Δόμηση ενός Εικονικού Ιδιωτικού Δικτύου πάνω σε MPLS

Τεχνολογία MPLS (Multi Protocol Label Switching)

- Αυξάνει την ευελιξία του IP
- Η προώθηση πακέτων στηρίζεται σε ειδικές ετικέτες (labels), που κατασκευάζονται και τοποθετούνται κατά την εισαγωγή των πακέτων στο Δίκτυο Μεταγωγής / Κορμού. Οι ετικέτες υποδεικνύουν τόσο τη δρομολόγηση των πακέτων όσο και τα χαρακτηριστικά ποιότητας των υπηρεσιών που παρέχονται από το δίκτυο.

Ορολογία και δομικά στοιχεία του MPLS

- **Ετικέτα (Label):** Είναι η επικεφαλίδα/ετικέτα που χρησιμοποιείται από τους LSR για την προώθηση των πακέτων

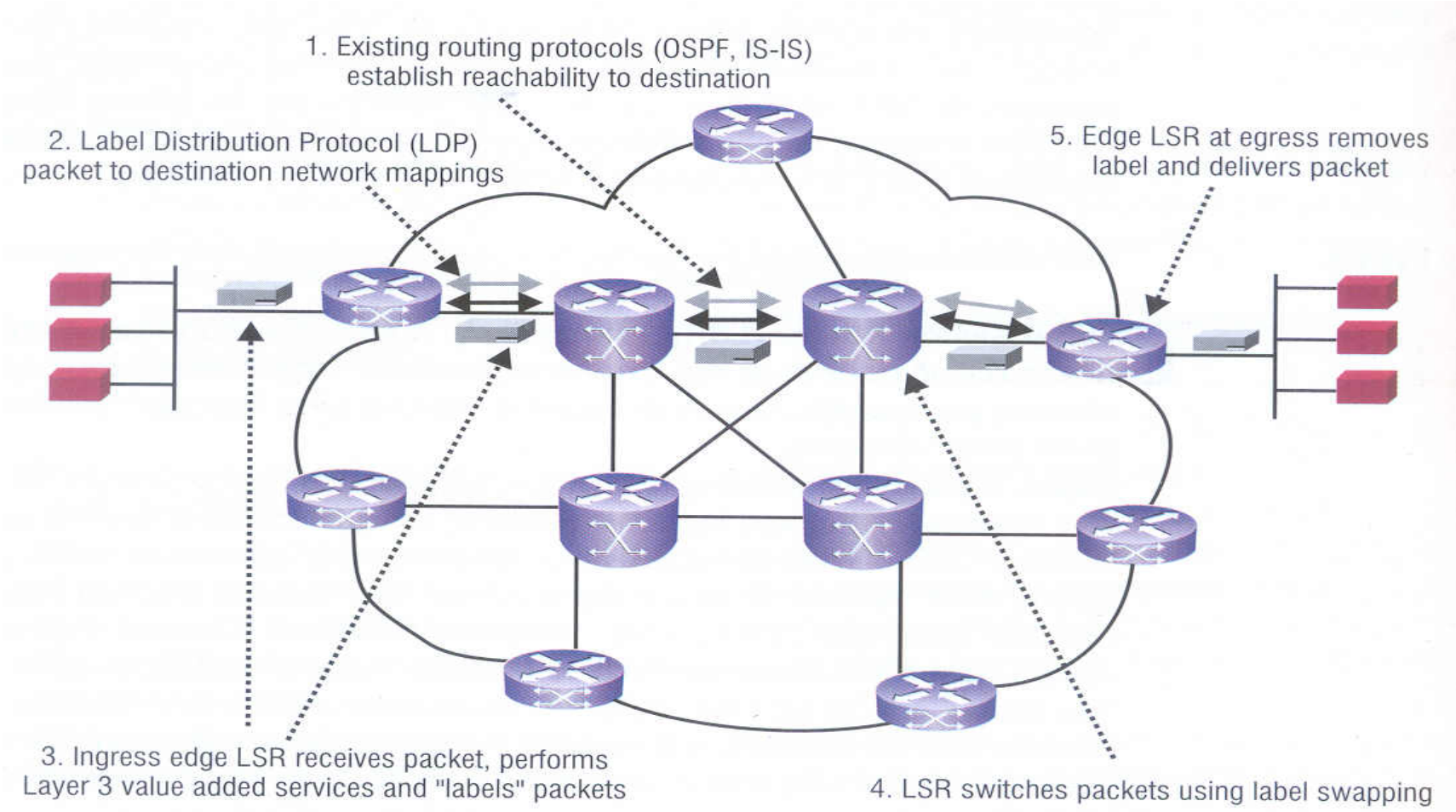
- **Δρομολογητής ετικέτας (Label Switch Router (LSR)):** Αποτελεί την συσκευή κορμού του δικτύου που μετάγει πακέτα εφοδιασμένα με το κατάλληλο label σύμφωνα με προϋπολογισμένους πίνακες μεταγωγής

- **Δρομολογητής ετικέτας άκρου (Edge Label Switch Router (Edge LSR)):** Είναι η συσκευή στην "άκρη" του δικτύου κορμού, η οποία εκτελεί την αρχική επεξεργασία του κάθε πακέτου, αναθέτοντάς του μία ετικέτα.

- **Μονοπάτι ετικέτας (Label Switched Path (LSP)):** Είναι το "μονοπάτι" που ορίζεται από το σύνολο των ετικετών μεταξύ των τελικών σημείων του δικτύου. Μπορεί να είναι είτε δυναμικό (η συνηθέστερη περίπτωση) είτε στατικό.

- **Πρωτόκολλο διανομής ετικετών (Label Distribution Protocol (LDP)):** Είναι το πρωτόκολλο που αναθέτει ετικέτες για τη δημιουργία των LSPs, καθώς επίσης δίνει τη δυνατότητα σε κάθε LSR να «μεταφράζει» την πληροφορία από τις ετικέτες. Η απόδοση των ετικετών γίνεται σε συνδυασμό με άλλα γνωστά πρωτόκολλα δρομολόγησης (όπως για παράδειγμα το Open Shortest Path First (OSPF) ή το Border Gateway Protocol (BGP).

Τεχνολογία MPLS

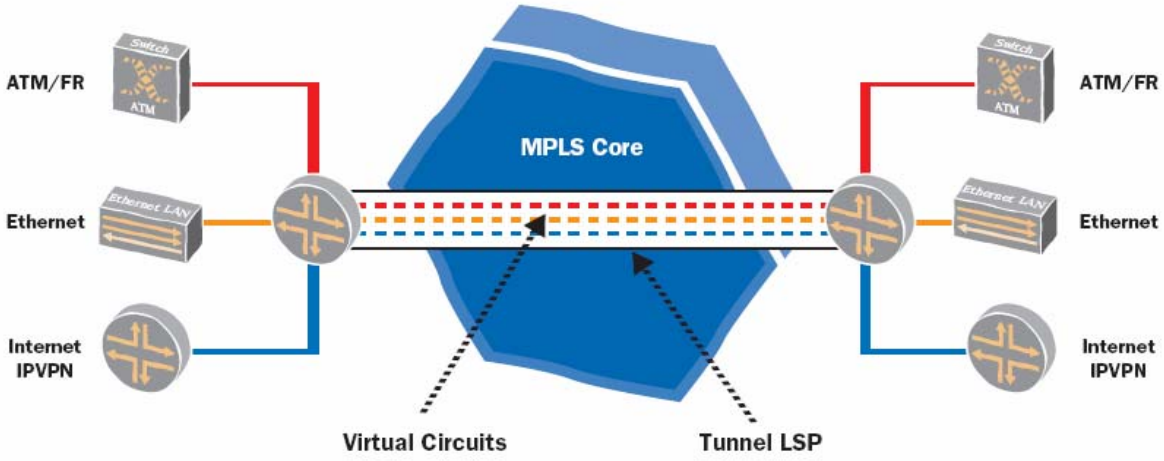


Πόσα είδη MPLS VPNs υπάρχουν?

- MPLS VPN επιπέδου 3: βασίζονται στην MPLS αρχιτεκτονική που έχει το δίκτυο κορμού του ISP. Η μετάδοση της πληροφορίας γίνεται πάνω στο IP πρωτόκολλο μόνο.
- MPLS VPN επιπέδου 2: υποστηρίζουν όχι μόνο IP αλλά διάφορες τεχνολογίες (ATM, X25 κ.ά). Οι αναπτυσσόμενες δίοδοι είναι ουσιαστικά το ιδεατό μονοπάτι LSP.

Layer 2 MPLS VPNs

- Μετάδοση πλαισίων του επιπέδου 2 (οποιουδήποτε πρωτοκόλλου – π.χ. ATM, Ethernet κτλ)
- **Αποφάσεις προώθησης με βάση την τιμή ετικέτας, και όχι τη διεύθυνση του πακέτου**
- Κάθε πακέτο ενθυλακώνεται στο MPLS πρωτόκολλο (δηλαδή αποκτά ετικέτα) και μέσω του LSP που έχει σχηματιστεί δρομολογείται προς τον προορισμό (όπου εκεί αποκαθίσταται στην αρχική του μορφή).
- Τα LSPs που παράγονται είναι στην ουσία ιδεατά κυκλώματα και αυτά αποτελούν τη δίοδο (tunnel) του σχηματιζόμενου VPN.

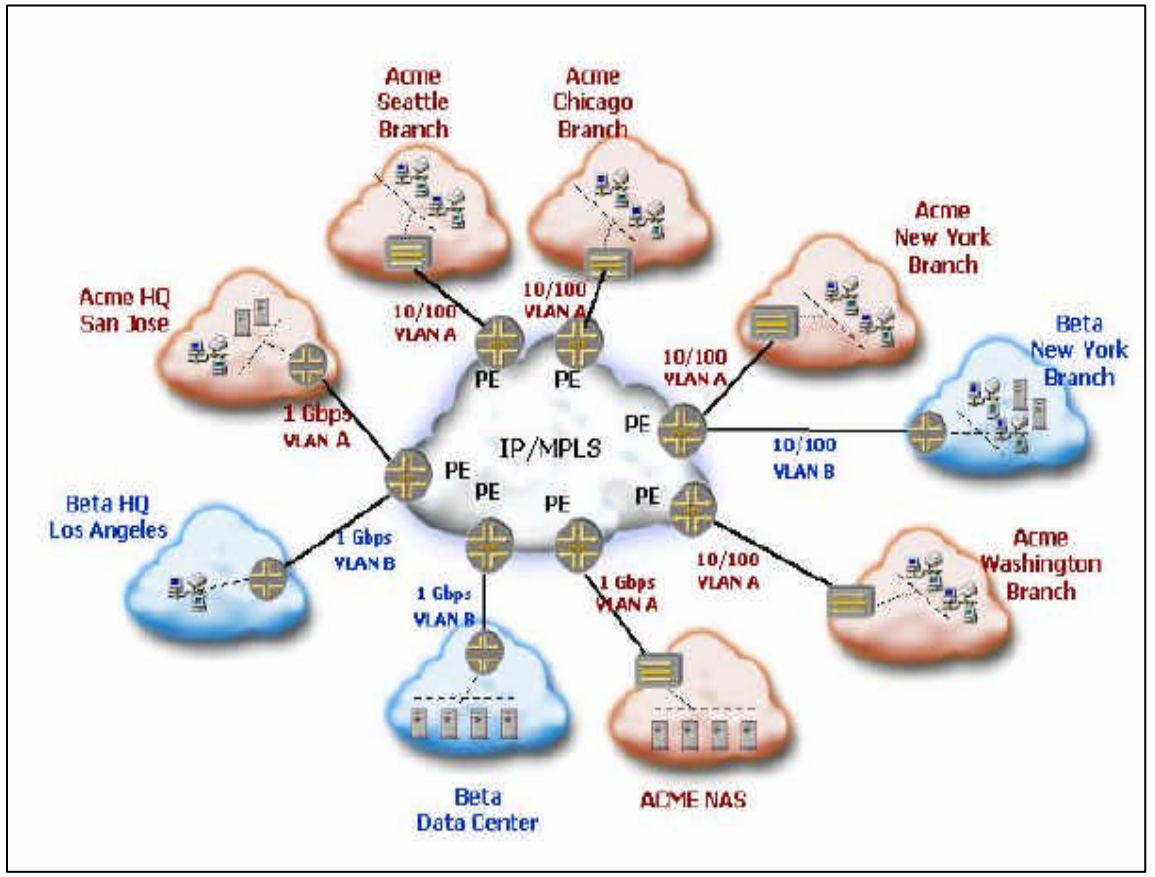


Υλοποιήσεις Layer 2 MPLS VPNs

- **Draft-Martini:** Σύνολο κανόνων που καθορίζουν το πώς γίνεται η MPLS ενθυλάκωση. Έχει το πλεονέκτημα της υποστήριξης πολλών διαφορετικών τεχνολογιών (ATM, Ethernet κτλ.). Χρησιμοποιεί το LDP για τη σηματοδοσία.
  - Μειονέκτημα: δεν είναι κλιμακούμενο
- **Draft-Kompella:** Σχεδιάστηκαν για να επιλύσουν τα προβλήματα των Draft-Martini VPNs. Χρησιμοποιούν το πρωτόκολλο BGP και όχι το LDP για τη δημιουργία tunnels. Αυτό είναι πλεονέκτημα αφενός γιατί το BGP μπορεί ήδη να χρησιμοποιείται και για την υλοποίηση των L3 VPNs που μπορεί να συνυπάρχουν στο δίκτυο κορμού, αφετέρου γιατί το BGP είναι αυτοματοποιημένο και δεν χρειάζεται παρέμβαση του διαχειριστή

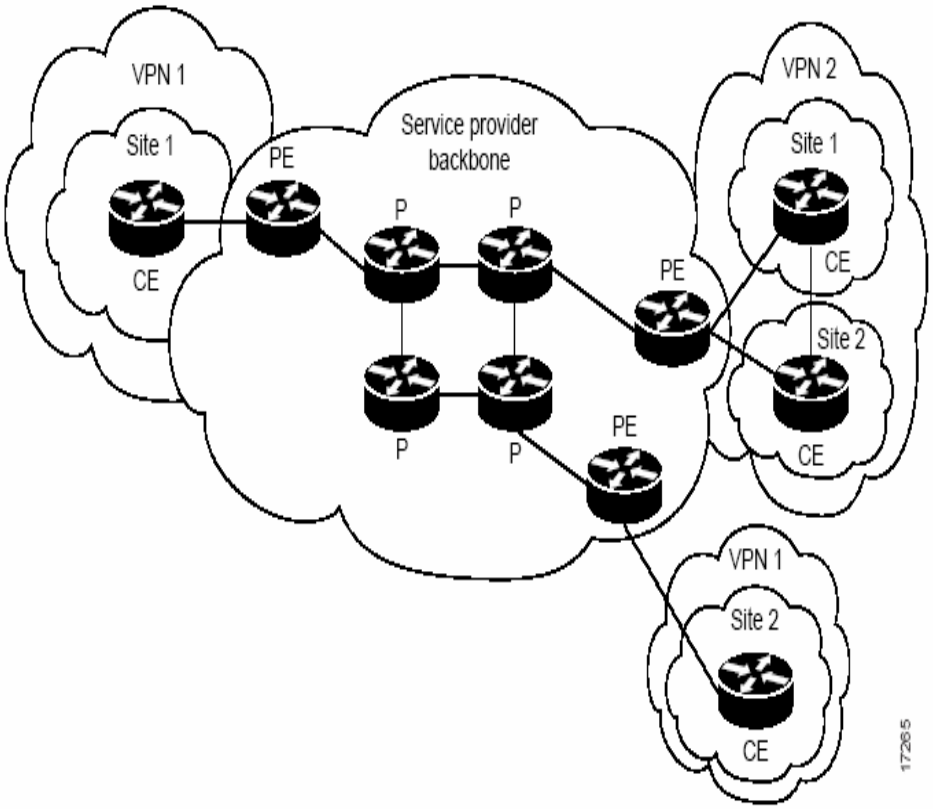
Εναλλακτική προσέγγιση L2 MPLS VPN - VPLS

- **Virtual Private LAN Services (VPLS):** Υλοποίηση μίας τοπολογίας Ethernet, η οποία εκτείνεται σε περισσότερα από ένα μητροπολιτικά δίκτυα
- Κάθε χρήστης συνδέεται με άλλον σε άλλη πόλη, σαν να ανήκαν στο ίδιο τοπικό δίκτυο Ethernet
- Εισαγωγή νέου Ethernet στο VPLS μπορεί να γίνει είτε αυτοματοποιημένα (η συνηθέστερη περίπτωση) είτε «χειροκίνητα» (manually)



Layer 3 MPLS VPNs – Είδη δρομολογητών

- **Δρομολογητές CE (customer edge)**
  - **Είναι οι δρομολογητές που τους διαχειρίζεται ο πελάτης και ανήκουν συνήθως σε αυτόν**
- **Δρομολογητές PE (provider edge)**
  - **Είναι οι δρομολογητές που αποτελούν τα σημεία εισόδου και εξόδου των VPNs.**
  - **Ανήκουν διαχειριστικά στον ISP.**
  - **Αποτελούν το πιο σημαντικό τμήμα στη «λογική» VPNs**
- **Δρομολογητές P (provider)**
  - **Είναι οι δρομολογητές που αποτελούν το δίκτυο κορμού του ISP και ανήκουν και αυτοί διαχειριστικά σε αυτόν.**
  - **Δε συμμετέχουν στη λογική VPN και ο κύριος σκοπός τους είναι η προώθηση των MPLS labels προς τους PE routers**



Δρομολογητές PE

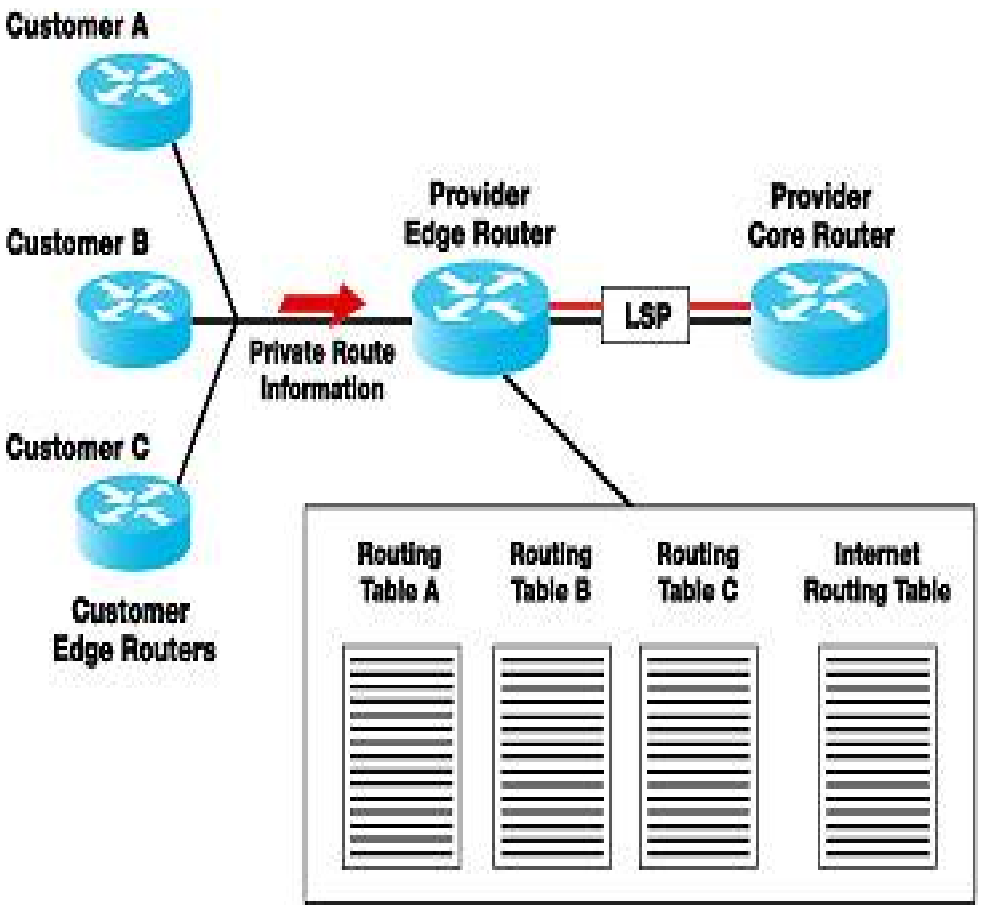
- Διαμοιράζουν τις πληροφορίες δρομολόγησης των διαφόρων VPNs και ενημερώνουν τους πίνακες δρομολόγησης που ανήκουν σε κάθε VPN. Μεταφέρουν αυτή την πληροφορία μεταξύ τους με τη χρήση του πρωτόκολλου BGP (Border Gateway Protocol).
- Με τη χρήση του MPLS λοιπόν ανταλλάσουν MPLS ετικέτες και έτσι είναι δυνατό κάθε στιγμή, ένα «μέλος» ενός VPN που συνδέεται σε έναν συγκεκριμένο δρομολογητή PE να επικοινωνήσει με οποιοδήποτε άλλο «μέλος» του ίδιου VPN που συνδέεται σε κάποιον άλλο PE.
- Επιπλέον είναι δυνατό, μέσω πολιτικής πρόσβασης στο BGP, να επιτρέπεται ή να απαγορεύεται η πρόσβαση από/προς συγκεκριμένα «μέλη» ενός VPN. (το BGP είναι πρωτόκολλο δρομολόγησης που παρέχει τέτοιες δυνατότητες)
- Για να αναγνωρίζει κάθε PE σε ποιο VPN ανήκει κάθε εισερχόμενο πακέτο (μια που από κάθε PE μπορεί να περνάνε πολλά VPN) χρησιμοποιείται μια δεύτερη ετικέτα.

Δρομολογητές P

- Δεν συμμετέχουν στην δρομολόγηση των VPNs. Συμμετέχουν μόνο στη δημιουργία MPLS LSPs ανάμεσα στους δρομολογητές. Αυτά τα LSPs χρησιμοποιούν οι PEs προκειμένου να μεταφέρουν την κίνηση ανάμεσα στα «μέλη» των VPNs.

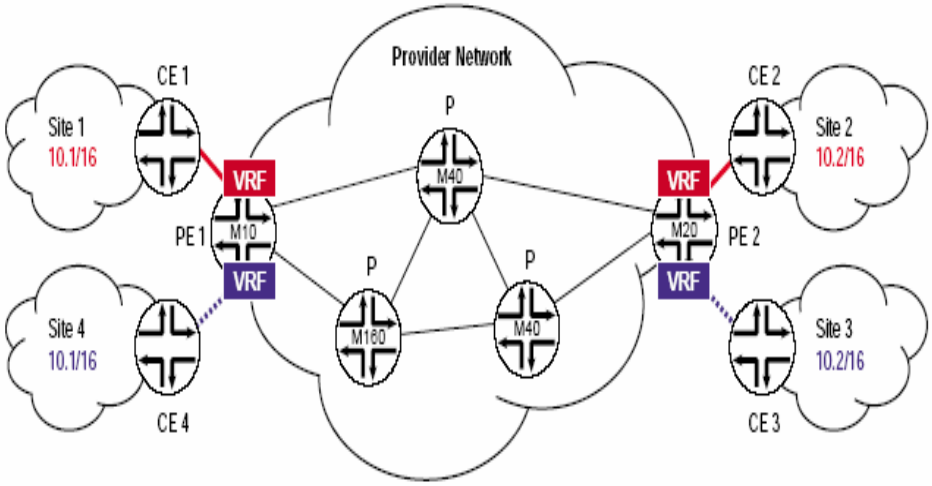
Πίνακες δρομολόγησης

- Με τη χρήση του BGP, οι δρομολογητές PE «γνωρίζουν» τους πίνακες δρομολόγησης των διαφόρων VPNs που συνδέονται σε άλλους PE δρομολογητές.
- Κάθε PE δρομολογητής διατηρεί έναν «υποπίνακα» δρομολόγησης που περιέχει μόνο την πληροφορία δρομολόγησης που αφορά τον συγκεκριμένο πελάτη και μόνον αυτόν. Αυτό προσφέρει μέγιστη ασφάλεια αφού ο πίνακας δρομολόγησης ανήκει μόνο σε συγκεκριμένο πελάτη.



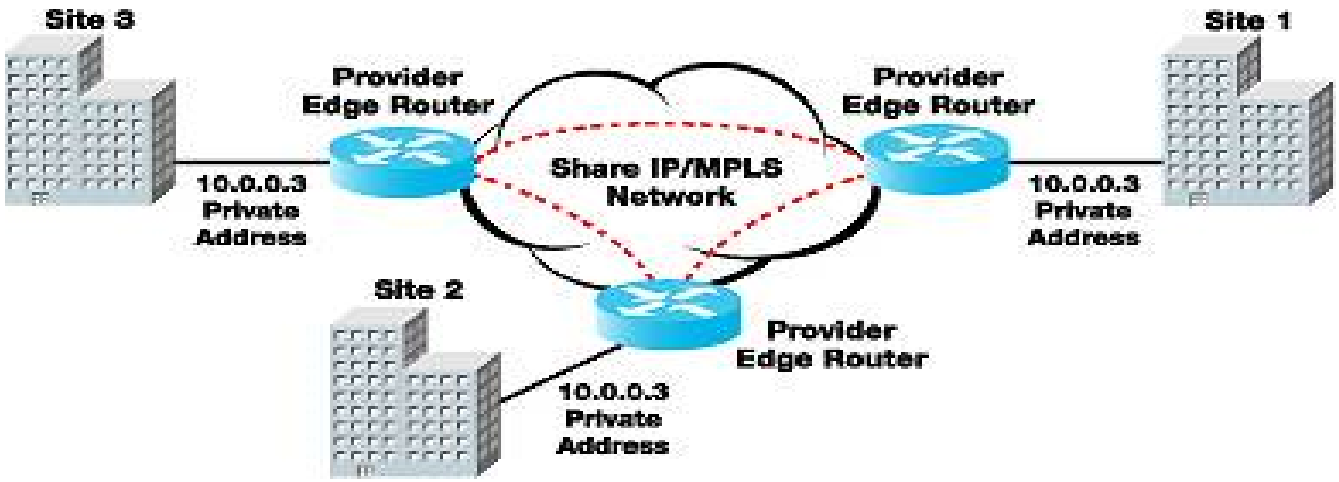
Τοπολογία BGP/MPLS VPNs

- **Κάθε PE δρομολογητής διατηρεί έναν** «υποπίνακα» δρομολόγησης (Virtual Routing & Forwarding Instance - VRF) **που περιέχει μόνο την πληροφορία δρομολόγησης που αφορά τον συγκεκριμένο πελάτη και μόνον αυτόν**



CE = Customer Edge
P = Provider Routers
PE = Provider Edge
VRF = VPN Routing and Forwarding Table

Αλληλοεπικάλυψη IP διευθύνσεων



- VPN-IP διευθύνσεις**:** Μοναδικές διευθύνσεις που δημιουργούνται συνδέοντας τον Route Distinguisher ή Route Descriptor (RD) με την IP διεύθυνση του πελάτη

- Μέλη ενός VPN μπορούν να είναι μόνο όσοι έχουν το κατάλληλο διαχωριστή δρομολόγησης RD. Αυτή η ιδιότητα καθιστά την είσοδο μη εξουσιοδοτημένων χρηστών στα MPLS VPNs θεωρητικά αδύνατη.

Εισαγωγή νέου κόμβου ενός παραρτήματος

- Ο πάροχος πρέπει να κάνει τα εξής:
  - να ενημερώσει τον δρομολογητή CE του νέου παραρτήματος για τον τρόπο σύνδεσης στο δίκτυο του παρόχου,
  - να διαμορφώσει τον PE δρομολογητή έτσι ώστε να αναγνωρίζει τη συμμετοχή του συγκεκριμένου CE στο συγκεκριμένο VPN.
  - Στη συνέχεια, το BGP που «τρέχει» στο συγκεκριμένο PE ενημερώνει αυτόματα όλους τους άλλους PEs για το νέο «μέλος».