγκατάσταση επιλέγουμε τα εργαλεία που θέλουμε να εγκαταστήσουμε. (συνίσταται να αφήσετε τις προκαθορισμένες επιλογές)



Εικόνα 3 : Επιλογή εργαλείων εγκατάστασης

Μετά το τέλος της εγκατάστασης ανοίξτε το πρόγραμμα για να βεβαιωθείτε για την σωστή εγκατάστασή του.



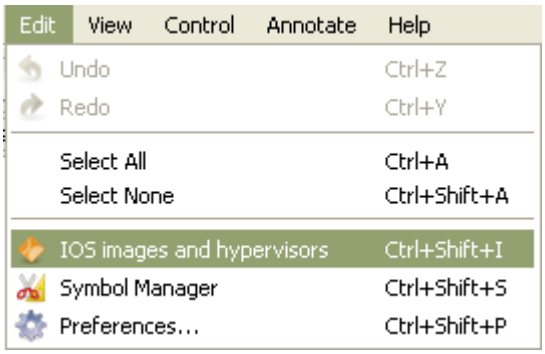
Εικόνα 4 : Επιβεβαίωση Εγκατάστασης GNS3

2. Βασικές ρυθμίσεις περιβάλλοντος GNS3

2.1 Καθορισμός IOS image

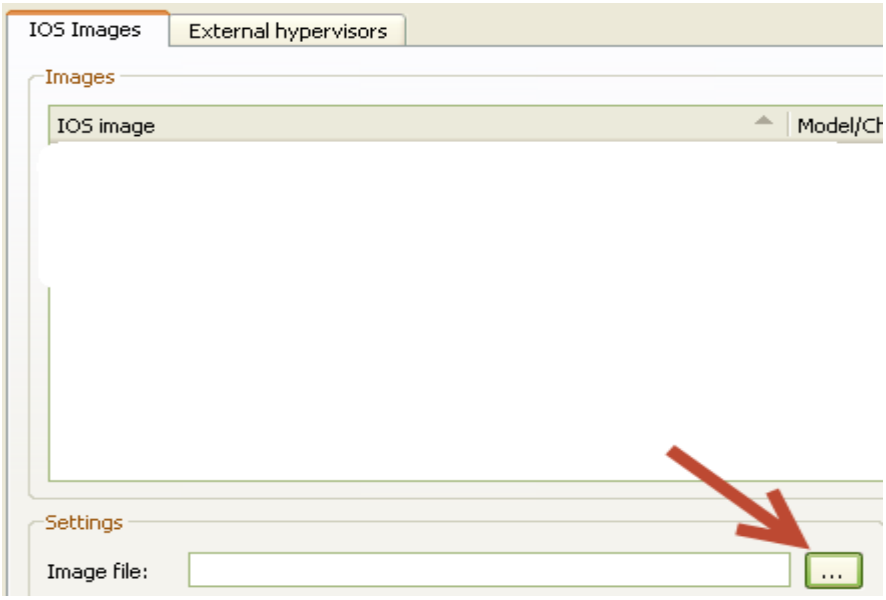
Για τον καθορισμό ενός IOS ακολουθήστε τα παρακάτω:

Στο *Edit* menu επιλέξτε *IOS images and hypervisors*



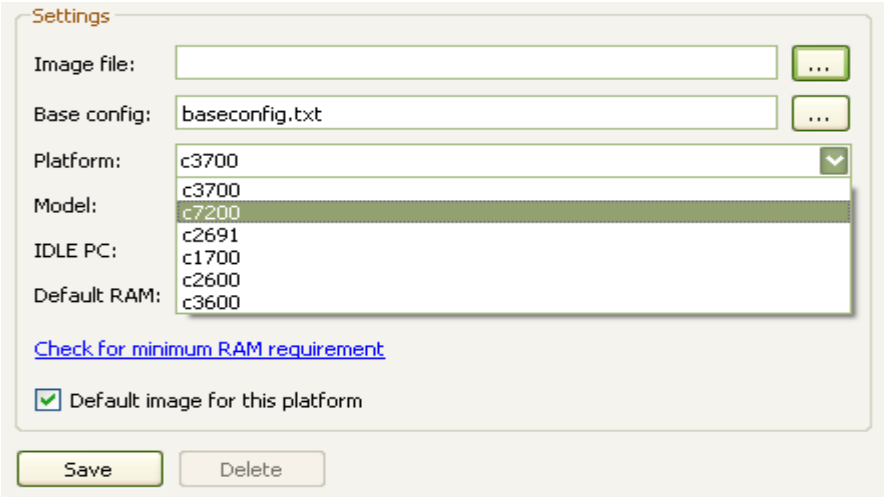
Εικόνα 5 : Καθορισμός IOS image

Κάτω από την καρτέλα *IOS Images*, κάντε κλικ στο κουμπί  και στη συνέχεια να βρείτε το IOS αρχείο και κάντε κλικ στο κουμπί Άνοιγμα.



Εικόνα 6 : Εύρεση αρχείου IOS

Στη συνέχεια επιλέξτε την πλατφόρμα *(Platform)* που αντιστοιχεί στο IOS image που έχετε καταχωρήσει και αντίστοιχα το μοντέλο *(Model).*



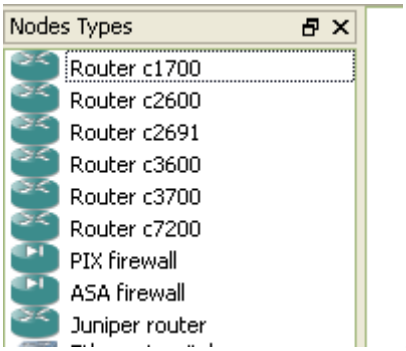
Εικόνα 7 : Καθορισμός και αντιστοίχηση πλατφόρμας για το IOS

Κάντε κλικ στο κουμπί *Save* και στη συνέχεια στο κουμπί *Close*.

2.2 Καθορισμός IDLE PC

Στην κεντρική οθόνη του GNS3 στο αριστερό τμήμα μπορούμε να δούμε όλους τους τύπους των routers,switches κλπ που μπορούν να χρησιμοποιηθούν. Επιπλέον μπορούμε να προσθέσουμε και άλλους τύπους και θα δούμε αργότερα πως μπορούμε να το κάνουμε αυτό. Το δεξιό τμήμα μας παρέχει μία σύνοψη της τοπολογίας που έχουμε σχεδιάσει, και θα δούμε αργότερα πως χτίζεται. Τέλος το μεσαίο και πιο σημαντικό τμήμα περιλαμβάνει δύο υπό-τμήματα (πάνω και κάτω). Το πάνω τμήμα είναι ο χώρος εργασίας όπου η τοπολογία μπορεί να χτιστεί. Το κάτω τμήμα καλείται Console και δείχνει τη λειτουργία του Dynagen.

Κάντε κλικ σε ένα εικονίδιο κάτω από το *Node Types*

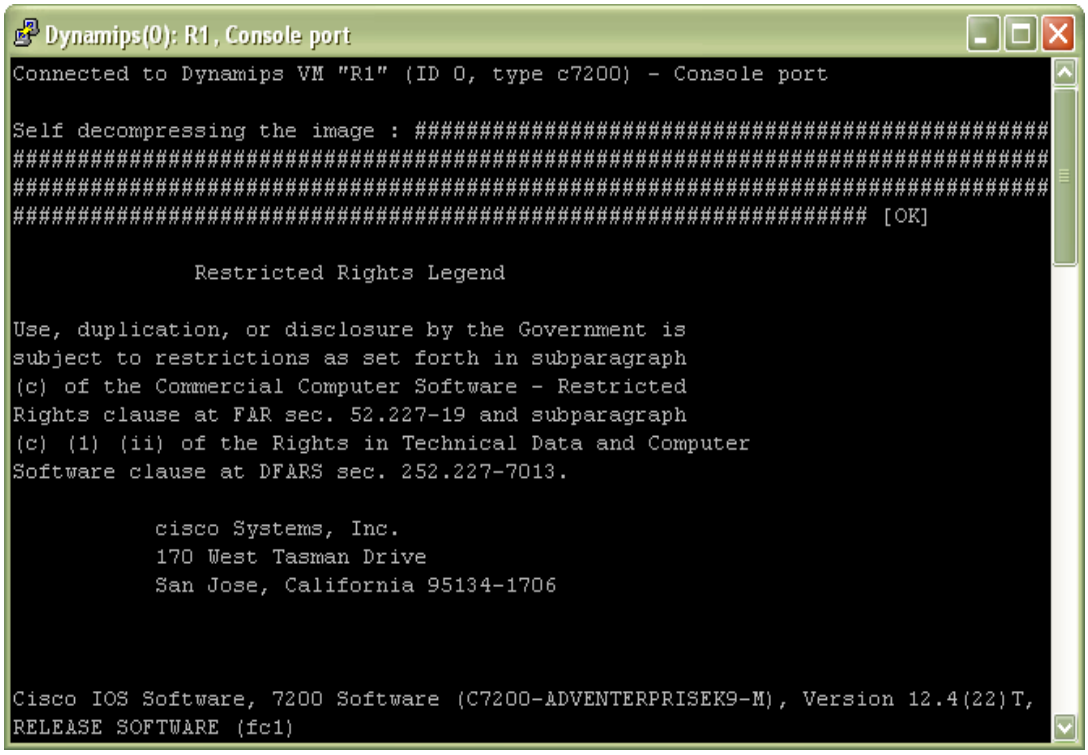


.

Στο παράδειγμά μας, χρησιμοποιούμε μια πλατφόρμα 7200, όπως αναφέρθηκε και

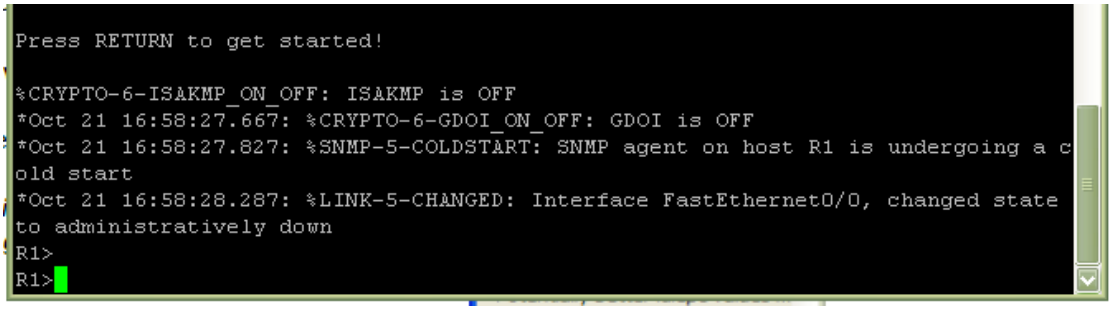
πιο πάνω. Σύρετε τον κατάλληλο τύπο router πάνω στο χώρο εργασίας ώστε να ξεκινήσετε να χτίζετε μία τοπολογία.

Κάνοντας δεξί κλικ πάνω στον router και επιλέγοντας *Configure* μπορούμε να δούμε και να κάνουμε κάποιες ρυθμίσεις. Τελειώνοντας κάνουμε δεξί κλικ πάνω στον router και *Start* και δεξί κλικ και *Console*



Εικόνα 8 : Router Console

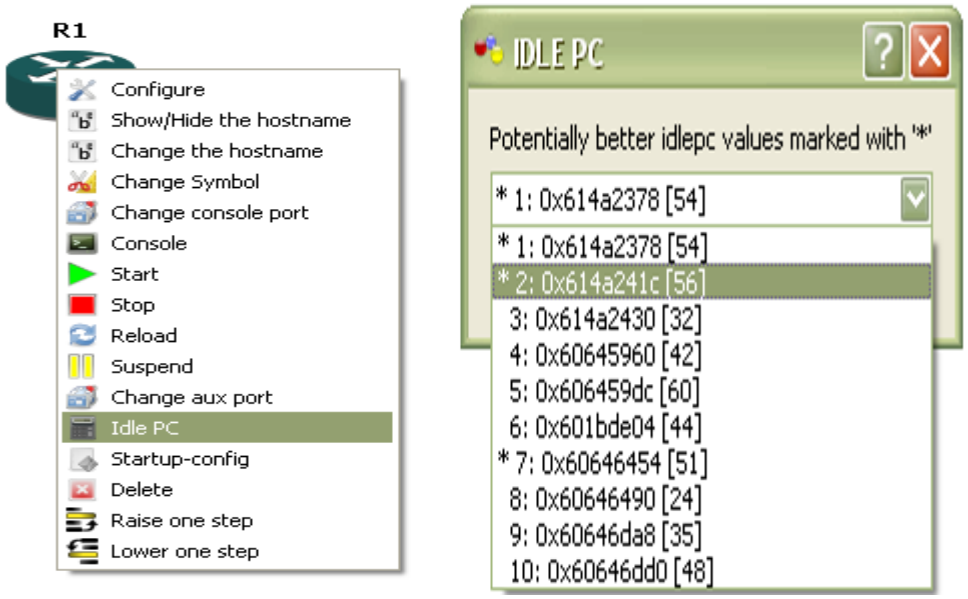
Στο σημείο αυτό ο router είναι έτοιμος για διαμόρφωση.



Εικόνα 9 : Διαμόρφωση Δρομολογητή

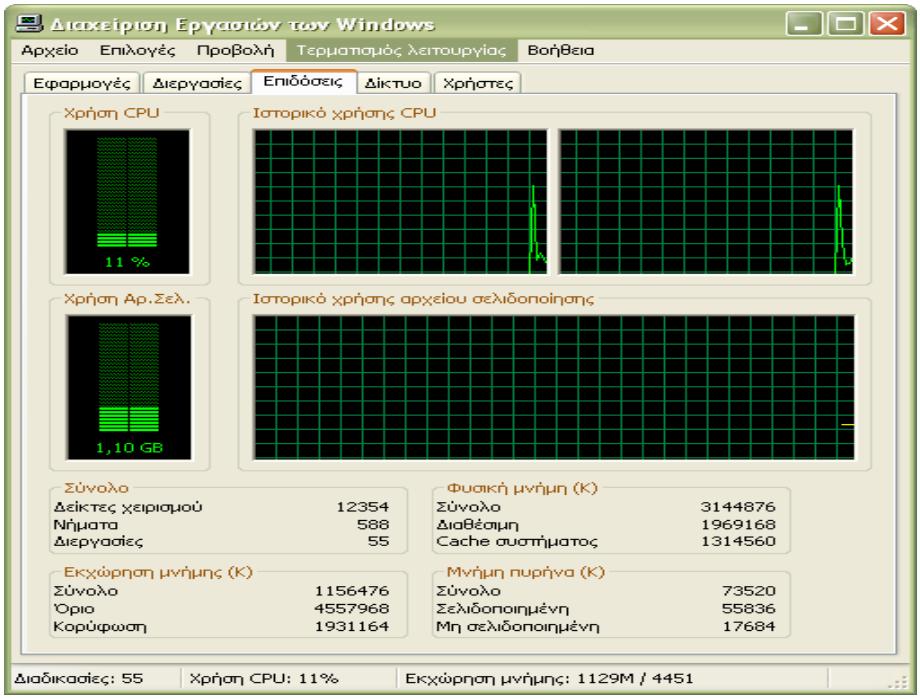
Λόγω του ότι όταν είναι σε λειτουργία (*Start*) οι router της τοπολογίας μας ανεβαίνει κατά πολύ η χρήση της CPU του συστήματός μας θα πρέπει να κάνουμε

μία τελευταία ενέργεια ώστε να θέσουμε τους routers της τοπολογίας να δουλεύουν ως *Idle PC.* Παρακάτω απεικονίζονται οι ενέργειες που χρειάζονται για να γίνει αυτό.



Εικόνα 10 : Καθορισμός IDLE PC

Η καλύτερη επιλογή για ένα Idle PC είναι αυτές που έχουν αστερίσκο (π.χ.1,2 ,7). Για να δούμε πόσο πολύ επηρεάζει θετικά αυτή η ενέργεια τον υπολογιστή μας πατάμε *Ctrl+ALT+DEL* και *Performance* για να δούμε τη χρήση της CPU ότι μειώθηκε με την επιλογή του *Idle PC*.



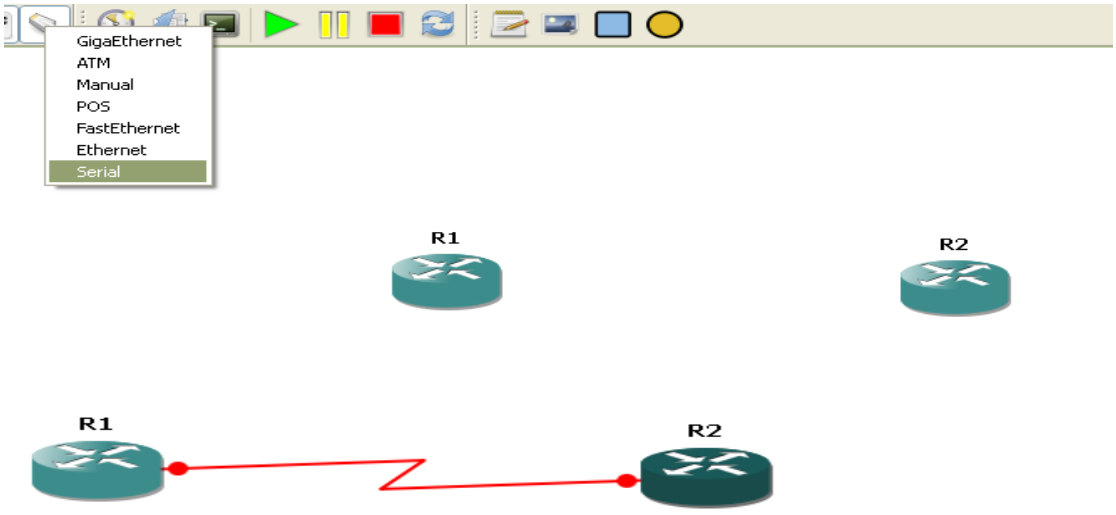
Εικόνα 11 : CPU & RAM επίδοση

Για να επιβεβαιώσουμε ότι η χρήση του *Idle PC* πραγματοποιήθηκε πηγαίνουμε στο *Edit* menu -> *IOS images and hypervisor* και ελέγχουμε ότι στο Idle PC έχει εισαχθεί η τιμή που επιλέξαμε.

Μπορείτε τώρα να επιστρέψετε στο παράθυρο του telnet σας (Console) και να χρησιμοποιήσετε το δρομολογητή σας.

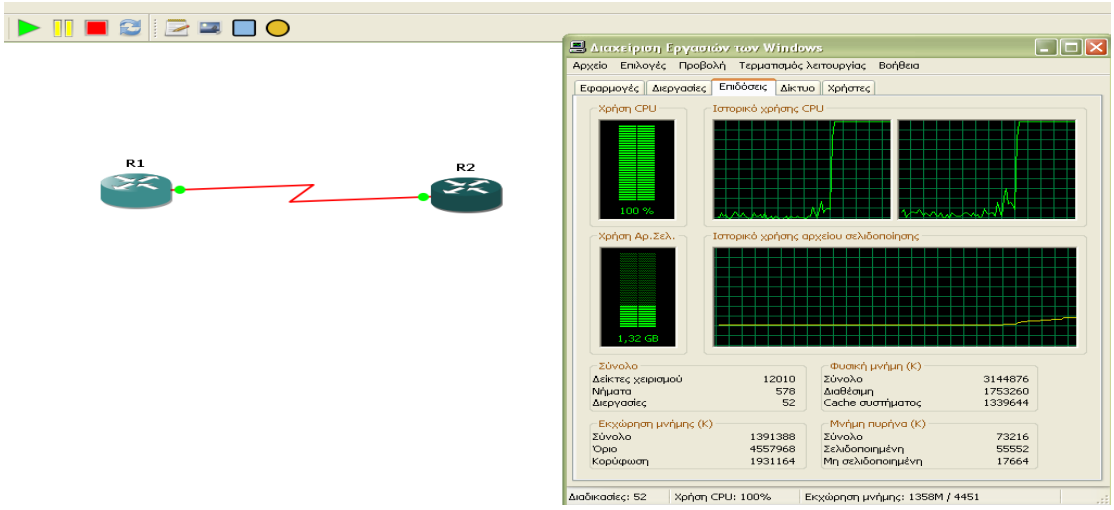
3. Δημιουργία Τοπολογίας

Παρακάτω παρουσιάζεται ένα απλό παράδειγμα σύνδεσης και επιτυχίας επικοινωνίας 2 δρομολογητών.



Εικόνα 13 : Σύνδεση δρομολογητών

Αφού έχουμε εισάγει και συνδέσει του δρομολογητές στη συνέχεια απαιτείται η εκκίνησή τους (Start) και ο καθορισμός IDLE PC για την ομαλότερη λειτουργία του συστήματος, όπως περιγράψαμε και στην ενότητα 2.2 του παρόντος Παραρτήματος.



Εικόνα 14 : Εκκίνηση δρομολογητών

Ανοίγουμε την Console του εκάστοτε router και πληκτρολογούμε τα παρακάτω (**bold**) ώστε να επιτύχουμε μια επικοινωνία μεταξύ των 2 routers.

R1**#enable**

R1**#configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)**#interface s1/0**

R1(config-if)**#ip add 192.168.1.1 255.255.255.252**

R1(config-if)**#no shutdown**

R1(config-if)#

*Jul 21 18:07:19.895: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up

R1(config-if)#

*Jul 21 18:06:19.895: %ENTITY_ALARM-6-INFO: CLEAR INFO Se1/0 Physical Port Administrative State Down

R1(config-if)#

*Jul 21 18:06:20.903: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up

R1(config-if)**#^Z (Πατάμε Ctrl+Z)**

R1#copy

*Jul 21 18:07:34.055: %SYS-5-CONFIG_I: Configured from console by console

R1**#copy run start**

Destination filename [startup-config]? **(Πατάμε enter)**

Building configuration...

[OK]

R2**#enable**

R2**#configure terminal**

Enter configuration commands, one per line. End with CNTL/Z.

R2(config)**#interface s1/0**

R2(config-if)**#ip add 192.168.1.2 255.255.255.252**

R2(config-if)**#no shutdown**

R2(config-if)#

*Jul 21 18:07:19.895: %LINK-3-UPDOWN: Interface Serial1/0, changed state to up

R2(config-if)#

*Jul 21 18:07:19.895: %ENTITY_ALARM-6-INFO: CLEAR INFO Se1/0 Physical Port Administrative State Down

R2(config-if)#

*Jul 21 18:07:20.903: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial1/0, changed state to up

R2(config-if)# **^Z (Πατάμε Ctrl+Z)**

R2#copy

*Jul 21 18:07:34.055: %SYS-5-CONFIG_I: Configured from console by console

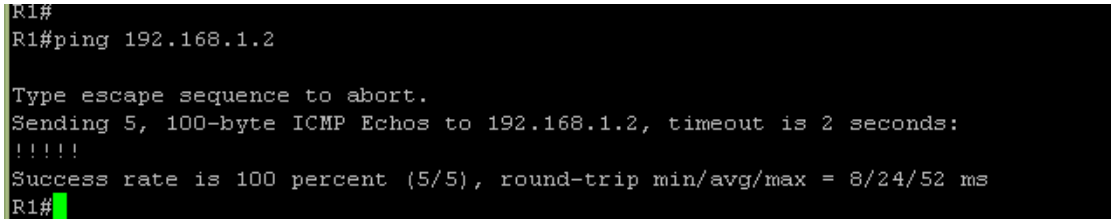
R2**#copy run start**

Destination filename [startup-config]? **(Πατάμε enter)**

Building configuration...

[OK]

Ελέγχουμε την επικοινωνία των 2 δρομολογητών με την εντολή ping από τον R1 προς τον R2

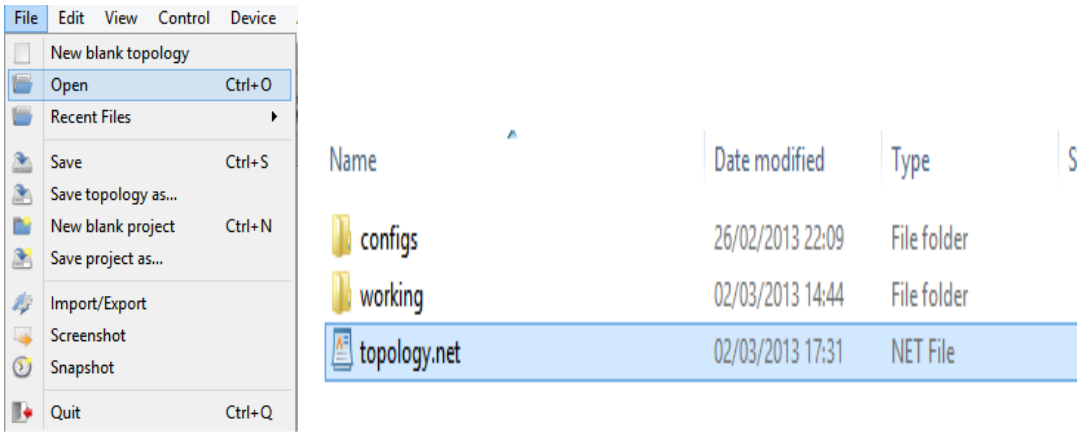


Εικόνα 15 : Επιβεβαίωση επικοινωνίας μέσω ping

4. Άνοιγμα υπάρχουσας τοπολογίας

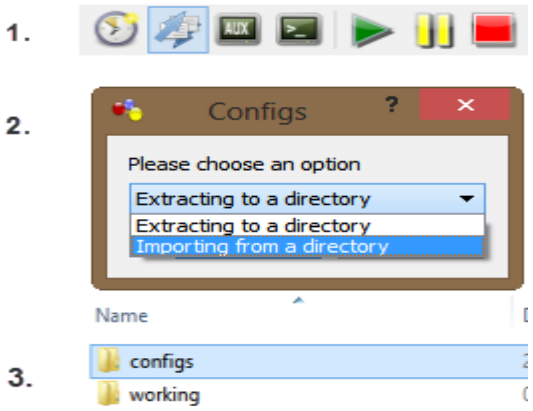
Για να ανοίξουμε μία τοπολογία και να εισάγουμε τα αντίστοιχα αρχεία διαμόρφωσης ώστε το δίκτυο μας να είναι λειτουργικό, ακολουθούμε την παρακάτω διαδικασία.

Ανοίγουμε το αρχείο .net που έχουμε αποθηκεύσει σε τοποθεσία της επιλογής μας



Εικόνα 16 : Άνοιγμα τοπολογίας

Στη συνέχεια εισάγουμε τα αρχεία διαμόρφωσης της συγκεκριμένης τοπολογίας που βρίσκονται στο φάκελο ../configs/ στην τοποθεσία που έχουμε αποθηκεύσει το project.



Εικόνα 17 : Εισαγωγή αρχείων διαμόρφωσης

Παράρτημα Β

Σχετικά με τα σενάρια υλοποίησης και λεπτομέρειες που αφορούν την δημιουργία και λειτουργία τους παρακαλώ επικοινωνήστε με το συγγραφέα της διπλωματικής εργασίας στο ακόλουθο email: sotirisbakas@gmail.com