ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

Πρόγραμμα Μεταπτυχιακών Σπουδών
Επιστήμη και Τεχνολογία της Πληροφορικής και των Υπολογιστών

Ειδίκευση Δικτύων Επικοινωνιών και Κατανεμημένων Συστημάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μεταφορά Ethernet υπηρεσιών σε MPLS δίκτυο

Κουλούρης Θεόδωρος

Α.Μ.18006

Ημερομηνία εξέτασης 08-06-2022

Επιβλέπων : Δρ Μπόγρης Αντώνιος , Καθηγητής

ΑΘΗΝΑ ΙΟΥΝΙΟΣ 2022

Μεταφορά Ethernet υπηρεσιών σε MPLS δίκτυο

Μέλη Εξεταστικής Επιτροπής συμπεριλαμβανομένου και του Εισηγητή

Η διπλωματική εργασία εξετάστηκε επιτυχώς από την κάτωθι Εξεταστική Επιτροπή:

Α/α	ΟΝΟΜΑ ΕΠΩΝΥΜΟ	ΒΑΘΜΙΔΑ/ΙΔΙΟΤΗΤΑ	ΨΗΦΙΑΚΗ ΥΠΟΓΡΑΦΗ
1	Μπόγρης Αντώνης	Καθηγητής	Antonios Bogris Digitally signed by Antonios Bogris Date: 2022.06.16 15:10:16 +03'00'
2	Καρκαζής Παναγιώτης	Αναπληρωτής καθηγητής	Panagiotis Karkazis Digitally signed by Panagiotis Karkazis Date: 2022.06.18 11:18:41 +03'00'
3	Ψαρράς Νίκος	Λέκτορας	Digitally signed by Nikolaos Psarras Date: 2022.06.16 23:24:35 +03'00'

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος **Κουλούρης Θεόδωρος** του **Νικολάου** , με αριθμό μητρώου **mcse18006** φοιτητής του Προγράμματος Μεταπτυχιακών Σπουδών **Επιστήμη και Τεχνολογία της Πληροφορικής και των Υπολογιστών** του Τμήματος **Μηχανικών Πληροφορικής και Υπολογιστών της Σχολής Μηχανικών** του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:

«Είμαι συγγραφέας αυτής της διπλωματικής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.
Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».
Επιθυμώ την απαγόρευση πρόσβασης στο πλήρες κείμενο της εργασίας μου μέχρι **08/06/2022** και έπειτα από αίτηση μου στη Βιβλιοθήκη και έγκριση του επιβλέποντα καθηγητή.

Ο Δηλών

Κουλούρης Θεόδωρος

*** Αντώνιος Μπόγρης /Καθηγητής**

Antonios Bogris

Digitally signed by Antonios Bogris
Date: 2022.06.16 15:10:42 +03'00'

Ψηφιακή Υπογραφή Επιβλέποντα

08/06/2022

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα διπλωματική εργασία ‘’Μεταφορά Ethernet υπηρεσιών σε MPLS δίκτυο’’ πραγματοποιήθηκε στο πλαίσιο του μεταπτυχιακού ‘’ Επιστήμη και Τεχνολογία της Πληροφορικής και των Υπολογιστών’’. Θα ήθελα να ευχαριστήσω τον κύριο Μπόγρη Αντώνιο που με καθοδήγησε μέχρι την ολοκλήρωση της διπλωματικής εργασίας.

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία ασχολείται με μεταφορά Ethernet υπηρεσιών σε MPLS δίκτυο. Το EoMPLS σημαίνει Ethernet over MPLS.Το Pseudowire είναι μια εξομοίωση μιας ενσύρματης σύνδεσης. Χρησιμοποιείται για την παροχή υπηρεσιών από άκρο σε άκρο σε ένα δίκτυο MPLS.

Το MPLS είναι μια τεχνολογία που μεταφέρει αρχιτεκτονικές πρωτοκόλλου όπως ATM και Ethernet. Το MPLS εγγυάται την ποιότητα υπηρεσιών , εξασφαλίζει υψηλή ταχύτητα μεταφορά πακέτων και διασφαλίζει μεταξύ άλλων την επικοινωνία μεταξύ των δρομολογητών εντός του κυρίου δικτύου.

Αυτή η τεχνολογία έχει πολλά πλεονεκτήματα όπως η καλή απόδοση δικτύου χωρίς να χρειάζεται να αλλάξουμε ολόκληρο το σύστημα. Δυναμικά, transparent δίκτυα L2 με υποστήριξη για traffic engineering. Χρησιμοποιούμε το Ethernet για όλες τις τοποθεσίες ανεξάρτητα από τη θέση.

Πειραματικά σε ένα IP/MPLS δίκτυο θα δούμε κάποια σενάρια με διάφορες τεχνικές MPLS L2 VPN (VPWS-AtoM). Στο πρώτο μέρος θα αποδείξουμε ότι κάθε VLAN αντικατοπτρίζεται με ένα Pseudowire circuit. Θα αποδώσουμε Layer 2 επικοινωνία μεταξύ κόμβων που ανήκουν στον ίδιο πελάτη. Έπειτα το attachment circuit (AC) είναι ένα Ethernet VLAN trunk, οι διεπαφές των Carrier Ethernet (CE) δρομολογητών συνδέονται με τους provider edge route (PE) δρομολογητές με 802.1Q sub interfaces.

Στο δεύτερο μέρος θα χρησιμοποιήσουμε Eompls μέσω EVC (Ethernet Virtual Circuits). Αυτό θα μας προσφέρει σε οικονομικό επίπεδο γιατί έτσι δεν θα δεσμεύουμε μια φυσική διεπαφή στους PE δρομολογητές για την εξυπηρέτηση κάθε καινούριου πελάτη.

Το τρίτο και τελευταίο μέρος θα υπάρξει η δυνατότητα backup L2 VPN κύκλωμα για την διασφάλιση της παροχής υπηρεσιών. Αυτό μας το διασφαλίζει το L2VPN Pseudowire Redundancy. Αυτό γίνεται μέσω μιας εναλλακτικής διαδρομής που βρίσκει το δίκτυο όταν η σύνδεση μεταξύ δρομολογητών αποτύχει.

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ : MPLS, EoMPLS , Ethernet VLAN, EVC, MPLS L2VPN Redundancy

Περιεχόμενα

Πίνακας Εικόνων

1. Εισαγωγή

Στο κεφάλαιο αυτό θα παρουσιάσουμε με σύντομο τρόπο τι δομή , τι σκοπό και με ποια μέσα θα υλοποιηθεί.

1.1 Περιγραφή του αντικειμένου

Η παρούσα διπλωματική εργασία ασχολείται με μεταφορά Ethernet υπηρεσιών σε MPLS δίκτυο. Το EoMPLS σημαίνει Ethernet over MPLS. Το Pseudowire είναι μια εξομοίωση μιας ενσύρματης σύνδεσης. Χρησιμοποιείται για την παροχή υπηρεσιών από άκρο σε άκρο σε ένα δίκτυο MPLS.

Θα αποδειχθεί ότι κάθε VLAN θα αντικατοπτριστεί με ένα pseudowire circuit. Έπειτα θα προσπαθήσουμε να μειώσουμε το κόστος χρησιμοποιώντας το EVC (Ethernet Virtual Circuits) στο EoMPLS. Τελικά θα θωρακίσουμε το δίκτυο χρησιμοποιώντας το backup L2 VPN κύκλωμα ώστε να διασφαλίζει μια εναλλακτική διαδρομή αν η σύνδεση μεταξύ δρομολογητών αποτύχει.

1.2 Ανασκόπηση της Διπλωματικής εργασίας

Στο κεφάλαιο 2 θα αναφερθούμε στο LAN, τους τύπους LAN και το μοντέλο αναφοράς OSI. Στο 2.4 θα υπάρξει αναφορά για τα πρωτόκολλα LAN όπως το 802.1q, encapsulation και το tunneling.

Στο κεφάλαιο 3 θα μιλήσουμε για το MPLS, την αρχιτεκτονική του, τις ετικέτες και τις βασικές αρχές προώθησης. Στο 3.4 θα αναφερθούμε στην λειτουργία, την εγκαθίδρυση μονοπατιών και την προώθηση κίνησης. Θα δούμε συνοπτικά τα βήματα προώθησης για το MPLS και θα αναφερθούμε στο traffic engineering.

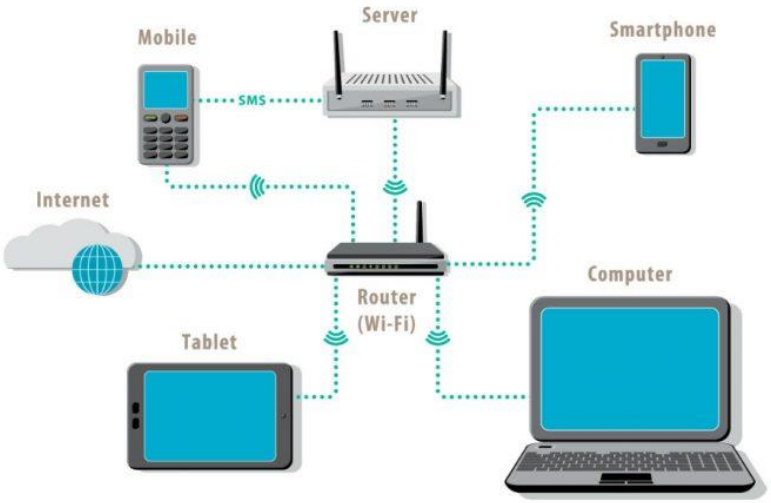
Στο κεφάλαιο 4 θα δούμε τα MPLS VPNs για layer 2 και layer 3. Στο 4.2.4 θα αναφερθούμε στο VPWS ή ATOM ενθυλάκωση πλαισίων layer 2. Μετά θα δούμε το EoMPLS που είναι το κύριο στοιχείο του πειραματικού μας μέρους. Θα δούμε ακόμα το VPLS και την αρχιτεκτονική του.

Τέλος , στο κεφάλαιο 5 θα υλοποιήσουμε το πειραματικό μέρος με 3 σενάρια . Το σενάριο 1 είναι το EoMPLS μεταφέροντας ένα CE VLAN και ένα CE Ethernet Trunk. Στο σενάριο 2 έχουμε EoMPLS μέσω EVC και στο σενάριο 3 έχω MPLS L2VPN Redundancy.

2. LAN (Local Area Network)

2.1 LAN (Local Area Network)

Το LAN είναι μια συλλογή από συνδεδεμένες συσκευές σε ένα συγκεκριμένο χωροταξικό μέρος όπως ένα γραφείο, ένα σπίτι και γενικά ένα κτίριο. Ανεξάρτητα από το μέγεθος το LAN πάντα συνδέει συσκευές σε ένα μέρος καθορισμένο. Αντίθετα το wide area network (WAN) και το metropolitan area network (MAN) καλύπτουν μεγαλύτερες εκτάσεις. Τα τελευταία συνήθως καλύπτουν πολλά LAN μαζί. Οι συσκευές έχουν πάντα μία καθορισμένη IP διεύθυνση εντός ενός συγκεκριμένου IP δικτύου με ίδιο subnet mask και gateway.



Εικόνα 1: LAN (source, networkencyclopedia.com)

2.2 Διαφορετικοί τύποι LAN:

Γενικά υπάρχουν δυο τύποι , οι client-server LAN και οι peer-to-peer LAN.

Ο client-server LAN αποτελείται από συσκευές συνδεδεμένες (clients) σε έναν κεντρικό server. Αυτός διαχειρίζεται την αποθήκευση αρχείων, το network traffic και την πρόσβαση σε αρχεία, συσκευές και στις εφαρμογές. Ο client μπορεί να είναι κάθε συνδεδεμένη συσκευή που τρέχει, έχει πρόσβαση σε εφαρμογές ή στο δίκτυο. Μια σειρά από εφαρμογές υπάρχουν στον LAN server. Οι χρήστες μπορούν να έχουν πρόσβαση σε mail, databases, εκτυπωτές και άλλες εφαρμογές . Αυτές τις προσβάσεις τις διαχειρίζεται το δίκτυο ή ο IT administrator. Επιχειρήσεις και κρατικές υπηρεσίες χρησιμοποιούν το Client-Server LAN.

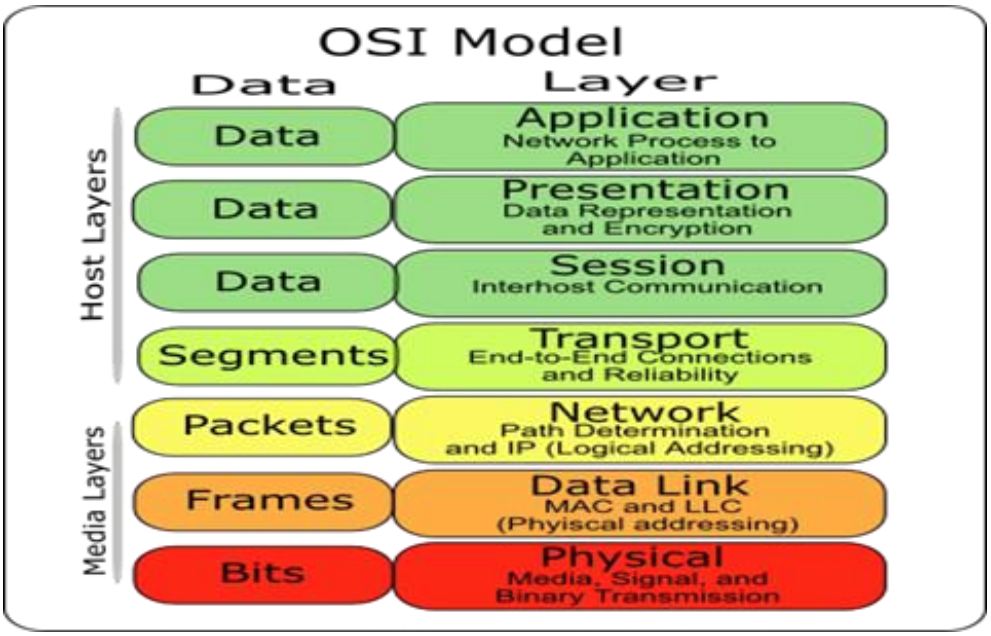
Το peer to peer LAN δεν έχει ένα κεντρικό server και δεν μπορεί να διαχειριστεί μεγάλο φόρτο εργασίας. Κάθε συσκευή μοιράζεται ισόποσα στο δίκτυο. Μοιράζονται αρχεία ή πόρους μέσω ασύρματης ή ενσύρματης σύνδεσης σε ένα router ή switch. Συνήθως χρησιμοποιείται σε μικρά δίκτυα όπως σε σπίτια.

2.3 ΜΟΝΤΕΛΟ ΑΝΑΦΟΡΑΣ OSI

Το μοντέλο OSI βασίζεται σε μια πρόταση, που ανέπτυξε ο Οργανισμός Διεθνών Προτύπων ISO, ως ένα πρώτο βήμα προς την κατεύθυνση της διεθνούς προτυποποίησης των πρωτοκόλλων που χρησιμοποιούνται στα διάφορα στρώματα. Το μοντέλο αποκαλείται μοντέλο αναφοράς OSI (Open Systems Interconnection) του ISO, επειδή αφορά ανοικτά συστήματα, δηλαδή συστήματα ανοικτά στην επικοινωνία με άλλα συστήματα.

Το μοντέλο αυτό έχει επτά στρώματα καθένα από τα οποία εκτελεί συγκεκριμένες λειτουργίες και επικοινωνεί με τα επίπεδα που είναι ακριβώς από πάνω και από κάτω του. Τα ανώτερα επίπεδα ασχολούνται κυρίως με τις υπηρεσίες, εφαρμογές και δραστηριότητες χρηστών και τα κατώτερα στρώματα ασχολούνται κυρίως με την καθεαυτού μετάδοση δεδομένων.

Το μοντέλο αναφοράς Ανοικτής Διασύνδεσης Συστημάτων, ή μοντέλο αναφοράς OSI (αγγλ. OSI reference model) είναι μια διαστρωματωμένη, αφηρημένη περιγραφή για τη σχεδίαση τηλεπικοινωνιακών και δικτυακών πρωτοκόλλων η οποία καθορίστηκε από την πρωτοβουλία Ανοικτή Διασύνδεση Συστημάτων – OSI. Είναι γνωστό και ως μοντέλο των επτά επιπέδων τα οποία φαίνονται στην παρακάτω εικόνα.



Εικόνα 2: OSI Model (source, www.lifewire.com)

Παρακάτω δίνεται μία ανάλυση των 2 βασικότερων επιπέδων των οποίων θα διαπραγματευτούμε στην συγκεκριμένη εργασία.

Το επίπεδο 2 το οποίο ονομάζεται ζεύξης δεδομένων (data link layer) δεδομένων παρέχει τα λειτουργικά και διαδικαστικά μέσα για τη μεταφορά δεδομένων από μια συσκευή ενός τοπικού δικτύου σε άλλη, αλλά και για την ανίχνευση και διόρθωση σφαλμάτων που συμβαίνουν στο φυσικό επίπεδο. Οι μη ιεραρχημένες διευθύνσεις των συσκευών εδώ είναι οι φυσικές (MAC διευθύνσεις), δηλαδή είναι προκαθορισμένες και αποθηκευμένες στις κάρτες δικτύου των επικοινωνούντων κόμβων από το εργοστάσιο. Το πιο γνωστό πρότυπο αυτού του επιπέδου είναι το Ethernet, για την επικοινωνία εντός των τοπικών δικτύων. Άλλα παραδείγματα πρωτοκόλλων ζεύξης δεδομένων αποτελούν τα: HDLC και ADCCP, για συνδέσεις από-σημείο-σε-σημείο (point-to-point), 802.11, για ασύρματα τοπικά δίκτυα. Στα τοπικά δίκτυα της οικογένειας πρωτοκόλλων IEEE 802, και σε κάποια άλλα όπως το FDDI, αυτό το επίπεδο μπορεί να διαιρεθεί σε δύο μικρότερα: Ένα επίπεδο ελέγχου πρόσβασης στο κοινό μέσο, το υποεπίπεδο MAC (Media Access Control) Έλεγχος Πρόσβασης Μέσου και ένα ανώτερο επίπεδο ελέγχου λογικών συνδέσεων, το υποεπίπεδο LLC (Logical Link Control), όπου επικρατεί καθολικά το πρωτόκολλο IEEE 802.2 ανεξάρτητα από το υποκείμενο πρωτόκολλο MAC ή φυσικού επιπέδου. Στο επίπεδο αυτό λειτουργούν οι δικτυακές γέφυρες (bridge) και οι δικτυακοί διακόπτες (switch). Η συνδεσιμότητα παρέχεται μόνο για κόμβους που συνδέονται στο ίδιο κοινό μέσο (τοπικό δίκτυο ή σύνδεση από-σημείο-σε-σημείο).

Το επίπεδο 3 το οποίο ονομάζεται επίπεδο δικτύου (network layer) παρέχει τα λειτουργικά και διαδικαστικά μέσα για τη μεταφορά δεδομένων μεταβλητού μήκους από μια προέλευση (source) σε έναν προορισμό (destination), μέσα από ένα ή και συνήθως περισσότερα ενδιάμεσα δίκτυα, ενώ διατηρεί την ποιότητα εξυπηρέτησης που απαιτεί το επίπεδο μεταφοράς. Το επίπεδο δικτύου εκτελεί λειτουργίες δρομολόγησης, και αναφέρει σφάλματα σχετικά με την παράδοση των πακέτων. Οι δρομολογητές (routers) λειτουργούν στο επίπεδο αυτό και διακινώντας δεδομένα σε διασυνδεδεμένα δίκτυα έκαναν το Διαδίκτυο πραγματικότητα. Εδώ υπάρχει μια λογική οργάνωση και τις τιμές των διευθύνσεων τις καθορίζει ιεραρχικά ο τεχνικός επικοινωνιών. Το πλέον αναγνωρίσιμο παράδειγμα πρωτοκόλλου δικτύου είναι το Πρωτόκολλο Διαδικτύου (Internet Protocol, IP).

2.4 ΠΡΩΤΟΚΟΛΛΑ LAN

2.4.1 802.1q πρωτόκολλο

Τα Encapsulation πρωτόκολλα συνδέουν το layer- 2(link layer) protocol με το layer-3 (network layer) protocol. Το encapsulation πρωτόκολλο δεν είναι απαραίτητα πάντα στο communications link, όμως, τυπικά, μεταφέρει παραπάνω από ένα layer-

3 protocol από το link. Για παράδειγμα, μπορείς να διαμορφώσεις ένα Frame Relay link να στέλνει μόνο IP πακέτα, σε αυτή την περίπτωση δεν χρειάζονται πακέτα encapsulation. Όμως, αν το link διαμορφωθεί να στέλνει και στο IPX, σε ένα EtherType ή RFC1490-type το encapsulation protocol πρέπει να εφαρμοστεί.

Οι επιλογές encapsulation πρωτοκόλλου (όπως η IP) δεν είναι όλες κατάλληλες για πρωτοκόλλα encapsulation. Για αυτό πρέπει να δούμε τι υπάρχει πάνω από το link layer.

Η μετατόπιση του encapsulation στο protocol-definition window δουλεύει μαζί με το πρωτόκολλο encapsulation. Αυτός ο μηχανισμός δίνει εντολή στο ASE να παρακάμψει μερικά από τα octets (μονάδα ψηφιακών πληροφοριών σε υπολογιστές και τηλεπικοινωνίες που αποτελείται από οκτώ bits) μετά το link-layer headers πριν αρχίσει να αποκωδικοποιεί το πακέτο χρησιμοποιώντας το πρωτόκολλο encapsulation.

Για το Frame Relay, η μετατόπιση encapsulation αναπαριστά τον αριθμό των octets που παραλείπουμε μετά το Frame Relay header

Για το HDLC, η μετατόπιση encapsulation είναι ο αριθμός των octets που παραλείπουμε στο opening flag.

ENCAPSULATION ΠΡΩΤΟΚΟΛΛΟ ΚΑΙ Cisco WAPMS

Το Cisco WAN Access Performance Management System (Cisco WAPMS) είναι ένα ολοκληρωμένο δίκτυο ευρείας περιοχής (WAN) service-level σύστημα διαχείρισης Cisco . Το σύστημα ενσωματώνει τη λειτουργικότητα πρόσβασης WAN με την παρακολούθηση απόδοσης end-to-end, την αντιμετώπιση προβλημάτων, τη λήψη της κυκλοφορίας και τον προγραμματισμό και την αναφορά Έχει σχεδιαστεί για να παρακολουθεί την κυκλοφορία σε δίκτυα χρησιμοποιώντας στατιστικά πολυπλεγμένες τεχνολογίες, Frame Relay, ATM, IP/Internet, and private line (HDLC/PPP).

ENCAPSULATION ΠΡΩΤΟΚΟΛΛΟ ΚΑΙ ΡΥΘΜΙΣΕΙΣ ΣΤΡΩΜΑΤΟΣ ΔΙΚΤΥΟΥ

Τα διαθέσιμα πρωτόκολλα ενθυλάκωσης για τη διαμόρφωση μέσω της Cisco WAPMS είναι τα εξής:

Cisco (EtherType) Μορφή πλαισίου ίντερνετ που χρησιμοποιείται από πολλούς routers ως ιδιωτικός. Έχει παρόμοιες δυνατότητες όπως το bridged Ethernet ή το Token Ring, αλλά είναι πιο αποδοτικό.

Ethernet (bridged) Μορφή πλαισίου Ethernet που χρησιμοποιείται από γέφυρες και δρομολογητές γεφύρωσης. Μπορεί να μεταφέρει οποιοδήποτε πρωτόκολλο στρώματος δικτύου που υποστηρίζεται από το Ethernet.

Frame Relay (Auto) (Frame Relay only) είτε RFC1490 είτε το πρωτόκολλο ενθυλάκωσης Ether Type με βάση τα ίδια τα πλαίσια. Αυτή είναι η καλύτερη επιλογή που θα χρησιμοποιηθεί με το Frame Relay επειδή λειτουργεί με τις δύο συνηθισμένες τεχνικές ενθυλάκωσης.

None - AppleTalk only Ένα πρωτόκολλο δικτύου που κατευθύνει το ASE για την ανάλυση των δεδομένων, υποθέτοντας ότι είναι πρωτόκολλο AppleTalk.

None - IP only Ένα πρωτόκολλο δικτύου που κατευθύνει το ASE για να αναλύσει τα δεδομένα που υποθέτει ότι είναι πρωτόκολλο IP.

None - IPX only Ένα πρωτόκολλο δικτύου που κατευθύνει το ASE για την ανάλυση των δεδομένων ανάλογα με το πρωτόκολλο IPX.

None - SNA only Ένα πρωτόκολλο δικτύου που κατευθύνει το ASE για την ανάλυση των δεδομένων ανάλογα με το πρωτόκολλο SNA.

Point-to-Point (PPP) Το πρότυπο πρωτόκολλο σημείων προς σημείο που χρησιμοποιείται κυρίως σε συνδέσμους σημείων προς σημείο που αναλύονται από το HDLC ASE, αλλά μπορούν να χρησιμοποιηθούν από το ρελέ πλαισίου.

RFC 1490 (IETF) (Frame Relay only) Τυποποιημένο ρελέ πλαισίου πολλαπλών πρωτοκόλλων. Αυτό είναι το πιο ευπροσάρμοστο και κοινό πρωτόκολλο encapsulation που χρησιμοποιείται με το ρελέ πλαισίου.

Router (proprietary) (HDLC only) Ένα πρωτόκολλο ενθυλάκωσης που αποκωδικοποιεί τις ιδιόκτητες πλαισιώσεις που χρησιμοποιούνται από δρομολογητές σε συνδέσμους σημείων προς σημείο.

Token Ring (bridged) Μορφή Token ring που χρησιμοποιείται από γέφυρες και δρομολογητές γεφύρωσης. Μπορεί να φέρει οποιοδήποτε πρωτόκολλο δικτύου που υποστηρίζεται από δίκτυα Token ring.

Unknown or Proprietary Το πρωτόκολλο encapsulation είναι άγνωστο. Το ASE δεν θα προσπαθήσει να αναλύσει δεδομένα πέρα από το στρώμα σύνδεσης. Μην χρησιμοποιήσετε μετατόπιση ενθυλάκωσης με αυτή τη ρύθμιση.

2.4.2 IEEE 802.1Q Tunneling

Το χαρακτηριστικό IEEE 802.1Q Tunneling μας δίνει ένα μοναδικό VLAN για να υποστηρίξουμε πολλούς πελάτες VLANs, ενώ προστατεύουμε τα VLAN IDs διαχωρίζοντας την κυκλοφορία σε διαφορετικούς πελάτες VLANs. Αυτή η ενότητα περιγράφει τη λειτουργία Tunneling IEEE 802.1Q και εξηγεί τον τρόπο διαμόρφωσης της σήραγγας IEEE 802.1Q στο λογισμικό Cisco.

Περιορισμοί για 802.1Q Tunneling

Μόνο οι ασύμμετροι σύνδεσμοι μπορούν να χρησιμοποιηθούν για την άμεση κυκλοφορίας σε μια σήραγγα ή για την απομάκρυνση της κυκλοφορίας από μια σήραγγα(tunnel).

Η εγγενής κυκλοφορία VLAN θα πρέπει πάντα να αποστέλλεται σε έναν ασύμμετρο σύνδεσμο, για τη διαμόρφωση της σήραγγας IEEE 802.1q.

Οι ασύμμετροι σύνδεσμοι δεν υποστηρίζουν το πρωτόκολλο δυναμικού καναλιού (DTP) επειδή μόνο μία θύρα στον σύνδεσμο είναι ένας κορμός.

Το χαρακτηριστικό σήραγγας IEEE 802.1Q.1Q δεν μπορεί να ρυθμιστεί σε θύρες που υποστηρίζουν ιδιωτικά VLAN.

Επισκόπηση της σήραγγας IEEE 802.1Q

Όταν μια θύρα σήραγγας λαμβάνει σήμανση επισκεψιμότητας πελατών από μια θύρα κορμού 802.1Q, δεν απογυμνώνεται η ληφθείσα ετικέτα 802.1Q από την κεφαλίδα του πλαισίου. Αντίθετα, η θύρα σήραγγα αφήνει την ετικέτα 802.1Q άθικτη, προσθέτει ένα πεδίο 2-byte Ethertype (0x8100) ακολουθούμενο από ένα πεδίο 2-byte που περιέχει την προτεραιότητα (κατηγορία υπηρεσίας) και το VLAN.

Η ληφθείσα επισκεψιμότητα πελατών προστίθεται στο VLAN στο οποίο έχει εκχωρηθεί η θύρα σήραγγας. Αυτή η κυκλοφορία Ethertype 0x8100, με την ετικέτα 802.1Q, ονομάζεται σήραγγα κυκλοφορίας. Ένα VLAN που μεταφέρει την κυκλοφορία σήραγγας είναι σήραγγα 802.1.1q.

Οι πόρτες σήραγγας στο VLAN είναι η είσοδος της σήραγγας και τα σημεία εξόδου.

Μια θύρα που έχει ρυθμιστεί για να υποστηρίξει σήραγγα 802.1Q ονομάζεται θύρα σήραγγας. Όταν διαμορφώνετε μια σήραγγα, ορίζετε μια θηρα σήραγγας σε ένα VLAN που αφιερώνετε στη σήραγγα, η οποία στη συνέχεια γίνεται ένα VLAN σήραγγας.

Για να διατηρήσουμε την κυκλοφορία των πελατών, κάθε πελάτης απαιτεί ξεχωριστή σήραγγα VLAN που υποστηρίζει όλα τα VLAN που χρησιμοποιεί ο πελάτης. Οποιαδήποτε θύρα σήραγγας σε VLAN είναι μια είσοδος σήραγγας και σημείο εξόδου.

Μια σήραγγα 802.1 μπορεί να έχει τόσες θύρες σήραγγας όπως απαιτείται για τη σύνδεση των customer switchers.

Η σήραγγα IEEE 802.1Q επιτρέπει τη χρήση ενός VLAN να υποστηρίξει πολλαπλούς πελάτες VLAN. Οι διακόπτες του πελάτη είναι συνδεδεμένοι με κορμό, αλλά με σήραγγα IEEE 802.1Q, ο πάροχος υπηρεσιών διακόπτει μόνο έναν πάροχο

υπηρεσιών VLAN για τη μεταφορά όλων των VLAN πελάτη, αντί να μεταφέρουν άμεσα όλους τους πελάτες VLAN.

Το χαρακτηριστικό σήραγγας IEEE 802.1.1Q δεν περιορίζεται στις διαμορφώσεις σήραγγας σημείων προς σημείο. Οποιαδήποτε θύρα σήραγγας σε μια σήραγγα VLAN είναι μια είσοδος σήραγγας και σημείο εξόδου.

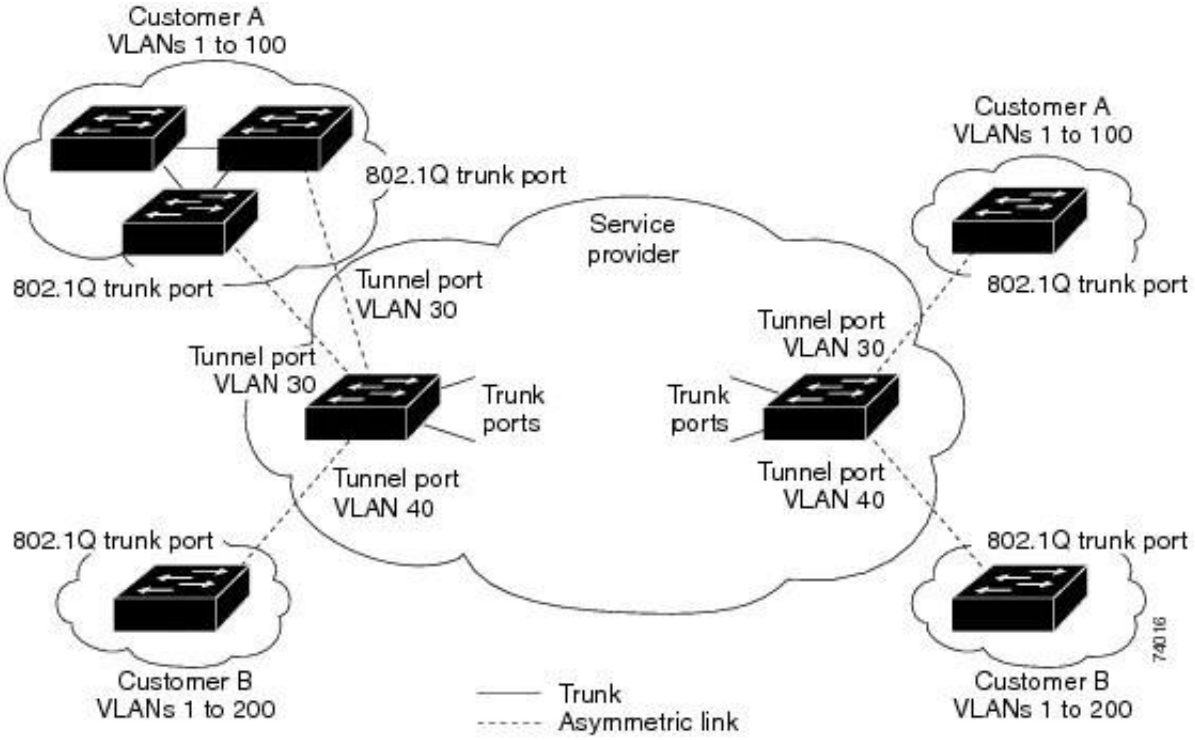
Μια σήραγγα 802.13 μπορεί να έχει τόσες θύρες σήραγγας όπως απαιτείται για τη σύνδεση των customer switchers.

IEEE 802.1Q Tunnel Ports

Στο χαρακτηριστικό σήραγγας IEEE 802.1Q, η επισήμανση της επισκεψιμότητας πελατών ετικετών προέρχεται από μια θύρα κορμού 802.1Q σε μια συσκευή πελάτη και εισάγει τη συσκευή άκρη του παρόχου υπηρεσίας μέσω μιας θύρας σήραγγας.

Ο σύνδεσμος μεταξύ της θύρας κορμού 802.1Q σε μια συσκευή πελατών και η θύρα σήραγγας ονομάζεται ασύμμετρη σύνδεση επειδή το ένα άκρο διαμορφώνεται ως θύρα κορμού 802.1q και το άλλο άκρο διαμορφώνεται ως θύρα σήραγγας. Αναθέτει τη θύρα σήραγγας σε ένα αναγνωριστικό VLAN Access σε κάθε πελάτη.

Τα πακέτα που προέρχονται από τη θύρα κορμού πελάτη στη θύρα διοχέτευσης στο διακόπτη άκρων της υπηρεσίας παροχής είναι συνήθως 802.1Q με ετικέτα με το κατάλληλο VLAN ID. Τα πακέτα με tag παραμένουν ανέπαφα μέσα στο διακόπτη και όταν εξέρχονται από τη θύρα κορμού στο δίκτυο παροχής υπηρεσιών, συμπυκνώνονται με ένα άλλο επίπεδο ετικέτας 802.1Q (που ονομάζεται metro tag) που περιέχει το αναγνωριστικό VLAN ID που είναι μοναδικό για τον πελάτη. Η αρχική ετικέτα πελάτη 802.1Q διατηρείται στο ενθυλακωμένο πακέτο. Επομένως, τα πακέτα που εισέρχονται στο δίκτυο παροχής υπηρεσιών έχουν διπλή ετικέτα, με την εξωτερική ετικέτα που περιέχει το αναγνωριστικό VLAN ID πρόσβασης του πελάτη και το εσωτερικό αναγνωριστικό VLAN να είναι αυτό της εισερχόμενης κυκλοφορίας. Όταν το πακέτο με διπλή ετικέτα εισέλθει σε μια άλλη θύρα κορμού σε έναν διακόπτη πυρήνα υπηρεσίας παροχής, η εξωτερική ετικέτα αφαιρείται καθώς ο διακόπτης επεξεργάζεται το πακέτο. Όταν το πακέτο εξέρχεται από μια άλλη θύρα κορμού στον ίδιο διακόπτη πυρήνα, η ίδια ετικέτα προστίθεται και πάλι στο πακέτο.



Εικόνα 3: Tunnel Ports (source, https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9500/software/release/16-9/configuration_guide/lyr2/b_169_lyr2_9500_cg/configuring_ieee_802_1q_tunneling.pdf)

Στον πελάτη A ανατέθηκε το VLAN 30 και στον πελάτη B ανατέθηκε το VLAN 40 πακέτο όπως φαίνεται στο σχήμα .Η εισαγωγή των θυρών διοχέτευσης διακοπτών άκρων με ετικέτες 802.1Q έχει διπλή ετικέτα κατά την είσοδό τους στο δίκτυο παροχής υπηρεσιών, με την εξωτερική ετικέτα που περιέχει το VLAN ID 30 ή 40, κατάλληλα, και την εσωτερική ετικέτα που περιέχει τον αρχικό αριθμό VLAN, για παράδειγμα, VLAN 100.

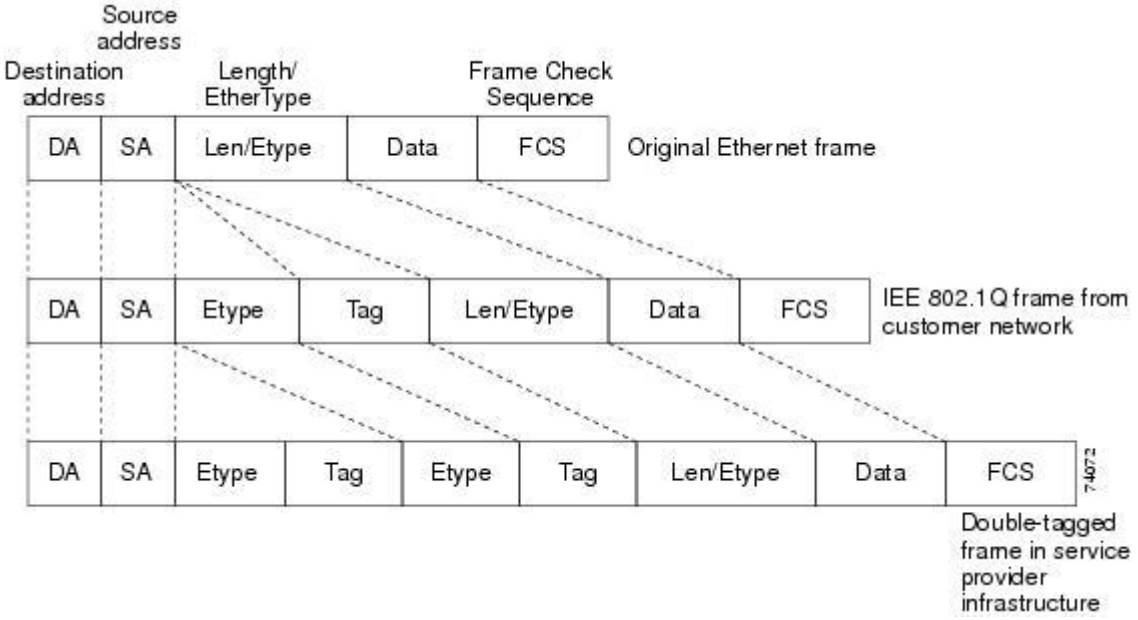
Ακόμη και αν οι πελάτες A όσο και B έχουν VLAN 100 στα δίκτυά τους, η κυκλοφορία παραμένει διαχωρισμένη στο δίκτυο παροχής υπηρεσιών επειδή η εξωτερική ετικέτα είναι διαφορετική.

Κάθε πελάτης ελέγχει το δικό του χώρο αρίθμησης VLAN, ο οποίος είναι ανεξάρτητος από το χώρο αρίθμησης VLAN που χρησιμοποιείται από άλλους πελάτες και τον χώρο αρίθμησης VLAN που χρησιμοποιείται από το δίκτυο παροχής υπηρεσιών. Στη θύρα εξερχόμενης σήραγγας, οι αρχικοί αριθμοί VLAN στο δίκτυο του πελάτη ανακτάται. Είναι δυνατό να έχετε πολλαπλά επίπεδα διοχέτευσης και προσθήκης ετικετών, αλλά ο διακόπτης υποστηρίζει μόνο ένα επίπεδο σε αυτήν την έκδοση.

Εάν η κυκλοφορία που προέρχεται από ένα δίκτυο πελατών δεν έχει επισημανθεί με ετικέτα (εγγενή πλαίσια VLAN), αυτά τα πακέτα γεφυρώνονται ή δρομολογούνται ως κανονικά πακέτα. Όλα τα πακέτα που εισέρχονται στο δίκτυο παροχής υπηρεσιών

μέσω μιας θύρας διοχέτευσης.Ένας διακόπτης άκρων αντιμετωπίζεται ως πακέτα χωρίς tag, είτε είναι μη tag είτε έχουν ήδη επισημανθεί με κεφαλίδες 802.1Q.

Τα πακέτα συμπυκνώνονται με την ετικέτα του μετρό VLAN ID (ρυθμισμένη στην πρόσβαση VLAN της θύρας διοχέτευσης) όταν αποστέλλονται μέσω του δικτύου παροχής υπηρεσιών σε μια θύρα κορμού 802.1Q. Το πεδίο προτεραιότητας στο metro tag έχει οριστεί στην προτεραιότητα κλάσης διασύνδεσης υπηρεσίας (CoS) που έχει ρυθμιστεί στη θύρα διοχέτευσης



Εικόνα 4: Frames

Όταν το πακέτο εισέλθει στη θύρα κορμού του διακόπτη egress της υπηρεσίας παροχής, το εξωτερικό tag απογυμνώνεται ξανά καθώς ο διακόπτης επεξεργάζεται εσωτερικά το πακέτο. Ωστόσο, το metro tag δεν προστίθεται όταν αποστέλλεται το πακέτο στη θύρα διοχέτευσης στο διακόπτη άκρης στο δίκτυο πελατών. Το πακέτο αποστέλλεται ως κανονικό πλαίσιο με ετικέτα 802.1Q για τη διατήρηση των αρχικών αριθμών VLAN στο δίκτυο πελατών.

3. Εισαγωγή MPLS

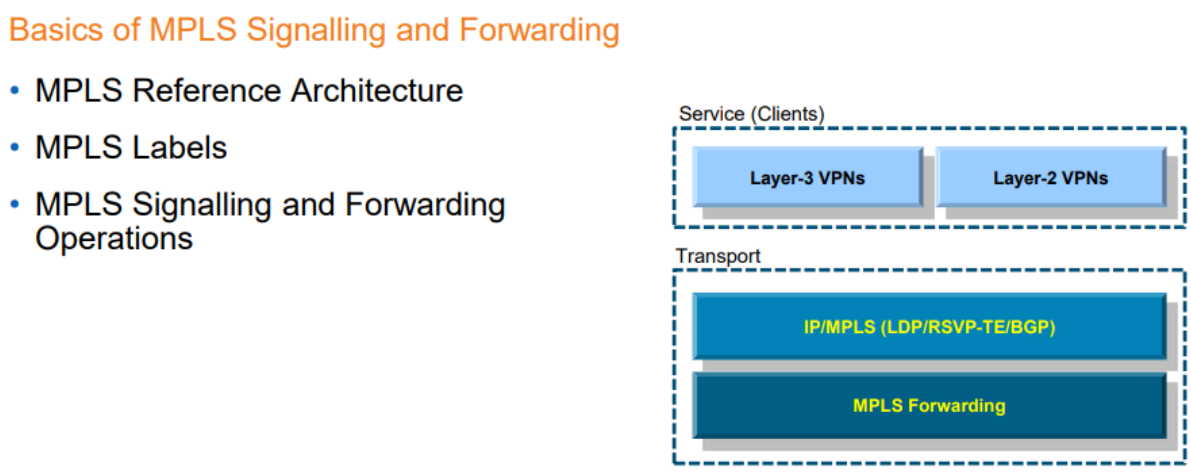
Από την πλευρά του παρόχου ο οποίος έχει εγκαταστήσει ένα MPLS δίκτυο συνοδεύεται μείωση κόστους σε CAPEX/OPEX. Παρέχεται μέγιστη χρήση πόρων χρήση των πόρων του συγκεκριμένου δικτύου του παρόχου καθώς παρέχει πολλαπλές υπηρεσίες Layer-2/3 μέσω της ίδιας υποδομής. (Service-provider Network). Ταυτόχρονα μπορεί να επιτευχθούν και να υποστηριχτεί end-to-end στο δίκτυο πολλαπλά SLAs (Voice, Video, http traffic.) Αποτέλεσμα όλων των παραπάνω να αντιμετωπίζεται η αυξανόμενη πολυπλοκότητα των υπηρεσιών σε επίπεδο IP. Από την πλευρά του πελάτη παρέχεται αποκλειστική συνδεσιμότητα για εξυπηρέτηση των χρηστών εντός ενός LAN που βρίσκονται σε διαφορετικά campus τα οποία μπορεί να εξυπηρετήσει ο πάροχος μέσω του MPLS core δικτύου. Ταυτόχρονα μπορεί να υποστηριχθεί και τμηματοποίηση δικτύου αν χρειαστεί.

Επίσης με την τεχνολογία Mpls πραγματοποιείται υποστήριξη πολλών διαφορετικών πρωτοκόλλων επικοινωνίας και μπορεί να επιτευχθεί ανεξαρτησία επιπέδου διασύνδεσης δεδομένων σε layer-2 και layer-3 σε διαφορετικούς πελάτες με ρητή δρομολόγηση (Traffic engineering). Σε ένα MPLS δίκτυο πρέπει να γνωρίζουμε ότι υπάρχει σαφής διαχωρισμός των λειτουργιών ελέγχου (control plane) και προώθησης (data plane) με υποστήριξη qos.

Αρχικά προτάθηκε σαν ένα μέσο για τη βελτίωση της ταχύτητας προώθησης και της απόδοσης των IP δρομολογητών αλλά στην συνέχεια έγινε απαραίτητο αντικείμενο που ενοποιεί τη λειτουργικότητα των επιπέδων IP μέσω των MPLS VPNs

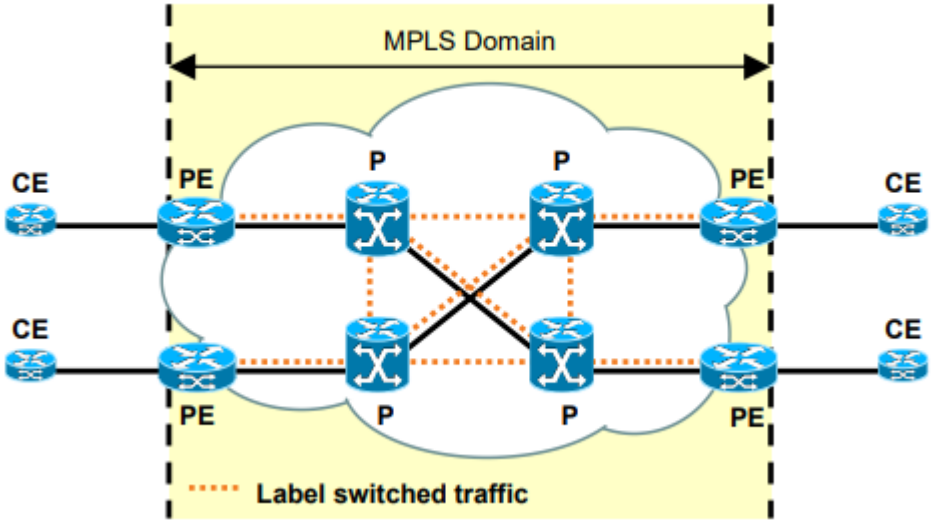
3.1 Αρχιτεκτονική MPLS

Το MPLS forwarding plane κάνει χρήση ετικετών για την προώθηση της κυκλοφορίας δεδομένων για αξιοποίηση διασύνδεσης πελατών που αναφέρονται σε layer-2/3 επικοινωνία. Η δρομολόγηση των πακέτων εντός του mpls δικτύου γίνεται με ετικέτες (labels) και κάθε label αντικατοπτρίζει ένα απομακρυσμένο δίκτυο (destination prefix). Το MPLS control plane κάνει χρήση των τοπικών ετικετών που έχουν αποθηκευμένοι οι mpls routers και η πληροφορία μεταβιβάζεται με τη χρήση κάποιου πρωτοκόλλου (LD, RSVP) στο mpls forwarding plane.



Εικόνα 5: Basics of MPLS(source, https://www.sanog.org/resources/sanog17/sanog17-mpls-intro-santanu.pdf)

Στο παρακάτω διάγραμμα το οποίο αντικατοπτρίζει ένα MPLS domain οι P (provider) δρομολογητές είναι ελέγξιμοι από το δίκτυο του παρόχου. Επίσης ονομάζονται και Label switching router (LSR) και λειτουργούν σαν διακόπτες πακέτων βασιζόμενοι με ετικέτες MPLS.

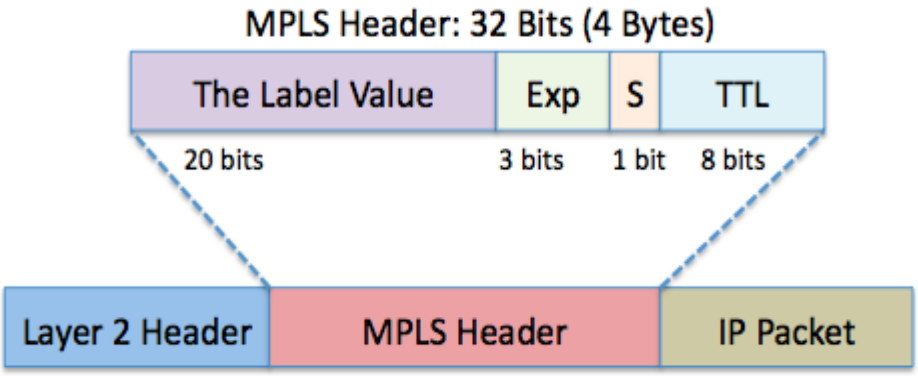


Εικόνα 6: Label switched traffic(source, https://www.sanog.org/resources/sanog17/sanog17-mpls-intro-santanu.pdf)

Οι PE (Provider Edge) δρομολογητές ονομάζονται και Edge router (LER) και είναι αυτοί που είναι υπεύθυνοι για να επιβάλλουν και καταργούν MPLS ετικέτες. Οι CE (Customer Edge) δρομολογητές συνδέουν το το δίκτυο πελατών με το δίκτυο MPLS core. Οι βασικές ενός MPLS δικτύου είναι οι κάτωθι: Το MPLS χρησιμοποιεί προώθηση που βασίζεται σε ετικέτες. Στο σημείο εισόδου, τα εισερχόμενα πακέτα επεξεργάζονται και εφαρμόζονται σε αυτά ετικέτες. Το δίκτυο κορμού εφαρμόζει τις κατάλληλες υπηρεσίες και προωθεί τα πακέτα βάση της ετικέτας. Η αναλυτική

επεξεργασία, η κατηγοριοποίηση και το ‘φιλτράρισμα’ γίνονται μόνο μια φορά, στο σημείο εισόδου**.** Στο σημείο εξόδου, οι ετικέτες αφαιρούνται και τα πακέτα προωθούνται στον τελικό προορισμό τους.

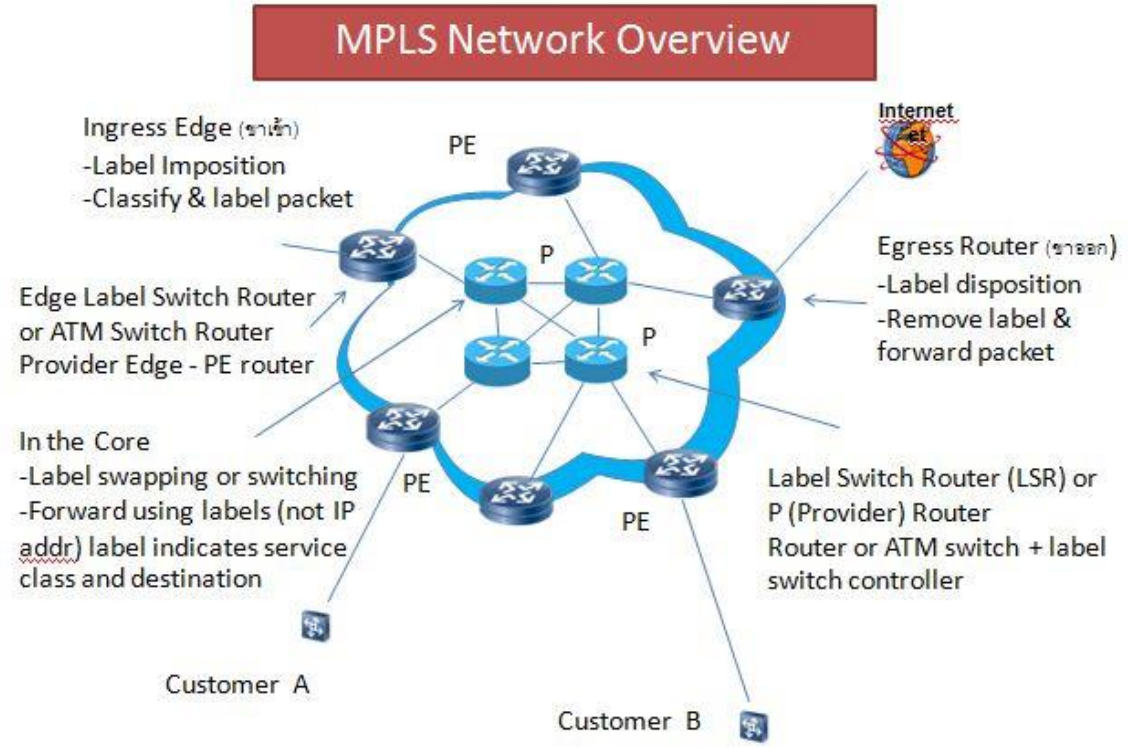
3.2 MPLS Ετικέτες



Εικόνα 7: MPLS ετικέτες(https://towardsdatascience.com/multiprotocol-label-switching-mpls-explained-aac04f3c6e94)

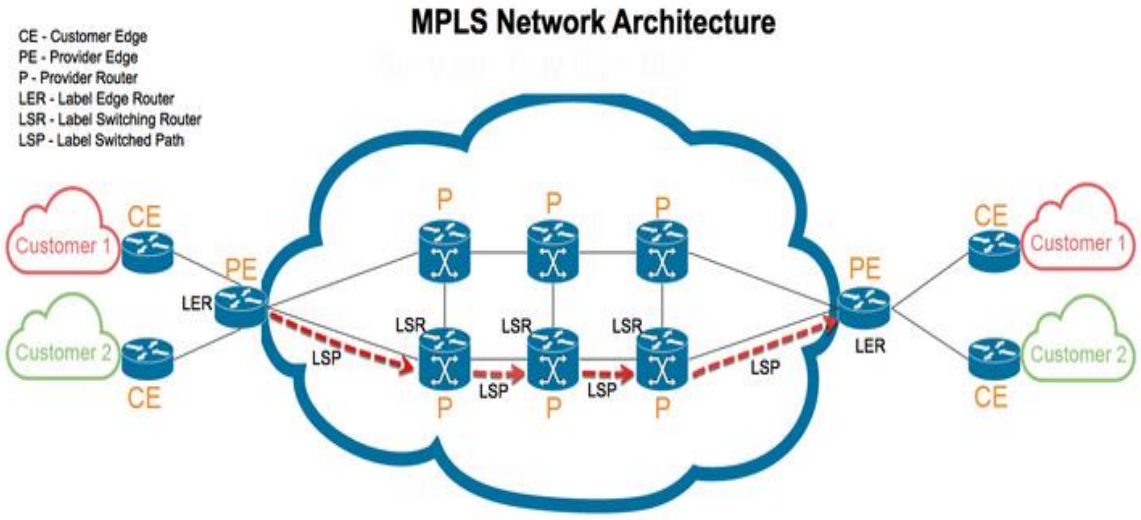
Το MPLS label ή απλώς ετικέτα έχει μέγεθος 4 Bytes (32Bits). Οι ετικέτες χρησιμοποιούνται για τη λήψη απόφασης προώθησης. Πολλές ετικέτες μπορούν να χρησιμοποιηθούν για την ενθυλάκωση πακέτων MPLS το οποίο ονομάζεται mpls label stack. Η ετικέτα βρίσκεται πάντα μεταξύ της MAC address διεύθυνσης και του layer 3 πακέτου (destination packet header). Σε αυτή την περίπτωση αυτή η μοναδική ετικέτα ονομάζεται Εξωτερική ετικέτα και χρησιμοποιείται πάντα για την εναλλαγή πακέτων MPLS εντός ενός MPLS core δικτύου. Οι υπόλοιπες εσωτερικές ετικέτες που χρησιμοποιούνται για υπηρεσίες (VPNs, Traffic engineering). Τα πρώτα 20 bits είναι η τιμή της ετικέτας (label value). Στην πραγματικότητα τα πρώτα 16 bits χρησιμοποιούνται για κανονική χρήση. Τα bits 20 έως 22 ονομάζονται EXP bits και χρησιμοποιούνται αποκλειστικά για QOS. Το bit 23 ονομάζεται bottom of stack bit και είναι 0 αν η ετικέτα mpls είναι η τελευταία στη στοίβα (mpls stack). Τα 8 τελευταία bits 24-31 χρησιμοποιούνται για το Time to Live (TTL).

3.3 Βασικές αρχές προώθησης MPLS



Εικόνα 8: MPLS Network Overview(source, https://commons.wikimedia.org/wiki/File:MPLS_Network_Overview.JPG)

Κάθε Label Switch Router (LSR) δρομολογητής πραγματοποιεί τη μεταγωγή των πακέτων με mpls ετικέτες. Ο Label edge router, (LER) Πραγματοποιεί την αρχική επεξεργασία και κατηγοριοποίηση του πακέτου, και εφαρμόζει την πρώτη ετικέτα εισόδου στο mpls δίκτυο. Το Forwarding Equivalence Class (FEC) αποτελείται από ένα σύνολο IP πακέτων (network prefixes) που προωθούνται με τον ίδιο τρόπο μέσω του mpls label και το Label Switched Path (LSP) είναι το μονοπάτι που καθορίζεται από όλες τις ετικέτες ενός FEC. Οι Ingress/Egress LSRs ονομάζονται LER και από αυτούς αρχίζει και τερματίζει ένα LSP.Το Label Switched Hop είναι το hop μεταξύ MPLS κόμβων και το Label Distribution Protocol είναι αυτό που αναθέτει ετικέτες με στόχο την εγκατάσταση των LSPs. Τέλος, στο Label Information Base (LIB) υπάρχει η βάση των πληροφοριών σχετικά με τις ετικέτες που δημιουργείται από το LDP.



Εικόνα 9: MPLS αρχιτεκτονική(source, https://medium.com/@blogstevej327stuff/what-is-multiprotocol-label-switching-mpls-f9e9cc7fe43b)

Η διαμεταγωγή πακέτων MPLS τα οποία ενθυλακώνονται σε Mpls labels μπορεί να πραγματοποιηθεί με τις ακόλουθες επιλογές προώθησης. Α) Δρομολόγηση Βήμα-προς-Βήμα στην οποία κάθε LSR επιλέγει ανεξάρτητα το επόμενο βήμα για μια δεδομένη κλάση ισοδύναμης προώθησης (FEC). Β) Ρητή δρομολόγηση στην οποία ο δρομολογητής LSR εισόδου ορίζει τη λίστα των κόμβων δια των οποίων διέρχεται το μονοπάτι ρητής δρομολόγησης. Κατά μήκος του μονοπατιού, δεσμεύονται οι πόροι έτσι ώστε να εξασφαλιστεί η ποιότητα της υπηρεσίας.

Συνεπώς, οι LSRs είναι υπεύθυνοι για τη διανομή των πληροφοριών δρομολόγησης και την εκτέλεση των διαδικασιών που χρησιμοποιούνται για να μετατρέψουν τις πληροφορίες σε πίνακα προώθησης. Ο πίνακας προώθησης περιλαμβάνει όλα τα συμβατικά πρωτόκολλα δρομολόγησης (π.χ. OSPF, BGP) που παρέχουν στους LSRs την αντιστοίχιση μεταξύ της FEC και των διευθύνσεων των επόμενων βημάτων. Τέλος ο LSR δημιουργεί τοπικά τις αντιστοιχίσεις μεταξύ ετικετών και FECs και διανέμει τις αντιστοιχίες αυτές στους άλλους LSRs.

Μια καταχώρηση του πίνακα προώθησης έχει πληροφορίες για:

– Το εξερχόμενο interface
– Μία καινούργια ετικέτα
– Λοιπές πληροφορίες (π.χ. εξερχόμενη πολιτική αναμονής)

Οι καταχωρήσεις πραγματοποιούνται ως εξής:

– Το επόμενο βήμα παρέχεται από τα πρωτόκολλα δρομολόγησης.

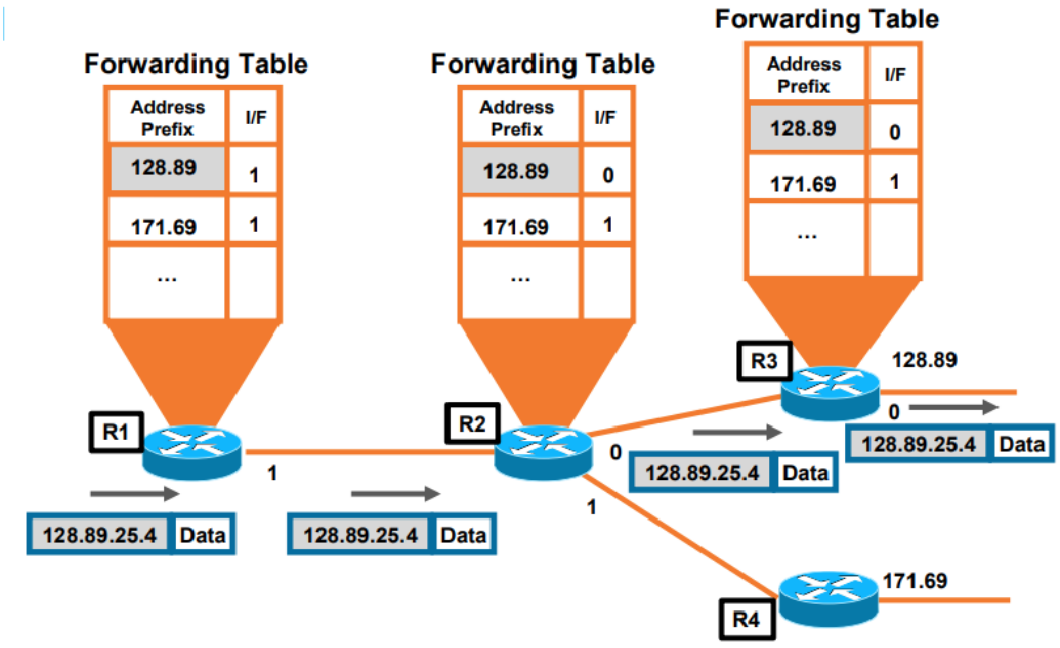
– Η εισερχόμενη και η εξερχόμενη ετικέτα παρέχονται από μια τοπική και απομακρυσμένη αντιστοίχιση ανάμεσα σε μια FEC και στην ετικέτα

Πολλά πρωτόκολλα έχουν επεκταθεί / δημιουργηθεί με σκοπό να υποστηρίζουν ανταλλαγή ετικετών (BGP, RSVP, LDP)

Ο Edge LSR (LER) διαδραματίζει έναν από τους σημαντικότερους ρόλους καθώς κατηγοριοποιεί την κυκλοφορία τοποθετώντας και αφαιρώντας τις ετικέτες. Επίσης υλοποιεί πολιτικές διαχείρισης και ελέγχους πρόσβασης στα σημεία του πελάτη (customer) και συναθροίζει την κυκλοφορία σε μεγαλύτερες ροές καθώς τις προωθεί στους LSRs.

3.4. Λειτουργία , εγκαθίδρυση μονοπατιών (LSP) και προώθηση κίνησης

Παρακάτω ακολουθεί ένα παράδειγμα το οποίο περιλαμβάνει διαμεταγωγή πακέτων (IP Packet Forwarding) εντός ενός κλασσικού IP backbone για το network prefix 128.89.25.0/24. Οι πληροφορίες δρομολόγησης IP που ανταλλάσσονται μεταξύ κόμβων μέσω ενός IGP (π.χ. OSFP, IS-IS) και τα πακέτα προωθούνται με βάση τη διεύθυνση IP προορισμού όπως αυτή εμφανίζεται εμφανίζονται στον εκάστοτε πίνακα δρομολόγησης (RIB) κάθε κόμβου.

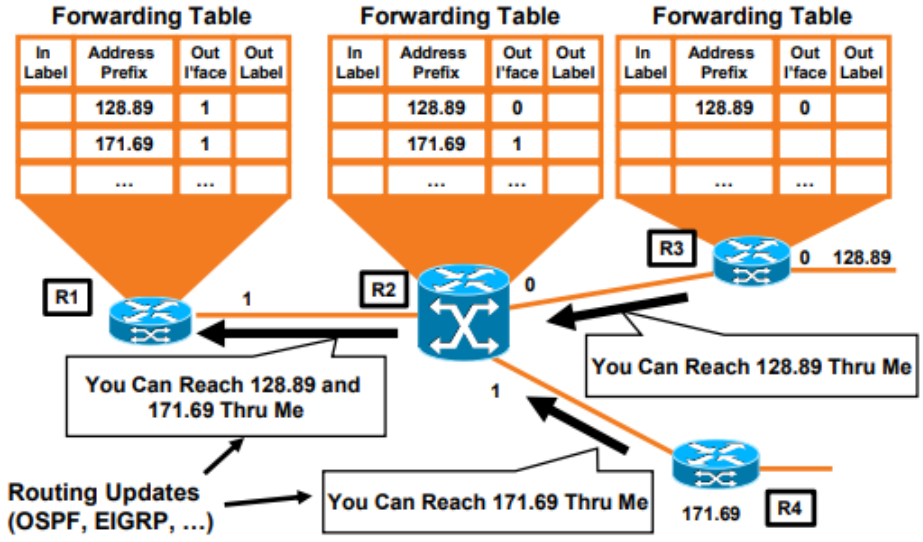


Εικόνα 10. 1: Δρομολόγηση(source, MPLS Technology fundamentals Sherif Toulan Technical Leader Cisco)

Εικόνα 10.1: Δρομολόγηση

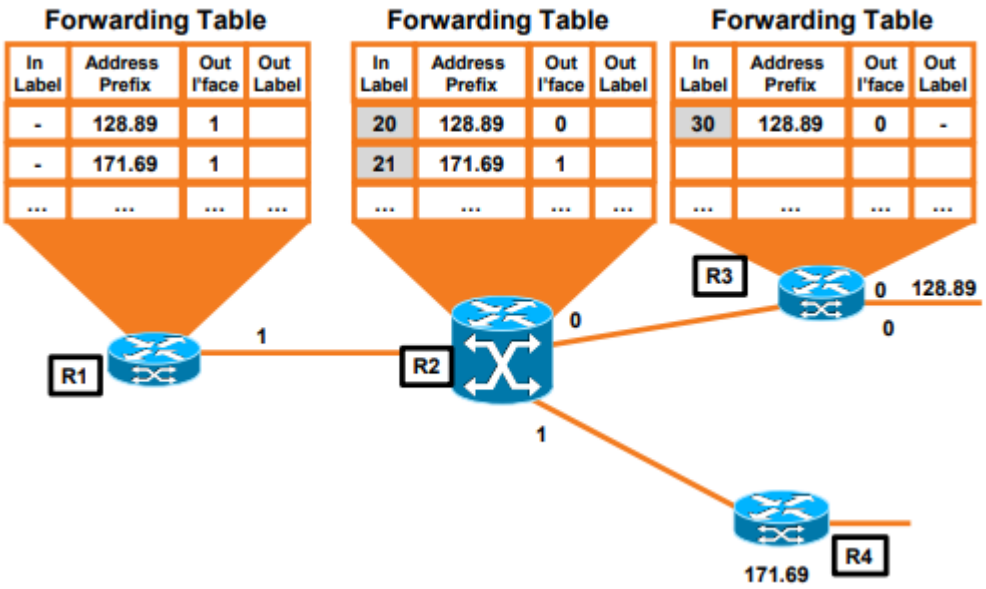
Εικόνα 10.1 : Δρομολόγηση

Στην παρακάτω εικόνα βλέπουμε την ενεργοποίηση ενός routing δυναμικού πρωτοκόλλου και παρατηρούμε ότι υπάρχει routing (igp) convergence στο IP backbone.



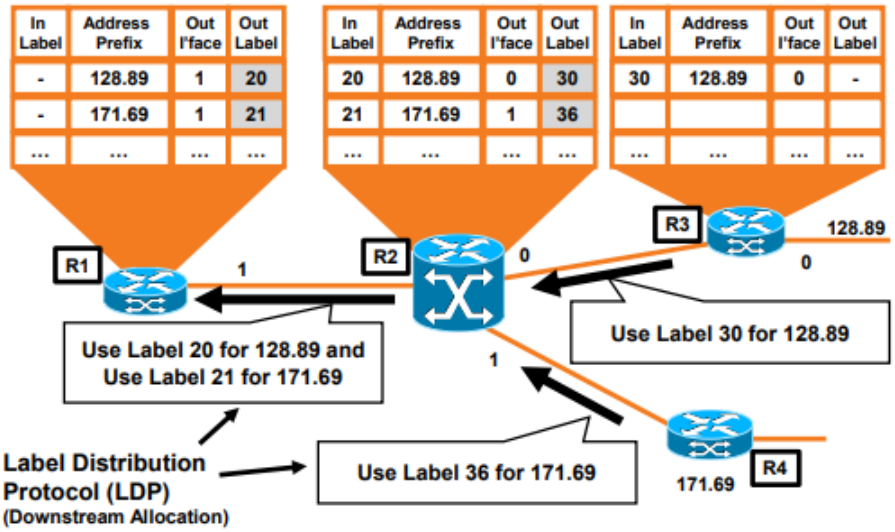
Εικόνα 10. 2: Ενεργοποίηση δυναμικού πρωτοκόλλου(source, MPLS Technology fundamentals Sherif Toulan Technical Leader Cisco)

Στην συνέχεια μετά την ενεργοποίησης MPLS στις διεπαφές των δρομολογητών (PE-P , P-P links) και LDP signaling πρωτοκόλλου επικοινωνίας προσδιορίζεται η προσβασιμότητα IP μέσω label ετικετών. (π.χ. για το prefix 128.89 ο R2 έχει local το label 20, ενώ για το prefix 172.69 έχει local το label 21). Αντίστοιχα ο R3 έχει Local το label 30 για το prefix 128.89. Με αυτό τον τρόπο κάθε κόμβος MPLS εκχωρεί μια τοπική ετικέτα σε κάθε διαδρομή στον τοπικό πίνακα δρομολόγησης (In Label)



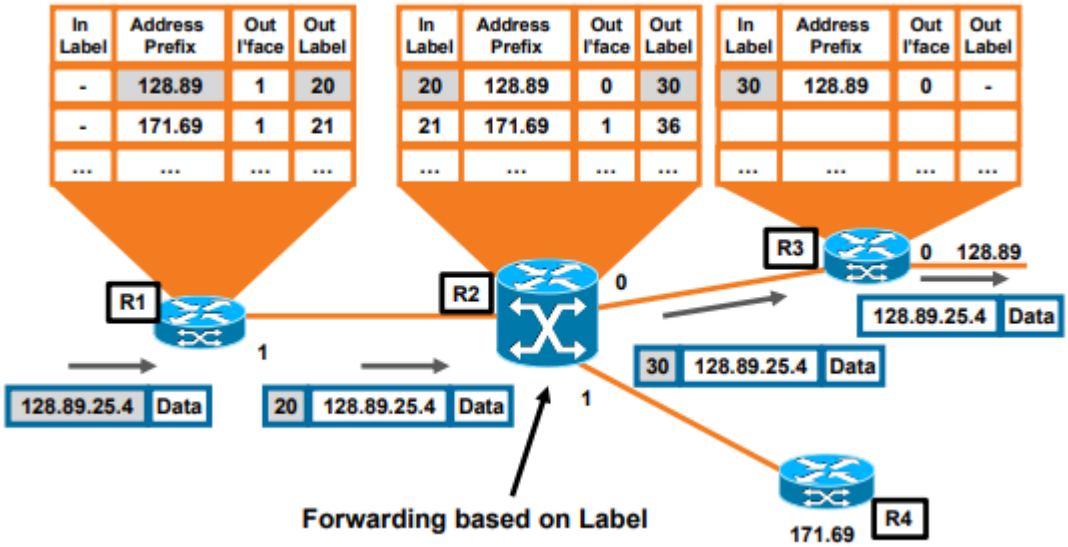
Εικόνα 10. 3: Προσβασιμότητα IP μέσω Label(source, MPLS Technology fundamentals Sherif Toulan Technical Leader Cisco)

Στη συνέχεια παρατηρούμε ότι Η τοπική αντιστοίχιση ετικετών αποστέλλεται σε συνδεδεμένους κόμβους (π.χ. ο R2 αποστέλλει το label 20 για το Prefix 128.89 στον R1 και ο R3 αποστέλλει το label 30). Με αυτόν τον τρόπο γίνεται η ενημέρωση στου εκάστοτε πίνακες προώθησης (Out Label)



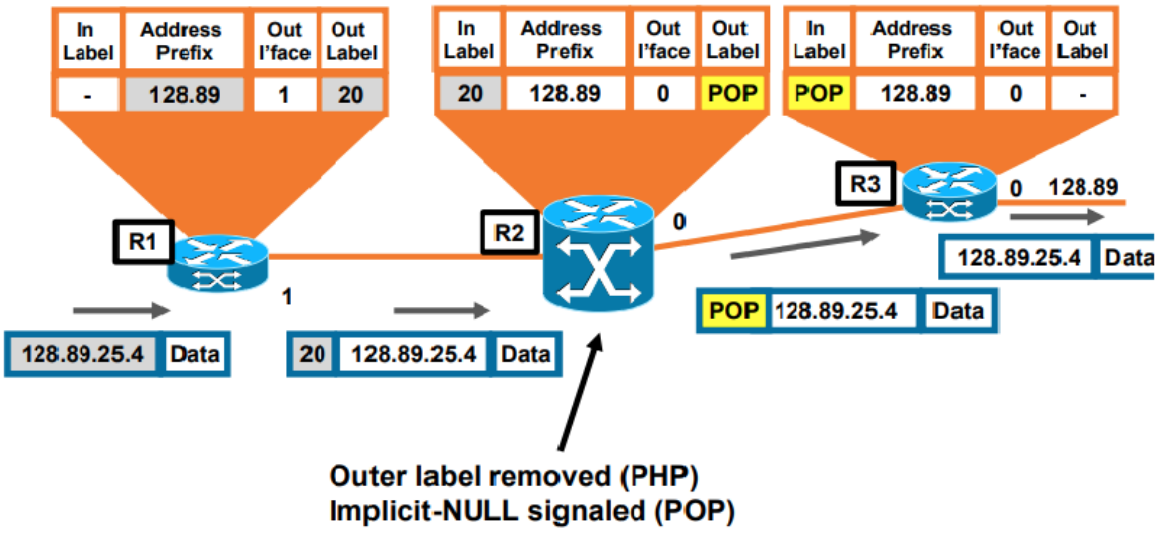
Εικόνα 10. 4: Ενημέρωση Out Label(source, MPLS Technology fundamentals Sherif Toulan Technical Leader Cisco)

Παρακάτω φαίνεται η hop by hop κίνηση χρησιμοποιώντας αποκλειστικά Labels εντός του MPLS δικτύου για τον host 128.89.25.4. Ο Ingress PE βάζει ετικέτα στο πακέτο (push) χρησιμοποιώντας το RIB και MPLS FIB και ο downstream node χρησιμοποιεί την ετικέτα για το forwarding (swap) με το out label και outgoing interface. Τέλος, ο egress PE καταργεί την ετικέτα και προωθεί το αρχικό πακέτο (pop)



Εικόνα 10. 5: Προώθηση βασισμένη στις ετικέτες(source, MPLS Technology fundamentals Sherif Toulan Technical Leader Cisco)

Τέλος ο τελευταίος egress PE MPLS Penultimate Hop Popping σηματοδοτεί την ετικέτα POP (Implicit NULL) προς τον upstream κόμβο ο τελευταίο LSR (P) αφαιρεί την εξωτερική ετικέτα πριν από την αποστολή στο LER (PE)



Εικόνα 10. 6: Αποστολή στο LER(source, MPLS Technology fundamentals Sherif Toulan Technical Leader Cisco)

Με αυτόν τον τρόπο βελτιώνεται η απόδοση του LER (PE) με τη μη εκτέλεση πολλών αναζητήσεων ετικετών για προώθηση στο τελικό πακέτο που βρίσκεται στον πελάτη.

3.5 Σύνοψη βημάτων για προώθηση MPLS

Κάθε κόμβος διατηρεί πληροφορίες δρομολόγησης IP μέσω IGP (Πρωτόκολλο Εσωτερικής δρομολόγησης) μέσω του πίνακα δρομολόγησης IP (RIB) και πίνακας προώθησης IP (FIB). Το LDP αξιοποιεί τις πληροφορίες δρομολόγησης IGP και η ανταλλαγή αντιστοίχισης ετικετών LDP (μεταξύ κόμβων MPLS) πραγματοποιείται μετά τη σύγκλιση του IGP. Οι ετικέτες ενώνουν πληροφορίες που είναι αποθηκευμένες στο LIB. Μόλις το LDP λάβει πληροφορίες σύνδεσης απομακρυσμένης ετικέτας, ενημερώνεται η προώθηση MPLS και οι ενώσεις ετικετών λαμβάνονται από απομακρυσμένους LDP peers. Η επιλογή του δρομολογητή μπορεί να θεωρηθεί σαν τη σύνθεση δύο λειτουργιών

– Η πρώτη λειτουργία χωρίζει τα πακέτα σε ένα σύνολο από FECs
– Η δεύτερη λειτουργία αντιστοιχεί σε κάθε FEC έναν επόμενο δρομολογητή

• Όλα τα πακέτα που ανήκουν στην ίδια FEC και ταξιδεύουν από ένα συγκεκριμένο κόμβο θα ακολουθήσουν το ίδιο μονοπάτι

• Η FEC κωδικοποιείται στην MPLS ετικέτα. Όταν ένα πακέτο προωθείται στον επόμενο δρομολογητή, η ετικέτα αποστέλλεται μαζί με αυτό

• Στη διαδρομή του πακέτου δεν πραγματοποιείται περαιτέρω ανάλυση της επικεφαλίδας του

• Η ετικέτα χρησιμοποιείται σαν ένας δείκτης σε ένα πίνακα που καθορίζει το επόμενο βήμα και μια νέα ετικέτα

• Η παλιά ετικέτα αντικαθίσταται από την καινούρια, και το πακέτο προωθείται στο επόμενο βήμα

• Έτσι, όλη η προώθηση οδηγείται από τις ετικέτες.

• Ορισμένοι δρομολογητές αναλύουν την επικεφαλίδα του επιπέδου δικτύου του πακέτου και για να καθορίσουν την προτεραιότητά του ή την κλάση υπηρεσίας

• Το MPLS επιτρέπει (αλλά δεν απαιτεί) η προτεραιότητα και η κλάση υπηρεσίας να εξάγονται πλήρως ή μερικώς από την ετικέτα

Η Μεταγωγή Ετικέτας (Label Switching) είναι ένας εξελιγμένος τρόπος προώθησης πακέτων που αντικαθιστά την προώθηση που βασίζεται στην αντιστοίχιση των διευθύνσεων.
Παρουσιάζει ένα πλήθος πλεονεκτημάτων σχετικά με τη συνηθισμένη δρομολόγηση:
– Η MPLS προώθηση μπορεί να γίνει και από switches που δεν μπορούν να αναλύσουν τις επικεφαλίδες δικτυακού επιπέδου.
– Ο δρομολογητής εισόδου καθώς αποφασίζει την ανάθεση, μπορεί να χρησιμοποιήσει οποιαδήποτε πληροφορία που διαθέτει σχετικά με το πακέτο.
– Ένα πακέτο που εισέρχεται στο δίκτυο μέσω ενός συγκεκριμένου δρομολογητή μπορεί να λάβει διαφορετική ετικέτα από αυτή που θα έπαιρνε αν έμπαινε στο δίκτυο από κάποιο διαφορετικό δρομολογητή
– Οι διαδικασίες που καθορίζουν τον τρόπο που ένα πακέτο ανατίθεται σε μια FEC μπορεί να γίνονται όλο και πιο πολύπλοκες χωρίς να επηρεάζουν τους δρομολογητές
– Οι αποφάσεις δρομολόγησης παραδοσιακά βασίζονται στη διεύθυνση, ενώ στο MPLS μπορεί να βασίζονται σε οποιοδήποτε πλήθος παραμέτρων, όπως ποιότητα υπηρεσίας, συμμετοχή σε VPN, κ.ά.
– Η διαδρομή του πακέτου επιλέγεται σαφώς πριν ή ακριβώς τη στιγμή που το πακέτο εισέρχεται στο δίκτυο

3.6 TUNNELS ΚΑΙ LABEL STACKS

• Το MPLS μπορεί να ελέγχει ολόκληρο το μονοπάτι ενός πακέτου χωρίς να καθορίζει ρητώς τους ενδιάμεσους δρομολογητές

• Από τη στιγμή που έχει πραγματοποιηθεί ανταλλαγή των ετικετών μεταξύ των LSRs που υποστηρίζουν ένα LSP, οι ενδιάμεσοι LSRs που ανήκουν στο LSP δε χρειάζεται να εξετάζουν το περιεχόμενο των πακέτων δεδομένων που περνούν από το LSP

• Για αυτό το λόγο, τα LSPs συχνά θεωρείται ότι σχηματίζουν tunnels κατά μήκος ολόκληρου ή ενός τμήματος του MPLS δικτύου κορμού

• Ένα tunnel μεταφέρει αδιαφανή δεδομένα μεταξύ του LSR εισόδου του tunnel και του LSR εξόδου του tunnel

• Αυτό σημαίνει ότι ολόκληρο το ωφέλιμο φορτίο, συμπεριλαμβανομένων των IP επικεφαλίδων, μπορεί να αποκρύπτεται με ασφάλεια χωρίς να επιβαρύνει την ικανότητα του δικτύου να προωθεί δεδομένα

• Επιπλέον το tunneling επιτρέπει τη διανομή ετικετών για πολλαπλά FECs και εγκατάσταση πολλαπλών LSPs

• Η ανάθεση πολλαπλών ετικετών καλείται Label Stacking και επιτρέπει καλύτερη κατηγοριοποίηση της κυκλοφορίας μεταξύ των κόμβων εισόδου και εξόδου

3.7 LABEL INFORMATION BASE – LIB

• LIB είναι η βάση των πληροφοριών σχετικά με τις ετικέτες

• Κάθε LSR κατασκευάζει έναν πίνακα για να καθορίσει πώς θα πρέπει να προωθηθεί κάποιο πακέτο – Αποθηκεύει όλες τις ετικέτες που έχουν διαφημιστεί από άλλους LSRs στο MPLS δίκτυο

• LFIB (cache) – Χρησιμοποιείται από τη διεργασία προώθησης πακέτων – Είναι ανάλογο του IP forwarding table – Περιέχει incoming και outgoing label, FEC, next hop

• LFIB = συνδυασμός LIB και IP routing table

3.8 TRAFFIC ENGINEERING

• Στα περισσότερα δίκτυα η κίνηση είναι ανομοιόμορφη

• Traffic engineering είναι η διαδικασία καταμερισμού της κίνησης μέσα στο δίκτυο, ώστε να ικανοποιηθούν οι απαιτήσεις των εφαρμογών

• Στόχο έχει να δρομολογηθεί η κίνηση πάνω από τις κατάλληλες συνδέσεις με τέτοιο τρόπο ώστε να αποφευχθεί η συμφόρηση και να μην υπάρχει άμεση ανάγκη για εφαρμογή άλλων σχημάτων QoS

• Ουσιαστικά βελτιστοποιεί την απόδοση μέσω της αντιστοίχισης των ροών κυκλοφορίας στην τοπολογία του δικτύου

• Η αντιστοίχιση των ροών κυκλοφορίας επιτυγχάνει την εξισορρόπηση του φορτίου στους συνδέσμους, δρομολογητές και switches

• Η διαδικασία αποτελείται από το σχεδιασμό του δικτύου (επιλογή των μονοπατιών) και τη βελτιστοποίηση

• Δύο κατηγορίες δρομολόγησης της κυκλοφορίας:

– ρητή δρομολόγηση: το μονοπάτι έχει προεπιλεγεί και μπορεί να γίνει και δέσμευση πόρων

– έμμεση δρομολόγηση: επιλέγεται μονοπάτι που ικανοποιεί τις απαιτήσεις προώθησης των ροών και δεσμεύονται οι πόροι

• Προϋπόθεση: Να γνωρίζει η πηγή τα πλήρη χαρακτηριστικά του δικτύου – να γίνεται διανομή των στοιχείων του δικτύου και να υπάρχει δυνατότητα δέσμευσης των πόρων

• Οι πιο γνωστοί και διαδεδομένοι μηχανισμοί σηματοδότησης για την διανομή των ετικετών είναι: – CR-LDP – RSVP-TE

ΠΛΕΟΝΕΚΤΗΜΑΤΑ

• Δρομολόγηση των κυρίων μονοπατιών

• Παροχή ακριβούς ελέγχου

• Αποδοτικότερη χρησιμοποίηση του εύρους ζώνης

•Ελαχιστοποίηση της απώλειας πακέτων, των παρατεταμένων περιόδων συμφόρησης και μεγιστοποίηση του throughput

• Παροχή περισσότερων επιλογών, χαμηλότερου κόστους και καλύτερης υπηρεσίας στους πελάτες

3.9 RESOURCE RESERVATION PROTOCOL (RSVP)

• Το RSVP είναι ένα πρωτόκολλο επιπέδου μεταφοράς για την δημιουργία μονοπατιών και δέσμευση πόρων

• Επιτρέπει σε τεχνολογίες που δεν παρέχουν εγγενώς QoS, να μπορούν να ζητούν συγκεκριμένους πόρους από το δίκτυο και να μίας χρησιμοποιούν κατά τη διάρκεια μίας σύνδεσης

• Πρέπει όλοι οι κόμβοι που παρεμβάλλονται από το ένα άκρο μέχρι το άλλο να υποστηρίζουν το πρωτόκολλο

3.10 RSVP ME TRAFFIC ENGINEERING EXTENSIONS

• Η RSVP σηματοδοσία λαμβάνει χώρα μεταξύ δρομολογητών (traffic trunk), ενώ το RSVP εφαρμόζεται σε μια συλλογή ροών που μοιράζονται ένα κοινό μονοπάτι και ένα κοινό σύνολο δικτυακών πόρων

– Επιτυγχάνεται διανομή των MPLS ετικετών

– Μειώνεται το πλήθος των μηνυμάτων ανανέωσης και οι σχετικές απαιτήσεις για επεξεργασία

– Το μονοπάτι δεν περιορίζεται από την τυπική δρομολόγηση που βασίζεται στον προορισμό

• Το RSVP δέχτηκε ειδικότερες επεκτάσεις για την υποστήριξη LSP Tunnels:

– Downstream-on-demand διανομή ετικέτας

– Αρχικοποίηση ρητών LSPs

– Κατανομή των δικτυακών πόρων στα ρητά LSPs

– Επαναδρομολόγηση των εγκατεστημένων LSP tunnels

– Ανίχνευση της πραγματικής διαδρομής που ακολουθεί ένα LSP tunnel

– Εισαγωγή της έννοιας των abstract κόμβων

3.11 ΕΦΑΡΜΟΓΕΣ MPLS

• Το MPLS μπορεί να χρησιμοποιηθεί ώστε να παρέχει:

– ποιότητα υπηρεσίας (QoS)

– δυνατότητα εφαρμογής traffic engineering

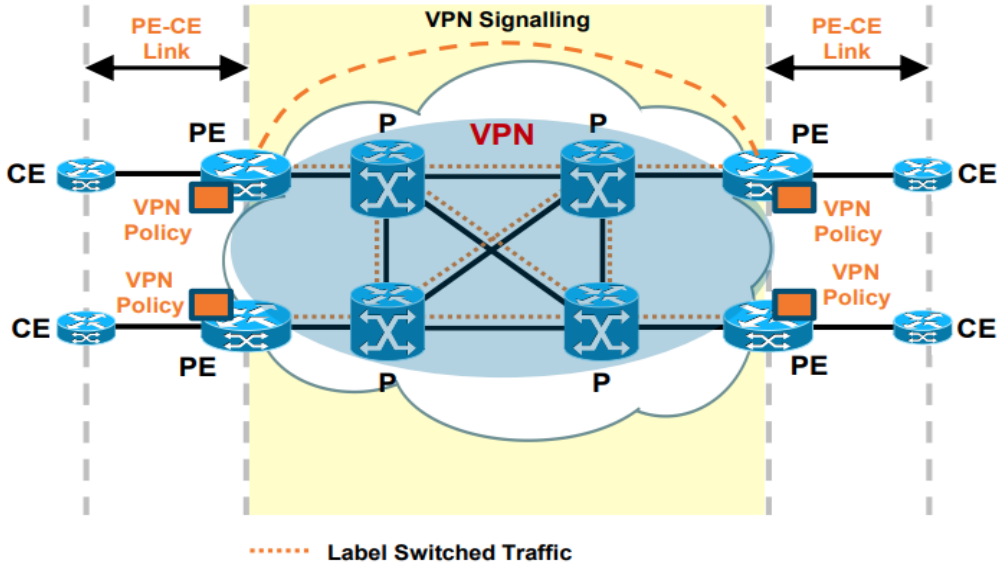
– πιο εύκολη και αποδοτική μεταφορά IP κυκλοφορίας πάνω από ATM υποδομή

– μια αποδοτική λύση στο πρόβλημα της ασφάλειας των προσωπικών δεδομένων καθώς και υποστήριξη της χρήσης μη μοναδικών, ιδιωτικών IP διευθύνσεων στο εσωτερικό ενός VPN

– ιδεατά κυκλώματα ή tunnels κατά μήκος ενός IP δικτύου

4. MPLS VPNs

4.1 Εισαγωγή



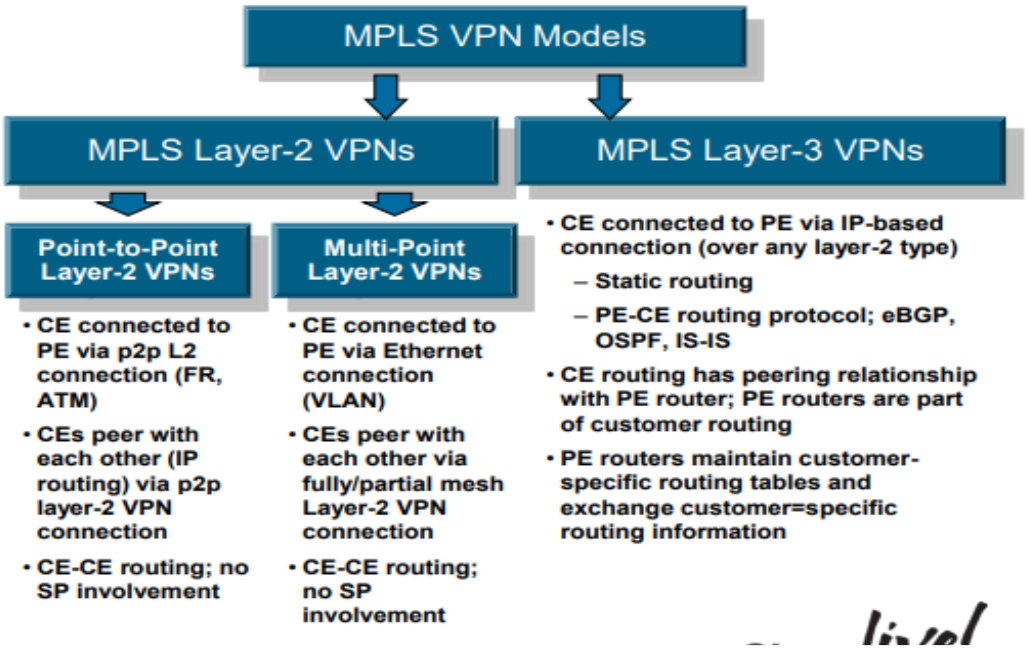
Εικόνα 11: MPLS VPNs

• Τα κλασικά ιδιωτικά δίκτυα βασίζονται σε μισθωμένες γραμμές με σημαντικό κόστος και δύσκολη και απαιτητική διαχείριση. Τα ιδεατά ιδιωτικά δίκτυα (Virtual Private Networks - VPN) είναι ένας τύπος ιδιωτικών δικτύων που χρησιμοποιούν δημόσιες διασυνδέσεις, όπως το Internet, αντί για leased lines. Έγιναν δημοφιλή καθώς οι εργαζόμενοι άρχισαν να εργάζονται από απομακρυσμένες τοποθεσίες

• Λύνουν τα προβλήματα κόστους αφού χρησιμοποιείται η δημόσια υποδομή και παράλληλα προσφέρουν την ασφάλεια και την αξιοπιστία των μισθωμένων γραμμών Τα VPNs μπορούν να βασίζονται σε IP tunnels.
– Η προς μετάδοση πληροφορία διαμορφώνεται σε IP πακέτα
–Έχουν χαμηλό κόστος και χαρακτηρίζονται από ευκολία στις συνδέσεις εκτός δικτύου
– Μειονέκτημα: απαιτούνται επιπλέον τεχνικές κρυπτογράφησης
– Μπορούν να χρησιμοποιηθούν για οποιονδήποτε τύπο επικοινωνίας

4.2 MPLS VPNs

Η MPLS τεχνολογία παρέχει τη δυνατότητα δημιουργίας ιδεατών ιδιωτικών δικτύων (MPLS VPNs). Υπάρχουν οι παρακάτω δύο κατηγορίες τέτοιων δικτύων όπως φαίνεται και στην παρακάτω εικόνα.
L3 MPLS VPN (επίπεδο 3)
L2 MPLS VPN (επίπεδο 2)



Εικόνα 12: MPLS VPNs Layers(source, Myron Ward)

4.2.1 L3 MPLS VPN

Ο πάροχος αναθέτει σε κάθε VPN ένα μοναδικό αναγνωριστή που καλείται αναγνωριστής διαδρομής (Route Distinguisher – RD) και είναι διαφορετικός για κάθε πελάτη εντός του δικτύου. Οι πίνακες προώθησης περιέχουν μοναδικές διευθύνσεις για κάθε τελικό σημείο στο δίκτυο, οι οποίες καλούνται VPN-IP διευθύνσεις. Επίσης κάθε VPN συσχετίζεται με ένα ή περισσότερα VPN στιγμιότυπα δρομολόγησης/προώθησης (VRFs) που καθορίζουν τη VPN συμμετοχή της τοποθεσίας ενός πελάτη που συνδέεται σε έναν PE δρομολογητή. Στο συγκεκριμένο σημείο χρειάζεται να αναφερθεί ότι ένα VRF αποτελείται από έναν πίνακα IP δρομολόγησης, έναν πίνακα προώθησης, ένα σύνολο από interfaces που χρησιμοποιούν τον πίνακα προώθησης και από ένα σύνολο κανόνων και παραμέτρων δικτυακών πρωτοκόλλων. Αυτό έχει σαν αποτέλεσμα οι πίνακες προώθησης να αποτρέπουν την προώθηση των πληροφοριών έξω από το VPN και την προώθηση πακέτων που βρίσκονται έξω από ένα VPN προς ένα δρομολογητή εντός του VPN. Βάση των πληροφοριών στους πίνακες IP δρομολόγησης και προώθησης, τα πακέτα προωθούνται στον προορισμό τους χρησιμοποιώντας MPLS. Τέλος, γίνεται χρήση των LSPs για προώθηση δεδομένων ανάμεσα στους ακραίους δρομολογητές που καθορίζουν τα όρια σε ένα VPN.

4.2.2 L2 MPLS VPNs

Αναφέρεται στη μετάδοση πλαισίων του επιπέδου 2 (layer 2 frames) μέσα σε ένα MPLS δίκτυο. Η υλοποίηση γίνεται στο επίπεδο 2 (data link) σαν να μην υπάρχει μετάδοση των πλαισίων πάνω από MPLS, αλλά σαν να υπήρχαν κανονικές συνδέσεις του επιπέδου 2 – επιτρέπει τη διατήρηση και διαχείριση μίας κοινής υποδομής στην επικοινωνία των πελατών μέσα από το δίκτυο του παρόχου (mpls core). Βασίζεται στη δυνατότητα ενθυλάκωσης και μεταφοράς των PDUs, για διάφορα πρωτόκολλα του επιπέδου 2, πάνω από ένα MPLS δίκτυο.

4.2.3 Τεχνολογίες Layer 2 VPNs

Οι τεχνολογίες στα MPLS Layer-2 VPNs χωρίζονται σε δυο κατηγορίες.

- Point to Point (PWs) - VPWS

Ο Customer Edge (CE) σε κάθε σημείο παρουσίας συνδέεται στον εκάστωτε PE με Point-to-Point L2 σύνδεση με οποιοδήποτε πρωτόκολλο διασύνδεσης (FR, ATM, Ethernet). Οι CEs μεταξύ διαφορετικών σημείων συνδέονται μέσω LAYER 2 VPNs σύνδεσης που πραγματοποιείτε στους PE routers και σαφώς οι πρώτοι δεν έχουν καμία ανάμειξη και εικόνα από την τοπολογία του δικτύου.

- Multipoint to Multipoint LAYER 2 VPNs (VPLS)

Το CE συνδέεται στο PE μέσω σύνδεσης Ethernet. Οι CEs συνδέονται με άλλους CEs που βρίσκονται σε διαφορετικά σημεία σύνδεσης σε περισσότερα από δύο σημεία που μπορεί να υποστηριχτεί σε ένα MPLS δίκτυο. Σχηματίζονται fully/partial mesh LAYER 2 VPNs μεταξύ των PE κόμβων που έχουν διασύνδεση με τους εκάστοτε CEs.

4.2.4 Virtual Private Wire Services (VPWS) ή ATOM Ενθυλάκωση πλαισίων του επιπέδου 2

Η παραπάνω μέθοδος χρησιμοποιείται για την εξομοίωση εικονικών κυκλωμάτων για τη μετάδοση των PDUs των layer 2 πρωτοκόλλων, κατά μήκος ενός IP/MPLS δικτύου. Για να επιτευχθεί αυτή η μετάδοση θα πρέπει τα (Protocol Data Units) PDUs των layer2 πρωτοκόλλων να ενθυλακωθούν. Διακρίνονται τρία επίπεδα ενθυλάκωσης:

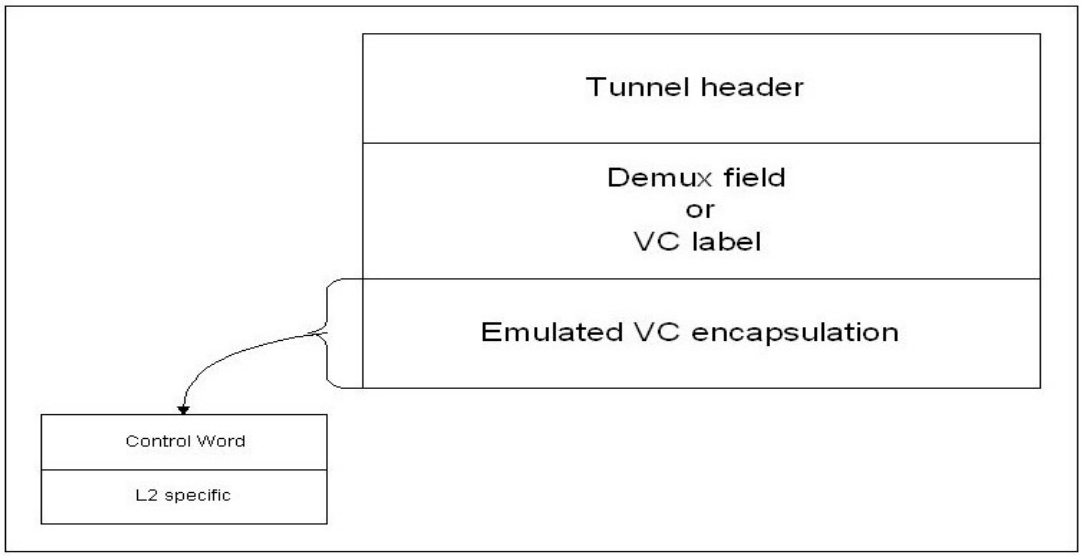
• η επικεφαλίδα του τούνελ (tunnel header), που περιέχει τις πληροφορίες που απαιτούνται για τη μμετάδοση της PDU πάνω από το IP ή το MPLS δίκτυο. Αυτή η επικεφαλίδα καθορίζεται από το πρωτόκολλο που χρησιμοποιείται για το μμηχανισμό των τούνελ, π.χ. MPLS, GRE, L2TP κ.λπ.

• το πεδίο αποπολυπλεξίας (demultiplexer field), που χρησιμοποιείται για τον διαχωρισμό των ξεχωριστών εξομοιούμενων εικονικών κυκλωμάτων μέσα σε ένα τούνελ. Το πεδίο αυτό πρέπει, επίσης, να γίνεται κατανοητό από το πρωτόκολλο που χρησιμοποιείται για το μμηχανισμό των τούνελ, π.χ. μπορεί να είναι μία MPLS ετικέτα (MPLS label), ένα πεδίο-κλειδί του GRE (GRE key field) κ.λπ.

• η ενθυλάκωση του εξομοιούμενου εικονικού κυκλώματος (emulated VC encapsulation), που περιέχει πληροφορία για την ενθυλακωμένη PDU και η οποία είναι απαραίτητη για την σωστή εξομοίωση του αντίστοιχου πρωτοκόλλου του επιπέδου 2. Αν και τα διάφορα πρωτόκολλα του επιπέδου 2 απαιτούν την τοποθέτηση διαφορετικής πληροφορίας σε αυτή τη θέση, η προτεινόμενη προτυποποίηση κάνει την ενθυλάκωση όσο πιο κοινή γίνεται. Για το λόγο αυτό η πληροφορία χωρίζεται σε δύο τμήματα

- τη λέξη ελέγχου (control word) που έχει κοινή δομή για κάθε πρωτόκολλο επιπέδου 2 που υποστηρίζεται και

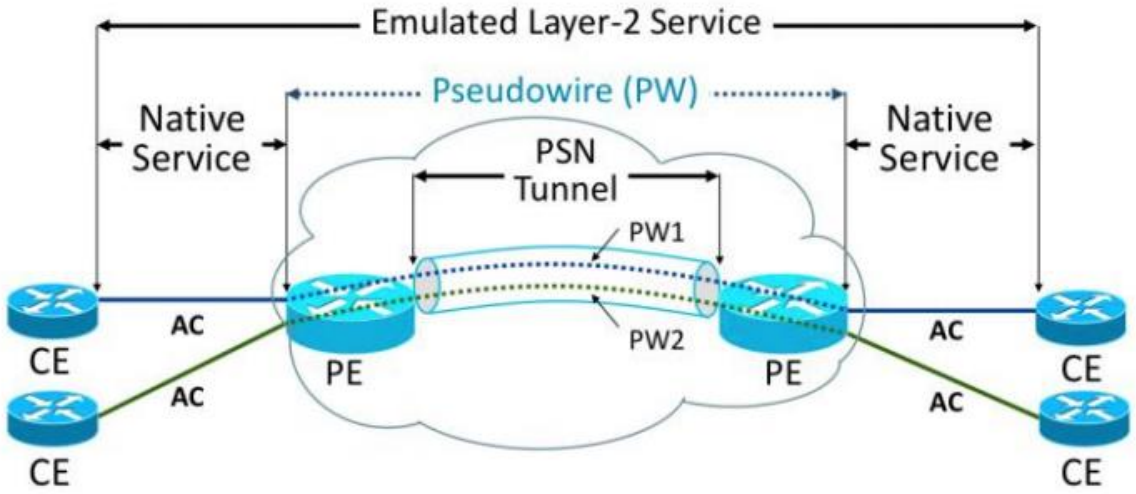
- την πληροφορία που διαφοροποιείται ανάλογα με το πρωτόκολλο (protocol specific)



Εικόνα 13: IETF's PW

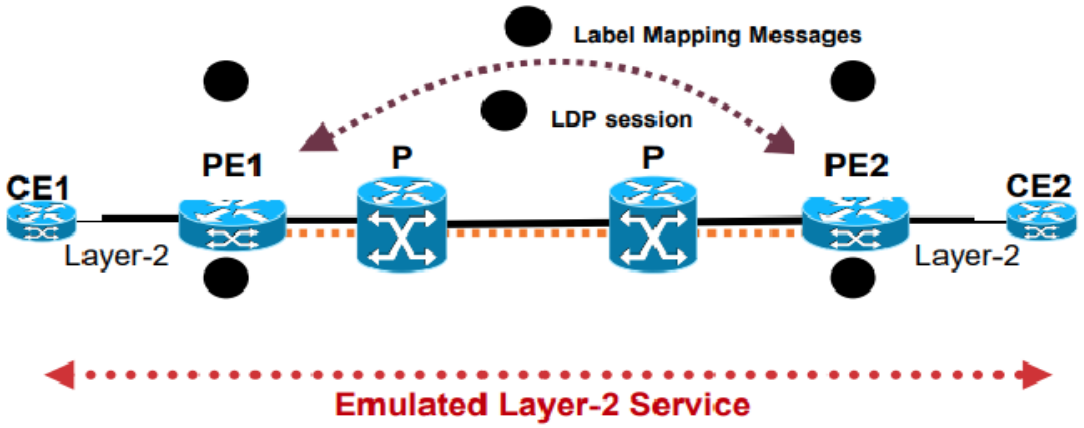
Η παραπάνω εικόνα είναι βασισμένη στο μοντέλο του IETF's Pseudowire (PW)

- Σε όλα τα layer – 2 traffic επιτρέπει την μεταφορά μέσω MPLS
- Περιλαμβάνει ετικέτες ενθυλάκωσης VC και μετάφραση L2 πακέτων (Ethernet, ATM, PPP ή FR)
- PE-CE σύνδεσμος αναφέρεται ως Attachment Circuit (AC)
- Υποστηρίζει δίκτυο L2
- Τα PW είναι διπλής κατεύθυνσης (PW1, PW2)



Εικόνα 14: MPLS VPNs Layer2(source, https://orhanergun.net/what-is-attachment-circuit-in-mpls-vpn/)

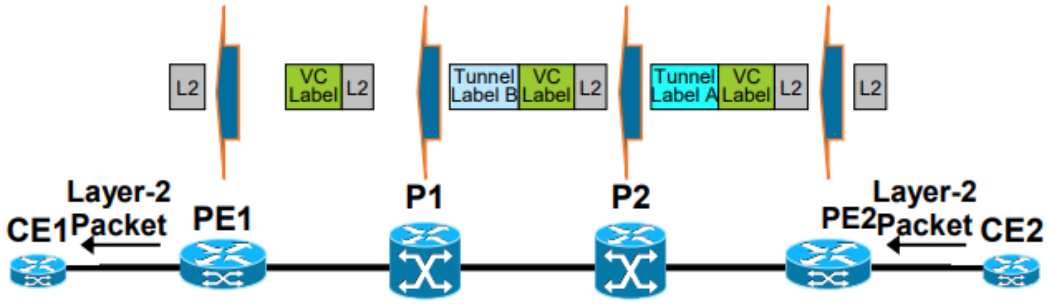
VPWS Control Plane Processing: Σηματοδοσία του νέου Pseudowire



Εικόνα 15: Emulated Layer 2 Service

Το νέο εικονικό κύκλωμα (VC) συνδέει Interface L2 πελατών σε νέο PW μέσω VC ID του τοπικού και του απομακρυσμένου PE Router-ID. Στους εκάστοτε PEs θα συνδεθεί και θα εξυπηρετηθεί ο πελάτης CE1, CE2. Στη συνέχεια θα δημιουργηθεί Νέα στενευμένη LDP συνεδρία (targeted LDP session) μεταξύ PE1 και PE2 αν δεν υπάρχει ήδη. Ο κάθε PE δημιουργεί και αντιστοιχεί το VC label σε κάθε L2 κύκλωμα και στέλνει τον χάρτη ετικετών στον απομακρυσμένο PE. Ο απομακρυσμένος PE παίρνει το μήνυμα ότι έγινε bind το LDP label και βάζει το σωστό VC ID με το τοπικό VC που έχει ήδη διαμορφωθεί.

VPWS Forwarding Plane Processing: Προώθηση του Layer-2 traffic μέσω Pseudowire



Εικόνα 16: Layer 2 traffic μεσω PW

Σύμφωνα με την παραπάνω εικόνα ο πελάτης CE2 προωθεί αρχικά το L2 πακέτο (frame) στο κόμβο PE2. Ο PE2 σπρώχνει την εσωτερική VC ετικέτα στο L2 πακέτο που ειχε παραληφθεί από το CE2. Στη συνέχεια ο PE2 σπρώχνει ένα εξωτερικο (Tunnel) label και προωθεί το πακέτο στο P2. Το P2 και το P1 προωθούν πακετα χρησιμοποιόντας το εξωτερικό (tunnel) label. (label swapping). Στη συνέχεια ο Router P1 αφαιρεί (pop) την ετικετα του tunnel διότι έχει δεχτεί implicit-null από τον PE1 και βασιζομενο στο VC label του PE1 ,το πακετο L2 προωθείται στο interface που είναι συνδεδεμένο με τον CE1 και το VC label διαγράφεται.

ATOM Πλεονεκτήματα

•Διαχωρισμός διαχειριστικών αρμοδιοτήτων

• Ανεξαρτησία από το πρωτόκολλο του επιπέδου 3

• Μειωμένο overhead

• Ομοιογένεια στις διαφορετικές L2 τεχνολογίες

• Πραγματική end-to-end connectivity

ATOM Μειονεκτήματα

• Απαίτηση για κοινή τεχνολογία επιπέδου 2 σε κάθε VPN

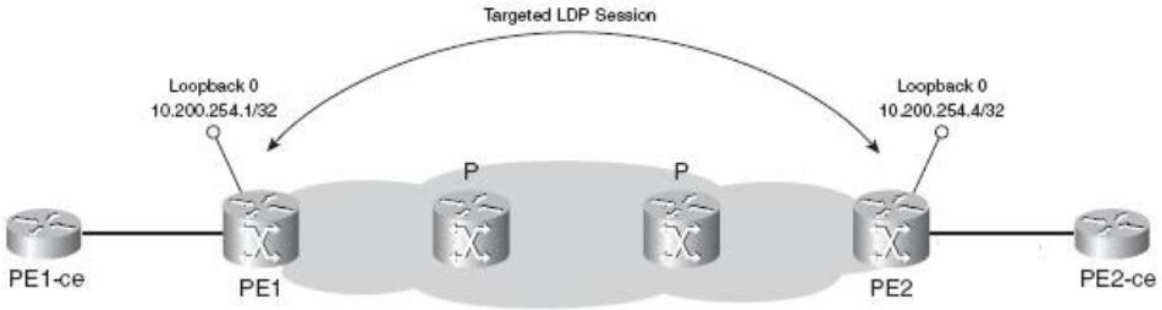
• Πολυπλοκότητα δρομολόγησης για τους πελάτες

Ethernet over MPLS Transport (EoMPLS)

Οποιαδήποτε μεταφορά μέσω MPLs (Atom) μεταφέρει το Layer 2 packets πάνω σε ένα MPLS. Το ATOM χρησιμοποιεί ένα Label Distribution Protocol (LDP) μεταξύ των δρομολογητών για τη δημιουργία και τη διατήρηση της σύνδεσης. Η προώθηση συμβαίνει μέσω της χρήσης ετικετών δύο επιπέδων που παρέχουν την εναλλαγή μεταξύ των edge routers. Η εξωτερική ετικέτα (ετικέτα σήραγγας- tunnel) δρομολογεί το πακέτο πάνω από το backbone του MPLS στην egress PE στην ingress PE. Η ετικέτα VC είναι μια ετικέτα απόρριψης που καθορίζει τη σύνδεση στη σήραγγα. Οι υπηρεσίες Ethernet μεταφέρονται μέσω δικτύων IP / MPLS που χρησιμοποιούν ένα ευρύ φάσμα πρωτοκόλλων που σχετίζονται με IP (πρότυπα IETF Pseudowire). Οι συνδέσεις Ethernet μεταφέρονται ως "Pseudowires" χρησιμοποιώντας διαδρομές διαδρομής ετικετών MPLS (LSP) μέσα σε ένα εξωτερικό MPLS tunnel. Αυτή η στρατηγική μπορεί να υποστηρίξει τόσο τις υπηρεσίες (Virtual Private Wire Service - VPWS) και Multipoint (Virtual Private Lan Service - VPLS) και πρόσφατα πέτυχε σημαντική ανάπτυξη σε δρομολογημένα δίκτυα.

EoMPLS- Ethernet PW Modes

Ένα Ethernet PseudoWire (PW) μιμείται μια ενιαία σύνδεση Ethernet μεταξύ δύο τελικών σημείων (συσκευές PE). Ταυτόχρονα, ένα Ethernet PW επιτρέπει τη μεταφορά PDUs Ethernet σε όλο το δίκτυο MPLS.



Εικόνα 17: Targeted LDP(source, https://www.ccexpert.us/mpls-network/ethernet.html)

Ένα Ethernet PW λειτουργεί με δυο τρόπους, με tag ή χωρίς tag (ακατέργαστη). Σε λειτουργία με tag, το πλαίσιο πρέπει να έχει τουλάχιστον μία ετικέτα 802.1Q/VLAN και ότι η ετικέτα VLAN έχει κάποιο νόημα για τις συσκευές άκρων PW (συσκευές PE), δηλαδή αυτές οι συσκευές PE θα έχουν κάποια συμφωνία για τον τρόπο επεξεργασίας αυτής της ετικέτας. Αντίθετα, στη λειτουργία χωρίς tag, το πλαίσιο μπορεί να έχει ετικέτα 802.1Q, αλλά μπορεί να περάσει απαρατήρητο μέσω των συσκευών PE. Όταν ο δρομολογητής PE λαμβάνει ένα πλαίσιο Ethernet με ετικέτα VLAN, μπορεί να είναι μία από τις δύο περιπτώσεις:

- Το tag οριοθετεί την υπηρεσία: Αυτό σημαίνει ότι το tag έχει εισαχθεί από τη συσκευή SP. Για παράδειγμα, τα LANs από διαφορετικούς πελάτες ενδέχεται να είναι συνδεδεμένα στον ίδιο διακόπτη SP και αυτός ο διακόπτης διαχωρίζει την επισκεψιμότητα των πελατών εισάγοντας ετικέτες VLAN και, στη συνέχεια, προωθεί τα πλαίσια στη συσκευή PE.
- Η ετικέτα δεν οριοθετεί την υπηρεσία: Αυτό σημαίνει ότι η ετικέτα εισήχθη στο πλαίσιο από μια συσκευή CE και δεν έχει νόημα για τη συσκευή PE.

Εάν το Ethernet PW εκτελείται σε λειτουργία Untagged στη συσκευή PE και η συσκευή PE λαμβάνει ένα πλαίσιο με ετικέτα οριοθέτησης υπηρεσίας στο κύκλωμα προσάρτησης, η ετικέτα πρέπει να απογυμνωθεί πριν από την προώθηση. Η ετικέτα δεν αποστέλλεται ποτέ μέσω του Ethernet PW.

Εάν το Ethernet PW εκτελείται σε λειτουργία με tag στη συσκευή PE, η συσκευή PE απαιτεί να λάβει το πλαίσιο με μια ετικέτα οριοθέτησης υπηρεσίας. Εάν δεν υπάρχει ετικέτα, η συσκευή PE προετοιμάζεται για μια εικονική ετικέτα στο πλαίσιο πριν προωθήσει το πλαίσιο στο Ethernet PW.
Και στις δύο λειτουργίες, οι ετικέτες που δεν οριοθετούν την υπηρεσία αποστέλλονται με διαφάνεια μέσω ethernet PW.

Σε ακατέργαστη λειτουργία, η ετικέτα δεν πρέπει να ξαναγραφεί ή να αφαιρεθεί πριν από την αποστολή του πλαισίου πάνω από το κύκλωμα.

4.2.5 VPLS (Virtual Private LAN Service)

Το Virtual Private LAN Service (VPLS) είναι ένας τρόπος για να παρέχουμε πολλαπλά σημεία με βάση το Ethernet σε πολλαπλή επικοινωνία μέσω δικτύων IP/MPLS. Με τον παραπάνω τρόπο επιτρέπεται σε γεωγραφικά διασκορπισμένους ιστοτόπους να μοιράζονται έναν τομέα εκπομπής Ethernet μέσω σύνδεσης ιστότοπων μέσω pseudowires (multipoint). Σε ένα VPLS, το τοπικό δίκτυο (LAN) σε κάθε τοποθεσία επεκτείνεται στην άκρη του δικτύου παρόχου. Το δίκτυο παροχου στη συνέχεια εξομοιώνει switch ή την bridge για τη σύνδεση όλων των πελατών LAN για να δημιουργήσει ένα μόνο-γεφυρωμένο LAN. Το VPLS έχει σχεδιαστεί για εφαρμογές που απαιτούν πρόσβαση πολλαπλών σημείων ή εκπομπής (broadcast access). Μπορούμε να χρησιμοποιήσουμε 2 μεθόδους για τη σηματοδοσία μιας VPLS σύνδεσης: Border Gateway Protocol (BGP) ή Label Distribution Protocol (LDP). Το "control plane" είναι το μέσο με το οποίο οι provider edge (PE) routers

επικοινωνούν για το Signaling και το auto-discovery. Το auto-discovery είναι η διαδικασία που βρίσκει άλλους PE routers που παίρνουν μέρος στο VPLS. Signaling ονομάζεται η διαδικασία της εγκατάστασης των pseudowires (PW). Τα PWs απαρτίζουν τα "data plane", τα PEs στέλνουν VPLS traffic στα άλλα PEs. Το BGP παρέχει τόσο αυτόματο εντοπισμό (auto discovery) όσο και σηματοδότηση (signaling). Οι μηχανισμοί που χρησιμοποιούνται είναι πολύ παρόμοιοι με εκείνους που χρησιμοποιούνται για τη δημιουργία VPN Layer-3 MPLS. Κάθε PE έχει ρυθμιστεί να συμμετέχει σε ένα δεδομένο VPLS. Ο PE, μέσω της χρήσης του BGP, ανακαλύπτει ταυτόχρονα όλους τους άλλους PEs στο ίδιο VPLS και καθιερώνει ένα πλήρες πλέγμα ψευδό-συρμάτων στους εν λόγω PEs.

Με το LDP, κάθε δρομολογητής PE πρέπει να ρυθμιστεί ώστε να συμμετέχει σε ένα δεδομένο VPLS και, επιπλέον, να λαμβάνει τις διευθύνσεις άλλων PEs που συμμετέχουν στο ίδιο VPLS. Στη συνέχεια, δημιουργείται ένα πλήρες πλέγμα περιόδων λειτουργίας LDP μεταξύ αυτών των PEs. Στη συνέχεια, το LDP χρησιμοποιείται για τη δημιουργία ισοδύναμου ματιού PWs μεταξύ των εν λόγω PEs. Ένα πλεονέκτημα από τη χρήση PWs ως υποκείμενης τεχνολογίας για το επίπεδο δεδομένων είναι ότι σε περίπτωση αποτυχίας, η κυκλοφορία θα δρομολογείται αυτόματα κατά μήκος των διαθέσιμων διαδρομών δημιουργίας αντιγράφων ασφαλείας στο δίκτυο του παρόχου υπηρεσιών. Η ανακατεύθυνση θα είναι πολύ ταχύτερη από ό, τι θα μπορούσε να επιτευχθεί με π.χ. πρωτόκολλο spanning tree (STP). Το VPLS είναι επομένως μια πιο αξιόπιστη λύση για τη σύνδεση δικτύων Ethernet σε διαφορετικές τοποθεσίες από την απλή σύνδεση μιας σύνδεσης WAN με διακόπτες Ethernet και στις δύο θέσεις.

Η VPLS έχει σημαντικά πλεονεκτήματα τόσο για τους παρόχους υπηρεσιών όσο και για τους πελάτες. Οι πάροχοι υπηρεσιών επωφελούνται επειδή μπορούν να δημιουργήσουν πρόσθετα έσοδα προσφέροντας μια νέα υπηρεσία Ethernet με ευέλικτο εύρος ζώνης και εξελιγμένες συμφωνίες επιπέδου υπηρεσιών (SLAs). Το VPLS είναι επίσης απλούστερο και οικονομικώς αποδοτικότερο να λειτουργήσει από μια παραδοσιακή υπηρεσία. Οι πελάτες επωφελούνται επειδή μπορούν να συνδέσουν όλους τους ιστότοπους τους σε ένα Ethernet VPN που παρέχει ένα ασφαλές, υψηλής ταχύτητας και ομοιογενές δίκτυο. Επιπλέον, το VPLS παρέχει ένα λογικό επόμενο βήμα στη συνεχή εξέλιξη του Ethernet από ένα κοινό πρωτόκολλο LAN 10 Mbit/s σε μια παγκόσμια υπηρεσία πολλαπλών Gbps.

Label stack

Τα πακέτα VPLS MPLS έχουν στοίβα δύο ετικετών. Η εξωτερικός ετικέτα χρησιμοποιείται για κανονική προώθηση MPLS στο δίκτυο της υπηρεσίας παροχής. Εάν χρησιμοποιείται BGP για τον καθορισμό του VPLS, η εσωτερική ετικέτα εκχωρείται από ένα PE ως μέρος ενός μπλοκ ετικέτας. Εάν χρησιμοποιείται LDP, η εσωτερική ετικέτα είναι ένα αναγνωριστικό εικονικού κυκλώματος που εκχωρείται από το LDP όταν καθιέρωσε για πρώτη φορά ένα πλέγμα μεταξύ των συμμετεχόντων PEs. Κάθε PE παρακολουθεί την αντιστοιχισμένη εσωτερική ετικέτα και τις συσχετίζει με την παρουσία VPLS.

Ethernet emulation

Τα PEs που συμμετέχουν σε ένα VPN που βασίζεται σε VPLS πρέπει να εμφανίζονται ως γέφυρα Ethernet σε συνδεδεμένες συσκευές άκρου πελάτη (CE). Τα ληφθέντα πλαίσια Ethernet πρέπει να αντιμετωπίζονται κατά τρόπον ώστε να εξασφαλίζεται ότι οι CEs μπορούν να είναι απλές συσκευές Ethernet.
Όταν ένα PE λαμβάνει ένα πλαίσιο από ένα CE, επιθεωρεί το πλαίσιο και μαθαίνει τη διεύθυνση MAC του CE, αποθηκεύοντας το τοπικά μαζί με πληροφορίες δρομολόγησης LSP. Στη συνέχεια, ελέγχει τη διεύθυνση MAC προορισμού του πλαισίου. Εάν πρόκειται για πλαίσιο εκπομπής ή η διεύθυνση MAC δεν είναι γνωστή στο PE, πλημμυρίζει το πλαίσιο σε όλα τα PEs στο πλέγμα.
Σε τακτικές αναπτύξεις Ethernet, το πρωτόκολλο spanning Tree χρησιμοποιείται για αυτό. Στο VPLS, η αποφυγή βρόχου τακτοποιείται με τον ακόλουθο κανόνα: Ένα PE δεν προωθεί ποτέ ένα πλαίσιο που λαμβάνεται από ένα PE σε άλλο PE. Η χρήση ενός πλήρους πλέγματος σε συνδυασμό με την προώθηση διαχωρισμένου ορίζοντα εγγυάται έναν τομέα μετάδοσης χωρίς βρόχους.

MAC addresses

Δεδομένου ότι το VPLS συνδέει πολλούς τομείς μετάδοσης Ethernet μαζί, δημιουργεί αποτελεσματικά έναν πολύ μεγαλύτερο τομέα μετάδοσης. Δεδομένου ότι κάθε PE πρέπει να παρακολουθεί όλες τις διευθύνσεις MAC και τις σχετικές πληροφορίες δρομολόγησης LSP, αυτό μπορεί ενδεχομένως να οδηγήσει σε μεγάλη ποσότητα μνήμης που απαιτείται σε κάθε PE στο πλέγμα.
Για την αντιμετώπιση αυτού του προβλήματος, οι τοποθεσίες ενδέχεται να χρησιμοποιούν ένα δρομολογητή ως συσκευή CE. Αυτό αποκρύπτει όλες τις διευθύνσεις MAC σε αυτόν τον ιστότοπο πίσω από τη διεύθυνση MAC του CE.
Οι συσκευές PE μπορούν επίσης να είναι εξοπλισμένες με μνήμη CAM, παρόμοια με τους διακόπτες Ethernet υψηλής ποιότητας.

PE auto-discovery

Σε ένα VPN που βασίζεται σε VPLS με μεγάλο αριθμό ιστότοπων, η χειροκίνητη διαμόρφωση κάθε συμμετέχοντος PE δεν κλιμακώνεται καλά. Εάν τεθεί σε λειτουργία μια νέα PE, κάθε υπάρχουσα PE πρέπει να προσαρμόσει τη ρύθμιση παραμέτρων της για να δημιουργήσει μια περίοδο λειτουργίας LDP με τη νέα PE. Οι εργασίες τυποποίησης βρίσκονται σε εξέλιξη για να καταστεί δυνατός ο αυτόματος εντοπισμός των συμμετεχόντων PEs. Υποβάλλονται σε επεξεργασία τρεις υλοποιήσεις:

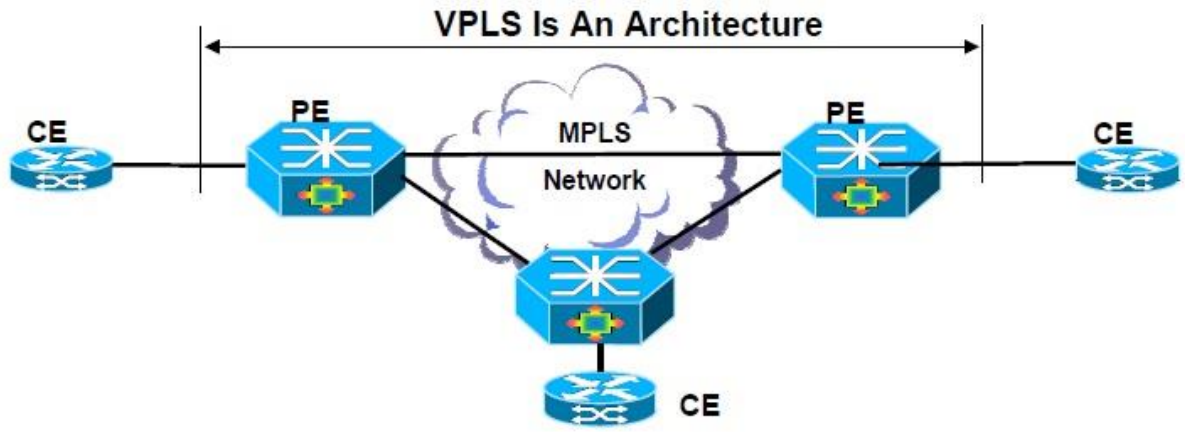
- Η μέθοδος LDP του αυτόματου εντοπισμού PE βασίζεται σε αυτήν που χρησιμοποιείται από το πρωτόκολλο διανομής ετικετών για την κατανομή ετικετών σε δρομολογητές P και PE μέσα σε ένα αυτόνομο σύστημα.

- Η μέθοδος BGP του αυτόματου εντοπισμού PE βασίζεται σε αυτή που χρησιμοποιείται από τα VPN Layer-3 MPLS για τη διανομή διαδρομών VPN μεταξύ PEs που συμμετέχουν σε ένα VPN. Οι επεκτάσεις πολλαπλών πρωτοκόλλων BGP4 (BGP-MP) χρησιμοποιούνται για τη διανομή VPN ID και πληροφοριών πρόσβασης ειδικά για VPN. Δεδομένου ότι το IBGP απαιτεί είτε ένα πλήρες πλέγμα περιόδων λειτουργίας BGP είτε τη χρήση ενός ανακλαστήρα διαδρομής, η ενεργοποίηση του αναγνωριστικού VPN σε μια υπάρχουσα διαμόρφωση BGP που συμμετέχει του παρέχει μια λίστα με όλα τα PEs σε αυτό το VPN. Σημειώστε ότι αυτή η μέθοδος προορίζεται μόνο για αυτόματο εντοπισμό. Το LDP εξακολουθεί να χρησιμοποιείται για σηματοδότηση. Η μέθοδος δημιουργίας VPLS με BGP που περιγράφεται παραπάνω επιτυγχάνει τόσο την αυτόματη ανακάλυψη όσο και τη σηματοδότηση.

Μέθοδος Radius, αυτή η μέθοδος απαιτεί τη ρύθμιση παραμέτρων ΟΛΩΝ των PEs με έναν ή περισσότερους διακομιστές RADIUS για χρήση. Όταν ο πρώτος δρομολογητής CE σε ένα συγκεκριμένο VPLS VPN συνδέεται με το PE, χρησιμοποιεί την ταυτότητα του CE για να ζητήσει έλεγχο ταυτότητας από το διακομιστή RADIUS. Η αναγνώριση αυτή μπορεί να παρέχεται από το CE ή μπορεί να διαμορφώνεται σε PE για το συγκεκριμένο CE. Εκτός από ένα όνομα χρήστη και έναν κωδικό πρόσβασης, η συμβολοσειρά αναγνώρισης περιέχει επίσης ένα όνομα VPN και ένα προαιρετικό όνομα παρόχου.

Ο διακομιστής RADIUS παρακολουθεί όλες τις PEs που ζήτησαν έλεγχο ταυτότητας για ένα συγκεκριμένο VPN και επιστρέφει μια λίστα αυτών στο PE που ζητά έλεγχο ταυτότητας. Στη συνέχεια, το PE δημιουργεί περιόδους λειτουργίας LDP σε κάθε PE της λίστας.

4.2.6 Σύνοψη Virtual Private LAN Service: Επισκόπηση της αρχιτεκτονικής του VPLS



Εικόνα 18: VPLS(source, https://www.rfwireless-world.com/Terminology/MPLS-vs-VPLS.html)

- Αρχιτεκτονική για υπηρεσίες πολλαπλών σημείων Ethernet μέσω MPLS
- Το δίκτυο VPLS λειτουργεί σαν ένας εικονικός διακόπτης που μιμείται τη συμβατική γέφυρα L2
- Υποστηρίζονται πλήρως δικτυωμένο ή hub-spoke ή τοπολογίες
- Ο σύνδεσμος PE-CE αναφέρεται ως κύκλωμα σύνδεσης (AC),συνήθως Ethernet

Technology Components

- Πολιτικές VPN
  - Εικονική παρουσία μεταγωγής ή VSI
  - Μία ή περισσότερες διεπαφές πελατών συνδέονται με VSI
  - Ένα ή περισσότερα PW για διασύνδεση με σχετικές παρουσίες VSI σε απομακρυσμένο PE

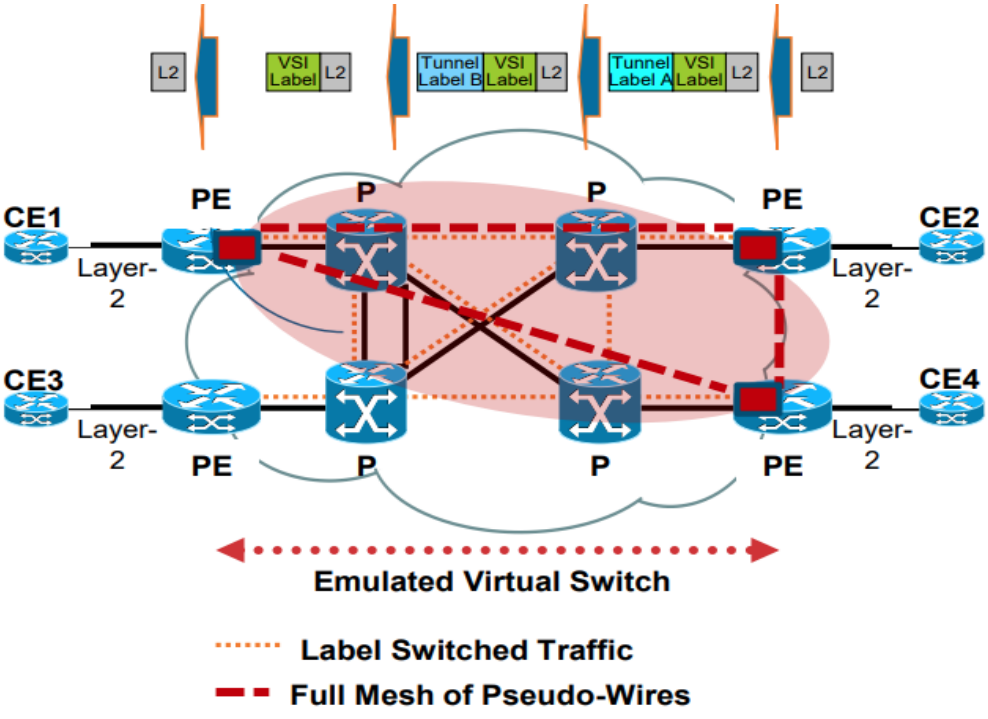
- Σηματοδότηση VPN
  - Πλήρες πλέγμα στοχευμένων συνεδριών LDP* (ανταλλαγή VC) ή/και BGP (ανακάλυψη και ανταλλαγή VC)
  - Διαπραγμάτευση ετικέτας εικονικής σύνδεσης (VC), απόσυρση, ειδοποίηση σφάλματος

- Προώθηση επισκεψιμότητας VPN
  - 1 ετικέτα VC που χρησιμοποιείται για την ενθυλάκωση + 1 (IGP) ετικέτα για την προώθηση
  - Εσωτερική ετικέτα αποπλέκτη (VC): προσδιορίζει το VSI
  - Εξωτερική ετικέτα σήραγγας (IGP): για να μεταβείτε από το Ingress στο egress PE χρησιμοποιώντας το MPLS LSP

- PE-CE link

  - Αναφέρεται ως κύκλωμα προσάρτησης (AC)
  - Οι VCs Ethernet είναι είτε κατάσταση λειτουργίας θύρας είτε αναγνωριστικό VLAN

VPLS Forwarding Plane Processing: Προώθηση της κίνησης επιπέδου-2 μέσω του δικτύου VPLS



Εικόνα 19: VPLS forwarding

Εκμάθηση MAC:

- Για νέα πακέτα L2
- Ο πίνακας προώθησης VSI ενημερώθηκε
- Πακέτα πλημμυρισμένα σε όλους τους PEs πάνω από PW

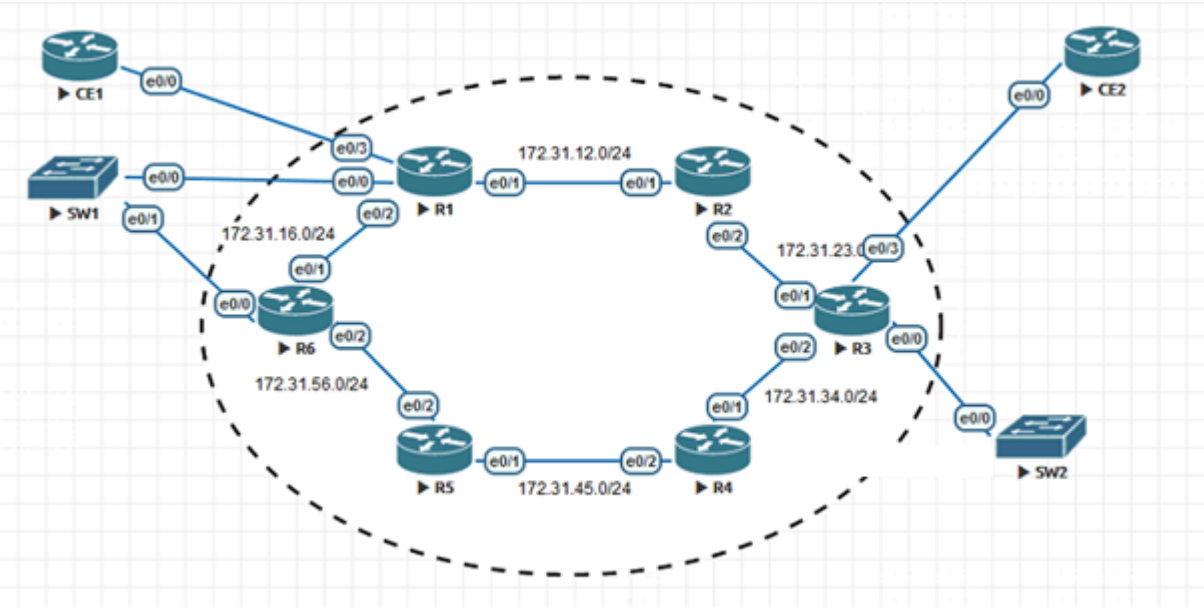
Layer-2 Packet Forwarding:

- Για πακέτα L2 με γνωστές διευθύνσεις MAC προορισμού
- Εμφάνιση στον πίνακα προώθησης VSI
- Πακέτο L2 που προωθείται σε PW σε απομακρυσμένο PE/VSI

5. Πειραματικό Μέρος

5.1 Τοπολογία

Η παρακάτω εικόνα απεικονίζει την τοπολογία του IP/MPLS δικτύου που θα χρησιμοποιήσουμε για τα σενάρια του πειραματικού μέρους της εργασίας. Το MPLS core δίκτυο του παρόχου αποτελείτε από τους δρομολογητές R1 – R6. Θα πραγματοποιήσουμε διαφορές τεχνικές που αφορούν MPLS L2 VPN (VPWS – AtoM)



Εικόνα 20: Δίκτυο IP/MPLS

5.2.1 Scenario 1a: EoMPLS μεταφέροντας ένα Customer Ethernet VLAN

Στο συγκεκριμένο σενάριο θα αποδώσουμε layer 2 επικοινωνία μεταξύ των κόμβων CE1 και CE2 οι οποίοι ανήκουν στον ίδιο πελάτη. Συγκεκριμένα θα σχηματίσουμε ένα 802.1q trunk μεταξύ των κόμβων CE1 – R1 και CE2 – R3. Θα αποδείξουμε ότι κάθε vlan αντικατοπτρίζεται με ένα Pseudowire circuit. Ακολουθεί το configuration των κόμβων που βρίσκονται στα άκρα του πελάτη.

CE1 router

interface Ethernet0/0 description Connected to R1 e0/3 no ip address	interface Ethernet0/0.50 description IP SubIF VLAN 50 encapsulation dot1Q 50 logging event subif-link-status ip address 50.0.0.2 255.255.255.0

CE2 router

interface Ethernet0/0 description Connected to R3 e0/3 no ip address	interface Ethernet0/0.50 description SubIF VLAN 50 encapsulation dot1Q 50 logging event subif-link-status ip address 50.0.0.1 255.255.255.0

R1 PE router

interface Ethernet0/3 description Connected to CE1 e0/0 no ip address	interface Ethernet0/3.50 description SubIF VLAN 50 encapsulation dot1Q 50 logging event subif-link-status xconnect 172.31.1.3 49 encapsulation mpls

R3 PE router

interface Ethernet0/3 description Connected to CE2 e0/0 no ip address	interface Ethernet0/3.50 description SubIF VLAN 50 encapsulation dot1Q 50 logging event subif-link-status xconnect 172.31.1.1 49 encapsulation mpls

Ακολουθεί η επαλήθευση μετά την εκτέλεση της παρακάτω εντολής στο δρομολογητή R1 (PE). Αντίστοιχη εντολή μπορεί να δοθεί και στο δρομολογητή R3 (PE).

R1#sh mpls l2transport vc 49

Local intf	Local circuit	Dest address	VC ID	Status
Et0/3.50	**Eth VLAN 50**	**172.31.1.3**	**49**	**UP**

R3#sh mpls l2transport vc 49

Local intf	Local circuit	Dest address	VC ID	Status
Et0/3.50	**Eth VLAN 50**	**172.31.1.1**	**49**	**UP**

Παρακάτω βλέπουμε περισσότερα στατιστικά στοιχεία του pseudowire που δημιουργείται από τον R1 προς τον R3 και αντίστοιχα από τον R3 στον R1.

R1#sh mpls l2transport vc 49 detail
Local interface: Et0/3.50 up, line protocol up, **Eth VLAN 50 up**
  Interworking type is Ethernet
  Destination address: 172.31.1.3, **VC ID: 49**, VC status: up
    Output interface: Et0/1, **imposed label stack {2003 3010}**
    Preferred path: not configured
    Default path: active
    Next hop: 172.31.12.2
  Create time: 16:16:31, last status change time: 14:44:27
    Last label FSM state change time: 14:44:27
  Signaling protocol: LDP, peer 172.31.1.3:0 up
    Targeted Hello: 172.31.1.1(LDP Id) -> 172.31.1.3, LDP is UP
    Graceful restart: not configured and not enabled
    Non stop routing: not configured and not enabled
    Status TLV support (local/remote)   : enabled/supported
      LDP route watch   : enabled
      Label/status state machine   : established, LruRru
      Last local dataplane   status rcvd: No fault
      Last BFD dataplane   status rcvd: Not sent
      Last BFD peer monitor status rcvd: No fault
      Last local AC circuit status rcvd: No fault
      Last local AC circuit status sent: No fault
      Last local PW i/f circ status rcvd: No fault
      Last local LDP TLV   status sent: No fault
      Last remote LDP TLV   status rcvd: No fault
      Last remote LDP ADJ   status rcvd: No fault
    MPLS VC labels: local 1012, remote 3010
    Group ID: local 0, remote 0

MTU: local 1500, remote 1500
Remote interface description: SubIF VLAN 50
Sequencing: receive disabled, send disabled
Control Word: On (configured: autosense)
Dataplane:
SSM segment/switch IDs: 16392/8196 (used), PWID: 2
VC statistics:
transit packet totals: receive 13, send 13
transit byte totals: receive 1266, send 1604
transit packet drops: receive 0, seq error 0, send 0

R1#show mpls forwarding-table labels 1012

Local Label	Outgoing Label	Prefix or Tunnel Id	Bytes Label Switched	Outgoing interface	Next Hop
1012	**No Label**	**l2ckt(49)**	**180**	**Et0/3.50**	**point2pointshow arp**

R3#sh mpls l2transport vc 49 detail
Local interface: Et0/3.50 up, line protocol up, **Eth VLAN 50 up**
Interworking type is Ethernet
Destination address: 172.31.1.1, **VC ID: 49**, VC status: up
Output interface: Et0/1, imposed label stack {2004 1012}
Preferred path: not configured
Default path: active
Next hop: 172.31.23.1
Create time: 16:21:03, last status change time: 14:51:54
Last label FSM state change time: 14:51:54
Signaling protocol: LDP, peer 172.31.1.1:0 up
Targeted Hello: 172.31.1.3(LDP Id) -> 172.31.1.1, LDP is UP
Graceful restart: not configured and not enabled
Non stop routing: not configured and not enabled
Status TLV support (local/remote) : enabled/supported
LDP route watch : enabled
Label/status state machine : established, LruRru
Last local dataplane status rcvd: No fault
Last BFD dataplane status rcvd: Not sent
Last BFD peer monitor status rcvd: No fault
Last local AC circuit status rcvd: No fault
Last local AC circuit status sent: No fault
Last local PW i/f circ status rcvd: No fault
Last local LDP TLV status sent: No fault
Last remote LDP TLV status rcvd: No fault
Last remote LDP ADJ status rcvd: No fault
MPLS VC labels: local 3010, remote 1012
Group ID: local 0, remote 0
MTU: local 1500, remote 1500
Remote interface description: SubIF VLAN 50
Sequencing: receive disabled, send disabled
Control Word: On (configured: autosense)
Dataplane:
SSM segment/switch IDs: 12295/8195 (used), PWID: 2
VC statistics:
transit packet totals: receive 13, send 13
transit byte totals: receive 1266, send 1604

transit packet drops: receive 0, seq error 0, send 0

R3#sh mpls forwarding-table labels 3010

Local Label	Outgoing Label	Prefix or Tunnel Id	Bytes Label Switched	Outgoing interface	Next Hop
3010	**No Label**	**l2ckt(49)**	**180**	**Et0/3.50**	**point2point**

Από την εκτέλεση όλων των παραπάνω αποδείξαμε ότι τα 2 εικονικά κυκλώματα με ID 49, από την διεπαφή Ethernet0/3.50 του δρομολογητή R1 (PE) για το vlan 50 που είναι συνδεδεμένος με τον customer δρομολογητή CE1 και από την διεπαφή Ethernet0/3.50 του δρομολογητή R3 (PE) για το vlan 50 που είναι συνδεδεμένος με τον customer δρομολογητή CE2 είναι πάνω. Στη συνέχεια θα αποδείξουμε με ICMP πακέτα από τον δρομολογητή CE1 προς τον δρομολογητή CE2 εισέρχεται στο vc 49.

Αρχικά από την παρακάτω εκτέλεση της εντολής παρατηρούμε ότι οι δύο CE δρομολογητές έχουν layer 2 επικοινωνία καθώς ο CE1 έμαθε την ARP διεύθυνση (aabb.cc00.b000) του CE2 και αντίστοιχα ο CE2 έμαθε την ARP διεύθυνση του CE1 (aabb.cc00.a000)

CE1#show arp

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	**50.0.0.1**	**17**	**aabb.cc00.b000**	**ARPA**	**Ethernet0/0.50**
Internet	50.0.0.2	-	aabb.cc00.a000	ARPA	Ethernet0/0.50

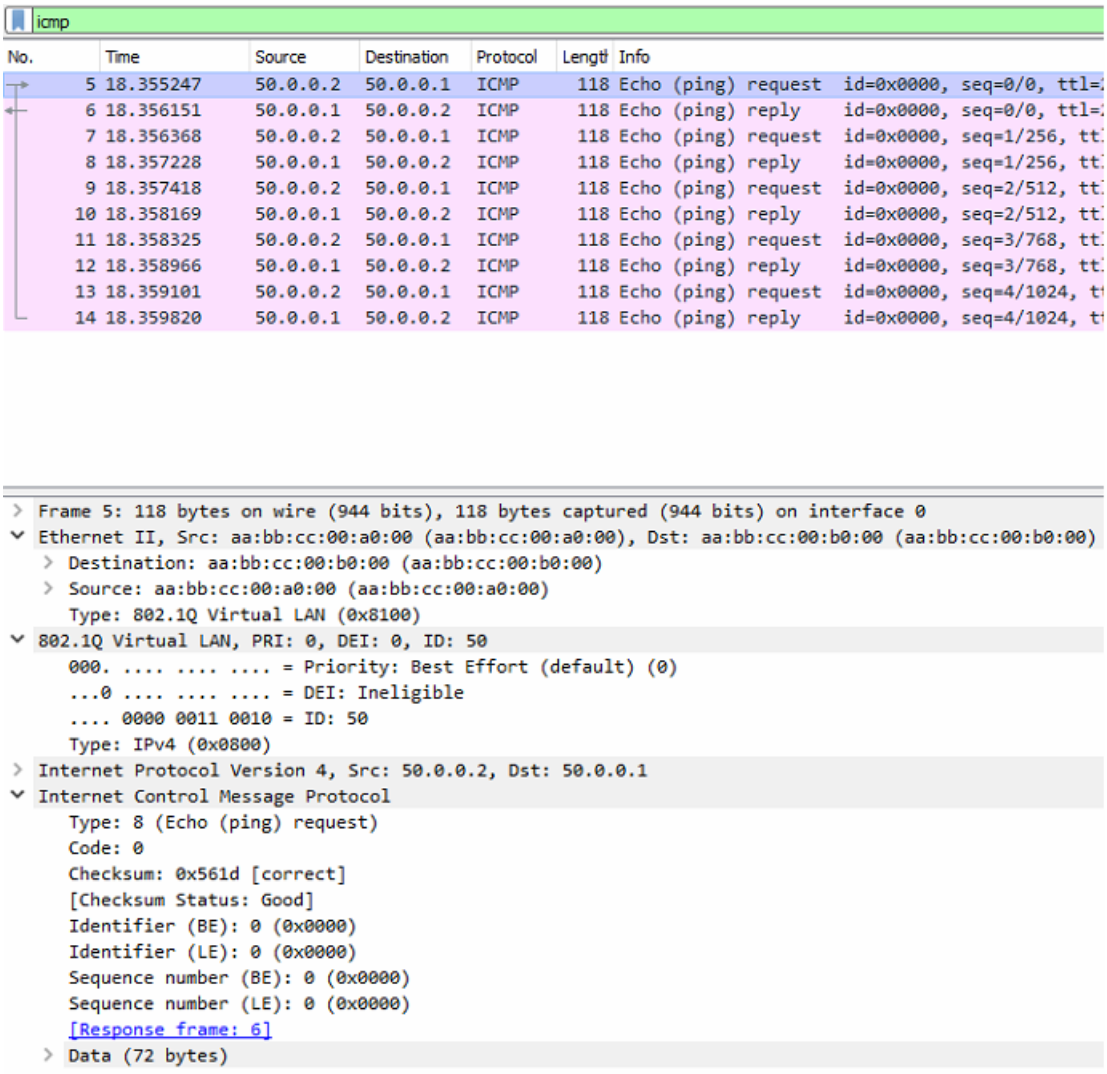
CE2#show arp

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	50.0.0.1	-	aabb.cc00.b000	ARPA	Ethernet0/0.50
Internet	**50.0.0.2**	**16**	**aabb.cc00.a000**	**ARPA**	**Ethernet0/0.50**

Στη συνέχεια θα χρησιμοποιήσουμε το Wireshark προκειμένου να κάνουμε εγγραφή (Capture) ICMP-Echo/Reply πακέτα μεταξύ των CE-1 και CE-2 στην εισερχόμενη διεπαφή (Ingress interface) Ethernet0/3 and MPLS interface (Ethernet0/1) του δρομολογητή PE R1.

– Packet Capture από την διεπαφή Eth0/3 του δρομολογητή R1 κατά τη διάρκεια εκτέλεσης της εντολής ping 50.0.0.1 στον δρομολογητή CE1.

Από την παραπάνω εικόνα παρατηρούμε ότι η source mac address προέρχεται από την διεπαφή 0/3 από τον CE1 (aabb.cc00.a000). Η destination mac address (aabb.cc00.b000) προέρχεται από την διεπαφή 0/3 του CE2. Άρα αποδείξαμε ότι αυτές οι mac addresses είναι στο ίδιο broadcast domain.

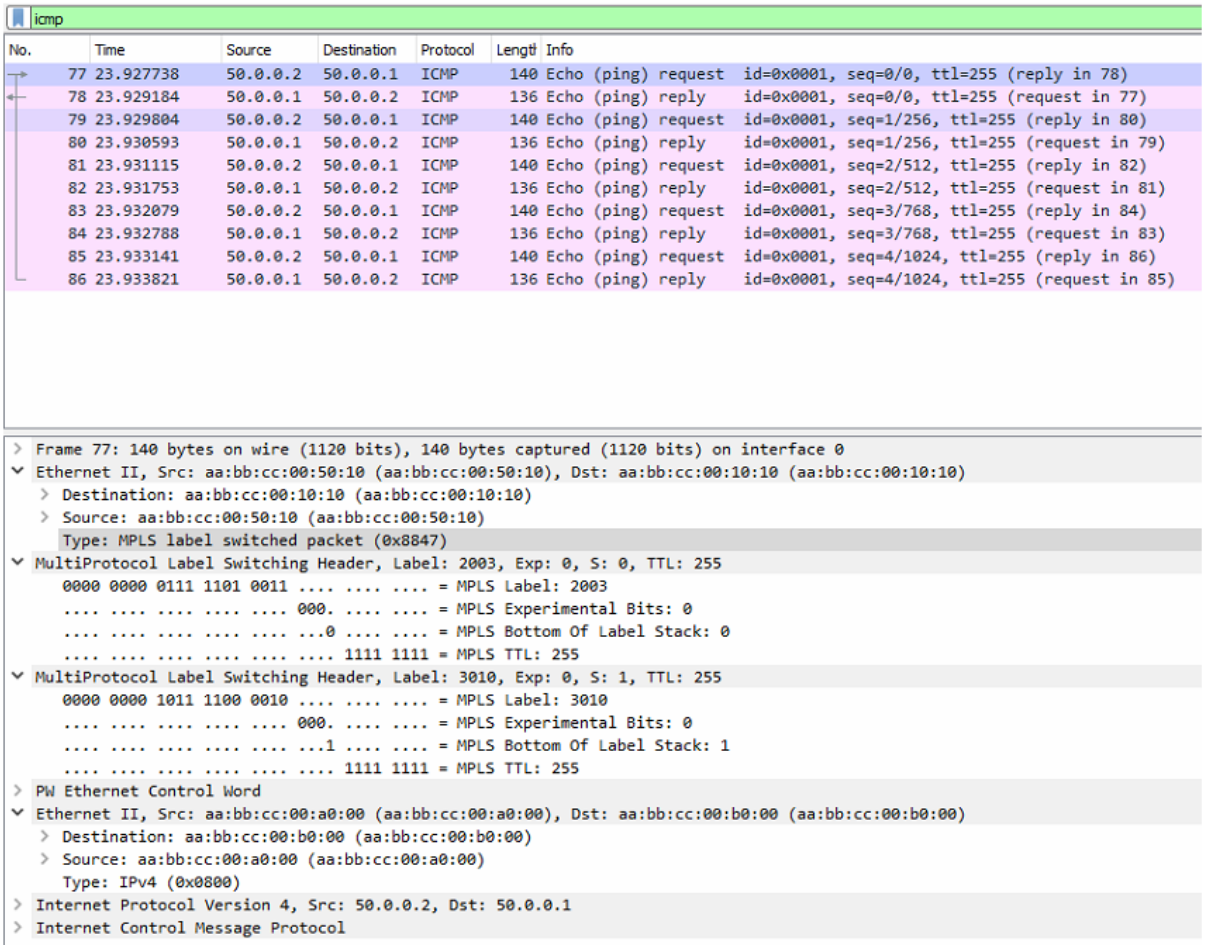


Εικόνα 21: Wireshark

– Packet Capture από την διεπαφή Eth0/3 του δρομολογητή R1 που ανήκει στο MPLS core δίκτυο.

R1#show arp | in 172.31.12
Internet 172.31.12.1 - **aabb.cc00.5010** ARPA Ethernet0/1
Internet 172.31.12.2 80 aabb.cc00.1010 ARPA Ethernet0/1

R2#show arp | in 172.31.12
Internet 172.31.12.1 81 aabb.cc00.5010 ARPA Ethernet0/1
Internet 172.31.12.2 - **aabb.cc00.1010** ARPA Ethernet0/1



Εικόνα 22

Στα παρακάτω captured πακέτα παρατηρούμε ότι η source mac address aabb.cc00.5010 είναι το Interface Eth0/1 του δρομολογητή R1 (PE) και η destination mac address aabb.cc00.1010 είναι το interface Eth0/1 του δρομολογητή R2 (P).

Παρατηρούμε ότι το mpls πρωτόκολλο στο frame λαμβάνει την παρακάτω μορφή Ethernet:mpls:ethernet:data. Επίσης παρατηρούμε ότι στη στοίβα έχουμε δύο MPLS ετικέτες. Η εξωτερική ετικέτα έχει την τιμή 2003 και προσδιορίζει το tunnel label και η εσωτερική ετικέτα έχει την τιμή 3010 και προσδιορίζει το vc label.
Χρειάζεται να αναφέρουμε ότι το πραγματικό ICMP πακέτο τοποθετείται μετά τις δύο επικεφαλίδες MPLS ετικετών . Στον δρομολογητή εξόδου R3 PE, η εξωτερική header ethernet και η διπλή ετικέτα MPLS αφαιρούνται από το πακέτο. Στη συνέχεια, το εσωτερικό πακέτο προωθήθηκε στον δρομολογητή CE-2.

5.2.2 Scenario 1b: EoMPLS μεταφέροντας ένα CE Ethernet Trunk

Στο συγκεκριμένο σενάριο το AC (attachment circuit) είναι ένα ethernet vlan trunk. Οι διεπαφές των CE δρομολογητών συνδέονται με τους PE δρομολογητές με 802.1Q subinterfaces. Με αυτό τον τρόπο τα ethernet frames γίνονται tag όταν ο εκάστοτε PE δρομολογητής R1 και P3 τα λαμβάνει από τους CE1 και CE2 αντίστοιχα. Αυτό έχει σαν αποτέλεσμα ο κάθε δρομολογητής PE να λαμβάνει ολόκληρη την πληροφορία του 802.1q truck κατά μήκος του Pseudowire. Στη συνέχεια δημιουργούμε στους CE δρομολογητές τα κατάλληλα 802.1q sub-interfaces.

CE1

```
interface et0/1
 description Connected to R1 e1/0
 no ip address
 no shutdown
!
interface e0/1.100
 encapsulation dot1q 100
 ip address 10.10.100.1 255.255.255.0
!
interface et0/1.150
 encapsulation dot1q 150
 ip address 10.10.150.1 255.255.255.0
```

CE2

```
interface et0/1
 description Connected to R3 e1/0
 no ip address
 no shutdown
!
interface e0/1.100
 encapsulation dot1q 100
 ip address 10.10.100.2 255.255.255.0
!
interface et0/1.150
 encapsulation dot1q 150
 ip address 10.10.150.2 255.255.255.0
```

R1

```
pseudowire-class MPLS_CE1-CE2
 encapsulation mpls
!
interface et1/0
 no shutdown
 description Connected to CE1 et0/1
 no ip address
 xconnect 172.31.1.3 99 pw-class MPLS_CE1-CE2
```

R3

```
pseudowire-class MPLS_CE2-CE1
 encapsulation mpls
!
interface et1/0
 no shutdown
 description Connected to CE2 et0/1
 no ip address
 xconnect 172.31.1.1 99 pw-class MPLS_CE2-CE1
```

Προηγουμένως έχουμε εκτελέσει την παρακάτω εντολή "***debug mpls l2transport signaling message"*** προκειμένου να παρατηρήσουμε τα vc labels που ανταλλάσσονται μεταξύ των R1-R3 PE δρομολογητών αφού έχει δημιουργηθεί το targeted-ldp session μεταξύ των loopback Ips των δρομολογητών αυτών. Το output δείχνει επίσης ότι κάθε δρομολογητής στέλνει ένα μήνυμα αντιστοίχισης ετικετών που περιέχει παραμέτρους FEC TLV, Label TLV και προαιρετικές παραμέτρους διεπαφής. Το VC Type 5 υποδεικνύει τη λειτουργία θύρας Ethernet mode και όχι Vlan mode όπως το σενάριο 1a κατά το οποίο είχαμε vc type 4.

```
*Jan 25 17:20:56.260: AToM LDP[172.31.1.3]: Sending label mapping msg
*Jan 25 17:20:56.260: AToM LDP[172.31.1.3]: Sending label mapping msg vc type 5, cbit 1,
```

```
*Jan 25 17:20:56.260: AToM LDP[172.31.1.3]:   , vc id 99,
*Jan 25 17:20:56.260: AToM LDP[172.31.1.3]:   group id 0, vc label 1013,
*Jan 25 17:20:56.260: AToM LDP[172.31.1.3]:   status 0x7/LDP 0x1/ADJ 0x0,
*Jan 25 17:20:56.260: AToM LDP[172.31.1.3]:   mtu 1500, vc handle 0xEB000003
*Jan 25 17:20:56.260: AToM LDP[172.31.1.3]:   VCCV CC 0x3, CV 0x2
R1(config-if)#
*Jan 25 17:20:56.274: %XCONNECT-5-PW_STATUS: MPLS peer 172.31.1.3 vcid 99, VC state DOWN
*Jan 25 17:20:56.292: %XCONNECT-5-PW_STATUS: MPLS peer 172.31.1.3 vcid 99, VC state UP
```

R1#sh mpls l2transport vc 99 detail

Local interface: Et1/0 up, line protocol up, Ethernet up
  Destination address: 172.31.1.3, **VC ID: 99**, VC status: up
    Output interface: Et0/1, **imposed label stack {2003 3011}**
    Preferred path: not configured
    Default path: active
    Next hop: 172.31.12.2
  Create time: 01:15:44, last status change time: 00:01:56
    Last label FSM state change time: 00:01:56
  Signaling protocol: LDP, peer 172.31.1.3:0 up
    Targeted Hello: 172.31.1.1(LDP Id) -> 172.31.1.3, LDP is UP
    Graceful restart: not configured and not enabled
    Non stop routing: not configured and not enabled
    Status TLV support (local/remote)   : enabled/supported
      LDP route watch   : enabled
      Label/status state machine   : established, LruRru
      Last local dataplane   status rcvd: No fault
      Last BFD dataplane   status rcvd: Not sent
      Last BFD peer monitor status rcvd: No fault
      Last local AC circuit status rcvd: No fault
      Last local AC circuit status sent: No fault
      Last local PW i/f circ status rcvd: No fault
      Last local LDP TLV   status sent: No fault
      Last remote LDP TLV   status rcvd: No fault
      Last remote LDP ADJ   status rcvd: No fault
    MPLS VC labels: local 1013, remote 3011
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description: Connected to CE2 et0/1
  Sequencing: receive disabled, send disabled
  Control Word: On (configured: autosense)
  Dataplane:
    SSM segment/switch IDs: 16408/12294 (used), PWID: 3
  VC statistics:
    transit packet totals: receive 539, send 539
    transit byte totals: receive 59376, send 73831
    transit packet drops: receive 1, seq error 0, send 0

R3#sh mpls l2transport vc 99 detail

```
Local interface: Et1/0 up, line protocol up, Ethernet up
  Destination address: 172.31.1.1, VC ID: 99, VC status: up
    Output interface: Et0/1, imposed label stack {2004 1013}
    Preferred path: not configured
    Default path: active
    Next hop: 172.31.23.1
  Create time: 01:17:14, last status change time: 00:04:55
    Last label FSM state change time: 00:04:55
  Signaling protocol: LDP, peer 172.31.1.1:0 up
    Targeted Hello: 172.31.1.3(LDP Id) -> 172.31.1.1, LDP is UP
    Graceful restart: not configured and not enabled
    Non stop routing: not configured and not enabled
    Status TLV support (local/remote)   : enabled/supported
      LDP route watch                   : enabled
      Label/status state machine        : established, LruRru
      Last local dataplane   status rcvd: No fault
      Last BFD dataplane     status rcvd: Not sent
      Last BFD peer monitor  status rcvd: No fault
      Last local AC  circuit status rcvd: No fault
      Last local AC  circuit status sent: No fault
      Last local PW i/f circ status rcvd: No fault
      Last local LDP TLV     status sent: No fault
      Last remote LDP TLV    status rcvd: No fault
      Last remote LDP ADJ    status rcvd: No fault
    MPLS VC labels: local 3011, remote 1013
    Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description: Connected to CE1 et0/1
  Sequencing: receive disabled, send disabled
  Control Word: On (configured: autosense)
  Dataplane:
    SSM segment/switch IDs: 20500/12294 (used), PWID: 3
  VC statistics:
    transit packet totals: receive 560, send 566
    transit byte totals:   receive 62061, send 77041
    transit packet drops:  receive 0, seq error 0, send 0
```

5.3 Scenario 2: EoMPLS μέσω EVC (Ethernet Virtual Circuits)

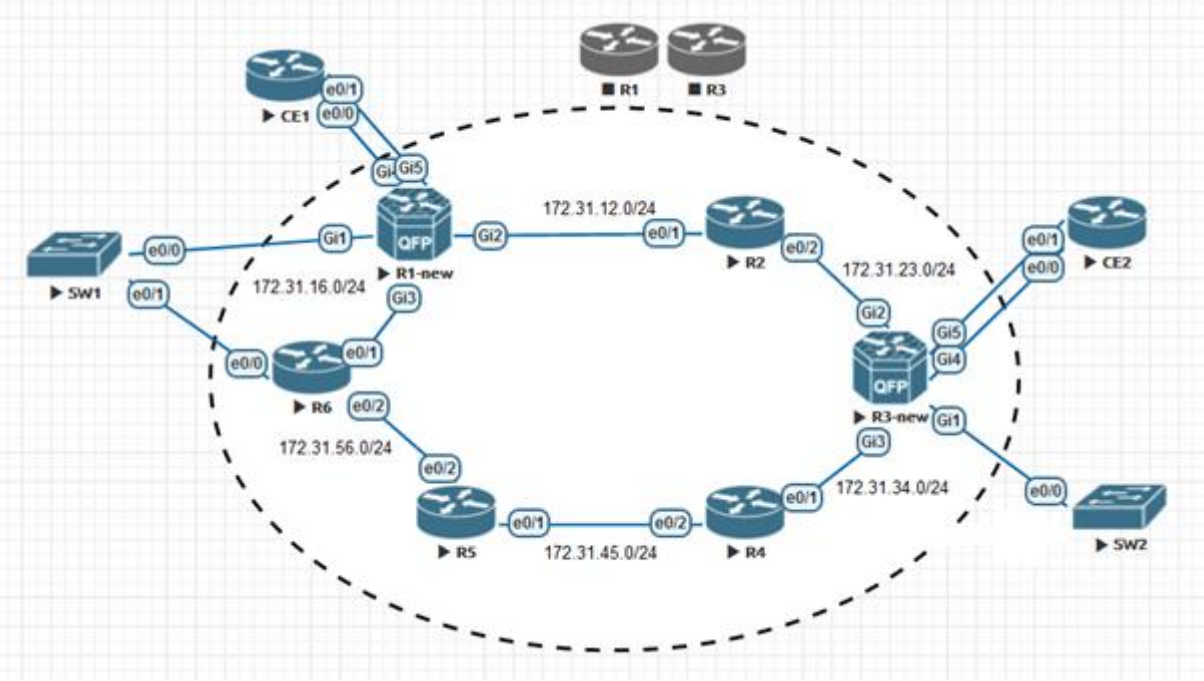
Στο συγκεκριμένο σενάριο θα γίνει μεταφορά των δύο υπηρεσιών (pseudowires) που δώσαμε για τη διασύνδεση των δρομολογητών CE1-CE2 (vc id: 49, vc id: 99) προς το backbone δίκτυο (δρομολογητές PE R1, R3) με ποιο ευέλικτο τρόπο μέσω της παρακάτω αποκλειστικής διασύνδεσης του πελάτη προς το MPLS

Core η οποία είναι η εξής: CE1-CE2→SW1-SW2→PE. Χρειάζεται να αναφερθεί ότι θα συνεχίσει να υπάρξει εξυπηρέτηση των υπαρχόντων υπηρεσιών χωρίς να γίνει κάποια αλλαγή στα άκρα του πελάτη (CE1, CE2) παρά μόνο στους PE δρομολογητές.

Η ανάγκη αλλαγής θα γίνει διότι δεν είναι εφικτό από οικονομικής απόψεως να δεσμεύουμε μία φυσική διεπαφή στους PE δρομολογητές του IP/MPLS core δικτύου προκειμένου να εξυπηρετήσουμε κάθε καινούριο πελάτη που χρειάζεται να επικοινωνήσει με το backbone δίκτυο.

Θα χρειαστεί να καταργήσουμε τους δρομολογητές PE R1 και R3, να τους κάνουμε stop και στη συνέχεια θα χρειαστεί να εγκαταστήσουμε δύο καινούριους PE δρομολογητές που θα χρησιμοποιηθούν για την αντικατάσταση των προηγούμενων δρομολογητών.

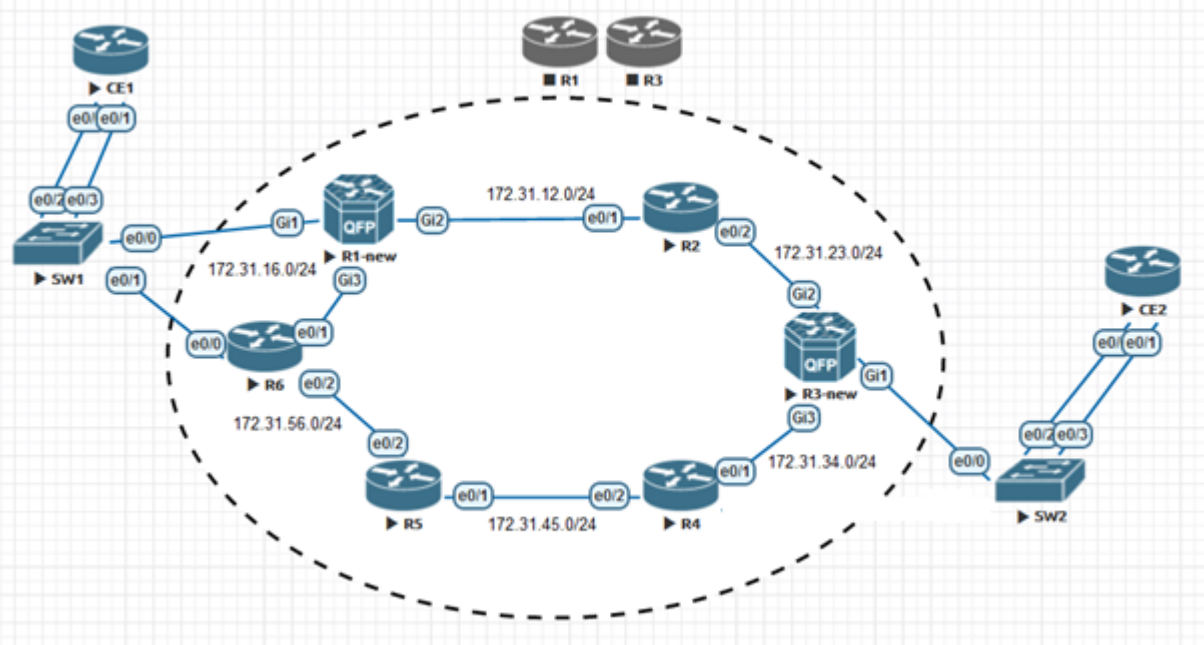
Οι νέοι PE δρομολογητές ονομάζονται R1-new και R3-new. Επίσης θα χρειαστεί να αλλάξουμε το IOS από το των παραπάνω δύο PE δρομολογητών (R1 και R3) από το IOS L3-ADVENTERPRISE9-15.5.2T.bin στο νέο IOS-XE που ονομάζεται csr1000v-universalk9.17.03.02 που υποστηρίζει τα χαρακτηριστικά EVC που θέλουμε να δώσουμε στην εργασία μας.Το νέο σχηματικό διάγραμμα φαίνεται στην παρακάτω εικόνα. Επίσης το configuration του δρομολογητή R1 έχει μεταφερθεί στο δρομολογητή R1-new και αντίστοιχα το configuration του δρομολογητή R3 έχει μεταφερθεί στον δρομολογητή r3-new



Εικόνα 23: Δικτυο IP/MPLS 2

Στη συνέχεια αποσυνδέουμε τις διεπαφές μεταξύ των δρομολογητών CE1 (e0/0, e0/01) και R1-new (G4, G5) και τις μεταφέρουμε στο SW1 (e0/2, e0/3) αντίστοιχα.

Ακολουθεί η σύνδεση του δρομολογητή CE1-SW1 είναι ως εξής: (CE1 e0/0 ←→ SW1 e0/2, CE1 e0/1 ←→ SW1 e0/3) και αντίστοιχα του δρομολογητή CE2-SW2 είναι ως εξής: (CE2 e/0 ←→ SW2 E0/2, CE2 e0/1←→ SW2 e0/3. Στην παρακάτω εικόνα βλέπουμε το τροποποιημένο σενάριο.



Εικόνα 24: Δίκτυο IP/MPLS 3

Στη συνέχεια χρειάζεται να δημιουργήσουμε το κατάλληλο configuration στο SW1 και στον δρομολογητή R1-new. Αντίστοιχη διαδικασία θα γίνει και στο SW2 και στον δρομολογητή R3-new.

R1-new#show run interface gi 1 ! interface GigabitEthernet1 no ip address negotiation auto no mop enabled no mop sysid service instance 1 ethernet description ** OLD VC ID 99 ** encapsulation dot1q 100 rewrite ingress tag pop 1 symmetric xconnect 172.31.1.3 1 encapsulation mpls ! service instance 2 ethernet description ** OLD VC ID 99 **	**R3-new**#show run interface gi 1 ! interface GigabitEthernet1 no ip address negotiation auto no mop enabled no mop sysid service instance 1 ethernet description ** OLD VC ID 99 ** encapsulation dot1q 100 rewrite ingress tag pop 1 symmetric xconnect 172.31.1.1 1 encapsulation mpls ! service instance 2 ethernet description ** OLD VC ID 99 **

encapsulation dot1q 150 rewrite ingress tag pop 1 symmetric xconnect 172.31.1.3 2 encapsulation mpls ! service instance 3 ethernet description ** OLD VC ID 49 ** encapsulation dot1q 50 rewrite ingress tag pop 1 symmetric xconnect 172.31.1.3 3 encapsulation mpls ! end	encapsulation dot1q 150 rewrite ingress tag pop 1 symmetric xconnect 172.31.1.1 2 encapsulation mpls ! service instance 3 ethernet description ** OLD VC ID 49 ** encapsulation dot1q 50 rewrite ingress tag pop 1 symmetric xconnect 172.31.1.1 3 encapsulation mpls ! end
SW1#sh run int et0/2 ! interface Ethernet0/2 switchport trunk encapsulation dot1q switchport trunk allowed vlan 50 switchport mode trunk duplex auto ! **SW1**#sh run int et0/3 ! interface Ethernet0/3 switchport trunk encapsulation dot1q switchport trunk allowed vlan 100,150 switchport mode trunk duplex auto ! **SW1**#sh run int et0/0 ! interface Ethernet0/0 switchport trunk encapsulation dot1q switchport trunk allowed vlan 10,20,50,100,150 switchport mode trunk duplex auto ! Vlan 50 Vlan 150 Vlan 100	**SW2**#sh run int et0/2 ! interface Ethernet0/2 switchport trunk encapsulation dot1q switchport trunk allowed vlan 50 switchport mode trunk duplex auto ! **SW2**#sh run int et0/3 ! interface Ethernet0/3 switchport trunk encapsulation dot1q switchport trunk allowed vlan 100,150 switchport mode trunk duplex auto ! **SW2**#sh run int et0/0 ! interface Ethernet0/0 switchport trunk encapsulation dot1q switchport trunk allowed vlan 10,20,50,100,150 switchport mode trunk duplex auto ! Vlan 50 Vlan 150 Vlan 100

Το παραπάνω σενάριο περιορίζει την κάτωθι πρόκληση που δημιουργείται από το γεγονός του ότι τα παραδοσιακά switches θέλουμε να εκτελούν τις 2 παρακάτω βασικές διαδικασίες:

Να έχουν το ίδιο vlan ρυθμισμένο μαζικά σε όλο το layer 2 broadcast domain.

Να εκτελούν mac learning διαδικασία (εκμάθηση mac addressing σε υφιστάμενο vlan)

Τα switches έχουν πεπερασμένο χώρο (cam table) για εκμάθηση MAC διευθύνσεων περιορίζοντας τον αριθμό των κεντρικών υπολογιστών που μπορεί να υποστηριχθεί.

Δεδομένου ότι το 802.1q vlan tag (vlan ετικέτα) έχει μήκος 12 bits ο μέγιστος αριθμός VLAN που μπορεί να διαμορφωθεί είναι 2^{12} vlans = 4096 vlans. Στα σύγχρονα περιβάλλοντα παρόχων και cloud υπηρεσιών υπάρχει ανάγκη να παρακάμψουμε αυτούς τους περιορισμούς. Επίσης χρειάζεται να λάβουμε υπόψιν ότι το vlan translation δεν είναι τόσο εύκολος μηχανισμός που μπορεί να υποστηριχθεί.

Στη συνέχεια γίνεται μία ανάλυση του μηχανισμού Ethernet EVC. Η ετικέτα του vlan (vlan tag) χρησιμοποιείται για ταξινόμηση και το service instance (SI) προσδιορίζει την ενέργεια προώθησης. Με την χρήση του SI μπορούμε να εκχωρήσουμε ένα VLAN σε διαφορετικούς πελάτες σε κάθε πόρτα ενός υφιστάμενου switch και να προωθήσουμε την κίνηση κάθε διαφορετικού πελάτη μέσω διαφορετικών MPLS pseudowires και να μην χρειαστεί ποτέ να διαμορφώσουμε αυτό το vlan σε παγκόσμια κλίμακα. Αποτέλεσμα των παραπάνω να υπάρχει η επιλογή το Customer vlan να μπορέσει να διατηρηθεί (vlan preservation) ή να μεταφραστεί (vlan translation).

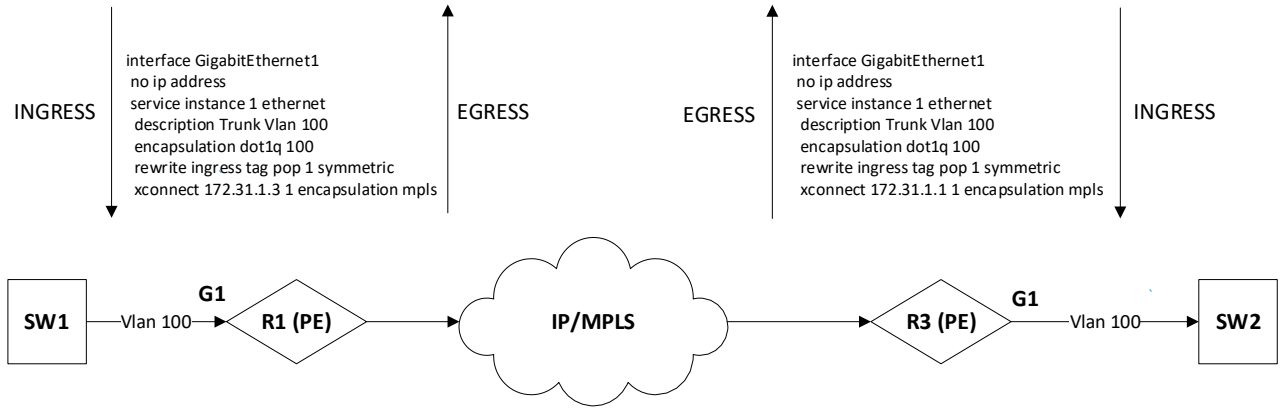
Τα EVCs μας επιτρέπουν να ταξινομούμε τα εισερχόμενα πλαίσια (inbound frames) με αρκετά ευέλικτο τρόπο με βάση 1 ή περισσότερες ετικέτες. Με την χρήση δηλαδή των Service Instances παρέχετε ταξινόμηση layer 2 ροών σε Ethernet διεπαφές. Ο κανόνας classification ενός SI είναι ο κάτωθι.

α) Από το πιο συγκεκριμένο στο πιο γενικό encapsulation

β) Δεν υπάρχει ακριβής αντιστοίχιση με βάση το εξωτερικό VLAN.

γ) Encapsulation untagged frames σε πακέτο χωρίς ετικέτα.

δ) Encapsulation default που συλλαμβάνει όλη την εναπομείνασα επισκεψιμότητα χωρίς συγκεκριμένη αντιστοίχιση.



Εικόνα 25: Δικτυο IP/MPLS EVC

Στο συγκεκριμένο παράδειγμα δημιουργούμε δύο service instances στις φυσικές διαπαφές (Gig1) των δρομολογητών PE (R1-new και R3-new) που συνδέονται με τα access switches SW1, SW2 αντίστοιχα) προκειμένου να δημιουργηθεί η Layer 2 διασύνδεση μεταξύ των πελάτων CE1-CE2. Αρχικά στην διαπεφή G1 δημιουργούμε ένα service instance με μοναδικό κάθε φορά αριθμό (identifier) το “1”, “2” και “3” και type of service “ethernet” (service instance 1 ethernet). Στη συνέχεια κατά το Ingress την κίνησης προς την διεπαφή Gi1 γίνεται match οποιοδήποτε frame (layer 2 packet) έρθει με vlan 100 (encapsulation dot1q 100). Με την εντολή “rewrite ingress tag pop 1 symmetric” αυτό σημαίνει ότι όταν λαμβάνεται το πακέτο στη διεπαφή 1, η εξωτερική ετικέτα vlan 100 (outmost vlan) αφαιρείται (pop). Στη συνέχει στέλνετε όλη αυτή η κίνηση στο l2vpn μέσω του command xconnect.Επίσης, λόγω της λέξης “symmetric” αυτό σημαίνει προσθήκη

(push) της ετικέτας vlan του 100 για οποιοδήποτε πλαίσιο που φεύγει από τη θύρα (egress traffic)

Στη συνέχεια προχωράμε με το verification για το οποίο βλέπουμε ότι υπάρχει layer 3 επικοινωνία για τα 3 vlans που εξυπηρετούν διαφορετικές υπηρεσίες μεταξύ των πελατών CE1 – CE2. Αρχικά βλέπουμε ότι έχουν ανέβει τα xconnect και στους 2 PE δρομολογητές

```
R1-new#show mpls l2transport vc
Local intf     Local circuit            Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
Gi1            Eth VLAN 100             172.31.1.3      1          UP
Gi1            Eth VLAN 150             172.31.1.3      2          UP
Gi1            Eth VLAN 50              172.31.1.3      3          UP
```

```
R3-new# show mpls l2transport vc
Local intf     Local circuit            Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
Gi1            Eth VLAN 100             172.31.1.1      1          UP
Gi1            Eth VLAN 150             172.31.1.1      2          UP
Gi1            Eth VLAN 50              172.31.1.1      3          UP
```

Στη συνέχεια ελέγχουμε στα 2 CE δρομογητές τις εγγραφές ARP για να πιστοποιήσουμε ότι υπάρχει layer 2 end-to-end σύνδεση. Παρατηρούμε ότι ο CE1 έχει ARP entries για τις IPs του CE2.

```
CE1#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  10.10.100.1             -   aabb.cc00.a010  ARPA   Ethernet0/1.100
Internet  10.10.100.2            86   aabb.cc00.b010  ARPA   Ethernet0/1.100
Internet  10.10.150.1             -   aabb.cc00.a010  ARPA   Ethernet0/1.150
Internet  10.10.150.2            22   aabb.cc00.b010  ARPA   Ethernet0/1.150
Internet  50.0.0.1               73   aabb.cc00.b000  ARPA   Ethernet0/0.50
Internet  50.0.0.2                -   aabb.cc00.a000  ARPA   Ethernet0/0.50
```

5.4 Scenario 3: MPLS L2VPN Redundancy

Τα MPLS-L2VPN όπως έχουμε αναφέρει επιτρέπουν στο πάροχο υπηρεσιών να παρέχουν διαφορετικά μοντέλα VPN χρησιμοποιώντας το ίδιο δίκτυο. Στις περισσότερες εφαρμογές δικτύου είναι επθυμητός να υπάρχει backup L2VPN

κύκλωμα για να υπάρχει συνέχεια στην παροχής υπηρεσιών. Η δυνατότητα L2VPN Pseudowire Redundancy επιτρέπει στους δρομολογητές άκρης να ανιχνεύουν μια αποτυχία στο δίκτυο και να επαναδρομολογούν την κίνηση του επιπέδου 2 (L2) σε άλλο τελικό σημείο. Αυτή η δυνατότητα παρέχει τη δυνατότητα ανάκτησης από αποτυχία είτε στην απομακρυσμένη σύνδεση PE είτε στη σύνδεση PE-CE.
Στα σύγχρονα δίκτυα πρέπει να χρησιμοποιούνται δύο επίπεδα redundancy για την επίπτευξη της βέλτιστης backup επικοινωνίας. Το 1ο επίπεδο αναφέρεται σε πλεονασμό δρομολόγησης (routing redundancy) κατά την οποία όταν η σύνδεση μεταξύ δρομολογητών PE από άκρο σε άκρο αποτυγχάνει, το δίκτυο πρέπει να μπορεί να βρει μια εναλλακτική διαδρομή για την κατευθυνόμενη LDP συνεδρία και τα δεδομένα χρήστη μπορούν να εξυπηρετηθούν.
Χρειάζεται να αναφέρουμε ότι υπάρχουν ορισμένα τμήματα του δικτύου όπου αυτός ο μηχανισμός επαναδρομολόγησης (re-routing) δεν προστατεύει από διακοπές στην υπηρεσία. Αυτά τα τμήματα αναφέρονται στο 2ο επίπεδο και περιλαμβάνουν οποιαδήποτε αστοχία που δεν μπορεί να ανακτηθεί με πρωτόκολλα δρομολόγησης, για παράδειγμα αστοχίες υλικού ή λογισμικού των τελικών σημείων PW (Είσοδος/Εξόδου PE) Βλάβες , HW ή SW σε CE, PE-CE AC (κύκλωμα προσάρτησης).
Η δυνατότητα πλεονασμού L2VPN σάς δίνει τη δυνατότητα να ρυθμίσουμε εφεδρικά κυκλώματα (pseudowires) . Μπορούμε συνεπώς να διαμορφώσουμε το δίκτυο με πλεονάζοντα PWs και πλεονάζοντα στοιχεία δικτύου για να επιτύχετε τη βέλτιστη λύση

Στην περίπτωση μας θα προστατεύσουμε μόνο την επικοινωνία μεταξύ της διασύνδεσης του κεντρικού access SW1 και R1-new η οποία είναι ο αποκλειστικός δρόμος εξυπηρέτησης μεταξύ R1-new και CE1. Θα χρησιμοποιήσουμε μία ακόμα διασύνδεση L2 μεταξύ του SW1 (e0/1) και του R6 (e0/0). Στη συνέχεια θα γίνει το απαραίτητο configuration στις 2 αυτές διασύνδεσης όπως φαίνεται παρακάτω.

SW1#sh run int et0/1 interface Ethernet0/1 switchport trunk encapsulation dot1q switchport trunk allowed vlan 10,20,50,100,150 switchport mode trunk duplex auto end	**R6#**sh run int et 0/0 interface Ethernet0/0.100 encapsulation dot1Q 100 no cdp enable end ! **R6#**sh run int et 0/0 interface Ethernet0/0 description ** Connection to SW1 e0/1 ** no ip address no keepalive

Η μεθοδολογία επίλυσης του συγκεκριμένου σεναρίου περιλαμβάνει τα παρακάτω βήματα σε περίπτωση αποτυχίας της επικοινωνίας μεταξύ SW1 και R1-new.
α) Ανίχνευση προστασίας υφιστάμενου/υφιστάμενων pseudowire κυκλωμάτων (active) στους κατάλληλους δρομολογητές. Θέλουμε να προστατευτεί το active pseudowire του δρομολογητή R1-new που εξυπηρετείται από το vc id “1” το οποίο μεταφέρει layer 2 κίνηση για το vlan 100 προς τον R3-new όπως φαίνεται παρακάτω.

```
R1-new#show mpls l2transport vc 1

Local intf     Local circuit              Dest address    VC ID      Status
```

```
-------------  ------------------------- --------------- ---------- ------
----
Gi1            Eth VLAN 100               172.31.1.3      1          UP
```

β) δημιούργία configuration στους παραπάνω δρομολογητές που χρειάζονται νέα εικονικά κυκλώματα προστασίας με σκοπό να δημιουργηθεί redundancy. Ο δρομολογητής R6 θα συνεχίσει να εξυπηρετήσει την επικοινωνία με τον CE1. Στον δρομολογητή R6 δημιουργούμε νέο Pseudowire προς τον δρομολογητή R3-new όπως φαίνεται παρακάτω.

R6
```
interface Ethernet0/0.100
 encapsulation dot1Q 100
 description ** STANDBY to R3 **
 xconnect 172.31.1.3 1000 encapsulation mpls
```

Παρακάτω φαίνεται το verification με το pseudowire Που αναλαμβάνει να πάρει κίνηση όταν πέσει το active pseudowire του R1-new

R6# show mpls l2transport vc

```
Local intf     Local circuit            Dest address    VC ID      Status
-------------  ------------------------- --------------- ---------- ----------
Et0/0.100      Eth VLAN 100             172.31.1.3      1000       STANDBY
```

R6#show xconnect all

```
Legend:    XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
  UP=Up       DN=Down          AD=Admin Down     IA=Inactive
  SB=Standby  HS=Hot Standby    RV=Recovering     NH=No Hardware

XC ST  Segment 1                  S1 Segment 2                S2
------+---------------------------------+--+---------------------------------+--
SB pri   ac Et0/0.100:100(Eth VLAN)     UP mpls 172.31.1.3:1000          SB
```

Στο υπάρχον active pseudowire κύκλωμα μεταξύ R3-new – R1-new θα προσθέσουμε το redundancy pseudowire με vc “1000” μεταξύ R3-new – R6 να είναι redundant σε περίπτωση αποτυχίας του 1ου pseudowire με vc ‘1”

R3-new
```
interface GigabitEthernet1
 no ip address
 negotiation auto
 service instance 1 ethernet
  encapsulation dot1q 100
  rewrite ingress tag pop 1 symmetric
  xconnect 172.31.1.1 1 encapsulation mpls
   backup peer 172.31.1.6 1000
```

Αυτή τη στιγμή είναι up το primary pseudowire “1”.

```
R3-new#sh mpls l2transport vc

Local intf     Local circuit            Dest address    VC ID      Status
-------------  ------------------------ --------------- ---------- --------
--
Gi1            Eth VLAN 100             172.31.1.1      1          UP
Gi1            Eth VLAN 100             172.31.1.6      1000       STANDBY

R3-new#sh xconnect interface gigabitEthernet 1
Legend:    XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
  UP=Up       DN=Down            AD=Admin Down      IA=Inactive
  SB=Standby  HS=Hot Standby     RV=Recovering      NH=No Hardware

XC  ST    Segment  1                                          S1  Segment  2
S2
------+---------------------------------+--+-------------------------------
--+--
UP  pri     ac  Gi1:1(Eth  VLAN)                    UP  mpls  172.31.1.1:1
UP
IA  sec     ac  Gi1:1(Eth  VLAN)                   UP  mpls  172.31.1.6:1000
SB
```

γ) έλεγχος active και standby κυκλωμάτων μετά τις αλλαγές (failover)
Ρίχνουμε το interface διασύνδεσης μεταξύ SW1-R1-new και παρατηρούμε ότι ανεβαίνει το backup pseudowire 1000 και γίνεται down το pseudowire 1 στον δρομολογητή R3-new με τον δρομολογητή R6, παράλληλα από standby γίνεται up το pseudowire στον R6. Με αυτό τον τρόπο συνεχίζεται να υπάρχει layer 2 επικοινωνία CE1-SW1-R6-R3-new-SW2-CE2.

```
R6#show mpls l2 vc 1000
Local intf     Local circuit            Dest address    VC ID      Status
-------------  ------------------------ --------------- ---------- ------
----
Et0/0.100      Eth VLAN 100             172.31.1.3      1000       UP


R6#show xconnect all
Legend:    XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
  UP=Up       DN=Down            AD=Admin Down      IA=Inactive
  SB=Standby  HS=Hot Standby     RV=Recovering      NH=No Hardware

XC ST  Segment 1                    S1 Segment 2                      S2
------+---------------------------------+--+-------------------------------
+--
UP pri   ac Et0/0.100:100(Eth VLAN)  UP mpls 172.31.1.3:1000           UP

R3-new#show mpls l2 vc
Local intf     Local circuit            Dest address    VC ID      Status
-------------  ------------------------ --------------- ---------- ------
----
Gi1            Eth VLAN 100             172.31.1.1      1          DOWN
```

```
Gi1            Eth VLAN 100               172.31.1.6      1000       UP

R3-new#sh xconnect interface gi1
Legend:    XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
  UP=Up       DN=Down            AD=Admin Down      IA=Inactive
  SB=Standby  HS=Hot Standby     RV=Recovering      NH=No Hardware

XC ST  Segment 1                     S1 Segment 2                          S2
------+-----------------------------------+--+-------------------------------
--+--
IA pri   ac Gi1:1(Eth VLAN)          UP mpls 172.31.1.1:1                  DN
UP sec   ac Gi1:1(Eth VLAN)          UP mpls 172.31.1.6:1000               UP
```

Τέλος αν θέλουμε στον R3-new Μπορεί να γίνει και manual failover οποιαδήποτε στιγμή με το παρακάτω command.

xconnect backup force-switchover peer 172.31.1.6 1000

R3-new#
*Jan 27 17:04:55.358: %XCONNECT-5-REDUNDANCY: XC VPWS: Activating secondary member 172.31.1.6:1000
*Jan 27 17:04:55.368: %XCONNECT-5-PW_STATUS: MPLS peer 172.31.1.1 vcid 1, VC state STANDBY
*Jan 27 17:04:55.368: %XCONNECT-5-PW_STATUS: MPLS peer 172.31.1.6 vcid 1000, VC state UP

Βιβλιογραφικές Πηγές.

1. MPLS Fundamentals by Luc De Ghein Published Aug 2, 2016 by Cisco Press

2. MPLS Configuration on Cisco IOS Software By Umesh Lakshman, Lancy Lobo by Cisco Press

3. Layer 2 VPN Architectures (paperback) By Wei Luo, Carlos Pignataro, Anthony Chan, Dmitry Bokotey by Cisco Press

4. Metro Ethernet by Sam Halabi by Cisco

5. Computer Networking: A Top-Down Approach, 6th Edition by James F. Kurose , Keith W. Ross

6. https://www.ciscopress.com/articles/article.asp?p=386788&seqNum=2#:~:text=A%20control%20word%20is%20an,Layer%202%20payload%2Dspecific%20information.

7. https://flylib.com/books/en/2.650.1/deploying_atom_pseudowires.html

8. https://www.cisco.com/c/dam/global/fr_ca/training-events/pdfs/Intro_to_mpls.pdf

9. https://sites.google.com/site/amitsciscozone/attachments

10. https://www.iptp.net/en_US/network/connectivity-services/eompls-pseudowire-service/

11. https://networklessons.com/switching/802-1q-encapsulation-explained

12. https://www.uio.no/studier/emner/matnat/ifi/IN3230/h19/kursmateriell/mpls-lecture.pdf

13. https://www.sanog.org/resources/sanog17/sanog17-mpls-intro-santanu.pdf