ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ
ΙΔΡΥΜΑ ΗΠΕΙΡΟΥ
TECHNOLOGICAL EDUCATIONAL INSTITUTE OF EPIRUS

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

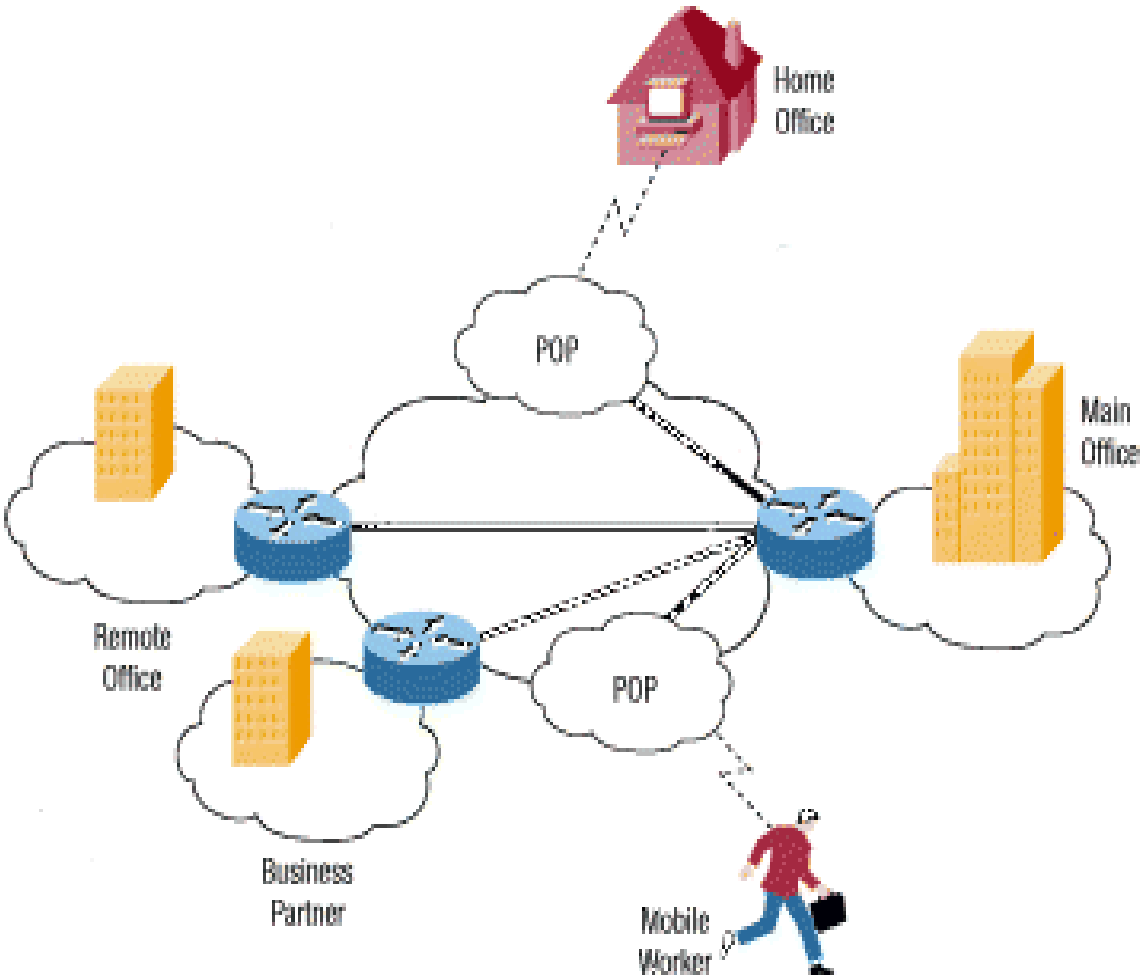
ΑΣΦΑΛΗΣ ΜΕΤΑΦΟΡΑ ΔΕΔΟΜΕΝΩΝ ΜΕ ΤΗΝ ΧΡΗΣΗ ΙΔΕΑΤΩΝ ΙΔΩΤΙΚΩΝ ΔΙΚΤΥΩΝ

ΣΚΟΔΡΑ ΧΡΙΣΤΙΝΑ
Α..Μ 2215
ΓΙΑΝΝΑΚΟΥΔΑΚΗΣ ΝΙΚΟΛΑΟΣ
Α.Μ 1965

ΚΑΘΗΓΗΤΗΣ : ΤΣΙΑΝΤΗΣ ΛΕΩΝΙΔΑΣ

ΑΘΗΝΑ
25/09/2006

ΑΣΦΑΛΗΣ ΜΕΤΑΦΟΡΑ ΔΕΔΟΜΕΝΩΝ ΜΕ ΤΗΝ ΧΡΗΣΗ ΙΔΕΑΤΩΝ ΙΔΩΤΙΚΩΝ ΔΙΚΤΥΩΝ



ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Είναι σίγουρο πως διψάμε για αλλαγές! Δε δικαιολογείται αλλιώς ο ραγδαίος ρυθμός με τον οποίο υιοθετούμε νέες τεχνικές, νέες τεχνολογίες, νέους τρόπους ζωής. Είμαστε ανταγωνιστικά και φιλόδοξα όντα και έτσι αρπάζουμε όλες τις ευκαιρίες που υπόσχονται να μας φέρουν μπροστά, να μας αναπτύξουν περισσότερο από τους άλλους, να μας δώσουν τον έλεγχο του επαγγελματικού μας περιβάλλοντος.

Η εποχή που βιώνουμε είναι επαναστατική, εκρήγνυται. Πολλά πράγματα απ' αυτά που συνηθίζαμε αλλάζουν και μάλιστα αλλάζουν με τέτοιους ρυθμούς που δύσκολα μπορούμε να ακολουθήσουμε και ακόμα πιο δύσκολα να αφομοιώσουμε. Οι μεγάλες ανακαλύψεις του προηγούμενου αιώνα, οι σιδηρόδρομοι, τα μηχανοκίνητα οχήματα, το τηλέφωνο, η τηλεόραση, αν και ήταν επαναστατικές αλλαγές που άλλαξαν το τοπίο σε όλα τα επίπεδα της δράσης μας, εντούτοις, είχαν ρυθμούς που επέτρεπαν την εξοικείωση μας μαζί τους.

Στην εποχή μας, η έκρηξη βρίσκεται στην επικοινωνία, στην πληροφορία. Μιλάμε για παγκόσμια δίκτυα υπολογιστών, για λεωφόρους πληροφορίας, για έλεγχο της πληροφορίας, για ταχύτητα επικοινωνίας, για κρυπτογράφηση, πιστοποίηση και ασφάλεια στην επικοινωνία.

Η τεχνολογία δικτύωσης υπολογιστών, το Internet, σε συνδυασμό με τις ανταγωνιστικές πιέσεις και την ανάγκη για δημιουργία μεγαλύτερων, ανθεκτικότερων και πιο ευέλικτων επιχειρηματικών σχημάτων, διαμόρφωσαν ένα τοπίο που η πληροφορία, η άμεση και η έγκυρη ενημέρωση, έχουν κυρίαρχο ρόλο στην αποτελεσματικότητα μας, στο λειτουργικό μας κόστος, στις ευκαιρίες που έχουμε για επιτυχία και για ανάπτυξη, και τελικά καθορίζουν όχι μόνο την επιτυχία αλλά και την άμεση επιχειρηματική μας βιωσιμότητα.

Οι επιχειρηματίες που αρνούνται να δούν τη νέα κατάσταση, θα είναι έξω από το παιχνίδι στο χιλιοστό του χρόνου που απαιτήθηκε για τους αντίστοιχούς τους, του

προηγούμενου αιώνα, που δεν εκτίμησαν ως επιχειρηματικά εργαλεία τους σιδηροδρόμους, τα αυτοκίνητα και το τηλέφωνο...
Μιλάμε λοιπόν για την ανάπτυξη των Ιδεατών Ιδιωτικών Δικτύων (Virtual Private Networks, VPNs), χάρη στα οποία μπορούμε να να συνδέσουμε πολλά απομακρυσμένα σημεία της επιχείρησής μας, πιθανώς τους συνεργάτες μας και σε μερικές περιπτώσεις τους προμηθευτές και τους πελάτες μας, με τέτοιο τρόπο ώστε να λειτουργούμε ιδιωτικά, ταχύτερα, οικονομικότερα και αποτελεσματικότερα.

Υπάρχουν πολλές τεχνολογίες υλοποίησης Ιδεατών Ιδιωτικών Δικτύων. Όλες τους έχουν δυνατά και αδύνατα σημεία. Ο κοινός παρονομαστής τους είναι η διασύνδεση δύο ή περισσότερων σημείων χρησιμοποιώντας ως υποδομή ένα δίκτυο δημόσιας χρήσης, αλλά με τέτοιο τρόπο που να εγγυάται η ασφάλεια της πληροφορίας από τα αδιάκριτα μάτια. Μπορούμε να θεωρήσουμε ότι η έννοια VPN είναι μια τεχνολογική καινοτομία των τελευταίων ετών.

Παρόλα αυτά τα VPN είναι μια έννοια που υπάρχει περισσότερο από δέκα χρόνια και είναι πολύ γνωστή στην ανάπτυξη εταιρικών δικτύων. Οι νέες υπηρεσίες και τα νέα προϊόντα απλώς καθιστούν περισσότερο αξιόπιστη και πολύ πιο αποδοτική την εφαρμογή του ίδιου μοντέλου. Με την μείωση του κόστους και τη δυναμική των τεχνολογιών, συσχετιζόμενων με τις νέες VPN προσεγγίσεις, δεν είναι έκπληξη ότι οι VPN υπηρεσίες είναι ανάμεσα στους μεγαλύτερους κινητήριους μοχλούς εφαρμογής state-of-the-art τεχνολογιών (όπως το MPLS & IPSec) στα επιχειρησιακά δίκτυα.Αυτό το κεφάλαιο δίνει μια σύντομη επισκόπηση των VPN υπηρεσιών, λεπτομερής ταξινόμηση και διάφορες χρήσεις και τοπολογίες των VPN.

1. Τι είναι τα VPN

Η ΕΝΝΟΙΑ ΤΩΝ ΙΔΕΑΤΩΝ ΙΔΙΩΤΙΚΩΝ ΔΙΚΤΥΩΝ

Ως ιδεατό ιδιωτικό δίκτυο VPN (Virtual Private Networks) χαρακτηρίζουμε ένα δίκτυο στο οποίο η διασύνδεση διαφορετικών απομακρυσμένων δικτύων (τοποθεσιών) πραγματοποιείται πάνω από κοινή υποδομή, παρέχοντας το ίδιο επίπεδο ασφαλείας, διαχείρισης και απόδοσης με ένα ιδιωτικό δίκτυο. Τα ιδεατά ιδιωτικά δίκτυα καθορίζουν λοιπόν την λογική διασύνδεση πολλών απομακρυσμένων δικτύων, έτσι ώστε όλα μαζί να αποτελούν ένα ενιαίο δίκτυο ανεξάρτητα από την τοποθεσία τους.

Για να κατανοήσουμε καλυτέρα την έννοια του ιδεατού ιδιωτικού δικτύου ας θεωρήσουμε μια επιχείρηση που διαθέτει ένα σύνολο από γεωγραφικά κατανεμημένα υποκαταστήματα .Για την επικοινωνία αυτών των υποκαταστημάτων η επιχείρηση χρειάζεται να υλοποιήσει ένα δίκτυο. Το δίκτυο αυτό είναι ιδιωτικό (private) με την έννοια ότι η δρομολόγηση της πληροφορίας και το πλάνο διευθυνσιοδότησης των συσκευών μέσα στο δίκτυο, είναι εντελώς ανεξάρτητα από την δρομολόγηση και το πλάνο διευθυνσιοδότησης που χρησιμοποιούνται σε άλλα δίκτυα. Το δίκτυο αυτό είναι ιδεατό με την έννοια ότι οι εγκαταστάσεις που χρησιμοποιούνται τόσο για την λειτουργία όσο και για την διαχείριση αυτού, μπορεί να μην είναι αφιερωμένες αποκλειστικά σε αυτήν την επιχείρηση, αλλά μπορεί και να μοιράζονται και με άλλες επιχειρήσεις που επιθυμούν και αυτές το δικό τους δίκτυο VPN.

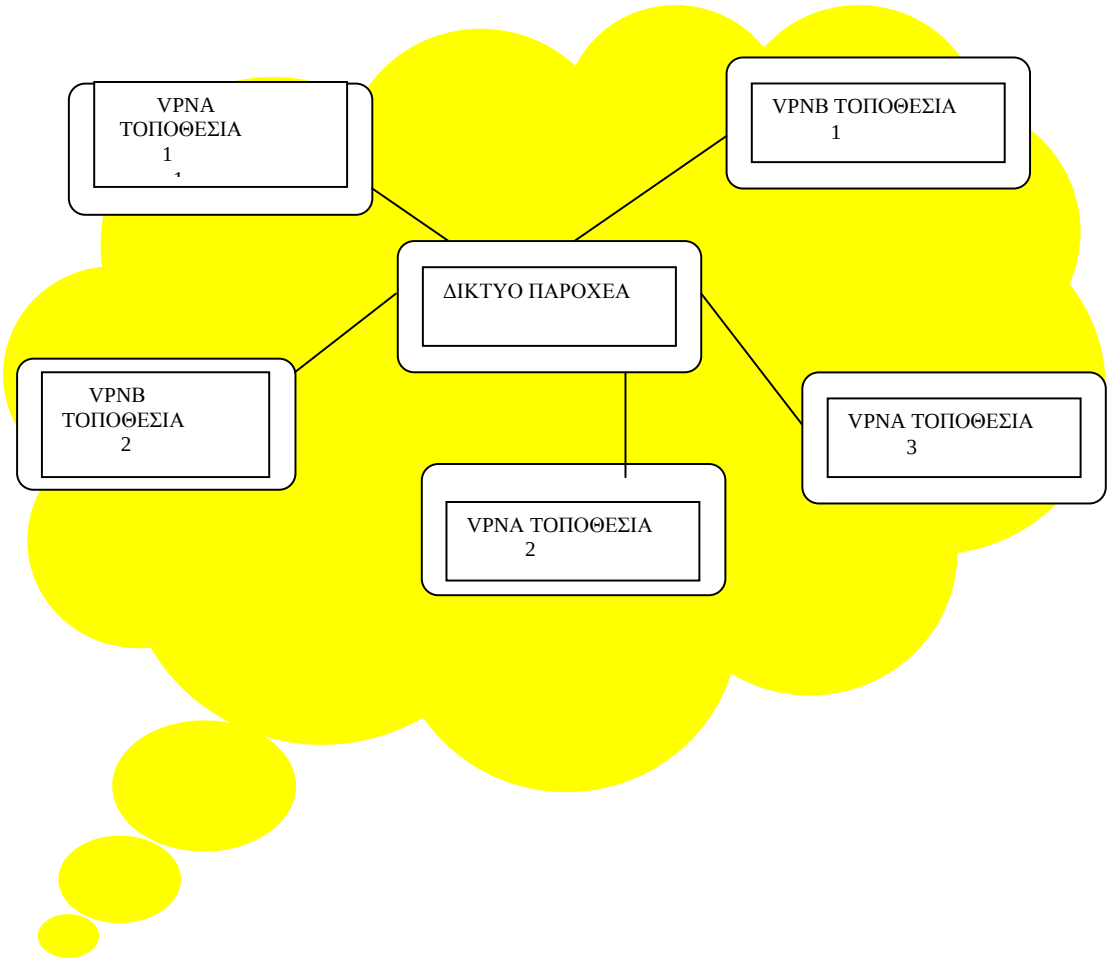
Οι εγκαταστάσεις και τα μέσα μετάδοσης που απαιτούνται για την υποδομή ενός τέτοιου δικτύου παρέχονται συνήθως από κάποιον παροχέα ο οποίος καλείται παροχέας υπηρεσιών VPN (VPN Service Provider), ενώ η επιχείρηση ή ο οργανισμός ή ο ιδιώτης οποιασδήποτε νομικής μορφής που χρησιμοποιεί αυτό το δίκτυο καλείται πελάτης VPN (VPN CUSTOMER).(εικόνα 1.1)

Στην εικόνα 1.1 το δίκτυο του παροχέα μπορεί να υποστηρίξει μέσα από την ίδια υποδομή δύο δίκτυα VPN που ανήκουν σε διαφορετικούς πελάτες. Επίσης είναι δυνατή και η επικοινωνία των δύο πελατών μεταξύ τους.

Γενικά μπορούμε να πούμε ότι ένα δίκτυο VPN, είναι ένα σύνολο από τοποθεσίες οι οποίες μπορούν να επικοινωνήσουν μεταξύ τους. Ένα δίκτυο VPN καθορίζεται από ένα σύνολο διεργασιών οι οποίες ελέγχουν τόσο τις διασυνδέσεις σε φυσικό και λογικό επίπεδο, όσο και το επίπεδο της παρερχόμενης ποιότητας υπηρεσίας (QoS) μεταξύ των διαφορετικών υπηρεσιών.

Τα δίκτυα VPN αποτελούν εξέλιξη των ιδιωτικών δικτύων δεδομένων (Private Networks) που είχαν αναπτύξει πολλές επιχειρήσεις στο παρελθόν, όπως για παράδειγμα οι τραπεζικοί οργανισμοί τα οποία στηρίζονται στη μίσθωση γραμμών μεταφοράς και στη χρήση των πρωτοκόλλων Frame Relay και ATM για την μεταφορά της πληροφορίας. Το κόστος υλοποίησης και συντήρησης αυτών των δικτύων είναι αρκετά υψηλό ανάλογα βέβαια και με το μέγεθός τους.

Σήμερα τα VPN παρέχουν υψηλή διαθεσιμότητα και κλιμάκωση, ενώ υποστηρίζουν πολλά πρωτόκολλα δρομολόγησης και μεταφοράς δεδομένων (IP, Frame Relay , ATM).



Εικόνα 1.1. Ένα Ιδεατό Ιδιωτικό Δίκτυο VPN

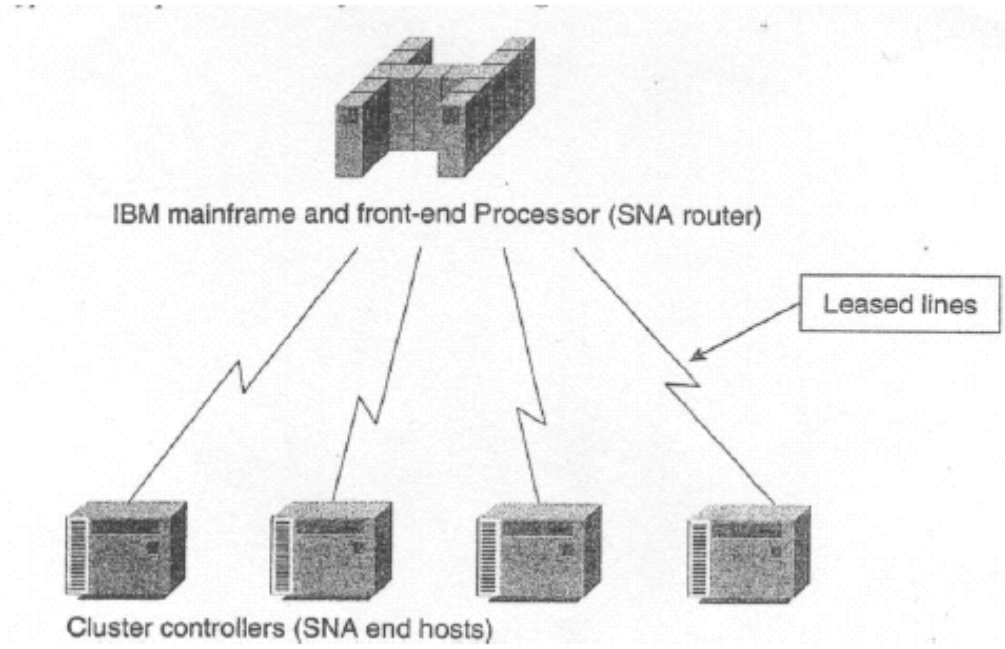
1.1 Η εξέλιξη των VPN

Η ιδέα της δημιουργίας δικτύων VPN δεν είναι καινούρια αλλά υπάρχει εδώ και 20 περίπου χρόνια. Απλά σήμερα, με την ανάπτυξη της τεχνολογίας χρησιμοποιείται ολοένα και περισσότερο τόσο λόγω των σημαντικών μειώσεων στο κόστος υλοποίησης και λειτουργίας των δικτύων όσο και στην εξαιρετική ευελιξία ανάπτυξης και υποστήριξης νέων υπηρεσιών στις ήδη υπάρχουσες υποδομές.

Τα πρώτα δίκτυα δεδομένων που αναπτύχθηκαν από τους διάφορους οργανισμούς βασίστηκαν κυρίως πάνω σε δύο τεχνολογίες, οι οποίες χρησιμοποιούνται ακόμα και σήμερα:

- Τις μισθωμένες γραμμές (leased-lines), οι οποίες ενοικιάζονται από τους παροχείς και είναι αφιερωμένες μόνιμα στον πελάτη, και

- Τις γραμμές με διεπιλογή (dial-up lines), οι οποίες χρησιμοποιούνται όταν υπάρχει ανάγκη και ύστερα από την πραγματοποίηση τηλεφωνικής κλήσης προς το δίκτυο του παροχέα. Το Σχήμα 1.1 δείχνει ένα τυπικό δίκτυο εκείνων των ημερων.



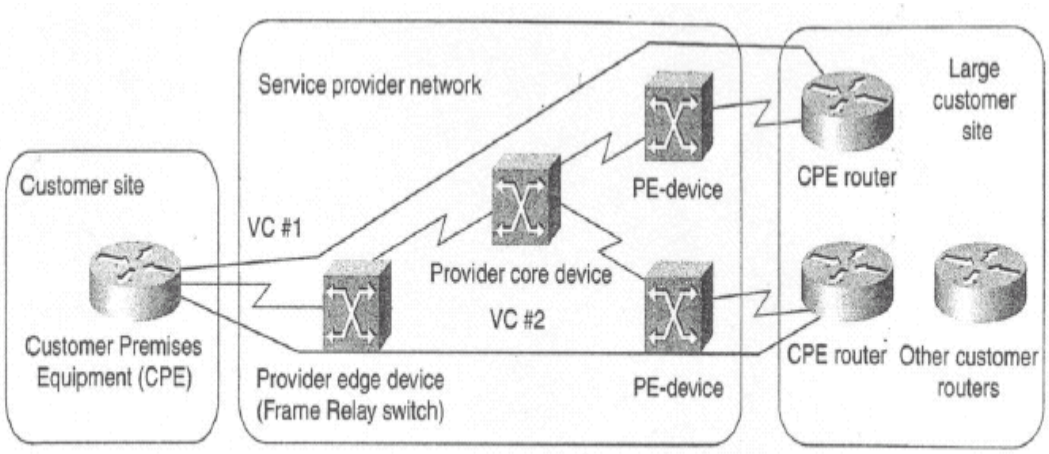
Σχήμα 1.1 Τυπικό Δίκτυο Υπολογιστων πριν 15 χρόνια

Η λειτουργία των αρχικών δικτύων υπολογιστών εξασφάλιζε στους πελάτες καλή ασφάλεια (Οι μισθωμένες γραμμές απαιτούν εξειδικευμένο εξοπλισμό και φυσική πρόσβαση στο δίκτυο), αλλά δεν εξασφάλιζε αποδοτική λειτουργία εξαιτίας δύο λόγων:

- Το προφίλ της κίνησης μεταξύ δυο οποιονδήποτε τοποθεσιών ποικίλει ανάλογα με την ώρα της ημέρας, την ημέρα του μήνα, ακόμα και στην περίοδο (Για παράδειγμα η κίνηση στα μαγαζιά λιανικής αυξάνεται γύρω στη Χριστουγεννιάτικη περίοδο).

- Οι τελικοί χρήστες ζητούν πάντα γρήγορες αποκρίσεις, καταλήγοντας σε απαίτηση υψηλού εύρους ζώνης μεταξύ των τοποθεσιών, παρόλο που στο δεσμευμένο εύρος ζώνης που είναι διαθέσιμο για μισθωμένες γραμμές χρησιμοποιούνται περιστασιακά (δηλαδή όταν οι χρήστες είναι ενεργοί).

Αυτοί οι δύο λόγοι υποκίνησαν τη βιομηχανία των επικοινωνιών δεδομένων και των προμηθευτών υπηρεσιών δικτύου να αναπτύξουν και να εφαρμόσουν ένα αριθμό τεχνικών στατιστικής πολυπλεξίας συνδέσεων που εξασφάλιζε στους πελάτες μια υπηρεσία που ήταν σχεδόν όμοια με τις μισθωμένες γραμμές. Το πρώτο VPN βασίστηκε πάνω σε τέτοιες τεχνολογίες όπως X.25, Frame relay και αργότερα SMDS, ATM. Το Σχήμα 1.2 αναπαριστά ένα χαρακτηριστικό VPN χτισμένο σύμφωνα με αυτές τις τεχνολογίες. (για παράδειγμα Frame Relay).



Σχήμα 1.2 Τυπικό Frame Relay Δίκτυο

Όπως μπορούμε να δούμε στο Σχήμα 1.2 η συνολική VPN λύση αποτελείται από τα παρακάτω:

- Ο πάροχος υπηρεσίας (service provider) είναι ο οργανισμός που κατέχει την υποδομή (τον εξοπλισμό για τη μετάδοση των δεδομένων), παρέχει στους πελάτες του εξομοιωμένες μισθωμένες γραμμές (emulated leased lines). Ο πάροχος υπηρεσίας σε αυτό το σενάριο προσφέρει στο πελάτη μια Υπηρεσία Εικονικού Ιδιωτικού Δικτύου (VPN υπηρεσία).

- Ο πελάτης συνδέεται με το δίκτυο παρόχου υπηρεσίας μέσω συσκευής που ονομάζεται Εξοπλισμός Τοποθεσίας Πελάτη (Customer Premises Equipment-CPE). Η CPE είναι συνήθως μια συσκευή σύνθεσης πακέτων δεδομένων που εξασφαλίζει σαφή συνδεσιμότητα τερματικού, μια γέφυρα (bridge) ή ένα δρομολογητή (router). Η CPE μερικές φορές καλείται σαν Customer Edge (CE) συσκευή.

- Η CPE είναι συνδεδεμένη με τον πάροχο υπηρεσίας με κάποιο μέσο μετάδοσης δεδομένων (συνήθως μια μισθωμένη γραμμή ή μέσω μιας dial-up σύνδεσης), ο οποίος μπορεί να είναι X.25, frame relay, ένας μεταγωγέας (switch) ATM ή και ακόμα και ένας router. Η περιφερειακή συσκευή παρόχου υπηρεσίας μερικές φορές καλείται και σαν PE (Provider Edge).

- Ο πάροχος υπηρεσίας συνήθως έχει επιπρόσθετο εξοπλισμό στο πυρήνα του δικτύου (επίσης καλούμενη και σαν P-Network). Αυτές οι συσκευές καλούνται σαν P-Devices (P-συσκευές), (για παράδειγμα, P-switches, P-δρομολογητές).

- Ένα συνεχόμενο ή παρακείμενο τμήμα του δικτύου πελάτη καλείται ένας ‘τόπος’ (site). Ένας τόπος μπορεί να συνδεθεί με το P-δίκτυο μέσω ενός ή αρκετών γραμμών μετάδοσης, χρησιμοποιώντας μια ή περισσότερες CPE και PE συσκευές, για λόγους αξιοπιστίας.

- Η εξομοιούμενη μισθωμένη γραμμή που είναι εξασφαλισμένη για τον πελάτη από τον παρόχου υπηρεσίας στο επικαλυπτόμενο μοντέλο VPN (δες στην παράγραφο Overlay and Peer-to-Peer VPN Model για περισσότερες πληροφορίες) συχνά καλείται σαν Virtual Circuit (VC). Το VC μπορεί να είναι είτε μόνιμα διαθέσιμο (Permanent Virtual Circuit-PVC) ή να είναι εγκατεστημένο (Switched Virtual Circuit-SVC). Κάποιες τεχνολογίες χρησιμοποιούν ειδικούς όρους για τα VCs, για παράδειγμα Data Link Connection Identifier (DLCI) στο Frame Relay.

- Ο πάροχος υπηρεσίας μπορεί να χρεώνει με ένα σταθερό ποσό για την υπηρεσία VPN, η οποία συνήθως εξαρτάται από το εύρος ζώνης που είναι διαθέσιμο στο πελάτη, ή με ένα ποσό βασισμένο στη χρήση, ο οποίος μπορεί να εξαρτάται από τον όγκο των ανταλλασόμενων δεδομένων ή την διάρκεια ανταλλαγής των δεδομένων.

1.1.1 Σύγχρονες Προσεγγίσεις στα VPN

Με την εισαγωγή νέων τεχνολογιών στα δίκτυα παρόχου υπηρεσίας και απαιτήσεων πελάτη, η έννοια VPN γίνεται όλο και περισσότερο σύνθετη. Οι πωλητές εισήγαγαν διαφορετικούς και συχνά αλληλοσυγκρουόμενους μεταξύ τους όρους, οι οποίοι έχουν αυξήσει ακόμα περισσότερο την πολυπλοκότητα των VPN. Έτσι, με αυτόν τον τρόπο, οι καινούργιες υπηρεσίες VPN μπορούν να αλληλοκαλύψουν μια ποικιλία από τοπολογίες και τεχνολογίες. Ο μόνος τρόπος να τα βγάλουμε πέρα με αυτή την ποικιλία είναι να εισαγάγουμε μια ταξινόμηση για τα VPN, η οποία γίνεται σύμφωνα με τα τέσσερα παρακάτω κριτήρια.

1. Το πρόβλημα επιχείρησης που το VPN προσπαθεί να επιλύσει. Τα μεγαλύτερα επιχειρησιακά προβλήματα που ένα VPN προσπαθεί να επιλύσει είναι η εσωτερική επικοινωνία των επιχειρήσεων- intracompany communication (που τώρα τελευταία ονομάζεται intranet),η επικοινωνία μεταξύ διαφορετικών επιχειρήσεων-intercompany communication (επίσης καλούμενη ως extranet)και η πρόσβαση για χρήστες κινητών μέσων (επίσης καλούμενη ως Virtual Private Dial up Network)

2. Το επίπεδο OSI στο οποίο ο πάροχος υπηρεσίας ανταλλάσσει την πληροφορία της τοπολογίας με τον πελάτη. Εδώ οι μεγαλύτερες κατηγορίες είναι το Overlay model στο οποίο ο πάροχος υπηρεσίας προμηθεύει τον πελάτη μόνο με ένα σετ από γραμμές point-to-point μεταξύ των τοποθεσιών του πελάτη και το peer model όπου ο πάροχος υπηρεσίας και ο πελάτης ανταλλάσσουν μεταξύ τους πληροφορίες διαδρομής του τρίτου επιπέδου.

3. Οι τεχνολογίες των επιπέδων δύο ή τρία που χρησιμοποιούνται για να εφαρμόσουν την υπηρεσία VPN μέσα στο δίκτυο παρόχου υπηρεσίας, το οποίο μπορεί να είναι:X.25, frame relay, SMDS, ATM ή IP.

4. Η τοπολογία του δικτύου, που μπορεί να εκτείνεται από απλή hub-and-spoke τοπολογία σε fully meshed δίκτυο και πολυεπίπεδες ιεραρχικές τοπολογίες (multilevel hierarchical topologies) για μεγαλύτερα δίκτυα.

1.2 Κατηγοριοποίηση βασισμένη στην Επιχειρηματική χρήση

Τα τρία προβλήματα επιχείρησης που ένας οργανισμός προσπαθεί να επιλύσει βασισμένος σε ένα VPN είναι:

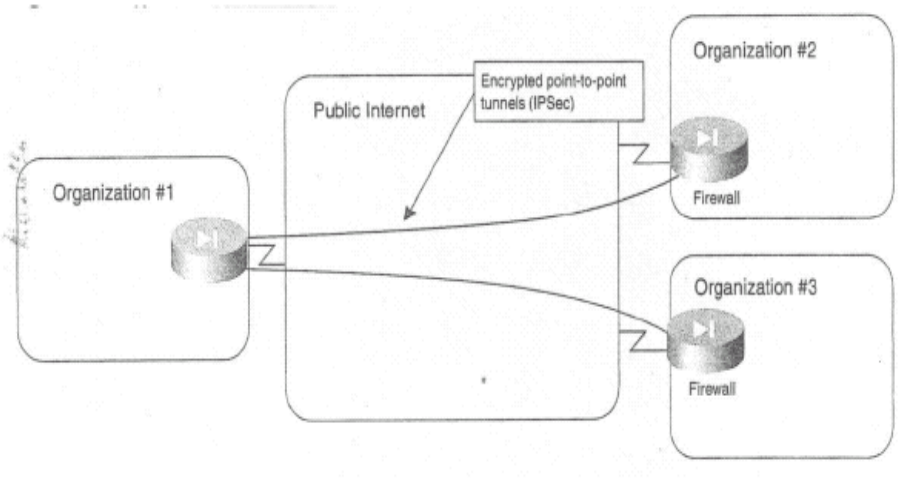
- Η επικοινωνία μέσα στον οργανισμό – intranet
- Η επικοινωνία με άλλους οργανισμούς – extranet
- Πρόσβαση των κινητών / απομακρυσμένων χρηστών, home workers, απομακρυσμένης υπηρεσίας-remote office κτλ μέσω φτηνών dial-up μέσων δεδομένων (Virtual Private Dial-up Network)

Οι τρεις τύποι των VPN λύσεων συνήθως καλύπτουν τις περισσότερες των τοπολογιών και τεχνολογιών που προσφέρονται από τους VPN παρόχους υπηρεσίας, αλλά διαφέρουν αρκετά στο επίπεδο ασφαλείας που απαιτείται στην εφαρμογή τους. Το intranet συνήθως δεν προστατεύεται από του εξυπηρετητές ή τα firewalls. Η VPN υπηρεσία χρησιμοποιείται για να δημιουργηθεί το intranet, συνεπώς πρέπει να προσφέρουν υψηλά επίπεδα ασφάλειας και απομόνωσης. Το intranet επίσης απαιτεί εγγυημένη ασφάλεια υπηρεσίας για mission-critical διεργασίες. Αυτοί είναι οι δύο κύριοι λόγοι που εξηγούν γιατί δεν βλέπουμε πολλούς οργανισμούς να χρησιμοποιούν το Internet, το οποίο δεν μπορεί να προσφέρει από άκρο σε άκρο ποιότητα υπηρεσίας, απομόνωσης ή ασφάλειας όπως η ιδιόκτητη υποδομή για τις δικές του intraorganizational επικοινωνίες.

Τα Intranet VPNs συνήθως αναπτύσσονταν βασισμένα σε παραδοσιακές τεχνολογίες όπως X.25, frame relay ή ATM. Οι Inter-Organizational επικοινωνίες επικεντρώνονται μεταξύ των κεντρικών τοποθεσιών των οργανισμών – συνήθως χρησιμοποιώντας αφιερωμένες συσκευές, όπως τα firewalls ή μηχανισμούς κρυπτογράφησης όμοιους με τη δομή που εικονίζεται στο Σχήμα 1.3.

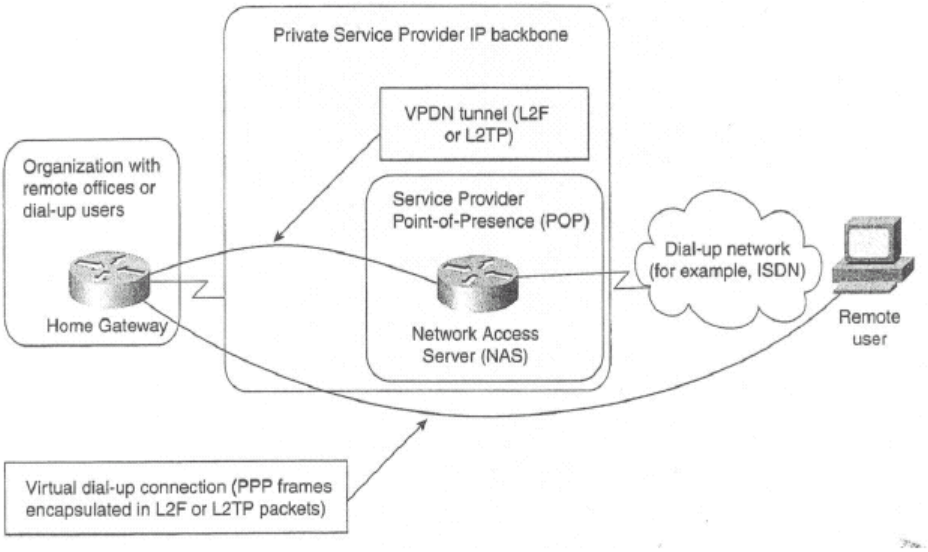
Αυτές οι επικοινωνίες επίσης μπορεί να έχουν λιγότερο αυστηρές απαιτήσεις για ποιότητα υπηρεσίας (QoS). Τέτοιες επικοινωνίες κάνουν το Internet όλο και περισσότερο ικανό για interorganizational επικοινωνίες, συνεπώς δεν είναι έκπληξη

που όλο και περισσότερη κίνηση ανάμεσα στις επιχειρήσεις αναπτύσσεται στο Internet.



Σχήμα 1.3 Τυπικό Extranet διαμόρφωση

Η απομακρυσμένη πρόσβαση σε ένα εταιρικό δίκτυο συνήθως γίνεται από μεταβαλλόμενες ή άγνωστες τοποθεσίες οπότε απαιτεί την επίλυση σειράς θεμάτων ασφαλείας πάνω σε μια end-to-end βάση, χρησιμοποιώντας τεχνολογίες όπως η κρυπτογράφηση ή κλειδάριθμους μιας χρήσης. Έτσι οι απαιτήσεις ασφαλείας για τις VPDN υπηρεσίες δεν ήταν ποτέ τόσο υψηλές όσο οι απαιτήσεις για τις intranet επικοινωνίες. Δεν αποτελεί λοιπόν έκπληξη πως οι περισσότερες από τις VPDN υπηρεσίες σήμερα χρησιμοποιούν το IP, είτε «πάνω» από το δημόσιο Internet ή χρησιμοποιώντας το ιδιωτικό δίκτυο κορμού ενός παρόχου υπηρεσίας, όπως αυτό που φαίνεται στο Σχήμα 1.4. Τα πρωτόκολλα που χρησιμοποιούνται για να εφαρμόσουμε VPDN υπηρεσία πάνω στο IP περιλαμβάνουν το L2F (Layer 2 Forwanding) ή το L2TP (Layer 2 Transport Protocol).



Σχήμα 1.4 Ο πάροχος υπηρεσίας προσφέρει χωρισμένο VPDN BACKBONE

Η τεχνολογία VPDN χρησιμοποιεί έναν αριθμό από ειδικούς όρους που είναι μοναδικοί στο κόσμο των VPDN.

1. **Network Access Server (NAS)**. Ο Remote Access Server (RAS) διαχειρίζεται από τον πάροχο υπηρεσίας που αποδέχεται την κλήση πελάτη, εκτελεί την αρχική διαδικασία πιστοποίησης και προωθεί την κλήση στην πύλη του πελάτη (μέσω L2F ή L2TP)

2. **Home Gateway**. Αποτελεί έναν διαχειριστή δρομολόγησης από την πλευρά του πελάτη (Customer Manager Router) που αποδέχεται την κλήση που έχει προωθηθεί από τον NAS, εκτελεί επιπρόσθετη αυθεντικοποίηση και πιστοποίηση και τερματίζει την PPP συνεδρία με τον Dial-up χρήστη. Οι παράμετροι της PPP συνεδρίας ανταλλάσσονται μεταξύ του Dial-up χρήστη και της Home Gateway, ο NAS το μόνο που κάνει είναι να προωθεί τα πλαίσια μεταξύ αυτών των δύο.

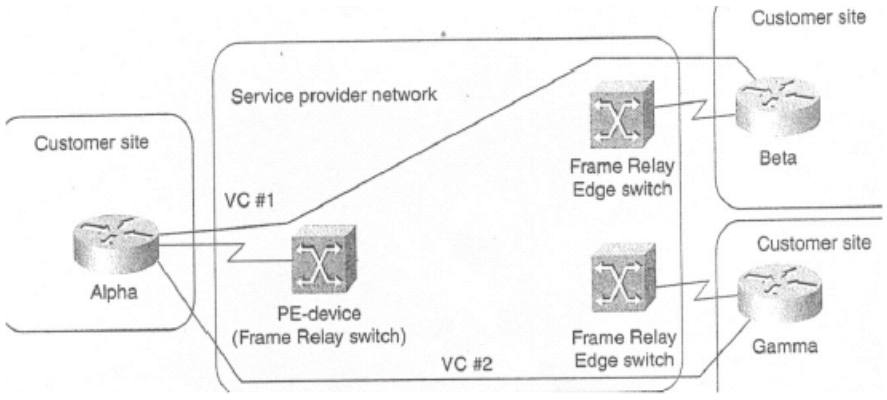
1.3 Τα μοντέλα Επικαλυπτόμενου VPN & Ομότιμων Οντοτήτων

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

1.3.1 Το Επικαλυπτόμενο (Overlay) VPN Μοντέλο

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

Το Σχήμα 1.5 δείχνει την τοπολογία του Overlay VPN και τα VCs που χρησιμοποιούνται.

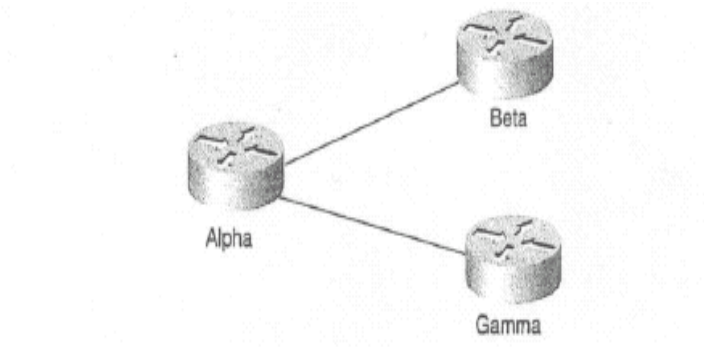


Σχήμα 1.5 Δείγμα Overlay VPN δικτύου

Ο πελάτης εγκαθιστά μια router-to-router επικοινωνία ανάμεσα στις CPE συσκευές στα VCs που είναι εφοδιασμένο από τον πάροχο υπηρεσίας. Στη συνέχεια το πρωτόκολλο δρομολόγησης δεδομένων ανταλλάσσει πληροφορία μεταξύ των συσκευών του παρόχου, και ο πάροχος υπηρεσίας δεν γνωρίζει τίποτα για την εσωτερική δομή του δικτύου του πελάτη.

Οι QoS εγγυήσεις του VPN μοντέλου συνήθως εκφράζονται σε όρους εγγυημένου εύρους ζώνης ανά VC (Committed Information Rate – CIR) και σε μέγιστο εύρος ζώνης διαθέσιμο σε συγκεκριμένο VC (Peak Committed Information Rate – PIR).

Το Σχήμα 1.6 δείχνει την τοπολογία του VPN δικτύου.



Σχήμα 1.6 Η δρομολόγηση στο δείγμα του Overlay VPN δικτύου

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

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

Encapsulation (GRE) και το IP Encryption. Αν και είναι σχετικά εύκολο να καταλάβει κανείς και να υλοποιήσει το Overlay VPN μοντέλο, υπάρχουν μια σειρά από μειονεκτήματα όπως:

- Πρόβλημα διαχειρισιμότητας. Είναι επαρκές για μη πλεονάζουσες διατάξεις (nonredundant) με λίγες κεντρικές τοποθεσίες και πολλές απομακρυσμένες, αλλά γίνεται υπερβολικά δύσκολο στη διαχείριση σε μια περισσότερο πολύπλοκη και σύνθετη διάταξη.

- Μερική γνώση και πρόβλεψη κίνησης. Η σωστή δημιουργία των VC με τις απαραίτητες χωρητικότητες, απαιτεί λεπτομερή γνώση της site-to-site κίνησης που συνήθως δεν είναι διαθέσιμη κατά τη δημιουργία των VCs.

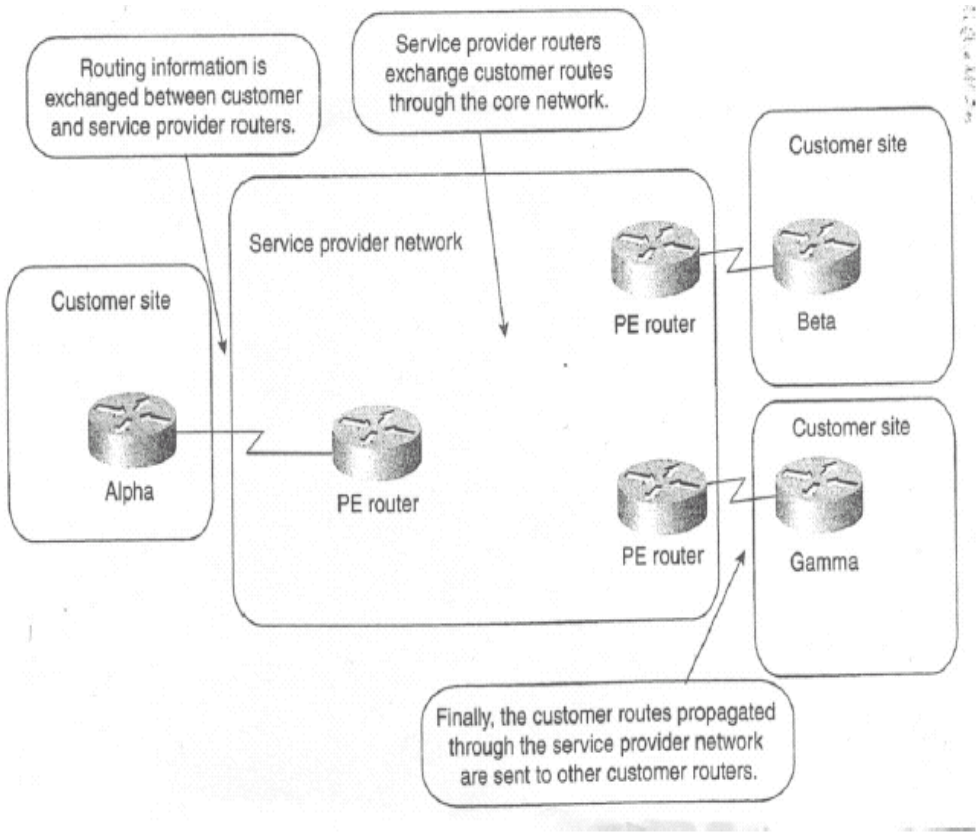
- Γραμμικό κόστος ανά αριθμό διασυνδέσεων για κάνε νέο κόμβο. Το κόστος εφαρμογής μεγαλώνει γραμμικά σε σχέση με τον αριθμό από point-to-point συνδέσεις στο δίκτυο, όχι με τον αριθμό των νέων δικτυακών τοποθεσιών που μπαίνουν στο VPN.

- Πολύπλοκη υποστήριξη επιχειρηματικού μοντέλου από τους παροχείς δικτυακών υπηρεσιών.

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

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

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



Σχήμα 1.7 Δείγμα Peer-to-Peer VPN

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

- Η δρομολόγηση (από την πλευρά του πελάτη) γίνεται ιδιαίτερα απλή καθώς ο δρομολογητής του πελάτη ανταλλάσσει πληροφορία δρομολόγησης με μόνο ένα (ή λίγους) PE δρομολογητές, ενώ αντιθέτως, στο Overlay VPN δίκτυο ο

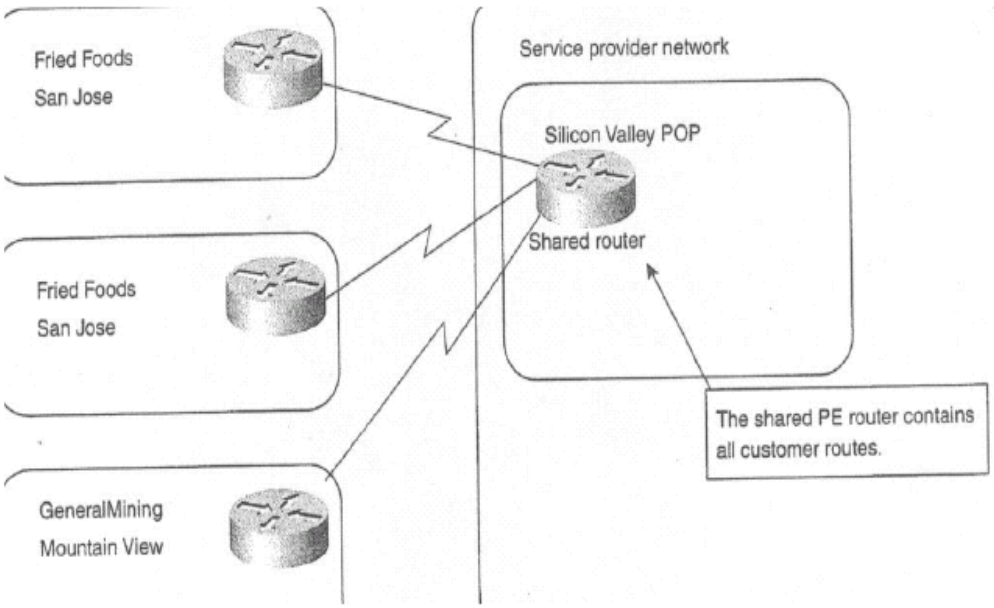
αριθμός των γειτονικών δρομολογητών μπορεί να αυξηθεί σε έναν μεγάλο αριθμό.

- Η δρομολόγηση μεταξύ των τοποθεσιών του πελάτη είναι πάντα η βέλτιστη, αφού οι δρομολογητές του παρόχου γνωρίζουν την τοπολογία του δικτύου του πελάτη και έτσι μπορούν να εγκαταστήσουν το καλύτερο μονοπάτι δρομολόγησης ανάμεσα στις υπηρεσίες. Η ανάθεση εύρους ζώνης είναι απλούστερη επειδή ο πελάτης μπορεί να καθορίσει μόνο το εσωτερικό και εξωτερικό εύρος ζώνης Committed Access Rate (CAR) και Committed Delivery Rate (CDR) και όχι το ακριβές site-to-site προφίλ κίνησης.

- Η πρόσθεση μια καινούργιας τοποθεσίας είναι απλούστερη επειδή ο πάροχος υπηρεσίας δημιουργεί μόνο μια επιπρόσθετη τοποθεσία και αλλάζει τους πίνακες δρομολόγησης στον συνδεόμενο PE. Αντίθετα στο Overlay VPN μοντέλο ο πάροχος υπηρεσίας πρέπει να παράσχει μια ολόκληρη ομάδα από VCs που να συνδέει τη νέα τοποθεσία σε όλες τις άλλες τοποθεσίες του πελάτη VPN.

Shared-Router Approach P-P VPN Model

Στη προσέγγιση του διαμοιραζόμενου δρομολογητή (shared router), πολλαπλοί πελάτες μπορεί να είναι συνδεδεμένοι στον ίδιο PE δρομολογητή. Οι λίστες πρόσβασης πρέπει να είναι διαμορφωμένες για κάθε VPN PE-to-CE διεπιφάνεια πάνω στον PE δρομολογητή έτσι ώστε να κατοχυρώνεται ο διαχωρισμός μεταξύ των VPN πελατών, και να εμποδίζεται ένας VPN πελάτης να παραβιάζει ένα άλλο VPN δίκτυο ή να εκτελεί μια επίθεση άρνησης υπηρεσίας σε έναν άλλο VPN πελάτη.
Το Σχήμα 1.8 απεικονίζει ένα παράδειγμα διαμοιραζόμενου δρομολογητή. Για να κατοχυρώσει το διαχωρισμό μεταξύ των πελατών η διάταξη θα πρέπει να έχει διαμορφωθεί κατάλληλα η λίστα πρόσβασης του POP δρομολογητή στο Σχήμα 1.8.



Σχήμα 1.8 Peer-to-Peer VPN μοντέλο: Διάταξη διαμοιραζόμενου Δρομολογητή

Dedicated-router Approach P-P VPN Model

Στην προσέγγιση του αποκλειστικού δρομολογητή (dedicated router) για το P-P μοντέλο κάθε VPN πελάτης έχει τους δικούς του αποκλειστικούς PE δρομολογητές και, με αυτόν τον τρόπο, έχει πρόσβαση μόνο στους δρομολογητές που εμπεριέχονται μέσα στο routing table αυτού του δρομολογητή.

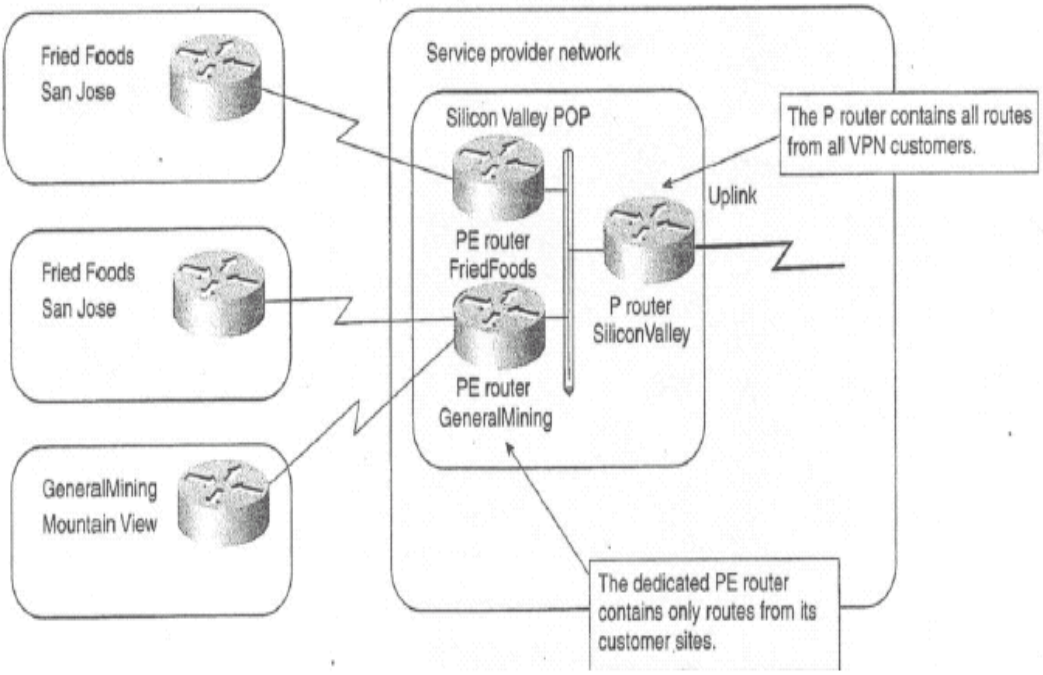
Το μοντέλο αποκλειστικού δρομολογητή χρησιμοποιεί πρωτόκολλα δρομολόγησης για να δημιουργήσει πίνακες μεταγωγής ανά VPN στους PE δρομολογητές. Οι πίνακες δρομολόγησης στους PE δρομολογητές περιέχουν τους δρομολογητές που γνωστοποιούνται από τον VPN πελάτη που είναι συνδεδεμένος σε αυτούς, έχοντας σαν αποτέλεσμα ένα σχεδόν τέλεια απομονωμένο μεταξύ των VPN πελατών.

Η μεταγωγή στο μοντέλο αποκλειστικού δρομολογητή μπορεί να υλοποιηθεί όπως παρακάτω:

- Κάθε πρωτόκολλο μεταγωγής «τρέχει» μεταξύ του PE δρομολογητή και του CE δρομολογητή.
- Το BGP «τρέχει» μεταξύ του PE και του P

- Ο PE ανακατανέμει τους δρομολογητές που παρελήφθησαν από τον CE στον BGP, σημειωμένοι με τον πελάτη ID (BGP «κοινωνία»),και μεταδίδει τις διαδρομές στους P. Οι P με αυτόν τον τρόπο συμπεριλαμβάνουν όλες τις διαδρομές από όλους τους δρομολογητές
- Οι P-δρομολογητές διαδίδουν μόνο διαδρομές με την κατάλληλη BGP «κοινωνία» στους PE-δρομολογητές. Οι PE-δρομολογητές με αυτόν τον τρόπο παραλαμβάνουν μόνο τις διαδρομές που προέρχονται από τους PE-δρομολογητές στο δικό τους VPN.

Σχετικά τμήματα του PE-router και της διάταξης P-router για τον πάροχο υπηρεσίας Point-of- Presence (POP) που απεικονίζονται στο Σχήμα 1.9.



Σχήμα 1.9 Peer-to-Peer VPN: Διάταξη εξειδικευμένου Δρομολογητή

Σύγκριση των Peer-to-Peer Μοντέλων

Όπως πολύ εύκολα μπορούμε να συμπεράνουμε από την προηγούμενη περιγραφή, το μοντέλο διαμοιραζόμενου δρομολογητή είναι αρκετά δύσκολο να διατηρηθεί επειδή αυτό απαιτεί την ανάπτυξη της αποτελεσματικότητας μακριών και πολύπλοκων λιστών πρόσβασης σε κάθε σχεδόν αλληλεπίδραση δρομολογητή. Η προσέγγιση της αποκλειστικής δρομολόγησης, αν και απλούστερη στη διαμόρφωση και διατήρηση, γίνεται πολύ ακριβή για τον πάροχο υπηρεσίας, όταν προσπαθεί να εξυπηρετήσει έναν μεγάλο αριθμό πελατών με γεωγραφικά διασκορπισμένες υπηρεσίες.

Και τα δύο P-P μοντέλα εμφανίζουν κάποια κοινά μειονεκτήματα που εμποδίζουν την ευρεία διάδοση τους.

- Όλοι οι πελάτες μοιράζονται την ίδια περιοχή IP διευθύνσεων, εμποδίζοντας έτσι τους πελάτες στο να αναπτύξουν ιδιωτικές IP διευθύνσεις. Έτσι οι πελάτες πρέπει να χρησιμοποιήσουν είτε κοινές IP διευθύνσεις ή ιδιωτικές IP διευθύνσεις διανεμημένες σε αυτούς από τον πάροχο υπηρεσίας.

- Οι πελάτες δεν μπορούν να εισάγουν τη δική τους δρομολόγηση πακέτων μέσα στο VPN τους. Αυτός ο περιορισμός εμποδίζει τη βελτιστοποίηση της δρομολόγησης και εμποδίζει τους πελάτες από το να έχουν πρόσβαση στο Internet και από άλλο πάροχο υπηρεσίας δικτύου (ISP).

Επιπρόσθετα στα δύο προηγούμενα μειονεκτήματα, το μοντέλο διαμοιραζόμένου δρομολογητή υποφέρει από επιπρόσθετη πολυπλοκότητα, όταν οι πελάτες χρησιμοποιούν διαφορετικά πρωτόκολλα δρομολόγησης (RIP, RIPv2, BEP, IS-IS).

1.4 Τυπικές τοπολογίες VPN

Η VPN τοπολογία που απαιτείται από έναν οργανισμό πρέπει να καλύπτει της απαιτήσεις της επιχείρησης. Παρόλα αυτά, υπάρχουν διάφορες πολύ γνωστές τοπολογίες που αξίζει να αναφερθούν. Οι ίδιες τοπολογίες μπορούν να λύνουν μια ποικιλία από διαφορετικά θέματα επιχείρησης ανάλογα με τις απαιτήσεις ης αγοράς αλλά και του επιχειρηματικού κλάδου στον οποίο δραστηριοποιούνται.

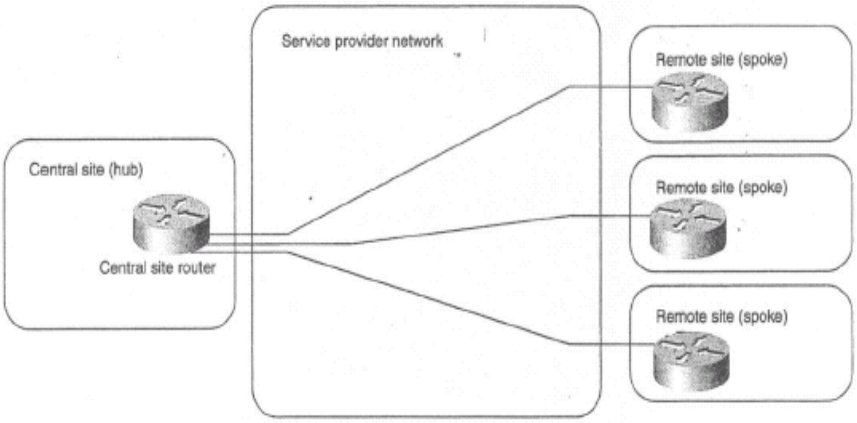
Οι VPN τοπολογίες που θα περιγραφούν μπορούν να διαιρεθούν σε τρεις μεγάλες κατηγορίες.

- Τοπολογίες επηρεασμένες από το Overlay VPN μοντέλο. Συγκεκριμένα προκειται για τις: Hub and Spoke τοπολογίες, partial ή full mesh τοπολογία και hybrid τοπολογία.
- Extranet τοπολογίες, και συγκεκριμένα τα any-to-any Extranet και Central Services Extranet
- Ειδικού σκοπού (Special Purpose) τοπολογίες, όπως οι VPDN backbone και Manager Network τοπολογία

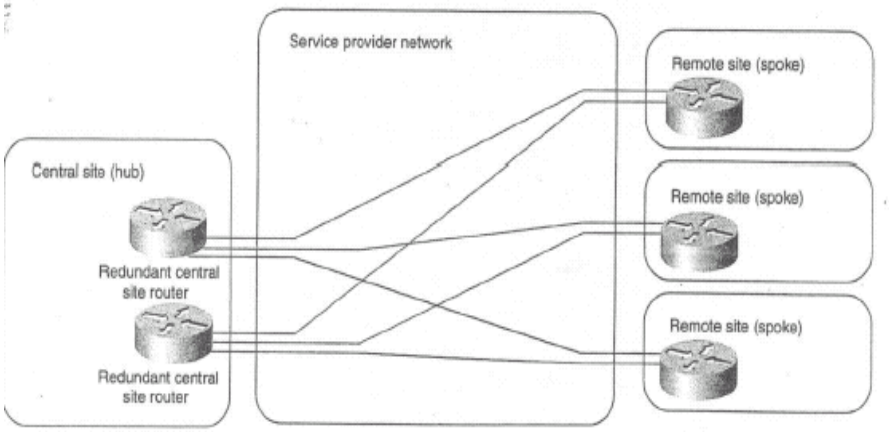
1.4.1 Τοπολογία Hub-and-spoke

Η τοπολογία που συνίσταται περισσότερο είναι η hub and spoke τοπολογία, όπου ένας αριθμός από απομακρυσμένα γραφεία (spokes), είναι συνδεδεμένα σε μια κεντρική τοποθεσία (hub) όμοια με το σενάριο στο Σχήμα 1.10.
Τα απομακρυσμένα γραφεία μπορούν να ανταλλάσσουν δεδομένα (συνήθως δεν υπάρχουν αυστηροί περιορισμοί ασφαλείας στην ανταλλαγή δεδομένων εσωτερικά στα γραφεία), αλλά το σύνολο των ανταλλασόμενων δεδομένων μεταξύ αυτών είναι αμελητέο. Η τοπολογία hub and spoke συχνά χρησιμοποιείται σε οργανισμούς με αυστηρές ιεραρχικές δομές, για παράδειγμα: σε τράπεζες, κυβερνήσεις ή διεθνείς οργανισμούς με περιορισμένα ανά χώρα γραφεία. Για τη κάλυψη των αυξημένων

απαιτήσεων σε επικαλυπτόμενες συνδέσεις, στην απλή hub and spoke τοπολογία (Σχήμα 1.10), συχνά προστίθεται ένας επιπρόσθετος δρομολογητής στην κεντρική τοποθεσία (Σχήμα 1.11), ή ένα κεντρικό site που χρησιμοποιείται σαν αντίγραφο, το οποίο σε αυτή τη περίπτωση είναι συνδεδεμένο με το πρωτεύον κεντρικό δίκτυο μέσα από μια σύνδεση μεγαλύτερης ταχύτητας.



Σχήμα 1.10 Hub and spoke τοπολογία



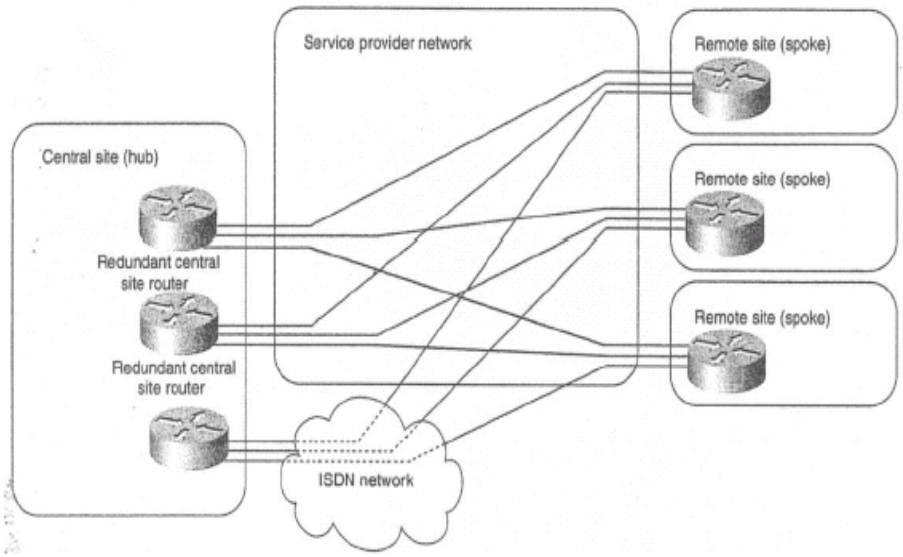
Σχήμα 1.11 Hub and spoke τοπολογία με δύο κεντρικούς δρομολογητές

Η υλοποίηση πλεονάζουσας (redundant) hub and spoke τοπολογίας με Overlay VPN μοντέλο βασισμένο σε VC, παρουσιάζει μια σειρά από προκλήσεις. Κάθε spoke τοποθεσία απαιτεί ένα VC προς τουλάχιστον δύο κεντρικούς δρομολογητές. Αυτά τα VCs μπορούν να είναι παρέχονται στη λογική της primary-backup διάταξης ή σε μια διάταξη διαμοιραζόμενου φορτίου λύσεις που έχουν μια σειρά από προβλήματα όπως:

1. Στη διάταξη primary-backup, το εφεδρικό (back-up) VC είναι αχρησιμοποίητο ενώ το πρωτεύον VC είναι ενεργό, έχοντας σα αποτέλεσμα πλεονάζουσες δαπάνες από τον πελάτη.

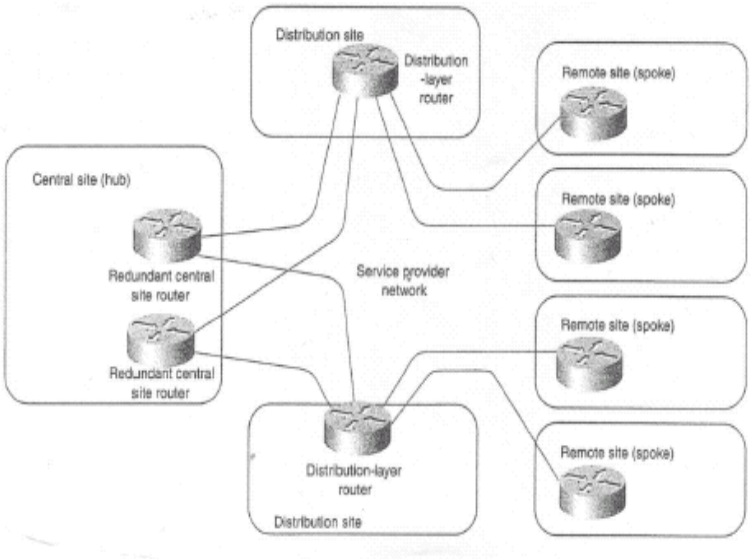
2. Στη διάταξη διαμοιραζόμενου φορτίου, η hub and spoke τοποθεσία αντιμετωπίζει μειωμένο throughput εάν ένα από τα VCs (ή ένας από τους κεντρικούς δρομολογητές) αποτύχει. Οι πάροχοι υπηρεσιών υψηλής ποιότητας προσπαθούν να ικανοποιήσουν τις απαιτήσεις των πελατών τους για εφεδρικές συνδέσεις με προηγμένες υπηρεσίες που προσφέρουν shadow PVCs. Με το shadow PVC ο πελάτης παίρνει δύο εικονικά κυκλώματα στην τιμή του ενός, στην περίπτωση όπου μπορούν να χρησιμοποιήσουν μόνο μια VC για κίνηση δεδομένων. Ένα μικρό σύνολο της κίνησης αφήνεται στη δεύτερη PVC ώστε να επιτρέψει αλλαγές πρωτοκόλλου δρομολόγησης πάνω στη δεύτερη PVC. Οι επιπλέον απαιτήσεις μπορούν να περιπλέξουν παραπάνω την hub and spoke τοπολογία με την εισαγωγή dial-backup χαρακτηριστικών.

3. Η dial-backup λύση εφαρμόζεται μέσω του δικτύου παρόχου υπηρεσίας, (για παράδειγμα μια ISDN σύνδεση φτιάχνει ένα αντίγραφο σε μια Frame Relay μισθωμένη γραμμή όπως φαίνεται στο Σχήμα 1.12) είναι προφανής σε ένα πελάτη αλλά δεν προσφέρει πραγματικά πλεονασμό επειδή δεν μπορεί να ανιχνεύσει πιθανές αποτυχίες (για παράδειγμα CPE ή αποτυχίες πρωτοκόλλων διακόσμησης). Ο πραγματικός end-to-end πλεονασμός σε ένα Overlay VPN Μοντέλο μπορεί να επιτευχθεί μόνο μέσω CPE συσκευών εγκαθιστώντας μια Dial-up σύνδεση έξω από μια VPN περιοχή.



Σχήμα 1.12 Dial Backup Λύση εντός ενός δικτύου παρόχου υπηρεσίας

Συνήθως μια απλή hub and spoke τοπολογία μετατρέπεται σε μια πολυεπίπεδη τοπολογία καθώς το δίκτυο αυξάνεται. Η πολυεπίπεδη τοπολογία μπορεί να είναι μια recursive τοπολογία hub and spoke, (όμοια με το Σχήμα 1.13) ή μια υβριδική τοπολογία η οποία αναλύεται αργότερα σε αυτό το κεφάλαιο.



Σχήμα 1.13 Πολυεπίπεδη hub and spoke τοπολογία

Η hub and spoke τοπολογία που εφαρμόζεται με ένα Overlay VPN μοντέλο είναι καλά προσαρμοσμένη σε περιβάλλον όπου απομακρυσμένες υπηρεσίες ανταλλάσσουν δεδομένα σε μεγαλύτερη κλίμακα με τις κεντρικές τοποθεσίες παρά μεταξύ τους, καθώς τα δεδομένα ανταλλάσσονται μεταξύ των απομακρυσμένων λειτουργιών συνήθως μέσα στις κεντρικές τοποθεσίες. Αν το πλήθος των απομακρυσμένων πληροφοριών που ανταλλάσσονται αντιπροσωπεύει ένα ορισμένο μερίδιο της συνολικής κίνησης του δικτύου, η partial-mesh τοπολογία ή η full-mesh τοπολογία μπορεί να είναι πιο κατάλληλες.

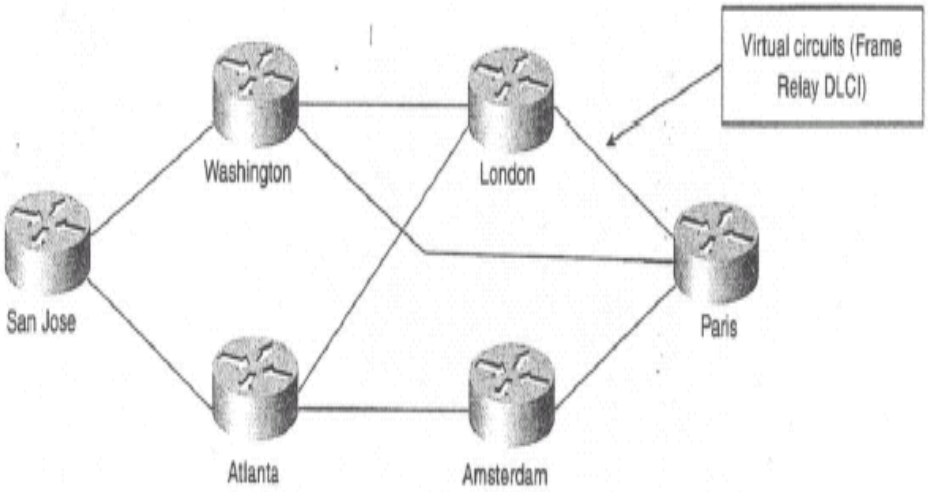
1.4.2 Τοπολογία Πλήρους ή Μερικού πλέγματος

Δεν μπορούν όλοι οι πελάτες να εφαρμόσουν τα δίκτυα τους χρησιμοποιώντας την hub-and-spoke τοπολογία για πολλούς λόγους:

1. Ο οργανισμός μπορεί να είναι λιγότερο ιεραρχικός στη δομή, απαιτώντας ανταλλαγή δεδομένων μεταξύ πολλών σημείων μέσα στον οργανισμό.

2. Το πρότυπο ανταλλαγής δεδομένων των εφαρμογών βασίζεται σε peer-to-peer επικοινωνία (συστήματα μηνυμάτων ή συστήματα επεξεργασίας).

3. Για κάποιες πολυεθνικές εταιρίες, το κόστος της hub and spoke τοπολογίας ίσως να είναι υπερβολικό εξαιτίας του υψηλού κόστους των διεθνών συνδέσεων. Σε αυτές τις περιπτώσεις το Overlay VPN μοντέλο που θα ήταν προτιμητέο θα ήταν το μερικού πλέγματος (partial-mesh), διότι οι τοποθεσίες στα VPN που θα είναι συνδεδεμένες μέσω των VCs, θα λάμβαναν υπόψη τις απαιτήσεις κίνησης (που τελικώς θα είναι υπαγορευμένες από τις απαιτήσεις επιχείρησης). Έτσι δεν θα είναι συνδεδεμένες όλες οι τοποθεσίες με όλες τις άλλες (Σχήμα 1.14). Αυτή η τοπολογία λέγεται partial mesh. Εάν κάθε τοποθεσία έχει συνδεσιμότητα με όλες τις άλλες τοποθεσίες η τοπολογία λέγεται full mesh.



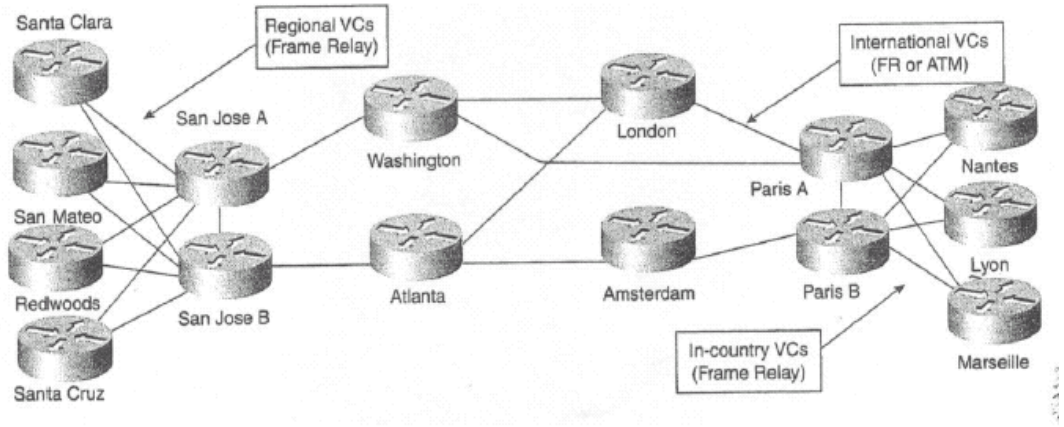
Σχήμα 1.14 Παράδειγμα ενός Partial mesh

Η υλοποίηση μιας full mesh τοπολογίας είναι αρκετά απλή, το μόνο που απαιτείται είναι ένα πλέγμα (matrix) που να υποδεικνύει την κίνηση μεταξύ των σταθμών, το απαιτούμενο εύρος ζώνης μεταξύ δύο τοποθεσιών του VPN και εν συνεχεία να γίνει δέσμευση των VCs από τον πάροχο υπηρεσίας. Από την άλλη μεριά η υλοποίηση μιας partial mesh τοπολογίας μπορεί να είναι μια πραγματική πρόκληση, καθώς πρέπει να γίνουν τα ακόλουθα:

1. Υπολογισμός της κίνησης του πλέγματος.
2. Σχεδίαση μιας partial mesh τοπολογίας βασισμένη σε μια κίνηση πλέγματος και επιπλέον λειτουργίες.
3. Καθορισμός επακριβώς πάνω σε ποίου VC την κίνηση, ανάμεσα σε δύο τοποθεσίες, η κίνηση θα αρχίσει να ρέει. Αυτό το βήμα θα πρέπει επίσης να αναμιγνύει ένα ρυθμισμένο routing protocol ότι η κίνηση ρέει πάνω στα σωστά Vcs.
4. Μέτρηση του μεγέθους των VCs σε σχέση με την κίνηση του πλέγματος και το άθροισμα της κίνησης πάνω στα VCs.

1.4.3 Υβριδική Τοπολογία

Μεγάλα VPN χτισμένα με Overlay VPN μοντέλο τείνουν να συνδυάσουν την hub and spoke τοπολογία με την partial mesh τοπολογία. Για παράδειγμα, ένας μεγάλος πολυεθνικός οργανισμός μπορεί να έχει δίκτυα πρόσβασης σε κάθε χώρα που εφαρμόζεται μία hub and spoke τοπολογία, ενώ το κεντρικό διεθνές δίκτυο θα πρέπει να εφαρμόζεται με μια full mesh τοπολογία (Σχήμα 1.15).



Σχήμα 1.15 Παράδειγμα μιας Υβριδικής τοπολογίας

Η καλύτερη προσέγγιση στο σχεδιασμό υβριδικής τοπολογίας είναι να ακολουθηθεί η προσέγγιση κλασσικού ιεραρχικού σχεδιασμού δικτύου.

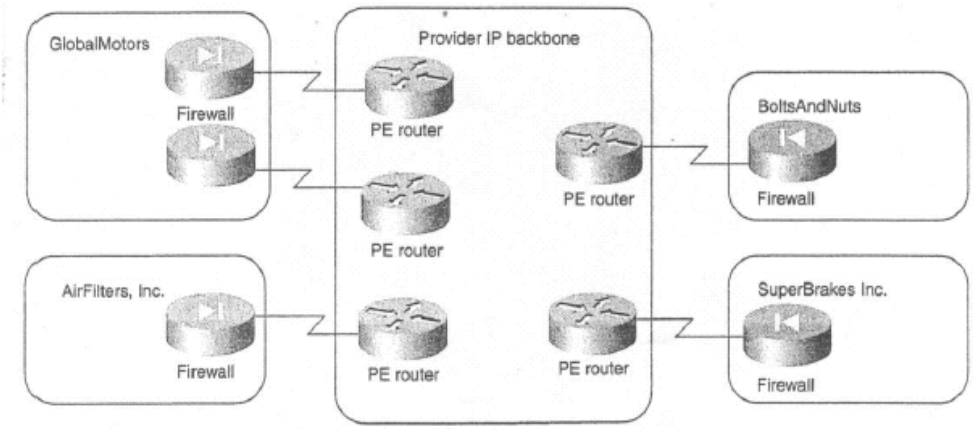
- Να διαιρεθεί το συνολικό δίκτυο σε πυρήνα, κατανεμημένα και δίκτυα πρόσβασης
- Να σχεδιαστεί ο πυρήνας και τα τμήματα πρόσβασης του δικτύου ατομικά (για παράδειγμα, Hub and spoke με dial backup στο δίκτυο πρόσβασης με το partial mesh στο κεντρικό δίκτυο
- Να συνδεθεί το κεντρικό δίκτυο και το δίκτυο πρόσβασης, μέσα από το επίπεδο διανομής με ένα τρόπο που να τα απομονώνει όσο το δυνατόν καλύτερα. Για παράδειγμα, ένα λάθος στον τοπικό βρόγχο σε ένα απομακρυσμένο γραφείο δεν θα πρέπει να αναμεταδίδεται μέσα στο κεντρικό δίκτυο. Ομοίως οι δρομολογητές του απομακρυσμένου γραφείου δεν θα πρέπει να αντιλαμβάνονται την αποτυχία ενός εκ των διεθνών συνδέσμων.

1.4.4 Τοπολογία Απλού Extranet

Οι Intranet τοπολογίες, που έχουν συζητηθεί ως τώρα, σχετίζονται περισσότερο με τη φυσική και τη λογική τοπολογία του VPN δικτύου, καθώς υπαγορεύονται από την VC τεχνολογία την οποία το Overlay VPN μοντέλο εφαρμόζει. Οι Extranet τοπολογίες εστιάζονται περισσότερο στις απαιτήσεις ασφαλείας του VPN δικτύου, το οποίο μπορεί να είναι εφαρμόσιμο με έναν αριθμό από διαφορετικές τεχνολογίες, είτε με το Overlay ή με το peer-to-peer μοντέλο

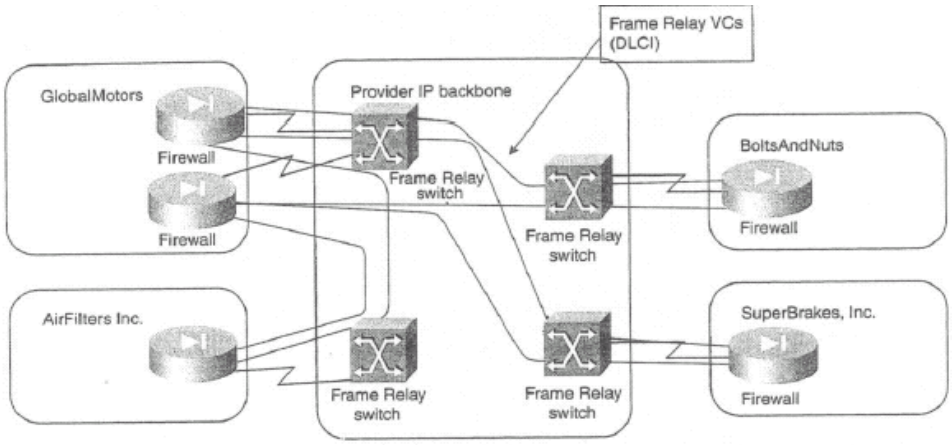
Η παραδοσιακή extranet τοπολογία μπορεί να είναι ένα extranet που επιτρέπει σε έναν αριθμό από εταιρίες να εκτελούν any-to-any ανταλλαγή δεδομένων. Για παράδειγμα μπορεί να περιλαμβάνει εταιρίες με κοινά ενδιαφέροντα (αεροπορικές εταιρίες, κατασκευαστικές αεροπλάνων κτλ), ή μια αλυσίδα εφοδιασμού (κατασκευαστές αυτοκινήτων και όλους τους προμηθευτές τους). Τα δεδομένα σε ένα τέτοιο extranet μπορεί να ανταλλάσσονται μεταξύ οποιουδήποτε αριθμό από τοποθεσίες. Το extranet από μόνο του δεν επιβάλει κανένα περιορισμό στην ανταλλαγή δεδομένων. Συνήθως κάθε τοποθεσία είναι υπεύθυνη για την δικιά της προστασία, φιλτράρισμα κίνησης και firewalling. Ο μόνος λόγος χρησιμοποίησης ενός extranet αντί του κοινού Internet είναι η ποιότητα υπηρεσίας που αυτό εγγυάται και η ευαισθησία των δεδομένων που ανταλλάσσονται πάνω σε ένα τέτοιο VPN δίκτυο, το οποίο είναι ακόμα ποιο ανθεκτικό σε επιθέσεις δεδομένων από ότι το γενικό Internet.

Εάν το Extranet εφαρμόζεται πάνω από ένα peer-to-peer μοντέλο (Σχήμα 1.16), κάθε οργανισμός καθορίζει μόνο πόσο κίνηση πρόκειται να λάβει και να στείλει από κάθε μια από τις τοποθεσίες. Με αυτό τον τρόπο ο εφοδιασμός και η πρόσβαση στη πλευρά του πελάτη και του παρόχου είναι πολύ απλή και αποτελεσματική.



Σχήμα 1.16 Παράδειγμα Extranet εφαρμοσμένο με Peer-to-Peer VPN μοντέλο

Παρόλα αυτά στο Overlay VPN μοντέλο η κίνηση μεταξύ των τοποθεσιών ανταλλάσσεται πάνω στο point-to-point VC, όμοια με το Σχήμα 1.17.



Σχήμα 1.17 Παράδειγμα Extranet εφαρμοσμένο με Overlay VPN μοντέλο

Στην extranet τοπολογία που είναι όμοια με αυτή στο Σχήμα 1.17, κάθε συμμετέχων οργανισμός συνήθως πληρώνει για τα VCs που χρησιμοποιεί. Φαινομενικά μόνο το απολύτως απαραίτητο VC εγκαθιδρύεται ώστε να ελαχιστοποιείται το κόστος. Ακόμα περισσότερο, οι συμμετέχοντες σε ένα τέτοιο VPN θα προσπαθήσουν να εμποδίσουν την δρομολόγηση κίνησης μεταξύ άλλων συμμετεχόντων με σκοπό να την προωθήσουν VCs που πληρώνουν άλλοι, έχοντας συνήθως σαν αποτέλεσμα τη μερική μόνο συνδεσιμότητα μεταξύ των τοποθεσιών στο extranet και μερικές φορές

τα προβλήματα στη βελτιστοποίηση της δρομολόγησης. Συνεπώς το VPN μοντέλο είναι ο προτιμότερος τρόπος εφαρμογής ενός any-to-any extranet.

1.4.5 Extranet Κεντρικών Υπηρεσιών

Οι οργανισμοί που σχετίζονται με συνδεσμολογία extranet και που ανήκουν στην ίδια ομάδα ενδιαφέροντος, είναι συχνά αρκετά ανοιχτοί, επιτρέποντας any-to-any συνδεσιμότητα μεταξύ των οργανισμών. Τα extranets επιτελούν ένα σκοπό (για παράδειγμα, ένα δίκτυο διαχείρισης αλυσίδας εφοδιασμού συνδέει έναν οργανισμό με όλους τους προμηθευτές του) και τείνουν να είναι περισσότερο κεντρικοποιημένα και επιτρέπουν την επικοινωνία μεταξύ των οργανισμών, χρήζοντας το extranet και όλους τους άλλους συμμετέχοντες.

Άλλα παραδείγματα ενός τέτοιου extranet περιλαμβάνουν δίκτυα χρηματιστηριακών συναλλαγών, όπου κάθε μεσίτης μπορεί να επικοινωνήσει με το χρηματιστήριο, αλλά όχι με άλλους μεσίτες ή οικονομικά δίκτυα χτισμένα μεταξύ εμπορικών τραπεζών και της κεντρικής τράπεζας. Αν και οι σκοποί ενός τέτοιου extranet μπορούν να ποικίλουν αρκετά, όλοι μοιράζονται μια γενική ιδέα. Ένας αριθμός διαφορετικών χρηστών δέχεται πρόσβαση σε μια κεντρική υπηρεσία (που περιλαμβάνει λογισμικό, εξυπηρετητές, τοποθεσία, δίκτυο κ.λ.π.).

Η ασφάλεια στις extranet κεντρικές υπηρεσίας τυπικά εξασφαλίζεται από τον κεντρικό οργανισμό που χορηγεί το extranet. Άλλοι συμμετέχοντες με mission-critical δίκτυα (για παράδειγμα, εταιρίες χρηματιστηριακών συναλλαγών ή κεντρικές τράπεζες) ίσως θέλουν να εφαρμόσουν τα δικά τους μέτρα ασφαλείας (για παράδειγμα, ένα firewall μεταξύ των internal δικτύων τους και του extranet).

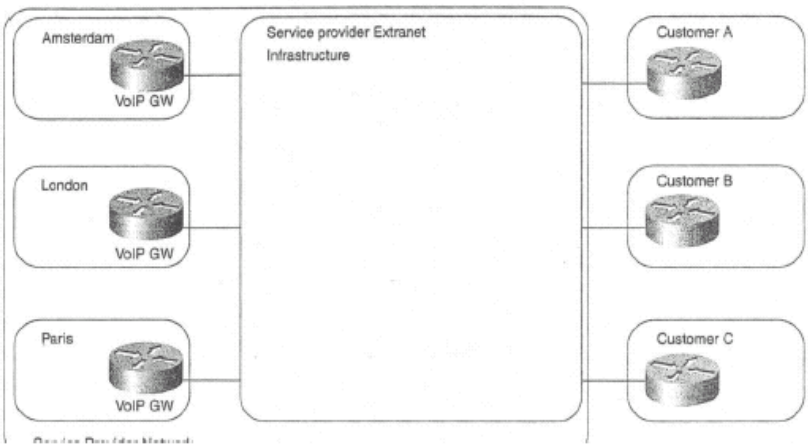
Όμοια με κάθε άλλο VPN δίκτυο, οι extranet κεντρικές υπηρεσίες μπορεί να είναι εφαρμοσμένες είτε με peer-to-peer ή Overlay VPN μοντέλο. Σε αυτή την περίπτωση, το peer-to-peer μοντέλο έχει αναμφισβήτητα μειονεκτήματα, επειδή ο πάροχος

υπηρεσίας πρέπει να προσέχει αρκετά ότι οι συμμετέχοντες του extranet δεν μπορούν να φτάσουν ο ένας στον άλλο.
Αντιθέτως, η υλοποίηση των κεντρικών υπηρεσιών extranet από ένα VPN μοντέλο είναι πολύ απλή και ακολουθεί τα παρακάτω βήματα:

1. Παρέχονται τα VCs μεταξύ όλων των συμμετεχόντων και της κεντρικής τοποθεσίας. Το μέγεθος κάθε VC ανταποκρίνεται στις απαιτήσεις κίνησης μεταξύ του συμμετέχοντος και της κεντρικής τοποθεσίας.
2. Η κεντρική τοποθεσία ανακοινώνει τα υποδίκτυα που είναι διαθέσιμα μόνο στην κεντρική τοποθεσία, στους υπόλοιπους συμμετέχοντες.
3. Η κεντρική τοποθεσία φιλτράρει την κίνηση που προέρχεται από άλλους συμμετέχοντες ώστε να σιγουρέψει πως δεν θα υπάρξει πρόβλημα δρομολόγησης ή σκόπιμη theft-of-service επίθεση η οποία θα επηρεάσει την σταθερότητα του VPN.

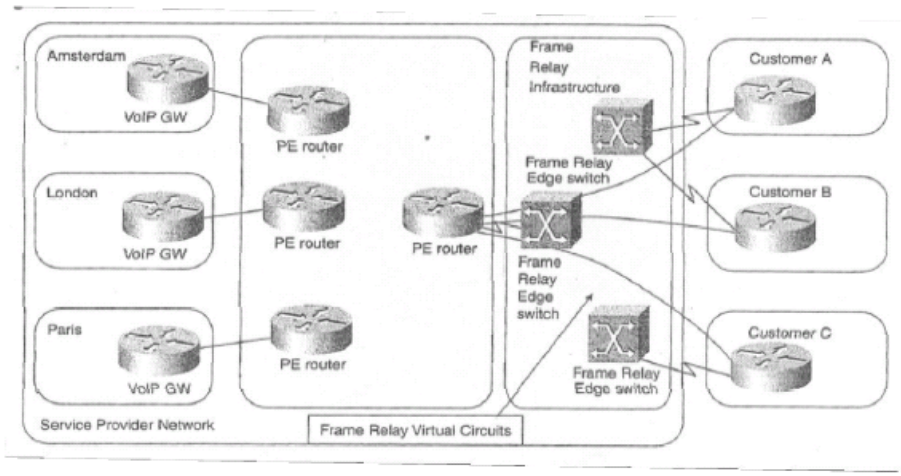
Ακολουθώντας τα τρία παραπάνω βήματα, το VPN δίκτυο του σχήματος Σχήμα 1.18 μετατρέπεται σε μια VC τοπολογία στο Σχήμα 1.17.

Μια ελάχιστα πιο πολύπλοκη τοπολογία extranet κεντρικών υπηρεσιών, ίσως να περιλαμβάνει έναν αριθμό από servers διασκορπισμένους κατά μήκος αρκετών τοποθεσιών και ένας αριθμός από τοποθεσίες πελάτη να έχουν πρόσβαση σε αυτούς τους servers, όμοια με το setup στο Σχήμα 1.18. Τυπικά παραδείγματα που θα απαιτούσαν αυτή την τοπολογία, εκφράζονται πάνω στα IP δίκτυα, όπου ένας αριθμός από χρήστες έχουν πρόσβαση σε κοινές πύλες, σε διαφορετικές πόλεις ή χώρες.



Σχήμα 1.18 Κεντρικές Υπηρεσίες με ένα μεγάλο αριθμό από Server τοποθεσίες

Ένα τέτοιο extranet μπορεί επίσης να υλοποιηθεί είτε με peer-to-peer μοντέλο ή με Overlay VPN μοντέλο. Ο αριθμός των VCs που απαιτείται στο Overlay VPN μοντέλο και η αντίστοιχη δημιουργούμενη πολυπλοκότητα συνήθως αποτρέπει από την υιοθέτηση του Overlay VPN μοντέλο σε αυτά τα σενάρια. Μια περισσότερο διαχειρίσιμη διαμόρφωση δικτύου θα χρησιμοποιούσε είτε ένα peer-to-peer μοντέλο είτε ένα συνδυασμό και των δύο μοντέλων, όπως απεικονίζεται στο Σχήμα 1.19.

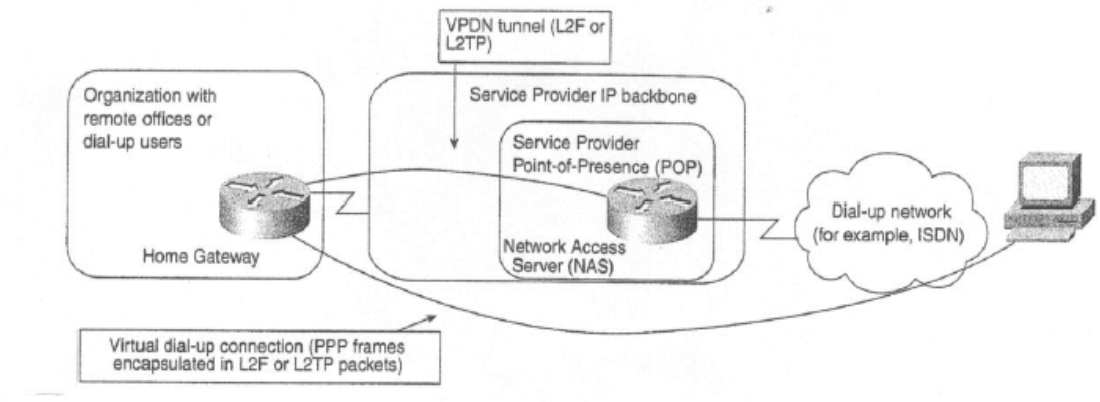


Σχήμα 1.19 Συνδυασμός από Peer-to-peer VPN με Overlay VPN

Λογικά, το δίκτυο στο Σχήμα 1.19 χρησιμοποιεί ένα peer-to-peer μοντέλο με δρομολογητή διανομής που δρά σαν PE δρομολογητής του peer-to-peer μοντέλου. Η πραγματική φυσική τοπολογία διαφέρει από την λογική όψη: Οι δρομολογητές διανομής είναι συνδεδεμένοι με τις τοποθεσίες του πελάτη (CE δρομολογητή) μέσω του Overlay μοντέλου (για παράδειγμα το Frame Overlay Network).

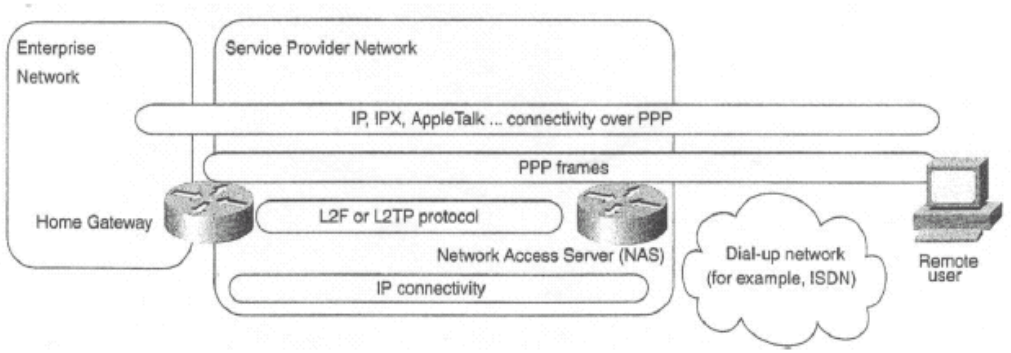
1.4.6 Τοπολογία VDPN

Η εικονική ιδιωτική Dial–up υπηρεσία (VDPN) (την περιγράψαμε στην προηγούμενη παράγραφο αυτού του κεφαλαίου 'Business Problem – based VPN Classification) συνήθως εφαρμόζεται ως tunneling PPP πλαίσια που ανταλλάσσονται μεταξύ του Dial – up user την home gateway του στα IP πακέτα που ανταλλάσσονται μεταξύ του network access server όπως φαίνεται στο Σχήμα 1.20.



Σχήμα 1.20 End-to-End συνδεσιμότητα σε μια VPDN λύση

Ο Dial – up χρήστης και η home gateway εγκαθιστούν IP (ή IPX, Appletalk κτλ) σύνδεση πάνω στο tunneled PPP σύνδεσμο και ανταλλάσσουν πακέτα δεδομένων πάνω σε αυτό. Το Σχήμα 1.21 δείχνει λεπτομερώς το φορτίο πρωτοκόλλου που χρησιμοποιείται μεταξύ διαφόρων μερών της VPDN λύσης.



Σχήμα 1.21 Στοίβα Πρωτοκόλλου σε μια VPDN λύση

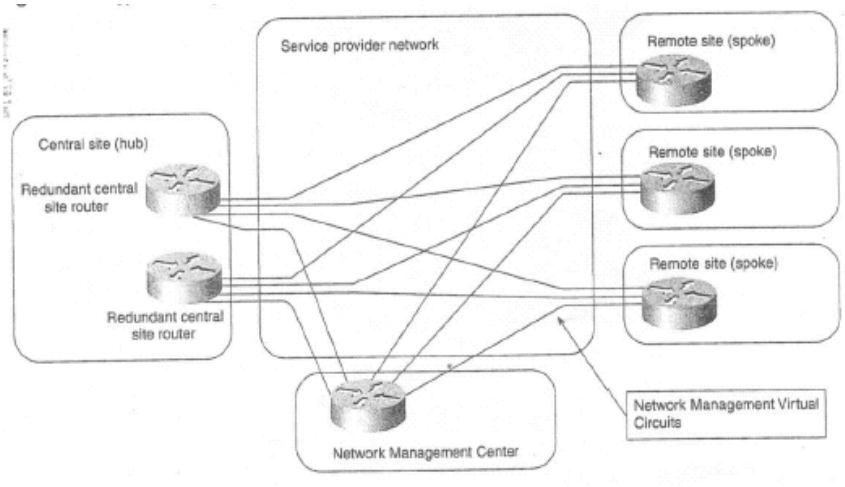
Κάθε VPDN λύση απαιτεί μία υποκείμενη IP υποδομή που αποτελεί τη βάση ώστε να ανταλλάσσει tunneled PPP πλαίσια μεταξύ του NAS και της home gateway. Στο απλούστερο σενάριο, το δημόσιο Internet μπορεί να χρησιμοποιηθεί ως η απαραίτητη υποδομή. Όταν οι απαιτήσεις ασφαλείας είναι αυστηρότερες, ένα VPN μπορεί να χρησιμοποιηθεί ώστε να ανταλλάσσει τα ενθυλακωμένα PPP πλαίσια.
Η συγκεκριμένη προσέγγιση θεωρείται ιδιαίτερα πολύπλοκη από μερικούς σχεδιαστές δικτύων. Η πολυπλοκότητα αυτή όμως μπορεί να γίνει κατανοητή αν γίνει ο παρακάτω διαχωρισμός:

- Ο NAS και η home gateway χρησιμοποιούν οποιαδήποτε IP υποδομή είναι διαθέσιμη, ώστε να ανταλλάξουν τα VPDN δεδομένα, τα οποία μπορούν να θεωρηθούν σαν μία αίτηση που δεν κάνει καμία ενέργεια στην κορυφή της IP ουράς. Συνεπώς η εσωτερική δομή της υποκείμενης IP υποδομής δεν επηρεάζει την ανταλλαγή των δεδομένων της αίτησης, και τα περιεχόμενα της αίτησης (τα IP πακέτα στα ενθυλακωμένα PPP πλαίσια σε ένα VPDN φάκελο) δεν αλληλεπιδρούν με τους δρομολογητές που παρέχουν την IP υπηρεσία.
- Το υποκείμενο IP δίκτυο θεωρείται ένα extranet κεντρικών υπηρεσιών με πολλές τοποθεσίες εξυπηρετητών (NES), και μία home gateway η οποία δρα σαν τοποθεσία πελάτης. Αυτή η υποδομή μπορεί να υλοποιηθεί με μια σειρά από τρόπους, από το αμιγώς Overlay VPN μοντέλο ως το αμιγώς peer–to–peer μοντέλο.

1.4.7 Τοπολογία Διαχειριζόμενου Δικτύου VPN

Η τελευταία VPN τοπολογία που αναλύεται σε αυτό το κεφάλαιο, είναι η τοπολογία που χρησιμοποιείται από τους παρόχους υπηρεσίας ώστε να διαχειρίζονται αποτελεσματικά τους δρομολογητές των πελατών τους μέσω σαφώς ορισμένων υπηρεσιών διαχείρισης δικτύου.

Σε μια τυπική διαμόρφωση, που φαίνεται στο Σχήμα 1.22 ο πάροχος υπηρεσίας προμηθεύει έναν αριθμό από δρομολογητές, συνδέοντας αυτούς μέσω των VCs που εφαρμόζονται με ATM η Frame Relay και χτίζει μία διαχωρισμένη hub-and-spoke τοπολογία συνδέοντας κάθε πελάτη – δρομολογητή με το NMC (Network Management Center).



Σχήμα 1.22 Τυπική τοπολογία δικτύου διεύθυνσης

Η VPN τοπολογία που χρησιμοποιείται στο τμήμα πελάτης του δικτύου μπορεί να είναι κάθε τοπολογία που υποστηρίζεται με το VPN μοντέλο που αποτελεί την κύρια βάση, που κυμαίνεται από την hub-and-spoke στη full mesh τοπολογία. Η τοπολογία που χρησιμοποιείται στο CPE μέρος διεύθυνσης του δικτύου, αποτελεσματικά θα μπορούσε να ήταν μία κεντρική extranet υπηρεσιών τοπολογία με τους δρομολογητές πελάτες να λειτουργούν σαν πελάτες και το Κέντρο Διαχείρισης Δικτύων (Network Management Center) να γίνεται η κεντρική τοποθεσία του extranet διεύθυνσης.

Όπως εξηγήθηκε στην παράγραφο Central – services – Extranet νωρίτερα σε αυτό το κεφάλαιο- τέτοια τοπολογία είναι ευκολότερο να υλοποιηθεί με μία hub-and-spoke τοπολογία του Overlay VPN μοντέλου, το οποίο επίσης εξηγεί γιατί οι περισσότεροι διαχειριστές δικτύων των παρόχων υπηρεσιών χρησιμοποιούν το setup του Σχήμα 1.22.

1.5 Σύνοψη

Τα VPN γίνεται να κατηγοριοποιηθούν με μια σειρά από κριτήρια. Η ευρύτερη τεχνολογική ιεράρχηση είναι βασισμένη πάνω στο τρόπο που η πληροφορία δρομολόγησης ανταλλάσσεται μέσα στο VPN.

Στο peer-to-peer VPN μοντέλο η πληροφορία δρομολόγησης του πελάτη ανταλλάσσεται μεταξύ των δρομολογητών του πελάτη και των δρομολογητών του προμηθευτή υπηρεσίας.

Στο Overlay VPN μοντέλο ο προμηθευτής υπηρεσίας εξασφαλίζει μόνο τα VCs (λογικές μισθωμένες γραμμές) και η πληροφορία δρομολόγησης ανταλλάσσεται επακριβώς μεταξύ των ακριανών δρομολογητών του πελάτη.

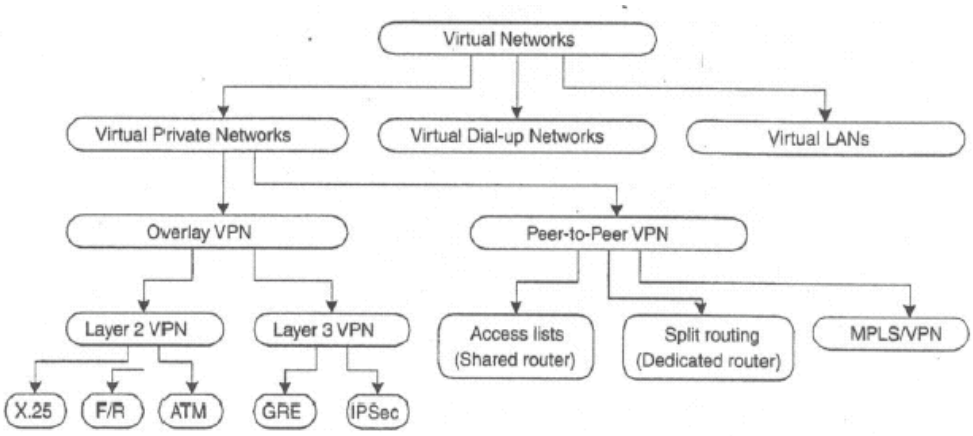
Τα δυο μοντέλα μπορεί να είναι συνδυασμένα σε ένα μεγάλο δίκτυο παρόχου υπηρεσίας: Το Peer-to-Peer ίσως να χρησιμοποιεί Overlay VPN μοντέλο στα τμήματα πρόσβασης (για παράδειγμα, οι πελάτες συνδέονται στους δρομολογητές ακριανού παρόχου μέσα από το Frame Relay) ή στο πυρήνα του.

Η πιο λεπτομερή VPN ιεράρχηση (απεικονίζεται στο Σχήμα 1.23) εστιάζει πάνω στη υποκείμενη τεχνολογία που χρησιμοποιείται στα πακέτα μεταφοράς του Επιπέδου 3 πάνω στο VPN.

Το Overlay VPN μοντέλο μπορεί να υλοποιηθεί με Επιπέδου 2 WAN τεχνολογίες μεταγωγής (X.25, SMDN, Frame Relay, ATM) ή tunneling τεχνολογίες Επιπέδου 3 (IP-over-IP, IPSec).

Το Peer-to-Peer VPN μοντέλο μπορεί να υλοποιείται παραδοσιακά με χρήση πολύπλοκων τεχνικών δρομολόγησης ή IP λίστες εισόδου, έχοντας και τα δύο έναν αριθμό από ελαττώματα που έχουν περιγραφεί στην παράγραφο «Peer-to-Peer VPN μοντέλο».

Το MPLS based VPN συμπληρώνει τις αδυναμίες άλλων Peer-to-Peer VPN τεχνολογιών. Αφήνοντας τους παρόχους υπηρεσίας να συνδυάζουν τα προτερήματα του Peer-to-Peer μοντέλου (απλούστερη δρομολόγηση, απλούστερη εφαρμογή των απαιτήσεων του πελάτη) με την ασφάλεια και την απομόνωση που κληρονομούνται από το Overlay VPN μοντέλο.



Σχήμα 1.23 VPN ιεράρχηση βασισμένη πάνω στις βαθύτερες τεχνολογίες

2. Το IPSec Πρωτόκολλο

2.1 Εισαγωγή στο IPSec

Το 1992 η IETF (Internet Engineering Task Force) ξεκίνησε την ανάπτυξη μιας σουίτας πρωτοκόλλων, που είχε ως σκοπό την ασφάλεια του δικτύου ανεξάρτητα από τις εφαρμογές. Η ασφάλεια θα επιτυγχάνονταν με την προσθήκη πρωτοκόλλων στο επίπεδο δικτύου τα οποία θα πρόσφεραν υπηρεσίες ασφάλειας. Η σουίτα αυτή ονομάστηκε IPSec (Internet Protocol Security) και αναπτύσσεται από την ομάδα IP Security.

Οι βασικοί στόχοι του IPSec, είναι:

- Τα πρωτόκολλα να αναπτυχθούν στο τρίτο επίπεδο (επίπεδο δικτύου).
- Να προσφέρει μυστικότητα, ακεραιότητα και έλεγχο πρόσβασης στα ανώτερα επίπεδα.
- Να είναι ανεξάρτητο από τις εφαρμογές και η υλοποίηση του να μην απαιτεί αλλαγές στις εφαρμογές.
- Να είναι ανεξάρτητο από αλγόριθμους κρυπτογράφησης και πιστοποίησης (ένα κοινό σύνολο από αλγόριθμους θα πρέπει να υλοποιείται σε κάθε σύστημα για να εξασφαλίζεται η διαλειτουργικότητα).
- Να είναι συμβατό με τα υπάρχοντα πρωτόκολλα.

Οι υπηρεσίες ασφάλειας που προσφέρει το IPSec είναι:

- Περιορισμός πρόσβασης. Ο περιορισμός πρόσβασης είναι μια υπηρεσία ασφάλειας, που αποτρέπει την μη εξουσιοδοτημένη χρήση ενός πόρου. Για ένα σταθμό (host) οι πόροι αυτοί μπορεί να είναι, τα δεδομένα του και η επεξεργαστική του ισχύς. Για μία ασφαλή πύλη αυτοί οι πόροι μπορεί να είναι, το δίκτυο πίσω από αυτή και οι το εύρος ζώνης της διασύνδεσης του με τα υπόλοιπα δίκτυα.

- Πιστοποίηση. Λέγοντας πιστοποίηση για το IPSec, εννοούμε την πιστοποίηση της προέλευσης των δεδομένων. Δηλαδή την διαβεβαίωση ότι τα δεδομένα ήρθαν από τον αρχικό παραλήπτη, χωρίς παραποίηση.
- Εμπιστευτικότητα. Η εμπιστευτικότητα είναι μια υπηρεσία ασφάλειας, που προστατεύει τα δεδομένα από μη εξουσιοδοτημένη πρόσβαση. Το IPSec προστατεύει όλα τα δεδομένα των ανώτερων επιπέδων κρυπτογραφώντας τα. Τα μόνα δεδομένα τα οποία δεν μπορεί να κρυπτογραφήσει, είναι κάποια δεδομένα τα οποία χρησιμοποιούνται για την δρομολόγηση.
- Ακεραιότητα. Το IPSec υποστηρίζει δυο μορφές ακεραιότητας: μία που αφορά την ακεραιότητα του κάθε πακέτου και μία που προστατεύει από την πολλαπλή αποστολή των ίδιων πακέτων. Τις παραπάνω υπηρεσίες τις προσφέρει το IPSec, εφαρμόζοντας τα πρωτόκολλα ασφάλειας AH (Authentication Header) και ESP (Encapsulation Security Payload).

2.2 IPSec Protocol Framework

Το πλαίσιο λειτουργίας των πρωτοκόλλων του IPSec περιγράφει τις βασικές έννοιες και δομές που χρησιμοποιούνται στην υλοποίηση του IPSec. Βασικά στοιχεία στη λειτουργία του πλαισίου αποτελούν οι συσχετίσεις ασφαλείας (Security Associations) και η διαχείριση τους.

2.2.1 Συσχέτιση Ασφάλειας SA (Security Association)

Συσχέτιση ασφάλειας είναι ένα κατασκεύασμα για την επιβολή πολιτικής ασφάλειας σε ένα περιβάλλον που υλοποιεί IPSec. Συσχέτιση ασφάλειας θεωρούμε μία μονόδρομη λογική σύνδεση μεταξύ δύο συστημάτων που χρησιμοποιούν IPSec. Για την σύνδεση των δύο αυτών συστημάτων απαιτούνται τουλάχιστον δύο συσχετίσεις ασφάλειας, μία για κάθε κατεύθυνση. Οι συσχετίσεις ασφάλειας μπορεί να είναι στατικές και να έχουν δημιουργηθεί από πριν για τα δυο συστήματα ή να δημιουργούνται δυναμικά όταν τα δύο συστήματα θέλουν να επικοινωνήσουν

χρησιμοποιώντας ένα πρωτόκολλο δημιουργίας και διαχείρισης συσχετίσεων, όπως το IKE.

Μία συσχέτιση ασφάλειας περιέχει όλες τις πληροφορίες που χρειάζεται ένα σύστημα για την δημιουργία και διαχείριση μίας (μονόδρομης) σύνδεσης. Οι πληροφορίες αυτές περιλαμβάνουν τους αλγόριθμους κρυπτογράφησης και πιστοποίησης, το πρωτόκολλο ασφάλειας που χρησιμοποιείται (AH ή ESP), το χρόνο ζωής της συσχέτισης ασφάλειας (αν δεν είναι στατική) και τον τρόπο με τον οποίο μετράται ο χρόνος ζωής (σε sec ή KB). Μία συσχέτιση ασφάλειας μπορεί να περιέχει μόνο ένα πρωτόκολλο ασφάλειας. Για να εφαρμόσουμε παραπάνω από ένα πρωτόκολλο ασφάλειας στην επικοινωνία δύο συστημάτων χρησιμοποιούμε μια δέσμη συσχετίσεων (SA bundle).

2.2.2 Δέσμη Συσχετίσεων (SA bundle)

Μια δέσμη συσχετίσεων είναι ένα σύνολο από συσχετίσεις ασφάλειας οι οποίες εφαρμόζονται σε μία (μονόδρομη) σύνδεση μεταξύ δύο ή περισσότερων συστημάτων υπό την απαίτηση μίας πολιτικής ασφάλειας. Η σειρά με την οποία εφαρμόζονται οι συσχετίσεις εξαρτάται από την πολιτική ασφάλειας. Οι συσχετίσεις ασφάλειας που περιέχονται σε μια δέσμη δεν τερματίζουν απαραίτητα στο ίδιο σύστημα. Για παράδειγμα μπορούμε να έχουμε δύο συσχετίσεις σε μια δέσμη, μία από ένα φορητό σταθμό με ένα firewall χρησιμοποιώντας το ESP (για να εξασφαλίσουμε μυστικότητα πάνω από ένα ανασφαλές δημόσιο δίκτυο) και μία δεύτερη συσχέτιση από τον φορητό σταθμό σε έναν σταθμό στο εσωτερικό δίκτυο της ασφαλής πύλης χρησιμοποιώντας το AH (για να προστατευτούμε από τυχόν spoofing επίθεση που έχει γίνει στην ασφαλή πύλη από το εσωτερικό δίκτυο).

2.2.3 Βάση Πολιτικής Ασφάλειας (SPD Security Policy Database)

Η βάση πολιτικής ασφάλειας ή SPD, περιέχει τις υπηρεσίες ασφάλειας που προσφέρονται στα πακέτα. Η SPD ορίζεται από τον διαχειριστή του συστήματος και αποτελεί ένα κεντρικό σημείο για επιβολή πολιτικής σε όλο το σύστημα.

Συνήθως οι υλοποιήσεις έχουν μία ξεχωριστή SPD για κάθε δικτυακή διασύνδεση (network interface) που έχει ενεργοποιημένο το IPSec η οποία έχει εγγραφές για εισερχόμενη και εξερχόμενη κίνηση. Η SPD εξετάζεται για όλα τα πακέτα, εισερχόμενα και εξερχόμενα, των δικτυακών διασυνδέσεων που έχουν ενεργοποιημένο το IPSec, συμπεριλαμβανομένων και των πακέτων στα οποία δεν προσφέρει τις υπηρεσίες του το IPSec. Τα πακέτα αυτά εξετάζονται, αφού όταν γίνεται αυτή η επεξεργασία δεν μπορούμε να ξέρουμε αν θα εφαρμοστεί σε αυτά ή όχι (η διαδικασία αυτή θα το κρίνει).

Για κάθε πακέτο πρέπει να υπάρχει μία εγγραφή στην SPD που θα αναφέρει πως θα επεξεργαστεί το πακέτο. Τα πακέτα ταιριάζουν στις πολιτικές της SPD με βάση τους selectors. Αν για ένα πακέτο δεν βρεθεί εγγραφή τότε το πακέτο απορρίπτεται και το γεγονός αναφέρεται στο σύστημα (π.χ. μέσω του syslog στο UNIX).

Υπάρχουν τρεις περιπτώσεις επεξεργασίας των πακέτων:

- Να απορριφθεί: το πακέτο δεν στέλνεται στο δίκτυο (εξερχόμενη κίνηση), δεν προωθείται στα ανώτερα πρωτόκολλα (εισερχόμενη κίνηση) και δεν δρομολογείται στο εσωτερικό δίκτυο.
- Να μην εφαρμοστεί IPSec: το πακέτο περνάει από την στοίβα χωρίς την επιπλέον προστασία του IPSec.
- Να εφαρμοστεί IPSec: στο πακέτο προσφέρονται υπηρεσίες ασφάλειας του IPSec. Ποιες υπηρεσίες πρωτόκολλα και αλγόριθμοι θα προσφερθούν περιέχεται στο SPD.

2.2.4 Selectors

Οι selectors είναι πεδία στα πακέτα με βάση τα οποία γίνεται η αντιστοίχηση των πακέτων σε πολιτικές ορισμένες στην SPD. Τα πεδία και ο τρόπος αντιστοίχησης θυμίζει την επεξεργασία των πακέτων από stateless firewalls.

Τυπικοί selectors που πρέπει να υποστηρίζει η κάθε υλοποίηση:

- IP διεύθυνση προορισμού.
- IP διεύθυνση πηγής.
- Όνομα (FQDN DNS ή X500).
- Πρωτόκολλο επιπέδου μεταφοράς (TCP, UDP,…).Μπορεί να είναι κρυπτογραφημένο από το ESP.
- Αριθμός θύρας πηγής και προορισμού στα TCP και UDP. Μπορεί να είναι κρυπτογραφημένο από το ESP.

2.2.5 Βάση Συσχετίσεων Ασφάλειας (SAD – Security Association Database)

Η βάση συσχετίσεων ασφάλειας (SAD) περιέχει τις ενεργές συσχετίσεις ασφάλειας ενός συστήματος και τις παραμέτρους των συσχετίσεων αυτών, όπως κρυπτογραφικούς αλγόριθμους, πρωτόκολλα ασφάλειας, χρόνο ζωής κ.α.. Για την εξερχόμενη κίνηση κάθε SA στην SAD συνδέεται με μία εγγραφή στην SPD. Αν το SA στην SAD δεν υπάρχει όταν γίνεται η σύνδεση των συστημάτων τότε δημιουργείται. Για την εισερχόμενη κίνηση, κάθε SA στην SAD αντιστοιχεί μοναδικά σε ένα συνδυασμό IP διεύθυνση προορισμού, IPSec πρωτόκολλο (AH ή ESP) και δείκτη παραμέτρων ασφάλειας (SPI).

2.3 Επεξεργασία Κίνησης

2.3.1 Εξερχόμενη IP Κίνηση

Κάθε εξερχόμενο πακέτο συγκρίνεται με την SPD για να καθοριστεί τι επεξεργασία θα επιβληθεί στο πακέτο. Αν το πακέτο θα απορριφθεί, αυτό θα αναφερθεί στο σύστημα (auditable event). Αν το πακέτο επιτρέπεται να περάσει, χωρίς την επιβολή του IPSec, τότε αυτό συνεχίζει την πορεία του χωρίς καμία περαιτέρω επεξεργασία από το IPSec. Αν για το πακέτο απαιτείται επιβολή υπηρεσιών του IPSec τότε αυτό αντιστοιχείται σε ένα SA ή SA bundle, ή ένα νέο SA ή SA bundle δημιουργείται για το πακέτο. Σε ένα σταθμό που υλοποιεί sockets, η SPD θα εξετάζεται κάθε φορά που δημιουργείται ένα socket για να αποφασιστεί αν θα προσφερθούν οι υπηρεσίες του IPSec στα πακέτα του socket.

2.3.2 Εισερχόμενη IP κίνηση

Πριν την επεξεργασία του AH ή του ESP τα τυχόν τμήματα του IP πακέτου (IP fragments) συναρμολογούνται. Τα πακέτα τα οποία θα επεξεργαστούν τα πρωτόκολλα AH και ESP αναγνωρίζονται από τον αντίστοιχο αριθμό του πρωτοκόλλου (51 και 50) στο πεδίο επόμενο πρωτόκολλο της επικεφαλίδας του IP. Κάθε πακέτο, το οποίο περιέχει AH ή ESP επικεφαλίδα, αντιστοιχίζεται σε μια συσχέτιση ασφάλειας (SA) σύμφωνα με την IP διεύθυνση προορισμού, το πρωτόκολλο ασφάλειας (AH ή ESP) και τον δείκτη παραμέτρων ασφάλειας.

Αν δεν βρεθεί συσχέτιση ασφάλειας στην SAD τότε το πακέτο απορρίπτεται και το γεγονός αναφέρεται στο σύστημα. Αν βρεθεί συσχέτιση ασφάλειας τότε στο πακέτο προσφέρονται οι υπηρεσίες του IPSec τις οποίες απαιτεί η πολιτική (π.χ. κρυπτογράφηση, πιστοποίηση). Εάν κατά την διάρκεια της επεξεργασίας προκύψει κάποιο σφάλμα τότε το πακέτο απορρίπτεται και το γεγονός αναφέρεται στο σύστημα. Αν η επεξεργασία τερματίσει με επιτυχία τότε το πακέτο προωθείται στα πρωτόκολλα επιπέδου μεταφοράς (σταθμός) ή δρομολογείται σε κάποια άλλη δικτυακή διασύνδεση (ασφαλής πύλη).

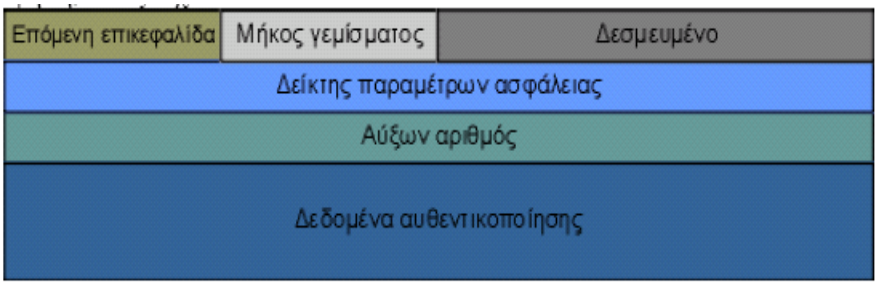
2.4 Τα Πρωτόκολλα του IPSec

Το Authenticated Header (AH) πρωτόκολλο είναι το πρωτόκολλο IPSec για την παροχή διαδικασιών αυθεντικοποίησης. Το Encapsulated Security Payload (ESP) πρωτόκολλο δίνει τη δυνατότητα για κρυπτογράφηση των δεδομένων. Παράλληλα παρέχει τη δυνατότητα αυθεντικοποίησης του αποστολέα. Το Internet Key Exchange (IKE) πρωτόκολλο χρησιμοποιείται για την αυτόματη παραγωγή & ανταλλαγή κλειδιών που χρησιμοποιούνται στα πλαίσια του IPSec.

Τα AH και ESP πρωτόκολλα υποστηρίζουν 2 τύπους λειτουργίας: μεταφοράς (transport) και σήραγγας (tunnel). Αυτοί οι δύο τρόποι λειτουργίας υποδεικνύουν το πώς θα δομηθεί το IPSec πακέτο. Ο τρόπος λειτουργίας με μεταφορά χρησιμοποιείται όταν και τα δύο άκρα του καναλιού ασφαλούς επικοινωνίας είναι hosts ενώ ο τρόπος λειτουργίας με σήραγγα χρησιμοποιείται όταν και τα δύο άκρα του καναλιού ασφαλούς επικοινωνίας είναι δικτυακές συσκευές (δρομολογητές ή/και firewalls)

2.4.1 Η επικεφαλίδα AH

Η επικεφαλίδα αυθεντικοποίησης (AH - Authentication Header) είναι ένα πρωτόκολλο του IPSec που χρησιμεύει στο να μας παρέχει πιστοποίηση της προέλευσης των δεδομένων, αξιοπιστία δεδομένων και προστασία επανάληψης. Το AH μπορεί να χρησιμοποιηθεί μόνο του ή σε συνδυασμό με το ESP. Σε σύγκριση με το ESP το AH δεν παρέχει κρυπτογράφηση των δεδομένων, αλλά προστατεύει τις επικεφαλίδες των πακέτων παρέχοντας αυθεντικοποίηση, κάτι που δεν κάνει από μόνο του το ESP, εκτός αν και αυτά τα πεδία εμπεριέχονται στη κρυπτογράφηση, όπως π.χ. στο tunnel mode.



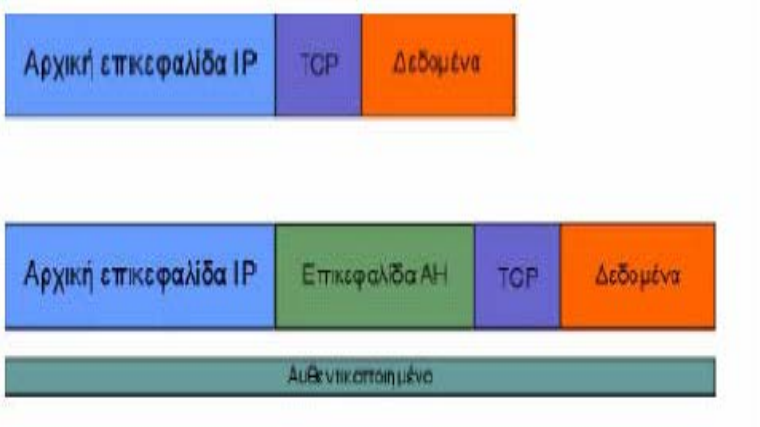
Σχήμα 2.1 Πεδία του Authentication Header (AH)

- Επόμενη επικεφαλίδα (next header). Είναι ένα πεδίο 8-bit που περιέχει τον τύπο του επόμενου σε σειρά τμήματος του πακέτου, μετά τον AH
- Μέγεθος πακέτου (payload length). Το μέγεθος του AH σε 32 bit χαρακτήρες
- Δεσμευμένος χώρος για μελλοντική χρήση.
- Δείκτης παραμέτρων ασφαλείας (security parameters index SPI). Ένας 32bit αριθμός που σε συνδυασμό με την διεύθυνση προορισμού και το ασφαλές πρωτόκολλο (AH) αναγνωρίζει μοναδικά μια ασφαλή διασύνδεση (SA) για το πακέτο.
- Αύξων αριθμός (sequence index). Ένας 32 bit αριθμός χρησιμοποιείται ως μετρητής για την προστασία επανάληψης
- Πληροφορίες Αυθεντικοποίησης (authentication data). Το πεδίο αυτό περιέχει το ICV του πακέτου. Είναι μεταβλητού μήκους το οποίο πρέπει να είναι πολλαπλάσιο του μήκους 32 bit. Αναλόγως με τον αλγόριθμο που χρησιμοποιούμε το πεδίο μπορεί να γεμίσει με κενές πληροφορίες έτσι ώστε να είναι ακριβές πολλαπλάσιο των 32 bit.

Τοποθεσία του Header

Το AH υποστηρίζει όπως και το ESP, μέθοδο μεταφοράς και μέθοδο σήραγγας. Στην μέθοδο μεταφοράς, το AH μπαίνει μετά την επικεφαλίδα IP του πακέτου και πριν από τις επικεφαλίδες των πρωτοκόλλων που βρίσκονται στο ανώτερο επίπεδο

(TCP,UDP,ICMP,OSFP και αλλά). Έτσι λοιπόν, η ενθυλάκωση της επικεφαλίδας AH στο πρωτόκολλο IPv4 γίνεται όπως φαίνεται και στο Σχήμα 2.2.



Σχήμα 2.2 ενθυλάκωση της επικεφαλίδας AH (transport mode)

Στο tunnel mode έχουμε δυο διαφορετικές επικεφαλίδες IP, την εσωτερική και την εξωτερική. Το AH μπαίνει μεταξύ τους και προστατεύει όλα τα εσωτερικά πακέτα και τα δεδομένα τους. Ο εσωτερικός IP header περιέχει τις πραγματικές IP διευθύνσεις των σταθμών και ο εξωτερικός τις διευθύνσεις των σταθμών που επικοινωνούν με IPsec.

Λειτουργία πρωτοκόλλου

Ένα πακέτο υπόκειται στον AH μόνο όταν το IPsec καθορίσει ότι το πακέτο ταυτίζεται με μια ασφαλή διασύνδεση. Όταν ένα πακέτο που περιέχει έναν AH φτάσει στον προορισμό του, ο δέκτης καθορίζει ένα SA βασισμένο στη IP διεύθυνση του προορισμού, στο πρωτόκολλο ασφάλειας (AH) και το SPI. Το SA καθορίζει αν ο αύξων αριθμός του πακέτου θα μαρκαριστεί και επιλέγει τον αλγόριθμο που θα χρησιμοποιηθεί για τον υπολογισμό του ICV όπως και το κλειδί για την αναγνώριση του ICV.

Κατάτμηση

Αν χρειαστεί κατάτμηση θα γίνει μετά την ολοκλήρωση του AH στο IPSec. Για αυτό στο transport mode ο AH εφαρμόζεται μόνο σε ολόκληρα πλαίσια δεδομένων του IP και όχι σε κομμάτια.

Τιμή ελέγχου γνησιότητας (Integrity Check Value)

Ο παραλήπτης υπολογίζει την τιμή ελέγχου γνησιότητας με βάση μερικά χαρακτηριστικά του πακέτου που θα αναφέρουμε παρακάτω. Αν αυτή η τιμή είναι ίδια με αυτή που περιέχεται στην επικεφαλίδα του AH τότε το πακέτο είναι γνήσιο, αν όχι, το πακέτο απορρίπτεται και η απόρριψη επισημαίνεται.

Το ICV υπολογίζεται από:

- Τα πεδία του IP header που δεν αλλάζουν ή που έχουν ένα
- προβλέψιμο αριθμό όταν θα φτάσει το πακέτο στον προορισμό του.
- Τον AH
- Από πληροφορίες που ανήκουν στα πιο πάνω επίπεδο και
- υποτίθεται ότι δεν αλλάζουν κατά τη μεταφορά.

Αν ένα πεδίο στο IP πακέτο μπορεί να αλλαχτεί τότε μηδενίζεται για τον υπολογισμό του ICV. Μηδενίζοντας τα πεδία που δεν χρησιμοποιούνται αντί να τα παραβλέπουμε προστατεύουμε το πακέτο και το μέγεθος των πεδίων του. Κάθε υλοποίηση του IPSec πρέπει να υποστηρίζει τους εξής αλγορίθμους αυθεντικοποίησης.

- HMAC-MD5-96 (RFC 2403)
- HMAC-SHA-1-96 (RFC 2404)

Αν σε ένα πακέτο το πεδίο πληροφοριών της αυθεντικοποίησης και πάλι δεν έχει μήκος 32 bit, γεμίζεται με τυχαίους αριθμούς ή μηδενικά ανάλογα με την περίπτωση έτσι ώστε να πληροί τις προδιαγραφές του IPSec.

Πεδία που δεν αλλάζουν:

- Έκδοση
- Μέγεθος του internet header
- Συνολικό μέγεθος
- Αναγνώριση
- Πρωτόκολλο
- Διεύθυνση αποστολέα
- Διεύθυνση προορισμού (εξαρτάται από τον τρόπο δρομολόγησης)

Πεδία που αλλάζουν αλλά είναι προβλέψιμα

- Διεύθυνση προορισμού (εξαρτάται από τον τρόπο δρομολόγησης)
- Πεδία που μπορούν να αλλαχθούν (μηδενίζονται για τον υπολογισμό του ICV)
- Type of service (TOS)
- Flags
- Fragment Offset
- TTL
- Header Checksum

Τα πεδία αυτά αλλάζουν τις περισσότερες φορές για λόγους που αφορούν την δρομολόγηση των πακέτων. Αν μια επικεφαλίδα ενός πακέτου περιέχει πεδία που αλλάζουν κατά την μεταφορά τότε αυτά πρέπει να μηδενίζονται για τον υπολογισμό του ICV.

Προστασία επανάληψης

Ο μετρητής του αποστολέα μηδενίζεται όταν δημιουργείται ένα SA, και αυξάνεται κατά ένα κάθε φορά που στέλνεται ένα πακέτο. Ο αποστολέας δεν πρέπει να αφήσει τον μετρητή να γυρίσει πάλι από την αρχή, πρέπει να δημιουργήσει ένα καινούργιο

SA πριν αυτό συμβεί. Η προστασία επανάληψης θεωρείται ότι είναι ενεργοποιημένη, εκτός αν το αντίθετο ειπωθεί από τον παραλήπτη. Σε μια τέτοια περίπτωση ο μετρητής δεν μηδενίζεται, μέχρι να φτάσει στη μέγιστη του τιμή και να γυρίσει πάλι από την αρχή.

Από την πλευρά του παραλήπτη, εάν αυτός έχει ενεργοποιημένη την προστασία επανάληψης, τότε μηδενίζει τον μετρητή του κάθε φορά που δημιουργείται ένα καινούργιο SA. Για κάθε πακέτο που λαμβάνεται, ο αποδέκτης θα πρέπει να επιβλέπει αν ο αύξων αριθμός του πακέτου υπάρχει και σε κάποιο άλλο πακέτο που ανήκει στο ίδιο SA. Αυτό θα πρέπει να γίνεται στην αρχή του ελέγχου για να αποφεύγονται περιττοί έλεγχοι και να επιταχύνεται η όλη διαδικασία. Τα διπλά πακέτα απορρίπτονται.

2.4.2 Η επικεφαλίδα ESP

Η επικεφαλίδα ESP (Encapsulating Security Payload) είναι σχεδιασμένη για να παρέχει υπηρεσίες ασφάλειας στα πρωτόκολλα IPv4 και IPv6. Μπορεί να εφαρμοστεί αυτόνομα, αλλά και σε συνδυασμό με την AH και οι υπηρεσίες ασφάλειας που προσφέρει μπορούν να χρησιμοποιηθούν κατά την επικοινωνία δύο σταθμών, δυο αντιπυρικών ζωνών, αλλά και μεταξύ ενός σταθμού και ενός firewall.

Οι υπηρεσίες ασφάλειας που προσφέρει η επικεφαλίδα ESP είναι:

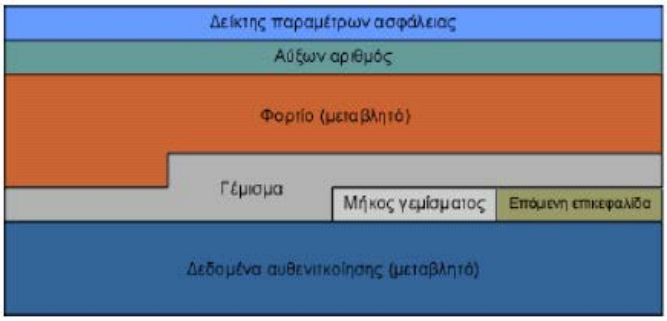
- Εμπιστευτικότητα (confidentiality)
- Διασφάλιση προέλευσης (data origin authentication)
- Ακεραιότητα (connectionless integrity)
- Προστασία πολλαπλής αποστολής πακέτου (anti-reply)
- Εμπιστευτικότητα ροής κίνησης (traffic flow confidentiality)

Το ποιες από αυτές τις υπηρεσίες θα χρησιμοποιηθούν κατά την διάρκεια μιας σύνδεσης, εξαρτάται από τις παραμέτρους που θα οριστούν κατά την δημιουργία του

συνδέσμου ασφάλειας (Security association) για την σύνδεση αυτή. Η εμπιστευτικότητα μπορεί να χρησιμοποιηθεί αυτόνομα. ωστόσο κάτι τέτοιο δεν έχει νόημα, γιατί χωρίς τις υπηρεσίες διασφάλισης προέλευσης και ακεραιότητας, η σύνδεση είναι ευάλωτη σε ενεργές επιθέσεις, οι οποίες μπορούν να καταστήσουν την υπηρεσία εμπιστευτικότητας άχρηστη.

Η υπηρεσία προστασίας πολλαπλής αποστολής μπορεί να εφαρμοστεί μόνο σε συνδυασμό με την διασφάλιση προέλευσης και η χρήση της αφορά μόνο τον παραλήπτη. Τέλος η υπηρεσία εμπιστευτικότητας ροής κίνησης απαιτεί την εφαρμογή της μεθόδου σήραγγας (tunnel mode) και είναι αποτελεσματική μόνο αν εφαρμοστεί κατά την επικοινωνία ενός firewall και ενός σταθμού, ή μεταξύ δύο αντιπυρικών ζωνών.

Τα πεδία της επικεφαλίδας ESP



Σχήμα 2.3 Πεδία του Encapsulating Security Payload (ESP)

Η επικεφαλίδα ESP περιέχει τα παρακάτω πεδία:

- Δείκτης παραμέτρων ασφάλειας (Security parameter index). Ο δείκτης παραμέτρων ασφάλειας είναι μία τιμή μήκους 32 bit, η οποία σε συνδυασμό με την διεύθυνση προορισμού προσδιορίζει μονοσήμαντα τον σύνδεσμο ασφάλειας, στον οποίο ανήκει το πακέτο αυτό. Την τιμή αυτή, την επιλέγει συνήθως ο παραλήπτης του πακέτου, κατά την δημιουργία του συνδέσμου ασφάλειας που διέπει την σύνδεση και η ύπαρξή της είναι υποχρεωτική. Οι τιμές από 1 έως 255 είναι δεσμευμένες από την IANA (Internet Assigned

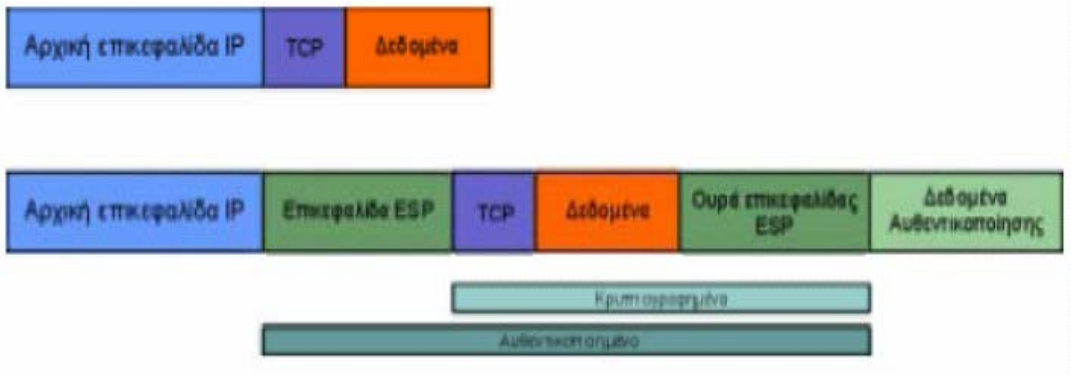
Numbers Authority) για μελλοντική χρήση. Η τιμή 0 είναι δεσμευμένη για τοπική χρήση, ανάλογα με την εκάστοτε υλοποίηση. Μπορεί να χρησιμοποιηθεί για παράδειγμα από το λογισμικό ενός υπολογιστή κατά την δημιουργία ενός συνδέσμου ασφάλειας. Άρα λοιπόν, επικεφαλίδα με δείκτη παραμέτρων ασφάλειας 0, δεν είναι λογικό να ταξιδεύει στο διαδίκτυο

- Αύξων αριθμός (Sequence number). Το πεδίο αύξοντος αριθμού είναι υποχρεωτικό και χρησιμοποιείται για την υπηρεσία προστασίας πολλαπλής αποστολής. Ο αύξων αριθμός περιέχεται στο πακέτο, ακόμα και αν ο παραλήπτης δεν επιθυμεί να χρησιμοποιήσει την υπηρεσία αυτή. Κατά την δημιουργία ενός συνδέσμου ασφάλειας ο αριθμός αυτός μηδενίζεται, έτσι ώστε το πρώτο πακέτο που θα στείλει ο αποστολέας να έχει την τιμή 1. Αν η υπηρεσία προστασίας πολλαπλής αποστολής είναι ενεργοποιημένη, ο αριθμός αυτός δεν πρέπει ποτέ να ανακυκλωθεί. Αν δηλαδή μεταδοθούν 232 πακέτα ο σύνδεσμος ασφάλειας πρέπει να καταστραφεί και να ξεκινήσει ένας νέος, για την συνέχεια της επικοινωνίας.
- Φορτίο (variable-length payload data). Αυτό το πεδίο περιέχει τα δεδομένα που περιγράφει το πεδίο «Επόμενη επικεφαλίδα». Το μήκος του φορτίου δεν είναι συγκεκριμένο, παρόλα αυτά είναι ακέραιο πολλαπλάσιο του ενός byte. Αν το φορτίο είναι κρυπτογραφημένο με κάποιον αλγόριθμο, ο οποίος απαιτεί δεδομένα συγχρονισμού για την αποκρυπτογράφηση, τότε αυτά τα δεδομένα περιέχονται μέσα σε αυτό το πεδίο.
- Γέμισμα (padding). Σε πολλές περιπτώσεις απαιτείται η χρήση αυτού του πεδίου. Για παράδειγμα, αν ο αλγόριθμος κρυπτογράφησης που έχει χρησιμοποιηθεί, απαιτεί τα δεδομένα να είναι πολλαπλάσια ενός αριθμού από byte, όπως δηλαδή γίνεται στην περίπτωση των αλγορίθμων που χρησιμοποιούν τμήματα (block) δεδομένων. Για αυτόν τον λόγο χρησιμοποιείται το γέμισμα, το οποίο μπορεί να είναι από 0 έως 255 bytes. Αυτό το πεδίο είναι προαιρετικό.
- Μήκος γεμίσματος (pad length). Το πεδίο μήκος γεμίσματος είναι μία τιμή των 8bit, που δείχνει πόσα byte γεμίσματος έχουν μπει στο πακέτο. Παίρνει δηλαδή τιμές από 0 έως 255, όπου 0 σημαίνει ότι δεν υπάρχει καθόλου γέμισμα.

- Επόμενη επικεφαλίδα (next header). Το πεδίο αυτό έχει μήκος 8 bit και προσδιορίζει τον τύπο των δεδομένων που περιέχονται στο πεδίο φορτίου. Προσδιορίζει δηλαδή, αν το φορτίο περιέχει ένα πακέτο IP ή ένα πακέτο ανώτερου επιπέδου. Οι τιμές αυτού του πεδίου καθορίζονται από την IANA.
- Δεδομένα αυθεντικοποίησης (authentication data). Το τελευταίο πεδίο, είναι το πεδίο πιστοποίησης, το οποίο είναι μεταβλητού μήκους. Το πεδίο αυτό περιέχει μία τιμή, η οποία υπολογίζεται από το πακέτο ESP χωρίς τα δεδομένα αυθεντικοποίησης και χρησιμοποιείται για έλεγχο ακεραιότητας από τον παραλήπτη. Το μήκος του πεδίου εξαρτάται από τον μηχανισμό ελέγχου που έχει επιλεχθεί. Το πεδίο αυτό είναι προαιρετικό και περιέχεται μόνο αν έχει επιλεχθεί από την υπηρεσία ασφάλειας.

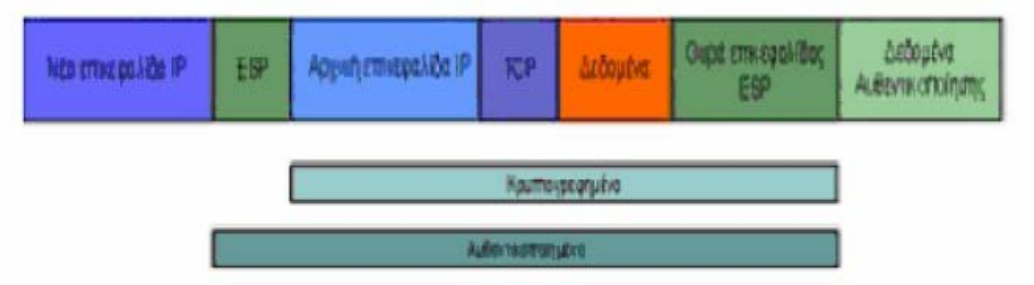
Η θέση της επικεφαλίδας ESP

Η Επικεφαλίδα ESP, όπως και η AH, μπορούν να χρησιμοποιηθούν με δύο μεθόδους. Την μέθοδο σήραγγας και την μέθοδο μεταφοράς. Η επικεφαλίδα ESP τοποθετείται μετά την επικεφαλίδα IP και πριν από την επικεφαλίδα του πρωτοκόλλου του ανώτερου επιπέδου, για παράδειγμα, πριν την επικεφαλίδα του πρωτοκόλλου TCP, που ενδεχομένως ακολουθεί. Για παράδειγμα, στην περίπτωση που θέλουμε να εισάγουμε την επικεφαλίδα ESP σε ένα πακέτο IPv4 το οποίο μεταφέρει ένα πακέτο TCP, η εισαγωγή θα γίνει όπως παρακάτω:



Σχήμα 2.4 ενθυλάκωση της επικεφαλίδας ESP (transport mode)

Όταν εφαρμόζεται σε μέθοδο σήραγγας το πακέτο διαμορφώνεται ως εξής:



Σχήμα 2.5 ενθυλάκωση της επικεφαλίδας ESP (tunnel mode)

Λειτουργία πρωτοκόλλου

Οι βασικές λειτουργίες του πρωτοκόλλου είναι οι εξής:

- Διαδικασία εύρεσης σε ποιο σύνδεσμο ασφάλειας ανήκει το πακέτο. Για την διαδικασία αυτή χρησιμοποιείται το πεδίο δείκτης παραμέτρων ασφάλειας (SPI). Για κάθε σύνδεσμο ασφάλειας καθορίζεται (συνήθως από τον παραλήπτη) αυτός ο αριθμός. Έστω ένας υπολογιστής λαμβάνει ένα πακέτο, με τιμή Α σε αυτό το πεδίο. Τότε αναζητά ποιος σύνδεσμος ασφάλειας από αυτούς που έχει αποκαταστήσει, έχει ως δείκτη παραμέτρων ασφάλειας αυτήν την τιμή. Αν δεν βρεθεί κανένας σύνδεσμος ασφάλειας με αυτήν την τιμή, τότε το πακέτο απορρίπτεται. Αν βρεθεί τότε συνεχίζεται η επεξεργασία του πακέτου.
- Προστασία πολλαπλής παραλαβής πακέτου. Κάθε φορά που ο αποστολέας στέλνει ένα πακέτο, αυξάνει την τιμή που είχε πριν ο μετρητής του αύξοντος αριθμού για αυτό τον σύνδεσμο ασφάλειας. Ο παραλήπτης, όταν παραλαμβάνει ένα πακέτο περιμένει ο αύξων αριθμός του να είναι κατά ένα μεγαλύτερος από τον αντίστοιχο αριθμό του προηγούμενου πακέτου. Αν αυτό δεν ισχύει, τότε το πακέτο απορρίπτεται. Επίσης θεωρείται δεδομένο, ότι η

αρίθμηση αυτή αρχίζει από το 1 και ότι το πρώτο πακέτο ενός συνδέσμου ασφάλειας έχει αύξων αριθμό 1. Αυτός ο μηχανισμός ασφάλειας, είναι στο χέρι του παραλήπτη να τον χρησιμοποιήσει, ωστόσο ο αποστολέας οφείλει να τον αυξάνει, εκτός και αν ο παραλήπτης του πει να μην κάνει κάτι τέτοιο κατά την δημιουργία του συνδέσμου ασφάλειας.

- Σύγκριση Τιμής ελέγχου ακεραιότητας. Ο αποστολέας υπολογίζει μία τιμή, με την χρήση της συνάρτησης κατακερματισμού (hash function) που έχει αποφασιστεί κατά την δημιουργία του συνδέσμου ασφάλειας. Στην είσοδο αυτής της συνάρτησης μπαίνουν όλα τα πεδία του πακέτου, εκτός του πεδίου αυθεντικοποίησης. Αυτός ο υπολογισμός, γίνεται πάντα μετά την κρυπτογράφηση. Ο παραλήπτης, αφού αφαιρέσει το πεδίο αυθεντικοποίησης, χρησιμοποιεί και αυτός την ίδια συνάρτηση. Αν η τιμή που θα υπολογίσει ο παραλήπτης, είναι ίση με την τιμή που έχει βάλει ο αποστολέας στο πεδίο αυθεντικοποίησης, τότε και μόνο το πακέτο γίνεται δεκτό, στην αντίθετη περίπτωση απορρίπτεται.
- Τεμαχισμός. Αν κριθεί απαραίτητο να τεμαχιστεί κάποιο πακέτο, τότε αυτό γίνεται αφού εισάγουμε την επικεφαλίδα ESP. Με άλλα λόγια ως φορτίο για την επικεφαλίδα ESP δεν πρέπει ποτέ να μπαίνει ένα τεμάχιο ενός πακέτου. Για αυτό και αν κάποιος παραλάβει ένα πακέτο ESP, το οποίο περιέχει ως φορτίο ένα πακέτο με μη μηδενικό πεδίο μετατόπισης, ή με την σημαία «περισσότερα τεμάχια» ενεργή, τότε το πακέτο ESP θεωρείται άκυρο και απορρίπτεται.
- Κρυπτογράφηση και αποκρυπτογράφηση. Ο αποστολέας τοποθετεί στο πεδίο φορτίου τα δεδομένα, τα οποία στην περίπτωση της μεθόδου μεταφοράς είναι το πακέτο του ανώτερου επιπέδου και στην περίπτωση σήραγγας όλο το αρχικό IP πακέτο. Στην συνέχεια προσθέτει όσα byte γεμίσματος είναι απαραίτητα. Τέλος κρυπτογραφεί με τον αλγόριθμο που υπαγορεύει ο σύνδεσμος ασφάλειας τα πεδία φορτίου, γεμίσματος, μήκος γεμίσματος και επόμενο πεδίο. Ο παραλήπτης όταν παραλάβει το πακέτο αποκρυπτογραφεί με την σειρά του τα πεδία αυτά και υποβάλει το πακέτο σε περαιτέρω επεξεργασία.

2.5 Διαχείριση κλειδιών και συσχετίσεων ασφάλειας

Η διαχείριση των κλειδιών και των συσχετίσεων ασφάλειας μπορεί να είναι είτε χειροκίνητη ή αυτόματη. Κάθε σταθμός πρέπει να υποστηρίζει και τους δύο τρόπους διαχείρισης για λόγους διαλειτουργικότητας σύμφωνα με το RFC 2401.

2.5.1 Χειροκίνητη διαχείριση κλειδιών

Στην χειροκίνητη διαχείριση κλειδιών και συσχετίσεων, οι συσχετίσεις ασφάλειας ορίζονται στατικά για κάθε ζευγάρι συνομιλούντων σταθμών. Η χειροκίνητη διαχείριση δεν είναι καλή αφού:

- Είναι επιρρεπής σε λάθη αφού απαιτεί εκτενείς ρυθμίσεις για πολλά ζευγάρια σταθμών.
- Τα κλειδιά για την επικοινωνία δύο υπολογιστών είναι στατικά και άρα υπάρχει μεγαλύτερη πιθανότητα να τα ανακαλύψει κάποιος εισβολέας.
- Τα κλειδιά συνήθως δεν είναι ισχυρά αφού η διαδικασία των ρυθμίσεων είναι κουραστική και πολλές φορές δεν χρησιμοποιούνται σωστές μέθοδοι για την δημιουργία τους.
- Δεν εφαρμόζεται σε ευρεία κλίμακα αφού απαιτούνται στατικές ρυθμίσεις για όλα τα ζευγάρια σταθμών. Από τα παραπάνω καταλαβαίνουμε ότι η διαχείριση των κλειδιών χρειάζεται αυτοματοποίηση.

2.5.2 Αυτόματη διαχείριση κλειδιών

Για την αυτόματη διαχείριση των συσχετίσεων χρησιμοποιούνται συγκεκριμένα πρωτόκολλα. Μερικά από τα πρωτόκολλα διαχείρισης είναι τα: Skip, Oakley, Photuris και IKE. Από αυτά κάθε σταθμός πρέπει να υποστηρίζει τουλάχιστον τον IKE.

Skip (in band keying)

Το πρωτόκολλο SKIP (Simple Key-Management for Internet Protocols) αναπτύχθηκε από την SUN το 1995 και σταμάτησε να προωθείτε το 1998. Το SKIP είναι πλέον «νεκρό» και δεν χρησιμοποιείται. Αναφερόμαστε σε αυτό επειδή είναι το μοναδικό πρωτόκολλο που διαφέρει υπερβολικά από τα υπόλοιπα. Η διαφορά του οφείλεται στο γεγονός ότι το κλειδί με το οποίο κρυπτογραφούνται τα δεδομένα περιλαμβάνεται μέσα στο πακέτο σε μία ξεχωριστή επικεφαλίδα του SKIP.

Το SKIP είναι σχεδιασμένο για πρωτόκολλα πακέτων (datagram oriented) όπως το IP. Κάθε σταθμός έχει ένα ζευγάρι κλειδιών Diffie Hellman. Το δημόσιο κλειδί του αυθεντικοποιείται μέσω X509 πιστοποιητικά, PGP πιστοποιητικά ή χειροκίνητα. Ένα κοινό αυθεντικοποιημένο κλειδί, έστω S, υπολογίζεται από το δημόσιο του κάθε σταθμού. Όταν ένας σταθμός στέλνει δεδομένα υπολογίζει ένα τυχαίο συμμετρικό κλειδί, έστω R. Κρυπτογραφεί ή/και πιστοποιεί τα δεδομένα με το κλειδί R χρησιμοποιώντας ένα από τα AH και ESP. Κρυπτογραφεί το κλειδί R με το κλειδί S και στέλνει τα κρυπτογραφημένα ή/και πιστοποιημένα δεδομένα το κρυπτογραφημένο R στον παραλήπτη. Ο παραλήπτης αποκρυπτογραφεί το R με το S και έπειτα περνάει τα δεδομένα και το κλειδί R στο τμήμα του IPSec για επεξεργασία.

Πλεονεκτήματα:

- Δεν γίνεται σύνδεση μεταξύ των δύο υπολογιστών για την ανταλλαγή κλειδιών
- Υποστηρίζει συνδέσεις μία κατεύθυνσης (π.χ. broadcast πάνω από δορυφόρους
- Υποστηρίζει multicast
- Αντιπυρικές ζώνες που χρησιμοποιούν το SKIP μπορούν να ρυθμιστούν ώστε να κάνουν άμεση ανάκαμψη από σφάλματα

Μειονεκτήματα:

- Ακόμα μεγαλύτερα πακέτα (περιέχουν και το κρυπτογραφημένο κλειδί του πακέτου)
- Επιπλέον επεξεργασία ανά πακέτο
- Δεν διαπραγματεύονται ρυθμίσεις για τις συσχετίσεις ασφαλείας IKE (Internet Key Exchange) Το IKE (Internet Key Exchange) είναι το πρότυπο πρωτόκολλο για την αυτόματη διαχείριση κλειδιών και συσχετίσεων ασφάλειας. Είναι ένα πρωτόκολλο επιπέδου εφαρμογής που χρησιμοποιεί το UDP ως πρωτόκολλο μεταφοράς και την θύρα 500. Βασίζεται στο ISAKMP (RFC 2408, RFC 2409). Το ISAKMP είναι ένα πρωτόκολλο που αποτελεί έναν σκελετό για την ανάπτυξη πρωτοκόλλων ασφαλείας. Το IKE έχει αρχιτεκτονική initiator-responder, ο initiator προτείνει κάποιες παραμέτρους επικοινωνίας και ο responder επιστρέφει ποιες από αυτές δέχεται χωρίς να μπορεί να προτείνει αυτός κάποιες παραμέτρους.

IKE (Internet Key Exchange)

Το IKE είναι πρωτόκολλο δύο φάσεων. Η πρώτη φάση χρησιμοποιεί το ISAKMP για να δημιουργήσει ένα ISAKMP SA. Η δεύτερη φάση χρησιμοποιεί το ISAKMP SA για να δημιουργήσει τουλάχιστον δύο IPSec SA (ένα για κάθε κατεύθυνση). Η πρώτη φάση έχει δύο modes, το main και το aggressive.

Στο main mode έχουμε τρία ζευγάρια μηνυμάτων:

1. Διαπραγματεύονται οι κρυπτογραφικοί αλγόριθμοι.
2. Γίνεται μια Difflie Hellman συναλλαγή και παράγεται ένα κοινό μυστικό.
3. Το κάθε σύστημα αποδεικνύει την ταυτότητά του και ότι γνωρίζει το κοινό μυστικό.

Στο aggressive mode έχουμε μόνο τρία μηνύματα:

1. Στα πρώτα δυο μηνύματα γίνεται μια συναλλαγή Diffie-Hellman και παράγεται ένα κοινό μυστικό.
2. Στα μηνύματα δυο και τρία, κάθε σύστημα αποδεικνύει ότι γνωρίζει το κοινό μυστικό.
3. Στο main mode τα δύο τελευταία μηνύματα είναι κρυπτογραφημένα, ώστε να έχουμε μη αποκάλυψη της ταυτότητας των συνομιλούντων, ενώ στο aggressive mode έχουμε λιγότερα μηνύματα. Στη δεύτερη φάση έχουμε δύο modes, το informational και το quick. Το informational mode χρησιμοποιείται για ανακοίνωση σφαλμάτων. Το quick mode χρησιμοποιείται για την δημιουργία IPSec SA και στο rekeying. Κατά την διάρκεια του quick mode έχουμε διαπραγμάτευση των παραμέτρων ασφάλειας και την δημιουργία κλειδιών και συσχετίσεων ασφάλειας.

3. Το Multiprotocol Label Switching (MPLS)

Η αντιμετώπιση των προβλημάτων του παραδοσιακού IP σίγουρα δεν είναι η εισαγωγή μιας νέας τεχνολογίας που θα το αντικαταστήσει και δεν θα λάβει υπόψη την υπάρχουσα εγκατεστημένη βάση των υπηρεσιών και εφαρμογών που χρησιμοποιούνται ευρέως. Μην ξεχνάτε για παράδειγμα το ATM δεν μπόρεσε να ανταγωνιστεί το IP παρόλο που μπορεί να παρέχει real-time υπηρεσίες, έχει μηχανισμούς traffic engineering και δεν εμφανίζει φαινόμενα αλληλοεπικάλυψης. Επομένως οποιαδήποτε νέα τεχνολογία που θα αναπτυχθεί και η οποία δεν θα υποστηρίζει τα υφιστάμενα IP πρωτόκολλα και εφαρμογές δεν θα γίνει αποδεκτή από την αγορά. Η τεχνολογία MPLS έχει αποφύγει αυτό το σκόπελο και έχει καταφέρει να αναπτύσσεται διατηρώντας την συμβατότητα, την συνεργασία και την υποστήριξη όλων των γνωστών πρωτοκόλλων.

Το MPLS (Multiprotocol Label Switching Protocol) είναι ένα πρωτόκολλο το οποίο δημιουργήθηκε από την IETF. Συνδυάζει την μεταγωγή με label και την παραδοσιακή δρομολόγηση του IP με στόχο να αυξήσει την ευελιξία και την απόδοση του πρωτοκόλλου IP και ταυτόχρονα να δώσει την δυνατότητα για την παροχή νέων υπηρεσιών στο Internet. Έτσι ενώ το MPLS συνεργάζεται με τα υφιστάμενα πρωτόκολλα επιτρέπει την μεταγωγή με κύκλωμα στο Internet.

Η μεταγωγή με label επιτυγχάνεται τοποθετώντας στην αρχή κάθε πακέτου, κατά την είσοδο του στο δίκτυο MPLS, μια ετικέτα (label). Σε κάθε δρομολογητή η απόφαση για το πως θα δρομολογηθεί το πακέτο εξαρτάται μόνο από αυτό το label και όχι από την IP διεύθυνση στο header. Η ετικέτα απομακρύνεται κατά την έξοδο του πακέτου από το δίκτυο MPLS. Οι δρομολογητές οι οποίοι χρησιμοποιούν την μεταγωγή με label ονομάζονται Label Switching Δρομολογητές (LSRs).

3.1 Εισαγωγή στο Multiprotocol Label Switching (MPLS)

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

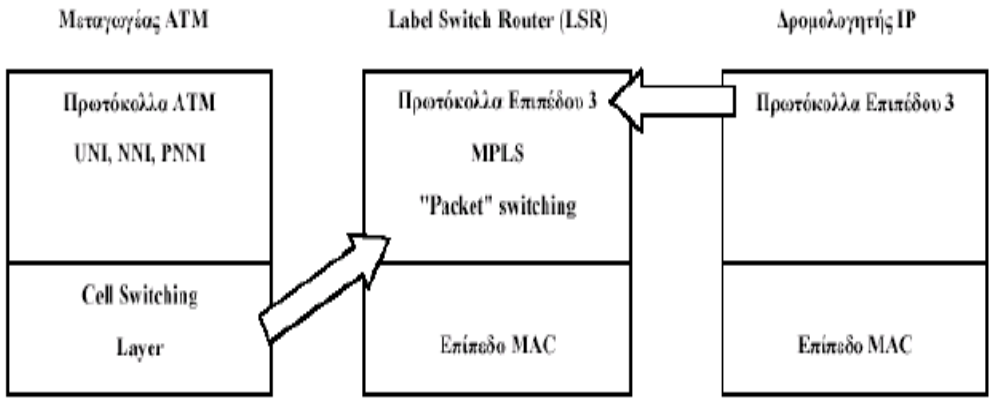
1. Οι δρομολογητές είναι stateless. Κάθε δρομολογητής δεν κρατάει καμία πληροφορία για τον τρόπο που δρομολογεί τα πακέτα. Αφού δρομολογήσει ένα πακέτο επιστρέφει στην αρχική κατάσταση και δρομολογεί οποιοδήποτε άλλο πακέτο ανεξάρτητα.

2. Δρομολογούνται πακέτα (σε αντίθεση π.χ. με το ATM όπου δρομολογούνται ροές). Πάντως τεχνολογίες όπως το flow switching και το CEF της Cisco προσομοιώνουν κάποιες από τις λειτουργίες αυτές του ATM. Όπως έχουμε δει, σε ένα δρομολογητή κάθε πακέτο προωθείται ανεξάρτητα από τα υπόλοιπα με μόνο κριτήριο τον προορισμό του, με μία επαναλαμβανόμενη ενέργεια για κάθε πακέτο που αποτελείται από δύο διαδικασίες, την δρομολόγηση και την μεταγωγή.

3.2 Η Αρχιτεκτονική του MPLS Architecture

3.2.1 Οι Δρομολογητές Μεταγωγής Ετικετών (LSR - Label Switching Router)

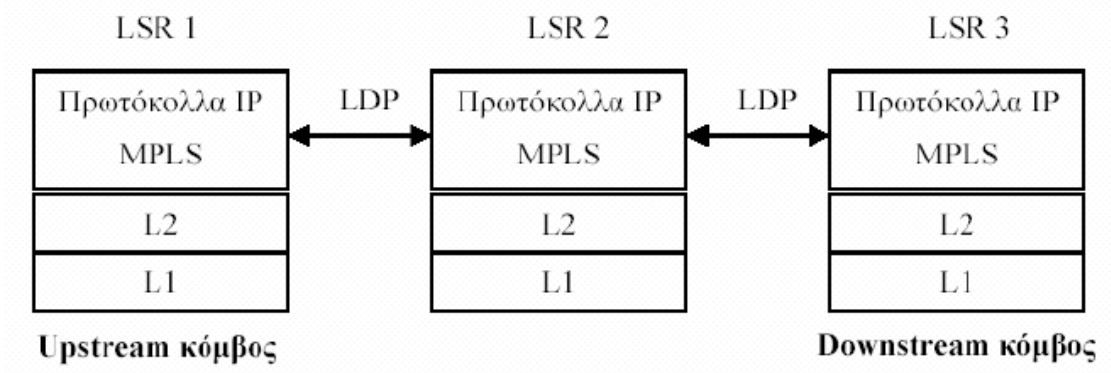
Η λύση που προσφέρει το MPLS βασίζεται στον διαχωρισμό των δύο διαδικασιών της δρομολόγησης και της μεταγωγής σε ένα δρομολογητή. Το νέο μηχάνημα ονομάζεται Label Switching Router ο οποίος κάνει την προώθηση των πακέτων βασισμένος σε ένα label το οποίο υπάρχει στην κεφαλή του πακέτου χωρίς να χρειάζεται να κάνει επιπλέον επεξεργασία του πακέτου (όπως ακριβώς γίνεται και στο ATM, όπου η δρομολόγηση γίνεται στην αρχή και φτιάχνονται τα μονοπάτια (VCs) και στην συνέχεια η μεταγωγή γίνεται μόνο με βάση ένα label, το VPI/VCI).
Η διαφορά είναι ότι σε ένα LSR η μεταγωγή με label γίνεται σε επίπεδο 3 (επίπεδο δικτύου) ενώ στο ATM γίνεται στο επίπεδο 2. Είναι δηλαδή οι LSRs δρομολογητές που χρησιμοποιούν το πρωτόκολλο MPLS και δανείζονται χαρακτηριστικά τόσο από το IP όσο και από το ATM. Συνδυάζουν τα παραδοσιακά πρωτόκολλα του IP για να φτιάξουν τους πίνακες δρομολόγησης αλλά παράλληλα χρησιμοποιούν τον τρόπο μεταγωγής που χρησιμοποιεί ένας μεταγωγέας ATM.
Όπως βλέπουμε στο Σχήμα 3.1 ο LSR χρησιμοποιεί τόσο τα πρωτόκολλα του IP επιπέδου όσο και το μηχανισμό cell switching ενός ATM switch.



Σχήμα 3.1 Η λογική ενός Label Switching Router (LSR)

Λειτουργία LSR

Για την ανταλαγή των labels μεταξύ των LSRs αναπτύχθηκε ένα νέο πρωτόκολλο γνωστό ως LDP (Label Distribution Protocol). Το LDP εφαρμόζεται μεταξύ δύο διαδοχικών LSRs όπως φαίνεται και στο Σχήμα 3.2. όπου ο πρώτος κόμβος (LSR 1) καλείται Upstream γείτονας του κεντρικού κόμβου (LSR 2) ενώ ο τρίτος κόμβος (LSR 3) Downstream γείτονας του κεντρικού κόμβου. Γενικά σε μια ροή πακέτων από ένα κόμβο A σε ένα κόμβο B όπου έχει γίνει δέσμευση μιας ετικέτας E ο A καλείται Upstream και ο B Downstream κόμβος.



Σχήμα 3.2 Επικοινωνία μεταξύ LSRs

Όπως φαίνεται στο Σχήμα 3.2, κάθε LSR υποστηρίζει στο επίπεδο 3 τόσο τα παραδοσιακά IP πρωτόκολλα όσο και το πρωτόκολλο MPLS. Η LDP επικοινωνία μεταξύ δύο LSR χωρίζεται σε τρεις φάσεις:

1. Αρχικά γίνεται ανίχνευση των γειτονικών LSRs, με την αποστολή 'DISCOVERY' μηνυμάτων. Μηνύματα ανταλλάσσονται επίσης περιοδικά για την συντήρηση της επικοινωνίας
2. Ακολούθως οι γειτονικοί LSRs ανοίγουν ένα LDP session χρησιμοποιώντας το πρωτόκολλο TCP, ώστε να εξασφαλιστεί η αξιόπιστη παράδοση, το οποίο θα χρησιμοποιηθεί για την ανταλλαγή των πληροφοριών μεταγωγής.
3. Τέλος ανταλλάσσονται μια σειρά από LDP μηνύματα ώστε α) να συμφωνηθούν διάφορες παράμετροι και επιλογές της επικοινωνίας και β) να

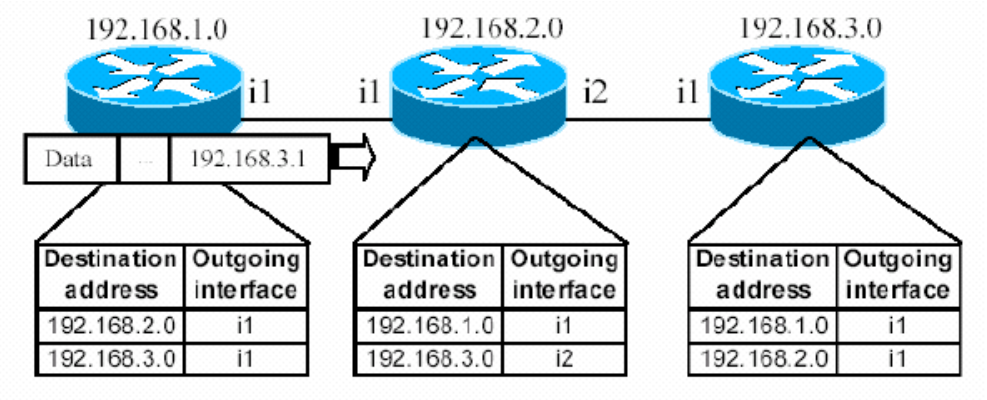
διαφημιστούν οι πληροφορίες δέσμευσης μεταξύ IP διευθύνσεων και labels Κατά αυτό τον τρόπο ένας LSR γνωρίζει τόσο με ποια labels θα του προωθεί ο upstream κόμβος πακέτα όσο και με ποιά labels και σε ποιους κόμβους θα τα προωθεί ο ίδιος.

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

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

3.2.2 Προώθηση MPLS Πακέτων

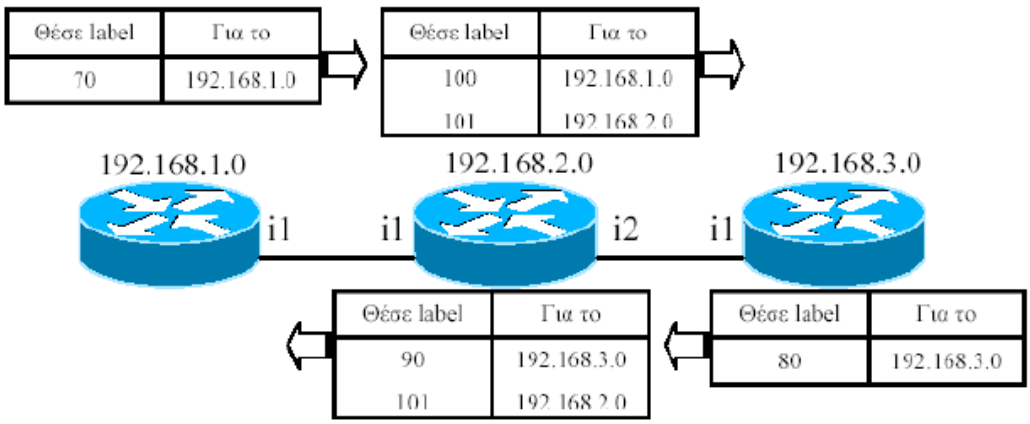
Η διαδικασία προώθησης σε ένα δίκτυο MPLS χωρίζεται σε δύο μέρη. Στο πρώτο μέρος εκτελούνται τα παραδοσιακά πρωτόκολλα δρομολόγησης και δημιουργούνται οι γνωστοί πίνακες δρομολόγησης. Στην συνέχεια, οι LSRs για κάθε εγγραφή του πίνακα δρομολόγησης επικοινωνούν με τους γειτονικούς τους κόμβους (σύμφωνα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



Σχήμα 3.3 Η δρομολόγηση στους παραδοσιακούς IP Δρομολογητές

Σύμφωνα με τον παραδοσιακό τρόπο δρομολόγησης (Σχήμα 3.3), πρώτα φτιάχνονται οι πίνακες δρομολόγησης από συγκεκριμένα πρωτόκολλα (RIP, OSPF κλπ) και στην συνέχεια τα δεδομένα αποστέλλονται σε πακέτα με την διεύθυνση προορισμού στην κεφαλή κάθε ενός από αυτά.

Στο παράδειγμα (Σχήμα 3.4), ο κόμβος 192.168.1.0 ενημερώνει τον Up/Down stream κόμβο 192.168.2.0 ότι πακέτα που προορίζονται για το 192.168.1.0 να φέρουν το label 70. Ο κόμβος αυτός (192.168.2.0) με την σειρά του ενημερώνει τον Up/Down stream κόμβο 192.168.3.0 ότι πακέτα με προορισμό τα 192.168.1.0 και 192.168.2.0 να φέρουν τα labels 100 και 101 αντίστοιχα.



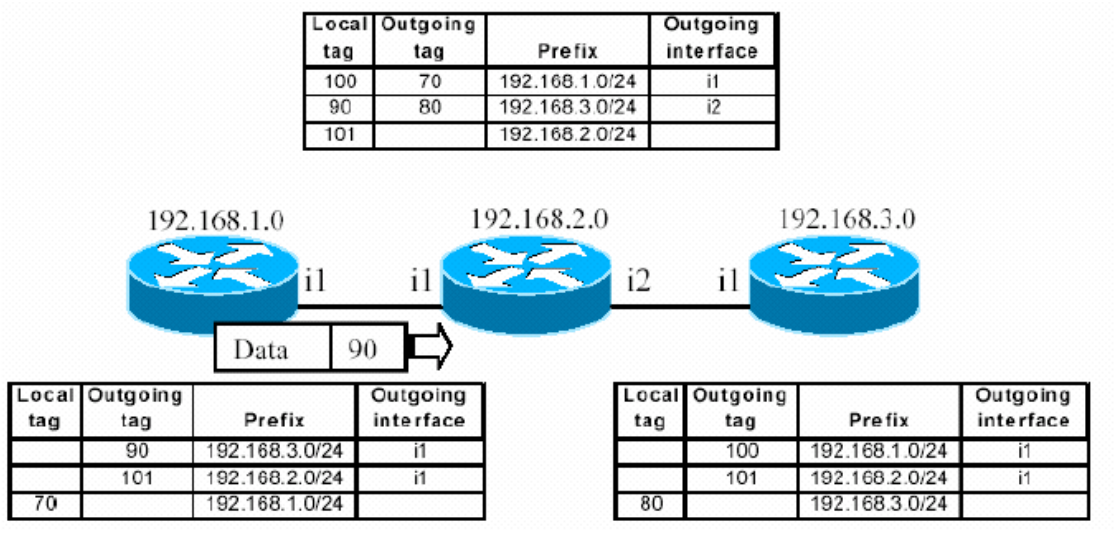
Σχήμα 3.4 Ανταλλαγή labels μεταξύ των LSRs (μέσω LDP)

Σχήμα 3.4 Ανταλλαγή labels μεταξύ των LSRs (μέσω LDP)

Οι διαδρομές αυτές, γνωστές ως FECs (Forwarding Equivalence Classes), δημιουργούνται μόνο προς την μία κατεύθυνση. Η αντίστροφη διαδικασία, στο παράδειγμα από τον κόμβο 192.168.3.0 προς τον κόμβο 192.168.1.0, είναι απαραίτητη για ολοκλήρωση της διαδικασίας.

Οι δύο κατευθύνσεις (FECs) μιας διαδρομής μεταξύ δύο κόμβων μπορεί να διέρχονται από διαφορετικούς ενδιάμεσους κόμβους. Όταν ο κόμβος 192.168.1.0 θέλει να στείλει ένα πακέτο στον κόμβο 192.168.3.0, αυτό το πακέτο πλαισιώνεται από το MPLS σύμφωνα με τα στοιχεία του πίνακα προώθησης (Forwarding Information Base – FIB).

Στο παράδειγμα (Σχήμα 3.5) τοποθετείται το label 90 στην κεφαλή του πακέτου και προωθείται στον επόμενο κόμβο διαμέσου του interface i1. Όταν ο ενδιάμεσος κόμβος 192.168.2.0 παραλάβει ένα πακέτο με label 90 χρησιμοποιεί την τιμή του label (και μόνο αυτή) ως δείκτη στον δικό του πίνακα προώθησης για να αποφασίσει πως θα προωθήσει το πακέτο αυτό. Στη προκειμένη περίπτωση, μεταβάλει την τιμή του label (από 90 σε 80) και προωθεί το πακέτο κατάλληλα. Στον κόμβο εξόδου, 192.168.3.0, το label απομακρύνεται και το πακέτο παραδίδεται στον προορισμό του.



Σχήμα 3.5 Η λειτουργία προώθησης στο MPLS

Γενικά, σε κάθε πακέτο που εισέρχεται στο MPLS δίκτυο ανατίθεται ένα label (π.χ. για δρομολογητές μία σταθερού και μικρού μήκους τιμή μεγέθους 32bits) το οποίο τοποθετείται στην κεφαλή του πακέτου. Η ανάθεση γίνεται στον κόμβο εισόδου του δικτύου. Στην συνέχεια το πακέτο προωθείται στον επόμενο κόμβο μαζί με την ετικέτα αυτή. Σε κάθε ενδιάμεσο κόμβο γίνεται επεξεργασία μόνο της ετικέτας του πακέτου (σε επίπεδο δικτύου) με τρόπο ώστε η ετικέτα να χρησιμοποιείται ως δείκτης μέσα στον πίνακα μεταγωγής (Label Information Base –LIB).

Στο πίνακα αυτό κάθε πλειάδα έχει την μορφή <ετικέτα εισόδου, διεπαφή εισόδου, διεπαφή εξόδου, ετικέτα εξόδου>. Η παλιά ετικέτα αντικαθίσταται από μία νέα ετικέτα και προωθείται στον επόμενο κόμβο. Στους κλασικούς IP δρομολογητές η κεφαλή του πακέτου υφίσταται επεξεργασία σε επίπεδο δικτύου όχι μόνο για να προωθηθεί το πακέτο στον επόμενο κόμβο αλλά και για να καθοριστεί η κλάση υπηρεσίας στην οποία ανήκει το πακέτο αυτό (π.χ. στα Integrated και Differentiated Services). Το MPLS επιτρέπει την μεταφορά όλης αυτής της πληροφορίας στην ετικέτα (αφού τα χαρακτηριστικά της κλάσης και οι διαδρομές έχουν εξαρχής προκαθοριστεί, όπως ισοδύναμα συμβαίνει στα δίκτυα ATM) και έτσι δεν χρειάζεται περαιτέρω επεξεργασία η κεφαλή του πακέτου σε επίπεδο 3.

Η παρουσία μιας LIB σε κάθε κόμβο επιτρέπει την δημιουργία ιδεατών μονοπατιών από κάθε κόμβο προς οποιοδήποτε άλλον κόμβο. Ένα τέτοιο μονοπάτι είναι μια ακολουθία από labels η οποία ξεκινάει από ένα LSR εισόδου και τελειώνει σε ένα LSR εξόδου. Τα LSPs μοιάζουν πολύ με τα μονής κατεύθυνσης VP/VCs του ATM.

Η αντιστοίχηση μεταξύ ενός παραδοσιακού πίνακα δρομολόγησης και μιας LIB είναι της μορφής «ένα προς πολλά» αφού σε κάθε κόμβο μπορούμε να δεσμεύσουμε πολλά labels για τον ίδιο προορισμό όχι όμως το ίδιο label για διαφορετικούς προορισμούς. Μια εγγραφή στην LIB αντιστοιχεί σε μία και μόνο μια εγγραφή του παραδοσιακού πίνακα δρομολόγησης. Έτσι εξασφαλίζεται η μοναδικότητα ενός label για κάθε προορισμό πράγμα απαραίτητο αφού πλέον η δρομολόγηση γίνεται αποκλειστικά με βάση τα labels.

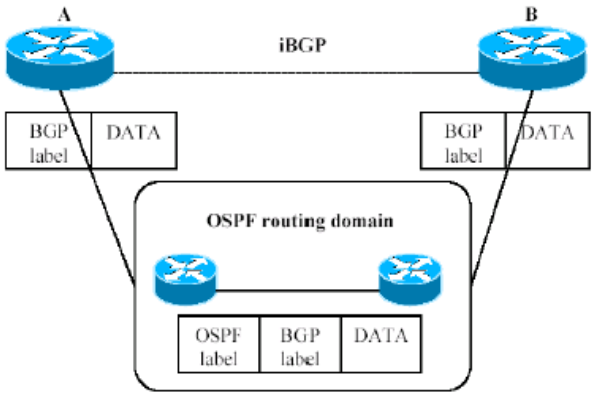
Το γεγονός ότι σε κάθε πακέτο που μπαίνει στο δίκτυο ανατίθεται μια ετικέτα, επιτρέπει την εφαρμογή μιας αποτελεσματικής τεχνικής προώθησης. Επιπλέον ο διαχωρισμός, μέσω του MPLS, των λειτουργιών της μεταγωγής και της δρομολόγησης δίνει την δυνατότητα να υποστηριχθούν διαφορετικές πολιτικές δρομολόγησης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

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

3.2.3 Μονοπάτια μεταγωγής βασισμένα σε ετικέτες

Ένα ιδιαίτερα ενδιαφέρον αποτέλεσμα της τεχνικής στοίβας ετικετών είναι η δημιουργία tunnels κατά τρόπο όμοιο των γνωστών tunnels που δημιουργούνται μέσω netwotk layer encapsulation. Εδώ το tunnel υλοποιείται ως ένα LSP μεταγωγής με ετικέτα. Είναι επίσης σημαντικό να πούμε ότι τα LSP tunnels μπορούν να οργανωθούν σε ιεραρχίες, όπου κάθε ιεραρχία αντιστοιχεί σε ένα επίπεδο της στοίβας ετικετών ως ένα παράδειγμα μιας ιδιαίτερα χρήσιμης εφαρμογής των MPLS tunnels είναι τα IP-VPNs.

Για παράδειγμα έστω ένα δίκτυο όπου οι εσωτερικοί δρομολογητές εντός του domain τρέχουν OSPF και γνωρίζουν μόνο πως να φτάσουν σε προορισμούς εντός του OSPF domain. Το domain αυτό μπορεί να έχει αρκετούς AS δρομολογητές (Autonomous System Border Δρομολογητές - ASBRs) που μεταξύ τους να μιλούν BGP (iBGP). Έστω επίσης ότι το BGP δεν διανέμεται στο OSPF και οι LSRs που δεν είναι στα άκρα δεν τρέχουν BGP.



Σχήμα 3.6 Labelled tunnel

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

Έστω ένα IP πακέτο χωρίς ετικέτα φτάνει στον κόμβο A, αυτός προσθέτει στη στοίβα μία ετικέτα, αυτή έχει νόημα μόνο για τον γειτονικό του (ως προς BGP) κόμβο B (θυμηθείτε ότι η ανταλλαγή των ετικετών εδώ έγινε μέσω του BGP).

Όταν το πακέτο εισέρχεται στο δίκτυο OSPF, ο κόμβος εισόδου του OSPF δικτύου προσθέτει μία ακόμη ετικέτα στη στοίβα, ένα OSPF label. Στην συνέχεια το προωθεί στο επόμενο κόμβο. Όταν το πακέτο φτάσει στο κόμβο εξόδου του OSPF δικτύου, αυτός θα αφαιρέσει το OSPF label από τη στοίβα και θα προωθήσει το πακέτο στον κόμβο B ο οποίος και θα δεί το BGP label.

4. VPN βασισμένα σε τεχνολογία MPLS

4.1 Υπηρεσίες των MPLS VPNs

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

- Μη προσανατολισμένες στην σύνδεση – ασυνδεσμικές - υπηρεσίες (Connectionless Service): ένα τεχνικό πλεονέκτημα των MPLS VPN είναι ότι είναι ασυνδεσμικά, που σημαίνει ότι δεν χρειάζεται εκ των προτέρων εγκατάσταση καναλιού επικοινωνίας ανάμεσα σε δύο σημεία. Αυτό έρχεται σε πλήρη ευθυγράμμιση με την λογική λειτουργίας του ίδιου του internet το οποίο βασίζεται στο πρωτόκολλο TCP/IP που είναι επίσης ασυνδεσμικό. Έτσι αποφεύγεται επιπλέον πολυπλοκότητα στην λειτουργία του δικτύου.
- Κεντρικός έλεγχος υπηρεσιών (Centralized service): τα VPNs δίνουν την δυνατότητα στους παροχείς υπηρεσιών να παρέχουν αρκετές υπηρεσίες σε ομάδες χρηστών. Οι χρήστες μπορούν να χρησιμοποιούν αυτές τις υπηρεσίες, ιδιωτικώς, μέσα στα δικά τους intranets και extranets. Επειδή τα MPLS VPNs «φαίνονται» σαν ιδιωτικά intranets μπορούν να χρησιμοποιήσουν και τις νέες IP υπηρεσίες όπως:
    1. πολυεκπομπή
    2. ποιότητας υπηρεσιών (QoS)
    3. τηλεφωνία εντός του VPN
    4. φύλαξη ιστοσελίδων (Web hosting)

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

- Δυνατότητα αναβάθμισης (Scalability): σε αντίθεση με τα άλλα είδη VPN (Frame Relay, ATM κλπ.) που χρησιμοποιούν προσανατολισμένες στην σύνδεση υπηρεσίες, η ασυνδεσμικότητα του MPLS δίνει την δυνατότητα της

εύκολης αναβάθμισης. Τα MPLS χρησιμοποιούν το λεγόμενο ομότιμο (peer) μοντέλο για να πετύχουν αυτήν την αναβάθμιση. Σύμφωνα με αυτό, το site ενός πελάτη το μόνο που χρειάζεται είναι να «συνδεθεί» (peer) με την άκρη ενός δρομολογητή του παροχέα (provider edge – PE – router) και όχι με όλους τους υπόλοιπους δρομολογητές που είναι μέλη του VPN. Η ασυνδεσμική του αρχιτεκτονική επιτρέπει τέτοιου είδους συνδέσεις χωρίς την ανάγκη δημιουργίας κρυπτογραφικών tunnels ή μόνιμων εικονικών κυκλωμάτων VCs. Επίσης την δυνατότητα αναβάθμισης διευκολύνει και ο διαχωρισμός των δρομολογητές του παροχέα σε δύο κατηγορίες

- PE δρομολογητής: είναι αυτοί που συντηρούν τα VPN δρομολόγια στα VPN που είναι μέλος ο δρομολογητής
- IP δρομολογητής: είναι αυτοί που δεν συντηρούν VPN δρομολόγια
- Ασφάλεια (Security): τα MPLS προσφέρουν το ίδιο επίπεδο ασφάλειας με τα προσανατολισμένα στην σύνδεση VPNs. Πακέτα συγκεκριμένου VPN δεν μπορούν χωρίς λόγο να βρεθούν σε άλλο VPN. Η ασφάλεια παρέχεται από την πλευρά του παροχέα, ο οποίος εξασφαλίζει τα πακέτα ενός πελάτη να πηγαίνουν στο σωστό VPN
- από το δίκτυο κορμού (backbone) του παροχέα: η κυκλοφορία των VPN πακέτων γίνεται ξέχωρα από άλλα πακέτα. Κάθε προσπάθεια παράνομης προσπέλασης αυτών είναι σχεδόν αδύνατη, διότι είναι πακέτα IP που φέρουν μοναδική ετικέτα του VPN δικτύου για το οποίο προορίζονται.
- Εύκολη δημιουργία (Easy Creation): για να γίνει πλήρη εκμετάλλευση της τεχνολογίας των VPN, πρέπει να παρέχεται ευκολία στους πελάτες να δημιουργήσουν νέα VPN και κοινότητες χρηστών. Εξαιτίας της ασυνδεσμικότητας των MPLS VPN δεν χρειάζονται συγκεκριμένες σημείου προς σημείο αντιστοιχήσεις συνδέσεων και τοπολογιών. Μπορούμε να προσθέσουμε εύκολα νέα sites στα intranets και στα extranets του VPN καθώς και να δημιουργήσουμε κλειστές ομάδες χρηστών. Έτσι δίνεται η δυνατότητα σε ένα site να είναι μέλος σε πολλά VPN αυξάνοντας την ευελιξία στην δημιουργία intranets και extranets.
- Ευέλικτη διευθυνσιοδότηση (Flexible Addressing): για να αυξήσουμε την προσπελασιμότητα ενός VPN, πελάτες ενός παροχέα υπηρεσιών μπορούν να

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

- Υποστήριξη κλάσεων υπηρεσιών (Class of Service –CoS- support): Η CoS είναι σημαντική απαίτηση για πολλούς πελάτες των VPN. Παρέχει την δυνατότητα να ικανοποιηθούν δύο βασικές παράμετροι των VPN
- Πρόβλεψη απόδοσης και πολιτική υλοποίησης
- Υποστήριξη πολλαπλών επιπέδων υπηρεσιών στα MPLS VPNs
- Άμεση εξάπλωση (Straightforward migration): Οι παροχείς υπηρεσιών για να αναπτύξουν γρήγορα τις υπηρεσίες ενός VPN χρησιμοποιούν ένα ευθύ και άμεσο μονοπάτι εξάπλωσης. Τα MPLS είναι μοναδικά επειδή μπορούν να χτιστούν πάνω σε πολλές και διαφορετικές αρχιτεκτονικές δικτύων όπως IP, Frame Relay, ATM κλπ. Η εξάπλωση μέχρι τον τελικό χρήστη είναι απλή γιατί δεν είναι απαραίτητο να γίνει κάποια αλλαγή ούτε στον δρομολογητή CE του πελάτη, ούτε στο intranet που δουλεύει ώστε να υποστηρίξουν το MPLS.

4.2 Αρχιτεκτονική των MPLS/VPN Δικτύων

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

Γενικά για να γίνει αυτό εφικτό απαιτούνται:

- Ελεγχόμενη διανομή των πληροφοριών δρομολόγησης (Constrained distribution)
- Πολλαπλοί πίνακες προώθησης
- Νέοι τύποι διευθύνσεων, οι VPN-IP
- Οι μηχανισμοί προώθησης του MPLS.
- Customer Edge device (CE). Πρόκειται για την ακραία συσκευή ενός πελάτη που ανήκει σε ένα VPN και συνδέεται σε ένα η περισσότερες συσκευές του παρόχου. Θεωρητικά μπορεί να είναι ένας μεμονωμένος εξυπηρετητής, ένας μεταγωγέας ή στη συνηθέστερη και πιο πρακτική μορφή ένας δρομολογητής.
- Provider Edge device (PE). Είναι ο ακραίος δρομολογητής του δικτύου του παρόχου στον οποίο συνδέονται οι CE δρομολογητές.
- Provider device (P). Κάθε ενδιάμεσος δρομολογητής του δικτύου του παρόχου.

Είναι σημαντικό να τονιστεί ότι το μοντέλο MPLS VPNs δεν ταυτίζεται με κάποιο είδος "overlay" στο δίκτυο του παρόχου, συνεπώς δεν υπάρχει κάποια ένοια ιδεατού δικτύου κορμού για τον πελάτη. Κάθε CE δρομολογητής ενός πελάτη έχει μία ομότιμη σχέση διασύνδεσης με τον PE δρομολογητή του παρόχου και όχι με κάποιον άλλον CE δρομολογητή του σε ένα άλλον σημείο παρουσίας. Ουσιαστικά δεν γνωρίζει όσο αφορά την δρομολόγηση, την ύπαρξη άλλων CE δρομολογητών.

4.2.1 Ελεγχόμενη διανομή των πληροφοριών δρομολόγησης

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

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

2. Από τον εισερχόμενο PE η πληροφορία αναδιανέμεται στο BGP του παρόχου.
3. Η πληροφορία δρομολόγησης διανέμεται ανάμεσα στους υπόλοιπους PE δρομολογητές του δικτύου.
4. Στους εξερχόμενους PE δρομολογητές η πληροφορία δρομολόγησης εισάγεται από το BGP του παρόχου.
5. Η πληροφορία δρομολόγησης αποστέλλεται από τον PE δρομολογητή εξόδου στον CE δρομολογητή. Αυτό μπορεί να γίνει με RIP, OSPF, static routes, BGP. Η ελεγχόμενη διανομή των πληροφοριών δρομολόγησης γίνεται με χρήση της τεχνικής φιλτραρίσματος με βάση την ιδιότητα / χαρακτηριστικό Community του BGP. Στο βήμα 2 της παραπάνω διαδικασίας ο PE δρομολογητής εισάγει μία κατάλληλη τιμή στο πεδίο Community πριν εξάγει τις πληροφορίες δρομολόγησης στο BGP. Στο βήμα 4 ο PE δρομολογητής εξόδου χρησιμοποιώντας τη τιμή του BGP Community ελέγχει την διανομή των πληροφοριών δρομολόγησης στον CE δρομολογητή. Σημειώστε ότι η λειτουργία αυτή ελέγχεται αποκλειστικά από τον πάροχο και ο πελάτης δεν χρειάζεται να γνωρίζει κάτι ή να εμπλακεί με κάποια σχετική ενέργεια.

Όσο αφορά τα μεγέθη, επειδή το πεδίο BGP Community έχει μέγεθος 32 bits εκ των οποίων ένα τμήμα των 16 bits κρατά το Autonomous System Number, επιτρέπει 216 διαφορετικές communities ή αλλιώς το πολύ 216 VPN πελάτες. Για ένα παγκόσμιο πάροχο αυτό μάλλον είναι περιοριστικό οπότε έχει εισαχθεί η έννοια των Extended Communities όπου τα 16 bits του AS Number χρησιμοποιούνται για την διάκριση 232 communities αφού στα ιδιωτικά VPNs τα AS Numbers έχουν εντελώς τοπική σημασία.

4.2.2 Πολλαπλοί πίνακες προώθησης

Επειδή ένας PE δρομολογητής θα έχει συνήθως πολλά διαφορετικά VPNs η διατήρηση ενός κοινού πίνακα δρομολόγησης για όλα τα ιδιωτικά δίκτυα αποτρέπει τον διαχωρισμό της πληροφορίας δρομολόγησης με αποτέλεσμα να είναι πιθανή η προώθηση πακέτων μεταξύ διαφορετικών VPNs. Το πρόβλημα αυτό αντιμετωπίζεται

με την υποστήριξη πολλαπλών πινάκων δρομολόγησης σε κάθε PE δρομολογητή. Ειδικότερα συντηρείται ένας πίνακας δρομολόγησης για κάθε ένα VPN.

4.2.3 Διευθύνσεις VPN-IP

Το πρωτόκολλο δρομολόγησης BGP, όπως και τα υπόλοιπα, προϋποθέτουν για να λειτουργήσουν, χρήση μοναδικών IP διευθύνσεων. Αντίθετα στα MPLS VPNs μπορούν να συνυπάρχουν τόσο επικαλύψεις διευθύνσεων μεταξύ διαφορετικών VPNs όσο και χρήση των ιδιωτικών διευθύνσεων (π.χ. διευθύνσεις 10.0.0.0). Το πρόβλημα αντιμετωπίζεται με τη δημιουργία ενός νέου τύπου διευθύνσεων, των IP-VPNS. Μία IP-VPN διεύθυνση κατασκευάζεται με την παράθεση ενός πεδίου με σταθερό μήκος, Route Distinguisher, και μιας συνηθισμένης IP διεύθυνσης. Το πεδίο Route Distinguisher παράγεται μοναδικά από το VPN πάροχο, ακόμα και για VPNs που κατανέμονται μεταξύ διαφορετικών παρόχων, και περιλαμβάνει τρία πεδία: Type (2 octets), Autonomous System Number (4 octets), Assigned Number (4 octets).

Το πεδίο Autonomous System Number περιέχει τον AS Number του παρόχου του VPN και το Assigned Number ένα μοναδικό αριθμό για αυτό το VPN που εκχωρείται από τον πάροχο. Συνεπώς ο Route Distinguisher είναι όχι μόνο τοπικά μοναδικός, στα πλαίσια του παρόχου, αλλά και καθολικά. Κατά συνέπεια οι IP-VPN διευθύνσεις είναι καθολικά μοναδικές, αφού φέρουν μοναδικό Route Distinguisher έστω και αν χρησιμοποιούν κοινές ή ιδιωτικές απλές IP διευθύνσεις.

Η διαχείριση των διευθύνσεων αυτών από το BGP είναι εφικτή λόγω τις ικανότητας του multiprotocol BGP να χειρίζεται δρομολογήσεις για multiple-address families. Η χρήση των διευθύνσεων αυτών, IP-VPNs, περιορίζεται αποκλειστικά στους PE δρομολογητές του παρόχου. Ο πελάτης, CE δρομολογητής, είναι άσχετος με αυτό το μοντέλο. Σημειώστε ότι οι IP-VPNs διευθύνσεις χρησιμοποιούνται και μεταφέρονται μόνο από τα πρωτόκολλα δρομολόγησης (εδώ το BGP) και όχι στο header του πακέτου IP.

4.3 Οι μηχανισμοί προώθησης του MPLS-VPN

Το καθοριστικό πλεονέκτημα του MPLS, στην προκειμένη περίπτωση, είναι ο διαχωρισμός της πληροφορίας προώθησης (ετικέτα) από το περιεχόμενο του header (IP διεύθυνση) του IP πακέτου που εφαρμόζει. Για την υποστήριξη των IP-VPN διευθύνσεων από το MPLS χρησιμοποιείται πολύ έξυπνα η τεχνική του label stack. Πρόκειται για στοίβα δύο επιπέδων (δηλαδή κάθε πακέτο φέρει δύο ετικέτες) όπου:

- η ετικέτα στην κορυφή της στοίβας (δεύτερο επίπεδο) συσχετίζεται με τους PE δρομολογητές εισόδου / εξόδου και υλοποιεί έτσι το μηχανισμό προώθησης από ένα PE δρομολογητή εισόδου σε ένα PE δρομολογητή ειξόδου. Η διανομήτων ετικετών αυτού του επιπέδου μπορεί να γίνει είτε με LDP είτε με CR-LDP ή RSVP αν απαιτείται Traffic Engineering.
- Η ετικέτα του πρώτου επιπέδου ελέγχει την προώθηση στο PE δρομολογητή ειξόδου. Οι ετικέτες αυτού του επιπέδου διανέμονται αποκλειστικά μέσω του BGP μαζί με τις IP-VPN διευθύνσεις. Είναι πολύ σημαντικό μα τονιστεί ότι όταν μία IP-VPN διεύθυνση (ουσιαστικά διεύθυνση πελάτη) διανέμεται μέσω του BGP μεταφέρει ως τιμή next-hop τη διεύθυνση του PE που τη δημιούργησε (και όχι τη διεύθυνση του CE όπως κανείς θα μπορούσε να φανταστεί). Αυτή η next-hop διεύθυνση του PE είναι προφανώς μία συνηθισμένη IP διεύθυνση του δικτύου του παρόχου και δρομολογείται σύμφωνα με τις συνήθεις διαδικασίες δρομολόγησης (π.χ. OSPF).

4.4 Πλεονεκτήματα χρήσης των MPLS VPNs

Γενικά τα IP VPNs είναι μία ελκυστική λύση γιατί:

1. μειώνουν το κόστος σύνδεσης των γραφείων μιας εταιρίας η οργανισμού, των τηλεπικοινωνιακών συσκευών και των κινητών χρηστών μέσα σε ένα intranet που λειτουργεί πάνω από μια δημόσια υποδομή του internet

2. είναι πιο οικονομικά από τα δημόσια δίκτυα που χρησιμοποιούν μισθωμένες γραμμές Επίσης τα συνηθισμένα είδη VPN δικτύων, αναβαθμίζονται πολύ δύσκολα. Αυτό συμβαίνει διότι βασίζονται σε πλήρεις τοπολογίες από κρυπτογραφικά tunnels ή από μόνιμα εικονικά κυκλώματα γεγονός που καθιστά την προσθήκη νέων πελατών εξαιρετικά δύσκολη.
   Τέτοιου είδους VPN είναι τα εξής:

- IPSec
- Layer 2 tunneling protocol (L2TP)
- Layer 2 forwarding protocol (L2F)
- Generic routing encapsulation (GRE)
- Frame relay
- ATM protocols

Η επιπλέον πληροφορία (overhead) που πρέπει να προστίθεται ώστε να εξασφαλιστούν οι προσανατολισμένες στην σύνδεση υπηρεσίες των παραπάνω VPN, δημιουργεί ανυπέρβλητα προβλήματα σε έναν παροχέα που πρέπει να υποστηρίζει εκατοντάδες ή και χιλιάδες VPNs, καθένα από τα οποία μπορεί να έχει εκατοντάδες ή και χιλιάδες sites και χιλιάδες η δεκάδες χιλιάδες δρομολόγια.

Τα MPLS VPNs τα οποία είναι πρωτόκολλα επιπέδου 3, μη προσανατολισμένα στην σύνδεση (ασυνδεσμικά) είναι ουσιαστικά περισσότερο αναβαθμίσιμα και πιο εύκολο να δημιουργηθούν και να διαχειριστούν, από ότι τα συμβατικά VPN.

Επιπλέον κάθε MPLS VPN μπορεί να παρέχει προστιθέμενης αξίας υπηρεσίες όπως φύλαξη δεδομένων και εφαρμογών, δίκτυα επιχειρήσεων και τηλεφωνικές υπηρεσίες.

Συνοψίζοντας τα MPLS VPNs προσφέρουν:

- Μια πλατφόρμα για την ταχύτατη ανάπτυξη προστιθέμενης αξίας IP υπηρεσιών όπως intranets, extranets, φωνή, πολυμέσα και δικτυακές επιχειρήσεις.
- Ιδιωτικότητα και ασφάλεια αντίστοιχη των Layer-2 VPNs περιορίζοντας τις VPN διαδρομές μόνο ανάμεσα σε εκείνους τους δρομολογητές που είναι μέλη του VPN
- Ενσωμάτωση των intranets των πελατών, χωρίς καμία περικοπή.
- Αυξημένη δυνατότητα αναβάθμισης έτσι ώστε, να μπορούν να φιλοξενηθούν χιλιάδες sites ανά VPN και δεκάδες ή και χιλιάδες VPN ανά παροχέα.
- IP - Class of Service (CoS), υποστήριξη πολλών κλάσεων υπηρεσιών και προτεραιοτήτων εντός του VPN ή ανάμεσα στα VPNs.
- Εύκολη διαχείριση των μελών ενός VPN.
- Κλιμακωτή διασύνδεση εξωτερικών intranets και extranets που περικλείουν πολλές επιχειρήσεις.

Χρήσιμη ορολογία

VPN: Η συντομογραφία αφορά στα Virtual Private Networks (ιδιωτικά ιδεατά δίκτυα). Η λογική τους στηρίζεται στην δημιουργία μιας αποκλειστικής σύνδεσης, μέσω του Internet, μεταξύ δύο επιμέρους σημείων. Η δημιουργία αυτής της σύνδεσης συνδυάζει την αποστολή κρυπτογραφημένων δεδομένων μεταξύ δύο διαφορετικών σημείων. Σύνηθης εφαρμογή αποτελεί η μεταφορά "ευαίσθητων" δεδομένων, μεταξύ διαφορετικών εγκαταστάσεων μιας εταιρίας.

SSL και IPsec: Πρόκειται για τις δύο πλέον γνωστές τεχνολογίες, μέσω των οποίων δημιουργούνται VPNs. Το IPsec, αποτέλεσε κατά το παρελθόν την βασική επιλογή στο στήσιμο ιδιωτικών ιδεατών δικτύων, ενώ για την λειτουργία του, απαραίτητη προϋπόθεση ήταν και η εγκατάσταση στους υπολογιστές client ξεχωριστού VPN client. Το SSL αντίθετα, λειτουργεί σε διαφορετικό επίπεδο δικτύου από το IPsec, και προσφέρει μία σειρά ιδιαίτερα χρήσιμων λειτουργιών, όπως authentication σε επίπεδο server, κρυπτογράφηση δεδομένων, μηχανισμούς εξασφάλισης της μεταφοράς δεδομένων και άλλα. Παράλληλα, φαίνεται να αποτελεί πλέον την κύρια επιλογή στην δημιουργία VPNs.

Firewall και IDS: Συσκευή, λογισμικό ή και συνδυασμός και των δύο παραπάνω που αναλαμβάνει να δράσει σαν "τείχος προστασίας" στο εταιρικό δίκτυο. Η πλέον τυπική λειτουργία των firewalls στηρίζεται σε ένα σύνολο κανόνων, είτε default, είτε καθορισμένων από το χρήστη/πελάτη. Τα Intrusion Detection Systems (αντίστοιχα συσκευή, λογισμικό ή και συνδυασμός και των δύο παραπάνω), αναλαμβάνουν να εντοπίσουν με την σειρά τους πιθανές απόπειρες προσβάσεις στο εταιρικό δίκτυο. Οι αλγόριθμοι πάνω στους οποίους βασίζεται η λειτουργία είναι, συνήθως, πιο προηγμένοι από τους αντίστοιχους των firewalls.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1." Building and Managing Virtual Private Netwarks"

[Dave Kasiur,John Wiley & Sons]

2." Διαλέξεις από το Πανεπιστήμιο Berkley"

[Gordon Chaffe]

3." Virtual Private Networks-Second Edition"

[Charlie Scott,Paul Wolfe,Mike Erwin]

4."IPSec VPN Desing"

[Vijay Bollapragada,Mohamed Khalid,Scott Wainner]

5."MPLS and VPN architectures"

[Jim Guichard,Ivan Pepelnjak,Jeff Apcar]

6."Intergrated Communications Managment of Broadband Netwarks"

[Griffin David]

7."Layer 2 VPN architectures"

[Luo,Wei,Bokotey,Dmitry]

8."Interworking with TCP/IP"

[Douglas E. Comer]

INTERNET LINKS

www.alliancedatacom.com

www.frama-relay-resourse.com/tutorials.asp

www.findvpn.com

www.shmoo.com

www.vpnc.org/vpn-standards.html

www.cisco.com/en/us/products/sw/secursw/ps2308

www.cert.org

www.ietf.org

www.rsa.com

www.dir.yahoo.com/computers_and_internet/security_and_encryption

www.corecom.com/html/vpn.html

www.esc.de/intranet/vpn.html

www.computerword.com/securitytopics/security/story/0.10801.97906.00,html