Τ.Ε.Ι. ΠΑΤΡΑΣ ΣΧΟΛΗ ΣΔΟ
ΤΜΗΜΑ ΕΠΙΧΕΙΡΗΜΑΤΙΚΟΣ ΣΧΕΔΙΑΣΜΟΣ ΚΑΙ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Ιδεατά Ιδιωτικά Δίκτυα
(Virtual Private Networks)
Πρωτόκολλα, Τεχνολογίες και Εφαρμογές

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ ΤΩΝ

- **ΚΑΜΖΕΛΗ ΑΝΝΑ &**
- **ΚΑΡΑΔΗΜΟ ΙΩΑΝΝΗ**

ΕΠΟΠΤΗΣ ΚΑΘΗΓΗΤΗΣ

Δρ. ΜΑΝΔΑΛΟΣ ΛΟΥΚΑΣ

ΠΑΤΡΑ 2013

ΠΕΡΙΕΧΟΜΕΝΑ

Αφιερωμένο σε όσους έχουν πληγεί από
την κατάθλιψη και τη ανασφάλεια

ΠΡΟΛΟΓΟΣ- ΕΥΧΑΡΙΣΤΙΕΣ

Την πτυχιακή εργασία επιμελήθηκαν οι σπουδαστές Καραδήμος Ιωάννης και Καμζέλη Άννα του Τμήματος Επιχειρηματικού Σχεδιασμού και Πληροφοριακών Συστημάτων του Α.Τ.Ε.Ι Πατρών.

Επιτηρητής του θέματος είναι ο καθηγητής Δρ. Λουκάς Μάνδαλος και σ' αυτό το σημείο θα θέλαμε να τον ευχαριστήσουμε θερμά για την πολύτιμη βοήθεια, την στήριξη και την καθοδήγηση που μας παρείχε αλλά κυρίως για την υπομονή που έδειξε στην διάρκεια της εκπόνησης εργασίας μας έτσι ώστε δεδομένων των συνθηκών και των απαιτήσεων της καθημερινότητας που έπρεπε να αντιμετωπίσουμε να καταφέρουμε τελικά να φτάσουμε και στην ολοκλήρωσή της.

Επίσης, ένα μεγάλο ευχαριστώ σε φίλους και στην οικογένειά μας για την ηθική και την ψυχολογική υποστήριξη που μας παρείχαν απλόχερα ώστε να αντεπεξέλθουμε στις απαιτήσεις της σημερινής εποχής και να καταφέρουμε παράλληλα να πραγματοποιήσουμε και τους στόχους μας.

Σκοπός αυτής της εργασίας είναι να προσπαθήσει να αναλύσει το θέμα τον ιδεατών ιδιωτικών δικτύων, κάτι που θα απασχολήσει πολλούς και για πολλές δεκαετίες ακόμη μιας και είναι ένας κλάδος ο οποίος ταχύτατα αναπτύσσεται και εξελίσσεται στο πέρασμα των χρόνων.

Η εργασία ανατέθηκε μετά την ολοκλήρωση των μαθημάτων του προγράμματος σπουδών του τμήματος Επιχειρηματικού Σχεδιασμού και Πληροφορικών Συστημάτων, μια μεταβατική περίοδο στην ζωή όλων. Είναι η περίοδος της επαγγελτικής καταξίωσης και βιοπορισμού, συν της στρατιωτικής θητείας για τους άντρες. Κάτι που αλλάξει της προτεραιότητες με αποτέλεσμα να έχει μερικά χρονικά κενά μέχρι την ολοκλήρωση της.

Στην επόμενες σελίδες αναπτύσσονται τα κύρια και βασικά σημεία που απαιτούνται για την δημιουργία ενός VPN, βασικό χαρακτηριστικό είναι ότι με μια πρώτη ανάγνωση θα νομίσει κάνεις ότι μιλάμε για διαφορετικά δίκτυα και όχι συγκεκριμένα για ένα Ιδεατό Ιδιωτικό Δίκτυο. Αναλύεται η ανάγκη για την δημιουργία τους και τα βασικά σημεία της εξέλιξης τους γενικότερα προσπαθούμε να δώσουμε μια όσο το δυνατόν πληρέστερη εικόνα.

Κεφάλαιο 1^{ο}

Η έννοια του δικτύου είναι γνωστή από αρχαιοτάτων χρόνων. Η σημασία του στην ανάπτυξη, έπαιξε και παίζει πολύ σημαντικό ρόλο. Οι μορφές που μπορεί να έχει ένα δίκτυο είναι πολλές και ποικίλες. Εξαρτάται από το σκοπό της χρήσης του και το τι μεταφέρει. Κύριος λόγος ύπαρξης ενός δικτύου, είναι η σύνδεση πολλών σημείων μεταξύ τους, αλλά και η εύκολη πρόσβαση και μεταφορά στοιχείων από το ένα στο άλλο.

Το πρώτο και σημαντικότερο δίκτυο που αναπτύχθηκε στην ανθρώπινη ιστορία είναι το οδικό, διευκολύνοντας την σύνδεση και μετακίνηση από οικισμό σε οικισμό. Άλλα σημαντικά δίκτυα της ιστορίας είναι: το δίκτυο υδροδότησης, το αποχετευτικό, το ακτοπλοϊκό, το δίκτυο ηλεκτροδότησης κτλ.

Η ανάγκη του ανθρώπου για επικοινωνία οδήγησε στην ανάπτυξη του τηλεφωνικού δικτύου. Με την σειρά του το τηλεφωνικό δίκτυο και μέσο της ανάπτυξης των υπολογιστών, έφτασε σήμερα να αποκαλείται τηλεπικοινωνιακό δίκτυο και να εισάγει στον σύγχρονο άνθρωπο την έννοια της πολυμορφικής επικοινωνίας.

Από το στάδιο της μεταφοράς φωνής μέσο ηλεκτροπαλμών σε ένα χάλκινο καλώδιο φτάσαμε σήμερα, στο στάδιο μεταφοράς δεδομένων και με την χρήση τον ηλεκτρονικών υπολογιστών, στην επεξεργασίας τους και την επικοινωνία με κείμενο, ήχο και εικόνα.

Η εξάπλωση του τηλεπικοινωνιακού δικτύου είναι σήμερα παγκόσμια, μπορεί κανείς να επικοινωνήσει με κάποιον που είναι στην άλλη άκρη της γης, αλλά και οι επιχειρήσεις να δραστηριοποιούνται σε περισσότερα από ένα σημεία παγκοσμίως. Έτσι η δημιουργία ενός δικτύου που απλά επικεντρώνεται στο να συνδέει απλά σταθερά σημεία δεν είναι αρκετό γιατί εκτός από την ευκολία της επικοινωνίας και την μετάδοση δεδομένων και πληροφοριών που παρέχει παράλληλα δημιουργούνται πολύ σοβαρά θέματα ασφάλειας και αξιοπιστίας.

Έχουν δαπανηθεί πολλά χρήματα όλα αυτά τα χρόνια ώστε να μπορεί να αυξηθεί το επίπεδο ασφάλειας στην επικοινωνία των υπολογιστών και όχι μονό.

Αυτός είναι και λόγος της δημιουργίας των **Εικονικών Ιδεατών Δικτύων** (Virtual Private Networking ***VPNs***), τα οποία αποτελούν την μεγαλύτερη μέχρι στιγμής στην εξέλιξη ασφάλειας με το χαμηλότερο δυνατό κόστος και τα οποία

συνδυάζουν τα πλεονεκτήματα των ιδιωτικών και των δημόσιων δικτύων, επιτρέποντας έτσι σε μια διάσπαρτη εταιρεία να έχει την αίσθηση ενός ιδιωτικού δικτύου μέσω της χρήσης ενός δημόσιου για την μεταφορά δεδομένων και πληροφοριών όπου και να βρίσκονται και κυρίως με ασφάλεια.

Στην εργασία αυτή θα δούμε μερικά πράγματα που αφορούν τα VPNs μιας και είναι κάτι που εξελίσσεται ακόμα και θα απασχολήσουν την ανθρωπότητα για πολλές ακόμα δεκαετίες..

1.1 Γενικά στοιχειά

Η τεχνολογία των Εικονικών Ιδιωτικών Δικτύων (Virtual Private Networking, **VPNs**) αν και αντικειμενικά καινούργια έλαβε πολύ γρήγορα μεγάλες διαστάσεις στην αγορά των δικτύων. Η τεχνολογία VPN πρωτοϋιοθετήθηκε από κάποιους που χρησιμοποίησαν την τεχνολογία για να προσφέρουν ελεύθερα δοκιμαστικά προϊόντα (trials) κι έτσι να ενημερώσουν το κοινό σχετικά με αυτά. Εφόσον η επιχειρηματική κοινωνία αναζητούσε έναν οικονομικό και ασφαλή τρόπο για να συνδέσει τις σελίδες της, πολλοί εμπορικοί οίκοι ξεκίνησαν να χρησιμοποιούν αυτήν την καινούργια τεχνολογία. Με αργά βήματα επέκτειναν αυτήν την υποδομή με στόχο να διευκολύνουν τους υπαλλήλους τους να συνδεθούν στην εταιρική σελίδα από τα σπίτια τους ή και κατά την διάρκεια ταξιδιών. Αυτό προετοίμασε τον δρόμο για την δεύτερη φάση της ανάπτυξης των Ιδιωτικών Εικονικών Δικτύων. Η τεχνολογία εφαρμόστηκε σε κάποιες όχι και τόσο κρίσιμες εφαρμογές και αργότερα σε άλλες κατεξοχήν σημαντικές, οι οποίες απαιτούσαν ανυπέρβλητη ασφάλεια στις πληροφορίες που περιείχαν. Οι ποικίλες φάσεις της ανάπτυξης της τεχνολογίας VPN παραθέτονται στον παρακάτω πίνακα:

ΧΡΟΝΙΚΟ ΠΛΑΙΣΙΟ	ΦΑΣΗ ΑΓΟΡΑΣ	ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΑΓΟΡΑΣ
1990	ΦΑΣΗ 1η: Πρώιμοι ενστερνιστές	• Δοκιμαστικά υπηρεσιών • Τηλεταξιδευτές (Telecommuters) • Ad-hoc employment
1998	ΦΑΣΗ 2η: ΚΛΗΣΗ ΑΠΟ ΕΞΩΤΕΡΙΚΟΥΣ ΕΡΓΑΖΟΜΕΝΟΥΣ	•Εργαζόμενοι από το σπίτι •Κινητές μονάδες εργαζομένων •Παραδοσιακή κλήση για την δημιουργία αντιγράφων ασφαλείας

1999	Φάση 3η: ΔΙΑΚΛΑΔΩΣΗ ΚΛΗΣΗΣ ΕΞΩΤΕΡΙΚΩΝ ΕΡΓΑΖΟΜΕΝΩΝ	• Χρήση για ανεφοδιασμό και για δημιουργία αντιγράφων ασφαλείας • Μερικά «tunnels», πολύ χρήστες • Μη κρίσιμη LAN-to-LAN κίνηση δεδομένων
2000	ΦΑΣΗ 4η: EXTRANETS	• End to end QoS & SLAs • Πολλά Tunnels, πολύ χρήστες • Μεγάλης κρισιμότητας LAN-LAN κίνηση δεδομένων • Ασφαλή Extranets

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 της 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 πια 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. 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. Η 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, ATM ή IP. (αναλύονται στα κεφαλαίο 3 & 5)

4. Η τοπολογία του δικτύου, που μπορεί να εκτείνεται από απλή τοπολογία σε δίκτυο με πολυεπίπεδες ιεραρχικές τοπολογίες για μεγαλύτερα δίκτυα.

1.2 Το μοντέλο αναφοράς OSI

Το μοντέλο αναφοράς **OSI** επηρέασε όχι τόσο τον τρόπο με τον οποίο σχεδιάζουμε, αλλά πολύ περισσότερο τον τρόπο με τον οποίο κατανοούμε τα δίκτυα υπολογιστών.

Αξίζει να παρατηρήσουμε ότι το μοντέλο αναφοράς OSI δεν αποτελεί μια αρχιτεκτονική δικτύου, καθώς δεν καθορίζει τα αναγκαία πρωτόκολλα και τα σημεία επαφής τους. Ο οργανισμός ISO, σε συνδυασμό με τη Διεθνή Ένωση Τηλεπικοινωνιών (International Telecommunication Union, **ITU**), καθόρισε μια σειρά από πρωτόκολλα βασισμένα στο μοντέλο αναφοράς OSI, τα οποία συχνά καλούνται ως η σειρά πρωτοκόλλων **«X»** (π.χ. X.25, X.400, X.500 κ.ά.). Τα πρωτόκολλα ISO δεν έτυχαν όμως ευρείας αποδοχής και χαρακτηρίστηκαν έτσι από την εμπορική αποτυχία τους.

*Το **μοντέλο αναφοράς OSI έχει επτά επίπεδα***. Τα τρία χαμηλότερα επίπεδα ασχολούνται με τον έλεγχο της μετάδοσης των μηνυμάτων μέσα στο δίκτυο, ενώ τα τέσσερα ανώτερα επίπεδα παρέχουν την αξιόπιστη μεταβίβαση των δεδομένων μεταξύ των τελικών χρηστών.

Τα VPNs έχουν κατά κύριο λόγο, εφαρμογή στο δεύτερο και τρίτο επίπεδο, καθώς είναι τα επίπεδα που συναντούνται παντού (πρωτόκολλα, δίκτυα, αρχιτεκτονικές κτλ). Έτσι, και τα επτά επίπεδα υλοποιούνται μόνο στους υπολογιστές που λειτουργούν ως τερματικοί σταθμοί.

Το φυσικό επίπεδο

Το φυσικό επίπεδο (**physical layer**) ασχολείται με τη μετάδοση ακατέργαστων bits σε ένα κανάλι επικοινωνίας. Τα θέματα σχεδίασης έχουν να κάνουν με τη διασφάλιση ότι , όταν η μία πλευρά στέλνει ένα bit 1, αυτό λαμβάνεται από την άλλη πλευρά ως bit 1 και όχι ως bit 0. Τα θέματα σχεδίασης εδώ, στην πλειοψηφία τους ασχολούνται με μηχανικές, ηλεκτρικές και διαδικασίες διασυνδέσεις καθώς και με το φυσικό μέσο μετάδοσης, το οποίο βρίσκεται κάτω από φυσικό επίπεδο.

Το επίπεδο σύνδεσης δεδομένων

Η κύρια αποστολή του επιπέδου σύνδεσης δεδομένων (**data link layer**) είναι να μετασχηματίσει το ακατέργαστο μέσο μετάδοσης σε μια γραμμή που εμφανίζεται ελεύθερη από σφάλματα μετάδοσης στο επίπεδο δικτύου. Ο σκοπός αυτός επιτυγχάνεται με τη διάσπαση των δεδομένων εισόδου από τον αποστολέα σε πλαίσια δεδομένων (data frames) μετάδοση αυτών με τη σειρά και επεξεργασία των πλαισίων επιβεβαίωσης λήψης (acknowledgement frames), που επιστρέφονται από τον αποδέκτη . Εφόσον το φυσικό επίπεδο απλώς αποδέχεται και μεταδίδει ένα συρμό bits , χωρίς να νοιάζεται για το νόημα και τη δομή , η δημιουργία και η αναγνώριση των ορίων των πλαισίων εξαρτάται πλέον από το επίπεδο σύνδεσης δεδομένων . Αυτή μπορεί να επιτευχθεί με την επισύναψη ειδικών ακολουθιών bits στην αρχή και στο τέλος των πλαισίων .

Το επίπεδο δικτύου

Το επίπεδο δικτύου (**network layer**) με τον έλεγχο της λειτουργίας του υποδικτύου. Ένα βασικό θέμα στη σχεδίαση είναι ο καθορισμός του τρόπου δρομολόγησης των πακέτων από την αφετηρία στον προορισμό τους. Οι διαδρομές θα μπορούσαν να βασιστούν σε στατικούς πίνακες οι οποίοι είναι «καλωδιωμένοι» (“wired”) στο δίκτυο και σπάνια τροποποιούνται . Ακόμη θα μπορούσαν να οριστούν στην αρχή κάθε συνομιλίας, για παράδειγμα μιας συνόδου τερματικών . Τέλος θα μπορούσαν να είναι δυναμικές και να καθορίζονται εκ νέου για κάθε πακέτο για να απεικονίζουν το τρέχων φορτίο του δικτύου. Εάν στο υποδίκτυο είναι παρόντα πολλά πακέτα την ίδια χρονική στιγμή, θα εμπλακεί το ένα στην διαδρομή του άλλου, δημιουργώντας συμφόρηση (bottleneck). Ο έλεγχος μιας τέτοιας συμφόρησης επίσης ανήκει στις αρμοδιότητες του επιπέδου δικτύου.

Το επίπεδο μεταφοράς

Η βασική λειτουργία του επιπέδου μεταφοράς (**transport layer**) είναι η αποδοχή δεδομένων από το επίπεδο συνόδου ή διάσπαση αυτών σε μικρότερες μονάδες εάν χρειαστεί , η μεταφορά τους στο επίπεδο δικτύου και η διασφάλιση ότι όλα τα τμήματα φτάνουν σωστά στην άλλη πλευρά . Επιπλέον όλα αυτά πρέπει να γίνουν αποδοτικά και με τέτοιο τρόπο ώστε να απομονώνουν το επίπεδο συνόδου από τις αναπόφευκτες αλλαγές στην τεχνολογία του υλικού . Υπό κανονικές συνθήκες , το επίπεδο μεταφοράς δημιουργεί μια ξεχωριστή σύνδεση δικτύου για κάθε σύνδεση

μεταφοράς που απαιτείται από το επίπεδο συνόδου . Εάν η σύνδεση μεταφοράς απαιτεί υψηλό ρυθμό εξυπηρέτησης (throughput) , το επίπεδο μεταφοράς μπορεί να δημιουργήσει πολλαπλές συνδέσεις δικτύου , μοιράζοντας τα δεδομένα ανάμεσα στις συνδέσεις δικτύου για να βελτιώσει το ρυθμό εξυπηρέτησης . Από την άλλη πλευρά εάν η δημιουργία ή η συντήρηση μιας σύνδεσης δικτύου είναι ακριβή , το επίπεδο μεταφοράς μπορεί να πολυπλέκει πολλές συνδέσεις μεταφοράς στην ίδια σύνδεση δικτύου για να ελαττώσει το κόστος . Σε όλες τις περιπτώσεις το επίπεδο μεταφοράς χρειάζεται πάντα για να κάνει την πολυπλεξία διάφανη στο επίπεδο συνόδου . Το επίπεδο μεταφοράς καθορίζει επίσης τι είδους υπηρεσίες θα παρέχει το επίπεδο συνόδου . Ο πιο γνωστός τύπος σύνδεσης μεταφοράς είναι ένα ελεύθερο από σφάλματα από σημείο σε σημείο κανάλι (**point to point**), το οποίο παραδίδει μηνύματα με την σειρά με την οποία έχουν σταλεί.

Το επίπεδο συνόδου

Το επίπεδο συνόδου (**session layer**) επιτρέπει στους χρήστες διαφορετικών μηχανημάτων να εγκαθιστούν συνόδους (sessions) μεταξύ τους. Μία σύνοδος επιτρέπει μια συνήθη μεταφορά δεδομένων, όπως και το επίπεδο μεταφοράς , αλλά παρέχει και μερικές πρόσθετες υπηρεσίες που είναι χρήσιμες σε πολλές εφαρμογές. Μία σύνοδος μπορεί να χρησιμοποιηθεί για να επιτρέψει τη σύνδεση ενός χρήστη σ' ένα απομακρυσμένο σύστημα καταμερισμού χρόνου (time sharing) ή για να μεταφέρει ένα αρχείο μεταξύ δύο μηχανών .

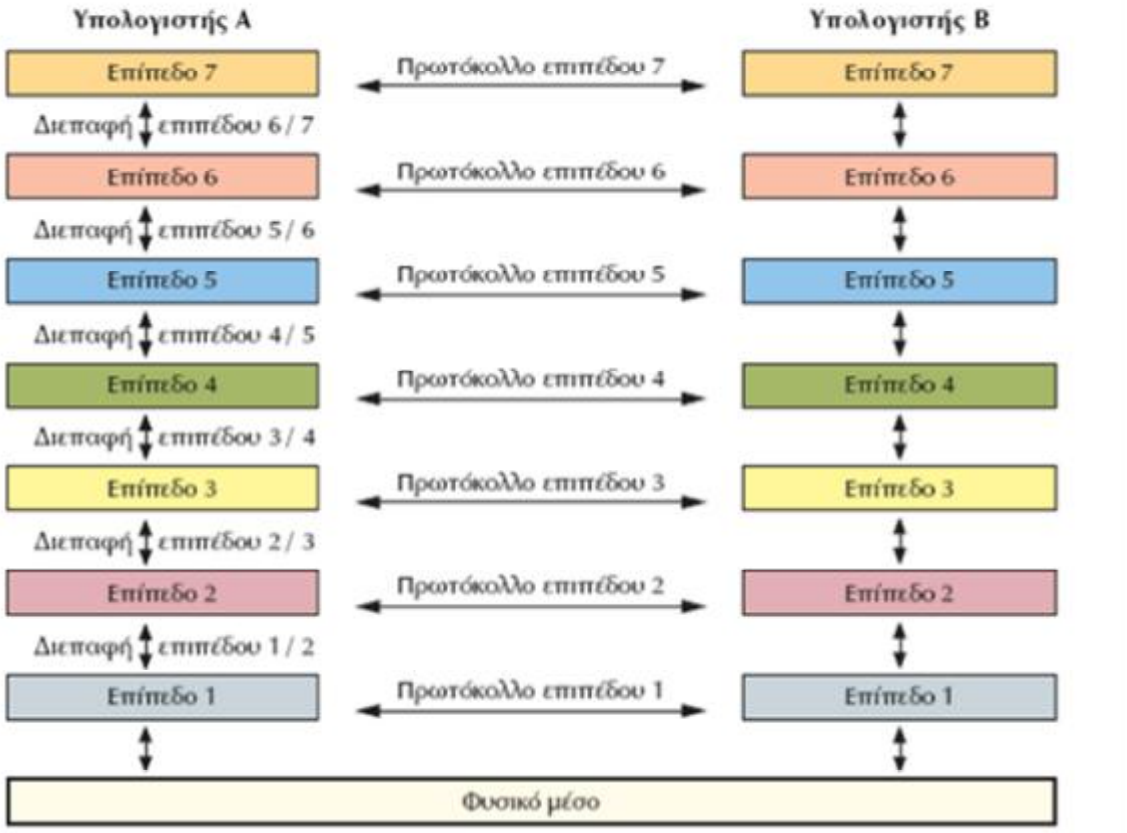
Το επίπεδο παρουσίασης

Το επίπεδο παρουσίασης (**presentation layer**) εκτελεί συγκεκριμένες λειτουργίες οι οποίες ζητούνται αρκετά συχνά από τους χρήστες , για να εξασφαλίζουν την εύρεση μιας γενικής λύσης γι' αυτούς , ώστε να μην αφήνεται ο κάθε χρήστης να λύνει τα προβλήματα μόνος του . Συγκεκριμένα , ενώ όλα τα κατώτερα επίπεδα ενδιαφέρονται μόνο για την αξιόπιστη μετακίνηση bits από το ένα μέρος στο άλλο , το επίπεδο παρουσίασης καταπιάνεται με το συντακτικό και τη σημασιολογία των πληροφοριών που μεταδίδονται . Ένα τυπικό παράδειγμα υπηρεσίας παρουσίασης είναι η κωδικοποίηση δεδομένων σε ένα κώδικα που συμφωνήθηκε στη διαδρομή . Επίσης το επίπεδο παρουσίασης ενδιαφέρεται και για άλλα θέματα όπως η αναπαράσταση πληροφοριών. Για παράδειγμα η συμπίεση των δεδομένων χρησιμοποιείται για να ελαττώσει τον αριθμό των bits που πρόκειται να

μεταδοθούν και συχνά απαιτείται κρυπτογράφηση για να εξασφαλιστεί η μυστικότητα (**privacy**) και η γνησιότητα (**authentication**) της πληροφορίας .

Το επίπεδο εφαρμογής

Το επίπεδο εφαρμογής (**application layer**) περιέχει μια ποικιλία πρωτοκόλλων που χρειάζονται συχνά . Για παράδειγμα μπορούμε να αναφέρουμε το λογισμικό των νοητών τερματικών δικτύων (network virtual terminals) ή την εφαρμογή της μεταφοράς αρχείων . Στην τελευταία περίπτωση διαφορετικά συστήματα αρχείων έχουν διαφορετικούς μεθόδους καθορισμού ονομασίας , διαφορετικούς τρόπους αναπαράστασης των γραμμών κειμένου και ούτω καθεξής . Η μεταφορά ενός αρχείου μεταξύ δύο διαφορετικών συστημάτων απαιτεί αντιμετώπιση αυτών και άλλων μη συμβατών καταστάσεων . Η εργασία αυτή επίσης ανήκει στο επίπεδο εφαρμογής , όπως επίσης και το ηλεκτρονικό ταχυδρομείο , η εμφάνιση καταλόγων αρχείων και διάφορες άλλες ειδικού και γενικού σκοπού ευκολίες .



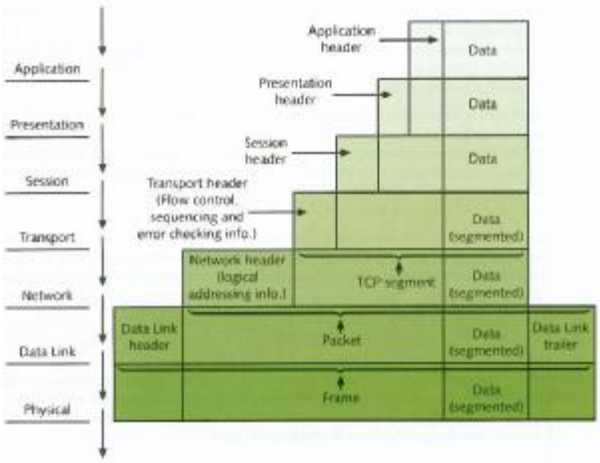
1.3 Ενθυλάκωση

Τα πρωτόκολλα του 3ου επιπέδου (η από άκρο σε άκρο επικοινωνία) δεν εξετάζουν το περιεχόμενο των δεδομένων που λαμβάνονται από την εφαρμογή. Η αποστολή τους είναι να μεταφέρουν τα δεδομένα αξιόπιστα στον απομακρυσμένο υπολογιστή. Ταυτόχρονα όμως θα πρέπει να μεταφέρουν και κάποιες πληροφορίες ελέγχου στο ομότιμό των πρωτόκολλων, οι οποίες θα προσδιορίζουν τις ενέργειες χειρισμού των δεδομένων στον απομακρυσμένο υπολογιστή. Αυτές οι πληροφορίες ελέγχου συνήθως επισυνάπτονται στα δεδομένα με τη μορφή επικεφαλίδας (header). Η ***επικεφαλίδα*** είναι μια δομή δεδομένων, συνήθως μικρού μεγέθους σε σχέση με τον όγκο των δεδομένων, που επισυνάπτεται στην αρχή του μηνύματος και χρησιμοποιείται για την επικοινωνία ομότιμων οντοτήτων. Επίσης, σε μερικές περιπτώσεις μέρος των πληροφοριών ελέγχου επισυνάπτονται στο τέλος του μηνύματος, σχηματίζοντας έτσι μια «ουρά» (trailer). Με αυτό τον τρόπο τα δεδομένα της εφαρμογής περιλαμβάνονται στο νέο μήνυμα που δημιουργείται από τα πρωτόκολλα του 3ου επιπέδου και η διαδικασία αυτή καλείται ***ενθυλάκωση***.

Για παράδειγμα, ένα πρωτόκολλο 3ου επιπέδου επισυνάπτει την επικεφαλίδα H3 στα δεδομένα που λαμβάνει από την εφαρμογή και μεταβιβάζει το νέο μήνυμα [H3 | data] στο αμέσως χαμηλότερο επίπεδο. Στο 2ο επίπεδο επισυνάπτεται η επικεφαλίδα H2 και το μήνυμα πλέον λαμβάνει τη μορφή [H2 | H3 | data].

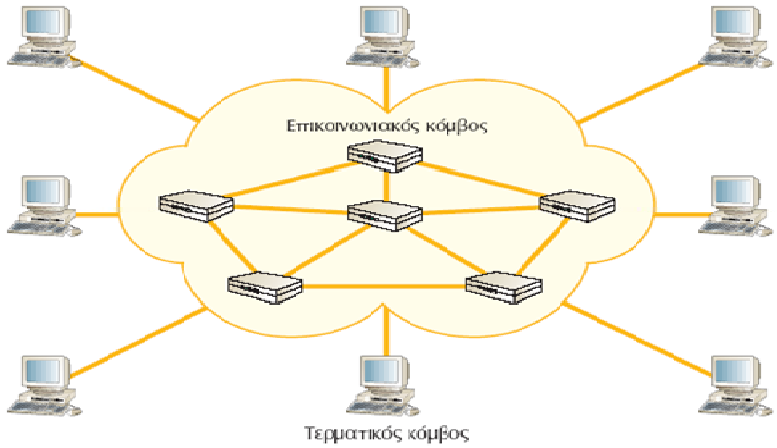
Στο φυσικό επίπεδο προστίθενται τόσο η επικεφαλίδα H1 όσο και η «ουρά» T1, και έτσι στον απομακρυσμένο υπολογιστή προωθείται το μήνυμα [H1 | H2 | H3 | data | T1].

Στον απομακρυσμένο υπολογιστή ακολουθείται η αντίστροφη διαδικασία. Στην πορεία του προς το υψηλότερο επίπεδο, το μήνυμα απαλλάσσεται σταδιακά από τις πληροφορίες ελέγχου (επικεφαλίδες και «ουρές») και τελικά παραδίδεται στην εφαρμογή εμπεριέχοντας μόνο το αρχικό μήνυμα της ομότιμης εφαρμογής.



1.4 Μεταγωγή κυκλώματος & πακέτου

Για τη μεταφορά στοιχείων πέραν μιας τοπικής περιοχής η επικοινωνία επιτυγχάνεται με τη μετάδοση δεδομένων από τη πηγή στον προορισμό τους διαμέσου ενός δικτύου με ενδιάμεσους κόμβους μεταγωγής. Αυτό το δίκτυο μεταγωγής σχεδιάζεται έτσι ώστε να μπορεί να εφαρμόζεται ορισμένες φορές σε τοπικά δίκτυα. Οι κόμβοι μεταγωγής δεν σχετίζονται με το περιεχόμενο των δεδομένων. Σκοπός τους είναι να εξασφαλίζουν μια εύκολη μεταγωγή που θα μετακινεί τα δεδομένα από κόμβο σε κόμβο μέχρι να φτάσουν στον προορισμό τους. Οι τερματικές συσκευές (DTE)[1] που επιθυμούν να επικοινωνήσουν αναφέρονται ως σταθμοί (stations DTE). Κάθε σταθμός (DTE) συνδέεται με έναν κόμβο, και το σύνολο των κόμβων ονομάζεται **δίκτυο επικοινωνιών** (communication network). Τα δεδομένα που εισέρχονται στο δίκτυο από ένα σταθμό δρομολογούνται στον προορισμό τους με την μεταγωγή τους από κόμβο σε κόμβο. Πρέπει να λάβουμε υπόψη :



1. **Ορισμένοι κόμβοι συνδέονται μόνο με άλλους κόμβους**. Η μόνη τους εργασία είναι η εσωτερική (στο δίκτυο) μεταγωγή των δεδομένων. Άλλοι κόμβοι έχουν έναν ή περισσότερους σταθμούς συνδεδεμένους. Επιπρόσθετα, μαζί με τις λειτουργίες μεταγωγής οι κόμβοι δέχονται δεδομένα από τους άλλους συνδεδεμένους σταθμούς καθώς και διανέμουν σε αυτούς δεδομένα.

[1] Η **τερματική** (**DTE**) είναι γενικά μια συσκευή που συνδέεται στο δίκτυο και προωθεί τα δεδομένα της ανταλλάσσοντας πακέτα.

2. **Οι συνδέσεις που γίνονται από κόμβο σε κόμβο πολυπλέκονται**, χρησιμοποιώντας είτε πολυπλεξία διαίρεσης συχνότητας είτε πολυπλεξία διαίρεσης χρόνου.
3. **Συνήθως το δίκτυο δεν είναι πλήρως συνδεδεμένο**. Αυτό σημαίνει πως δεν υπάρχει πάντα μια άμεση σύνδεση μεταξύ κάθε πιθανού ζευγαριού κόμβων. Εντούτοις, είναι πάντα επιθυμητό να έχει περισσότερο από ένα πιθανό δρόμο μέσω του δικτύου για κάθε ζευγάρι σταθμών. Αυτό αυξάνει την αξιοπιστία του δικτύου.

Δύο αρκετά διαφορετικές τεχνολογίες χρησιμοποιούνται στην ευρεία περιοχή των δικτύων μεταγωγής : **μεταγωγή κυκλώματος** και **μεταγωγή πακέτου**. Οι δύο αυτοί τρόποι διαφέρουν στον τρόπο με τον οποίο οι κόμβοι μεταφέρουν την πληροφορία από τη μία σύνδεση στην άλλη, από την πηγή στον προορισμό.

1.4.1 Δίκτυο μεταγωγής κυκλώματος

Η επικοινωνία μέσω της μεταγωγής κυκλώματος υπονοεί ότι υπάρχει ένα κανάλι επικοινωνίας μεταξύ των σταθμών. Αυτό το κανάλι είναι μια ακολουθία συνδέσεων μεταξύ δικτύων και κόμβων. Σε κάθε φυσική σύνδεση ένα λογικό κανάλι είναι αφιερωμένο στη σύνδεση. Η επικοινωνία μέσω της μεταγωγής κυκλώματος περιλαμβάνει τρεις φάσεις :

1. **Εγκατάσταση κυκλώματος (circuit establishment)**: Πριν κάθε σήμα μπορέσει να διαβιβαστεί στον προορισμό του ένα κύκλωμα από άκρη σε άκρη του δικτύου πρέπει να εγκατασταθεί. Πριν ολοκληρωθεί η σύνδεση, μια δοκιμή γίνεται για να καθορίσει εάν ο δέκτης είναι απασχολημένος ή προετοιμάζεται να δεχτεί τη σύνδεση.
2. **Μεταφορά δεδομένων (data transfer)**: Οι πληροφορίες μπορούν τώρα να διαβιβαστούν από τον πομπό μέσω του δικτύου στον δέκτη. Τα δεδομένα μπορεί να είναι αναλογικά ή ψηφιακά, εξαρτάται από τη φύση του δικτύου. Γενικά, η σύνδεση γίνεται σε αμφίδρομο κανάλι επικοινωνίας (full-duplex).
3. **Αποσύνδεση κυκλώματος (circuit disconnect)**: Μετά από μια περίοδο μεταφοράς δεδομένων, η σύνδεση ολοκληρώνεται, συνήθως από έναν από τους δύο σταθμούς. Τα σήματα πρέπει να διαδίδονται στον αντίστοιχο κόμβο για να απελευθερώσουν τις διεξόδους που τους ανήκουν.

Το κανάλι σύνδεσης εγκαθίσταται πριν αρχίσει η μεταφορά δεδομένων. Η απαιτούμενη χωρητικότητα καναλιού πρέπει να είναι διαθέσιμη ανάμεσα σε κάθε ζευγάρι κόμβων, και κάθε κόμβος πρέπει να έχει διαθέσιμη εσωτερική ικανότητα μεταγωγής για να διατηρεί την απαιτούμενη σύνδεση. Οι μεταγωγείς πρέπει να έχουν την ικανότητα να κάνουν αυτές τις κατανομές και να βρίσκουν μια διαδρομή μέσω του δικτύου.

Η μεταγωγή κυκλώματος μπορεί να είναι ανεπαρκής. Η σύνδεση διατηρείται ακόμα και αν δεδομένα δεν μεταφέρονται. Για μια σύνδεση τερματικού-υπολογιστή, η χωρητικότητα μπορεί να είναι ανενεργή (idle) κατά το μεγαλύτερο τμήμα της διάρκειας της σύνδεσης. Όσον αφορά την απόδοση, υπάρχει μια εκ των προτέρων καθυστέρηση στο σήμα προς μετάδοση πριν την εγκατάσταση της κλήσης. Ωστόσο, όταν το κύκλωμα εγκατασταθεί, το δίκτυο είναι εντελώς «διαφανές» στο χρήστη. Οι πληροφορίες μεταδίδονται με σταθερό ρυθμό χωρίς επιπλέον καθυστέρηση, εκτός από αυτή που απαιτείται για τη διάδοση μέσω των συνδέσεων. Η καθυστέρηση σε κάθε κόμβο είναι αμελητέα.

Η μεταγωγή κυκλώματος είναι ευρέως διαδεδομένη επειδή προσαρμόζεται πολύ καλά στην αναλογική μετάδοση των σημάτων. Παρά την ανεπάρκεια της στο σημερινό ψηφιακό κόσμο η μεταγωγή κυκλώματος εξακολουθεί να είναι μια καλή επιλογή για τα τοπικά δίκτυα περιοχής και τα δίκτυα ευρείας περιοχής. Ένα από τα βασικότερα πλεονεκτήματά της είναι πως είναι διαφανής. Εφόσον το δίκτυο εγκατασταθεί φαίνεται σαν μια απευθείας σύνδεση ανάμεσα στους δύο συνδεδεμένους σταθμούς. Κανένα ειδικό δίκτυο δεν απαιτείται.

1.4.2 Δίκτυο μεταγωγής πακέτων

Τα δεδομένα μεταφέρονται με τη μορφή μικρών πακέτων. Ένα ανώτατο όριο για το μέγεθος του πακέτου είναι 1024 bytes. Εάν η πηγή έχει μεγαλύτερο μήνυμα να στείλει, το μήνυμα χωρίζεται σε μια σειρά από μικρά πακέτα (τεμαχισμός). Κάθε πακέτο περιέχει ένα τμήμα με τα στοιχεία του χρήστη και μερικές πληροφορίες ελέγχου. Οι πληροφορίες ελέγχου περιέχουν τις πληροφορίες που απαιτούνται από το δίκτυο έτσι ώστε να μπορεί να δρομολογήσει το πακέτο μέσω του δικτύου και να το παραδώσει στον προορισμό του. Σε κάθε κόμβο κατά τη δρομολόγηση, το πακέτο παραλαμβάνεται, αποθηκεύεται για λίγο, και περνά στον επόμενο κόμβο. Το ερώτημα που προκύπτει είναι πώς το δίκτυο θα χειριστεί τη ροή των πακέτων καθώς

προσπαθεί να τα δρομολογήσει μέσω του δικτύου και να τα διανείμει στον προορισμό τους. Υπάρχουν δύο τεχνικές μεταγωγής πακέτου που χρησιμοποιούνται εξίσου στα σύγχρονα δίκτυα: τεχνική αυτοτελών πακέτων (datagram) και τεχνική εικονικού κυκλώματος (virtual-circuit).

1. **Τεχνική αυτοτελών πακέτων** : Σε αυτή την τεχνική κάθε πακέτο χρησιμοποιείται ανεξάρτητα, χωρίς αναφορά στα πακέτα που έχουν ήδη περάσει. Έτσι τα πακέτα, που έχουν την ίδια διεύθυνση προορισμού, μπορεί να μην ακολουθούν τον ίδιο δρόμο. Είναι δυνατόν το "πακέτο 2" να φτάσει πριν από το "πακέτο 1". Είναι ακόμα πιθανό τα πακέτα να διανέμονται στον προορισμό με διαφορετική σειρά αλληλουχίας από αυτή που στάλθηκαν. Για αυτό πρέπει να υπάρχει η κατάλληλη διάταξη που να τα τοποθετεί στην αρχική τους σειρά. Ένα πακέτο μπορεί να καταστραφεί στο δίκτυο. Πάνω σε αυτή την τεχνική λογική βασίζονται τα VPNs με τείχος προστασίας (firewall VPNs) που αναφέρονται και αναλύονται στα επόμενα κεφάλαια.
2. **Τεχνική εικονικού κυκλώματος** : Σε αυτή την τεχνική μια προσχεδιασμένη διαδρομή καθιερώνεται πριν σταλούν τα πακέτα. Ο κόμβος πομπών (S) αρχικά στέλνει ένα ειδικό πακέτο ελέγχου, που ονομάζεται πακέτο αίτησης κλήσης, ζητώντας μια λογική σύνδεση στον κόμβο προορισμού (D). Εάν ο κόμβος προορισμού είναι προετοιμασμένος να δεχτεί τη σύνδεση στέλνει πίσω ένα πακέτο αποδοχής κλήσης. Οι δυο σταθμοί μπορούν τώρα να ανταλλάξουν δεδομένα μέσω της διαδρομής που έχει δημιουργηθεί. Επειδή η διαδρομή είναι σταθερή κατά τη διάρκεια της λογικής σύνδεσης το κύκλωμα είναι όμοιο με αυτό που χρησιμοποιείται στο δίκτυο μεταγωγής κυκλώματος και ονομάζεται εικονικό κύκλωμα (virtual circuit). Πάνω σε αυτή την τεχνική βασίζονται τα VPNs σηράγγων (tunneling VPNs) που αναφέρονται και αναλύονται στα επόμενα κεφάλαια.

Κάθε κόμβος στην προκαθορισμένη διαδρομή γνωρίζει πού θα στείλει τα πακέτα, έτσι καμία απόφαση δρομολόγησης δεν απαιτείται. Τελικά ένας σταθμός ολοκληρώνει τη σύνδεση με ένα πακέτο αίτησης διαγραφής. Κάθε στιγμή, κάθε σταθμός μπορεί να έχει περισσότερα από ένα εικονικά κυκλώματα όπως και μπορεί να έχει εικονικά κυκλώματα σε περισσότερους από έναν σταθμούς. Το κύριο χαρακτηριστικό της τεχνικής εικονικού κυκλώματος είναι ότι η διαδρομή μεταξύ των σταθμών δημιουργείται πριν από τη μεταφορά των στοιχείων. Κάτι τέτοιο δε

σημαίνει ότι τμήμα του εικονικού δικτύου χρησιμοποιείται αποκλειστικά όπως στη μεταγωγή κυκλώματος. Ένα πακέτο αποθηκεύεται σε κάθε κόμβο. Εκεί περιμένει στην ουρά για την έξοδο μέσω μιας γραμμής. Η διαφορά από την datagram τεχνική είναι ότι με τα εικονικά κυκλώματα ο κόμβος δεν χρειάζεται να πάρει κάποια απόφαση για τη δρομολόγηση κάθε πακέτου, απλά τα διακινεί στον προκαθορισμένο κόμβο.

Εάν δύο σταθμοί επιθυμούν να ανταλλάξουν στοιχεία σε μια παρατεταμένη χρονική περίοδο τα εικονικά κυκλώματα παρέχουν ορισμένα πλεονεκτήματα.

- Το δίκτυο μπορεί να παρέχει υπηρεσίες συνδεδεμένες με το εικονικό κύκλωμα συμπεριλαμβανομένου του ελέγχου σφάλματος.
- Τα πακέτα μπορούν να διέλθουν από το δίκτυο γρηγορότερα με ένα εικονικό κύκλωμα επειδή δεν είναι απαραίτητο να παρθεί απόφαση δρομολόγησης για κάθε πακέτο σε κάθε κόμβο.

Αντίθετα εάν ο σταθμός επιθυμεί να στείλει μόνο ένα ή ορισμένα μόνο πακέτα η μετάδοση αυτοτελών πακέτων (datagram) είναι γρηγορότερη επειδή αποφεύγεται η δημιουργία εικονικού κυκλώματος. Επιπλέον, καθώς είναι πιο παλιά τεχνική είναι πιο αποτελεσματική στην αντιμετώπιση των προβλημάτων. Παραδείγματος χάριν, εάν αναπτύσσεται συμφόρηση σε ένα τμήμα του δικτύου η datagram μπορεί να την αποφύγει. Με τη χρήση εικονικού κυκλώματος τα πακέτα ακολουθούν μια προκαθορισμένη διαδρομή και είναι δυσκολότερο να αποφύγουν τη συμφόρηση. Τέλος, η τεχνική αυτή είναι πιο αξιόπιστη. Εάν ένας κόμβος αποτύχει, τα επόμενα πακέτα μπορεί να βρουν μια εναλλακτική διαδρομή για να παρακάμψουν αυτόν τον κόμβο Με τη χρήση των εικονικών κυκλωμάτων ,αντίθετα, εάν ένας κόμβος αποτύχει όλα τα εικονικά κυκλώματα που διέρχονται από αυτόν τον κόμβο θα χαθούν. Τα πακέτα φωνής γενικά μεταδίδονται με τεχνικές αυτοτελών πακέτων.

Τα VPNs μέσω διαφόρων πρωτόκολλων και τεχνολογιών δικτύων, προσπαθούν να επιτύχουν την ασφάλεια της μεταδιδόμενης πληροφορίας. Ελέγχοντας την ενθυλάκωση ή την μεταγωγή πακέτων, αναλόγως με το σε πιο επίπεδο εφαρμόζονται δεύτερο ή τρίτο. Χωρίς όμως να αποκλείεται ο συνδυασμός όλων μαζί.

Κεφάλαιο 2ο

Αποτελεί γεγονός πως έχει αναπτυχθεί μία αρκετά μεγάλη φιλολογία γύρω από το τι είναι τα VPN, ποιά η λειτουργία τους και ποία η θέση τους στην αρχιτεκτονική των δικτύων. Θα μπορούσε λοιπόν να υποστηρίξει κανείς πως το VPN είναι ένα δίκτυο επιχείρησης ανεπτυγμένο σε μία διανεμημένη υποδομή και έχει την ίδια ασφάλεια, διαχείριση και υφίσταται την ίδια πολιτική σε όλο το μήκος του σαν να επρόκειτο για ιδιωτικό δίκτυο.

Τα VPN είναι μια εναλλακτική λύση της υποδομής που παρέχουν τα WAN[2] και που αντικαθιστούν ή επαυξάνουν τα υπάρχοντα ιδιωτικά δίκτυα που χρησιμοποιούν μισθωμένες γραμμές ή Frame Relay/ATM δίκτυα που ανήκουν στην επιχείρηση. Τα VPN δεν έχουν άλλες απαιτήσεις από αυτές των WAN όπως υποστήριξη πολλαπλών πρωτοκόλλων, υψηλή αξιοπιστία και εκτεταμένη διαβάθμιση, απλά ικανοποιούν αυτές τις απαιτήσεις λιγότερο δαπανηρά.

Ένα VPN μπορεί να αξιοποιήσει τις πιο γνωστές τεχνολογίες μεταφοράς που υπάρχουν σήμερα όπως το **δημόσιο Internet**, **IP backbones** διαφόρων παροχέων υπηρεσιών όπως επίσης και τα **Frame Relay** και **ATM** δίκτυά τους. Η λειτουργικότητα του VPN καθορίζεται κυρίως από τον εξοπλισμό που είναι ανεπτυγμένος στο δίκτυο και την ολοκλήρωση των χαρακτηριστικών του WAN και όχι κάθε αυτό, το πρωτόκολλο μεταφοράς που αυτό χρησιμοποιεί.

Τα VPN χωρίζονται σε τρεις κατηγορίες, απομακρυσμένης πρόσβασης, intranets και extranets. Τα **remote access VPNs** συνδέουν τηλεργαζόμενους, κινούμενους χρήστες ή ακόμα και μικρότερα απομακρυσμένα γραφεία με περιορισμένη κίνηση από και προς το WAN της επιχείρησης και των συλλογικών υπολογιστικών της πόρων.

Τα **intranet VPNs** συνδέουν σταθερά σημεία, παρακλάδια και γραφεία σπιτιών με το WAN της επιχείρησης. Τα **extranet VPNs** επεκτείνουν την περιορισμένη πρόσβαση στους υπολογιστικούς πόρους της επιχείρησης στους διαφόρους συνεργάτες της που μπορεί να είναι προμηθευτές ή πελάτες επιτρέποντας πρόσβαση σε διαμοιράσιμη πληροφορία. Κάθε τύπος VPN έχει διαφορετικά θέματα ασφάλειας και ποιότητας παρεχόμενων υπηρεσιών να αντιμετωπίσει.

---

[2] **WAN** είναι ένα σύνολο υπολογιστών που εκτείνονται σε μια ευρεία γεωγραφική περιοχή ή αλλιώς πολλά LAN's(Local Area Networks) μαζίκαι δημιουργούν μεταξύ τους ένα δίκτυο επικοινωνίας.

2.1 Βασικά πρωτοκόλλα VPN

Η λειτουργία όμως των VPN στηρίζονται σε δύο βασικές κατηγορίες πρωτοκόλλων, των **PPTP** και του **IPSEC**.

Το **Point-to-Point Tunneling Protocol** (PPTP) αποτελεί ανάπτυξη της Microsoft που προορίζεται για VPN. Το PPTP προσφέρει ταυτοποίηση χρήστη που χρησιμοποιεί πρωτόκολλα ελέγχου ταυτότητας όπως το MS-CHAP, CHAP[3] και PAP[4]. Το πρωτόκολλο στερείται της απαραίτητης ευελιξίας που προσφέρουν οι άλλες λύσεις και δεν διαθέτουν το ίδιο επίπεδο διαλειτουργικότητας με τα άλλα πρωτόκολλα των VPN, αλλά η χρήση του είναι εύκολη και άφθονη στον πραγματικό κόσμο. Αποτελείται από τρία είδη επικοινωνίας:

- ***PPTP σύνδεση**, όταν ένας πελάτης καθορίζει μια σύνδεση PPP σε έναν ISP.*
- ***PPTP σύνδεση ελέγχου**, όπου ο χρήστης δημιουργεί μια σύνδεση PPTP στο διακομιστή VPN και διαπραγματεύεται τα χαρακτηριστικά της σήραγγας.*
- ***PPTP σηράγγων δεδομένα**, όπου οι δύο πελάτη και επικοινωνιών Exchange Server μέσα σε μια κρυπτογραφημένη σήραγγα.*

Τέλος το PPTP χρησιμοποιείται συνήθως για τη δημιουργία ασφαλών διαύλων επικοινωνίας. Πρέπει να είναι κανείς προσεκτικός στην επιλογή των PPTP, αφού συνήθως χρησιμοποιεί κατώτερου βαθμού αλγόριθμους κρυπτογράφησης, όπως MD4 ή DES.

Η δεύτερη κατηγορία πρωτοκόλλων είναι εκείνη του IPSec. Το IPSec αναγνωρίζεται ευρέως, με την υποστήριξη, και τυποποίηση όλων των πρωτοκόλλων VPN. Είναι η απόλυτη επιλογή για λόγους διαλειτουργικότητας. Το IPSec είναι ένα πλαίσιο ανοικτών προτύπων που παράγει μια ασφαλή σουίτα πρωτοκόλλων που μπορεί να λειτουργήσει πάνω από την υπάρχουσα σύνδεση IP.

Παρέχει αυθεντικότητα των δεδομένων και υπηρεσίες κρυπτογράφησης κατά το τρίτο επίπεδο OSI, μπορούν να εφαρμοστούν σε οποιαδήποτε συσκευή επικοινωνεί μέσω του IP. Αντίθετα με πολλά άλλα συστήματα κρυπτογράφησης για την

[3] Το **Challenge-Handshake Authentication Protocol (**CHAP) είναι πρωτόκολλο αυθεντικοποίησης που χρησιμοποιείται από servers Point to Point Protocol (PPP) για να πιστοποιήσει την ταυτότητα των απομακρυσμένων χρηστών.

[4] Το **Password Authentication Protocol** (PAP) είναι ένα απλό πρωτόκολλο αυθεντικοποίησης που χρησιμοποιείται για την αυθεντικοποίηση ενός χρήστη σε κάποιο Διακομιστή Πρόσβασης Δικτύου (Network Access Server, NAS) που μπορεί να χρησιμοποιείται για παράδειγμα από παρόχους υπηρεσιών ίντερνετ. Το PAP χρησιμοποιείται από το πρωτόκολλο PPP. Το PAP μεταδίδει μη κρυπτογραφημένους ASCII κωδικούς μέσω δικτύου και γι αυτό θεωρείται μη ασφαλές. Χρησιμοποιείται ως έσχατη λύση όταν ο απομακρυσμένος διακομιστής δεν υποστηρίζει πιο ισχυρό πρωτόκολλο αυθεντικοποίησης, όπως το CHAP.

προστασία πρωτόκολλου υψηλού στρώματος, το IPSec, που εργάζεται στο χαμηλότερο στρώμα, μπορεί να προστατεύσει το σύνολο της κίνησης που πραγματοποιείται μέσω του IP. Χρησιμοποιείται επίσης σε συνδυασμό με επιπέδου 2 πρωτόκολλα ενθυλάκωσης για την παροχή τόσο κρυπτογράφησης όσο και ελέγχου ταυτότητας για μη-IP κίνησης.

Το πρωτόκολλο περιλαμβάνει τρία σημαντικά μέρη. Το Authentication Header (**AH**), Encapsulating ωφέλιμου φορτίου ασφάλειας (**ESP**), και Internet Key Exchange (**IKE**). Το AH προστίθεται μετά την κεφαλίδα IP και παρέχει σε επίπεδο πακέτου έλεγχο ταυτότητας και ακεραιότητα των υπηρεσιών, εξασφαλίζοντας ότι το πακέτο δεν είχε παραβιαστεί κατά μήκος της διακίνησης του και προήλθε από το αναμενόμενο αποστολέα. Το ESP παρέχει εμπιστευτικότητα, ταυτοποίησης των δεδομένων προέλευσης, ακεραιότητα, προαιρετική υπηρεσία antireplay, και περιορισμένη εμπιστευτικότητα ροής της κυκλοφορίας. Τέλος, το IKE διαπραγματεύεται συσχετίσεις ασφαλείας, που περιγράφουν τη χρήση των υπηρεσιών ασφαλείας μεταξύ των συμμετεχόντων φορέων. Τα παραπάνω αναλύονται στα επόμενα κεφάλαια.

Πρωτόκολλα επιπέδου 2

Ορισμένα πρωτόκολλα που χρησιμοποιούνται από VPN εφαρμογές βρίσκονται στο επίπεδο δυο του μοντέλου αναφοράς OSI , όπως το **Point-to-Point Tunneling Protocol** (PPTP), το **Layer 2 Forwarding** (L2F) και το **Layer 2 Tunnelling Protocol** (L2TP).

Όλα αυτά τα πρωτόκολλα λειτουργούν με την εξής διαδικασία . Ενσωματώνουν το 2ο επίπεδο (Data Link layer) στο πρωτόκολλο IP . Σε αυτό το επίπεδο λειτουργεί και το πρωτόκολλο PPP (Point-to-Point Protocol) , το οποίο χρησιμοποιείται για να μεταφέρει τα IP πακέτα και άλλα μέσω σειριακών και ψηφιακών συνδέσεων .Τυπικά οι συνδέσεις PPP πραγματοποιούνται μεταξύ ενός πελάτη και ενός κεντρικού υπολογιστή (host-server) . Με παρόμοιο τρόπο τα PPTP , L2F και L2TP χρησιμοποιούνται για να «διασωληνώσουν» (tunnel) συνδέσεις τύπου PPP μέσω του διαδικτύου που θα τερματίζουν σε κάποιον κεντρικό υπολογιστή .Αυτά τα πρωτόκολλα επειδή χρησιμοποιούν τη δομή του PPP πρωτοκόλλου, ενσωματώνουν

κάποια χαρακτηριστικά όπως δυναμική ανάθεση διεύθυνσης (DHCP[5]), βασική αυθεντικοποίηση και συμπίεση .

Το πρωτόκολλο PPTP αναπτύχθηκε από κοινού από τις εταιρίες Ascend Communications, U.S. Robotics, 3Com Corporation, Microsoft Corporation, και ECI Telematics για να προσφέρει εικονική ιδιωτική δικτύωση ανάμεσα σε απομακρυσμένους χρήστες και κεντρικούς δικτυακούς εξυπηρετητές . Αυτές οι εταιρίες δημιούργησαν το PPTP Forum ενώ τον ίδιο καιρό μια άλλη εταιρία , η Cisco ανάπτυσσε το πρωτόκολλο **Layer 2 Forwarding** (L2F) . Συνεργαζόμενοι με την Internet Engineering Task Force (IETF), το PPTP-Forum και η Cisco δημιούργησαν το **Layer 2 Tunneling Protocol** (L2TP), ένα νέο πρωτόκολλο που συνδυάζει τα καλύτερα χαρακτηριστικά των PPTP και L2F, ενώ διατηρεί μερική συμβατότητα προς τα πίσω.

Τα πρωτόκολλα PPTP και L2F επιτρέπουν να χρησιμοποιηθεί όποια μέθοδος αυθεντικοποίησης χρησιμοποιεί και το PPP, συμπεριλαμβανομένων των PAP και CHAP . Στην διαδικασία της κρυπτογράφησης το PPTP χρησιμοποιεί τον αλγόριθμο RC4 με κλειδιά μήκους 40 και 128 bits , ενώ το L2F υποστηρίζει 40 ή 56 bit DES κρυπτογράφηση καθώς και το πρωτόκολλο IPSec . Το πρωτόκολλο L2TP μπορεί να χρησιμοποιηθεί στη θέση των PPTP και L2F και μπορεί να εφαρμόσει τις ίδιες μεθόδους αυθεντικοποίησης ενώ σαν μέθοδος κρυπτογράφησης προτιμάται το IPSec .

Το πρωτόκολλο PPTP είναι μια επέκταση του πρωτοκόλλου PPP. Οι υπηρεσίες διασωλήνωσης «tunneling» που προσφέρονται από το PPTP είναι κατασκευασμένες «πάνω» από το επίπεδο IP , ενώ το παραδοσιακό PPP πρωτόκολλο βρίσκεται «κάτω» από το επίπεδο IP . Η μεταποίηση του PPP για να δημιουργηθεί το PPTP ήταν ιδανική αφού η συμπεριφορά του PPP μιμείται την συμπεριφορά ενός VPN, δηλαδή την διασωλήνωση σημείου με σημείο «point-to-point tunnel» .

Αυτό που ουσιαστικά έλειπε από το PPP πρωτόκολλο ήταν η ασφάλεια . Το πρωτόκολλο PPTP αναφέρεται κυρίως σε ασφάλεια ενός επικοινωνιακού καναλιού συστήματος-με-σύστημα παρά LAN με LAN . Αν και μπορεί κανείς να δρομολογήσει δικτυακή κίνηση μέσω ενός καναλιού PPTP , ιδανικότερη είναι η χρησιμοποίηση του πρωτοκόλλου IPSec . Το PPTP ενσωματώνει το PPP και το MPPE (Microsoft Point to Point Encryption), το οποίο χρησιμοποιεί 40bit RC4 και 128bit RC4 κρυπτογράφηση , για να δημιουργήσει κρυπτογραφημένα κανάλια επικοινωνίας . Η

[5] Με τον όρο DHCP (Dynamic Host Configuration Protocol) αναφερόμαστε σε ένα μηχανισμό διαχείρισης πρωτοκόλλων TCP/IP .

διακίνηση των δεδομένων γίνεται μέσω της θύρας TCP 1723 και του πρωτοκόλλου IP GRE (Generic Routing Encapsulation) όπως έχει ορίσει η αρχή IANA (Internet Assigned Numbers Authority).

Η τεχνική ενθυλάκωσης PPTP βασίζεται στο πρωτόκολλο GRE ή πρωτόκολλο 47 το οποίο χρησιμοποιείται για να «περάσει» πρωτόκολλα σύνδεσης πάνω από το διαδίκτυο . Η έκδοση που χρησιμοποιείται στο PPTP είναι η GREv2, η οποία προσθέτει επεκτάσεις για ειδικά χαρακτηριστικά όπως το Call ID και η ταχύτητα σύνδεσης . Ένα πακέτο PPTP αποτελείται από την κεφαλή (Delivery Header), την κεφαλή GRE , και το φορτίο του πακέτου .Το **delivery header** είναι ένα πρωτόκολλο πλαισίου για κάθε είδους πακέτου που «ταξιδεύει» στο δίκτυο . Η IP κεφαλή περιέχει πληροφορίες για το IP datagram , όπως το μήκος πακέτου τη διεύθυνση αποστολέα και παραλήπτη . Η GREv2 κεφαλή περιέχει πληροφορίες σχετικά με τον τύπο του πακέτου που ενθυλακώνεται και πληροφορίες σχετικά με το PPTP μεταξύ του πελάτη και του εξυπηρετητή . Το φορτίο του πακέτου είναι το ενθυλακωμένο «datagram» . Στην περίπτωση του PPP το datagram είναι τα αρχικά δεδομένα της συνεδρίας PPP που αποστέλλονται μεταξύ πελάτη και εξυπηρετητή και μέσα του μπορεί να είναι πακέτα τύπου IP , IPX ή NetBEUI .

Πρωτόκολλο GRE

Το πρωτόκολλο GRE χρησιμοποιείται σε συνδυασμό με το πρωτόκολλο PPTP για την δημιουργία εικονικών ιδιωτικών δικτύων . Προσφέρει ένα μηχανισμό για να ενθυλακώνονται πακέτα δεδομένων σε ένα συγκεκριμένο πρωτόκολλο επικοινωνίας. Γενικά ο μηχανισμός είναι ως εξής . Το φορτίο του πακέτου ενθυλακώνεται μέσα σε ένα πακέτο τύπου GRE , το οποίο συχνά έχει και πληροφορίες δρομολόγησης . Το τελικό πακέτο GRE ενθυλακώνεται με την σειρά του σε κάποιο άλλο πρωτόκολλο και προωθείται (πρωτόκολλο αποστολής) . Η μέθοδος ενθυλάκωσης GRE πολύ συχνά εφαρμόζεται στην περίπτωση που πρωτόκολλο αποστολής είναι το πρωτόκολλο IP όπως και στη θέση του φορτίου του πακέτου .

Πρωτόκολλο L2F

Λόγω της μεγάλης ανάπτυξης των dial-up υπηρεσιών και την παροχή πολλών διαφορετικών πρωτοκόλλων χρειαζόταν ένας τρόπος για να δημιουργείται μία εικονική dial-up σύνδεση, όπου οποιοδήποτε από τα μη IP πρωτόκολλα να μπορεί να χρησιμοποιεί τα πλεονεκτήματα που παρέχει το Internet. Μέσω του L2F, οι χρήστες

έχουν τη δυνατότητα να κάνουν μία Point to Point σύνδεση σε ένα dial-up πάροχο υπηρεσιών και, εν συνεχεία, να συνδεθούν στα υπολογιστικά συστήματα της εταιρίας τους. Το L2F έχει δικούς του μηχανισμούς για την ενθυλάκωση των πακέτων και δεν χρησιμοποιεί το GRE.

Ορισμένα από τα οφέλη που προσέφερε το L2F είναι :

- Ανεξαρτησία πρωτοκόλλων (IPX, SNA)
- Αυθεντικοποίηση (PPP, CHAP, TACACS ή RADIUS)
- Διαχείριση διευθύνσεων
- Δυναμικά και ασφαλή tunnels
- Υπηρεσίες χρέωσης (accounting)
- Έλεγχος ροής

Σε μία τυπική εγκατάσταση ο χρήστης κάνει μία PPP ή άλλη παρόμοια σύνδεση στον ISP και κατά την διάρκεια της αίτησης, ο **NAS** (Network Access Server), χρησιμοποιώντας το λογισμικό του L2F, αρχικοποιεί μία δίοδο προς τον προορισμό του χρήστη. Στη συνέχεια, ο προορισμός απαιτεί το password του χρήστη και αφού γίνει η πιστοποίηση ταυτότητας, παραχωρείται στο χρήστη η IP διεύθυνση σαν μία τυπική dial-up απομακρυσμένη πρόσβαση. Στην ουσία, η πιστοποίηση ταυτότητας γίνεται σε δύο επίπεδα: μία αρχικά από τον ISP (Internet Service Provider) στον οποίο συνδέεται ο χρήστης και μία μετέπειτα από την πύλη (gateway) που υπάρχει στο απομακρυσμένο δίκτυο που συνδέεται ο χρήστης

Πρωτόκολλο L2TP

Το αποτέλεσμα της συγχώνευσης του PPTP και του L2F είναι το πρωτόκολλο L2TP, το οποίο ορίστηκε για λόγους συμβατότητας όλων των δικτύων μεταξύ τους. Το L2TP παρέχει συμπίεση βασισμένη σε λογισμικό. Ένας μικρός αριθμός τεχνικών συμπίεσης έχει προστεθεί στο επίπεδο της κρυπτογράφησης. Επειδή το L2TP χρησιμοποιεί πολλά χαρακτηριστικά του IPSec για να επιτύχει μεγαλύτερη ασφάλεια, θεωρείται ότι παρέχει υπηρεσίες όχι μόνο δεύτερου αλλά και τρίτου επιπέδου. Το L2TP χρησιμοποιεί δύο servers για τη σύνοδο:

- τον **LAC** (**L2TP Access Concentrator**) – Βρίσκεται στον ISP και χρησιμοποιείται για την εγκαθίδρυση μίας διόδου σε ένα δημόσιο δίκτυο π.χ. PSTN, ISDN, η οποία τερματίζεται στον LNS του κόμβου προορισμού

- τον **LNS** (**L2TP Network Server**) – Βρίσκεται στον προορισμό και χρησιμοποιείται για τον τερματισμό της σήραγγας. Αναλαμβάνει την αυθεντικοποίηση του χρήστη. Όταν ο LNS λάβει αίτηση για σύνδεση (δημιουργία διόδου) από έναν LAC, αυθεντικοποιεί τον αιτούντα και εγκαθιδρύει η σήραγγα.

Στη δίοδο που δημιουργείται μεταξύ του Access Concentrator και του Network Server μπορούν να υπάρχουν ταυτόχρονα πολλές σύνοδοι (επικοινωνίες) κάθε σύνοδος έχει ένα δικό της μοναδικό αριθμό Call ID, που υπάρχει στην επικεφαλίδα κάθε L2TP πακέτου. Μπορούν επίσης να υπάρχουν ταυτόχρονα πολλές διαφορετικές δίοδοι μεταξύ του ίδιου Access Concentrator και του Access Server. Η κάθε μία τότε μπορεί να ικανοποιεί διαφορετικό QoS.

Όπως και στο PPTP, η αρχική σύνδεση του χρήστη με τον LAC (ο οποίος παίζει το ρόλο που έχει ο NAS στο PPTP) γίνεται με χρήση του PPP, μέσω του οποίου ενθυλακώνονται διαφόρων ειδών πακέτα (Apple Talk, IP, IPX και NETBEUI) και πραγματοποιείται μία πρώτη αυθεντικοποίηση του χρήστη (με PAP ή CHAP). Μία δεύτερη πιστοποίηση της ταυτότητας του χρήστη λαμβάνει χώρα αμέσως μετά, με χρήση του RADIUS. Επίσης, μία άλλη αναλογία του L2TP με το PPTP είναι τα δύο είδη μηνυμάτων που μπορεί να ανταλλάσσονται: μηνύματα ελέγχου και μηνύματα δεδομένων. Τέλος, όπως και στο PPTP, ένα VPN που υλοποιείται με βάση το L2TP μπορεί να υποστηρίζει τόσο αυθόρμητες (voluntary) όσο και αναγκαστικές (compulsory) συνδέσεις σήραγγας.

Τα στάδια που ακολουθούνται για τη δημιουργία μίας L2TP σύνδεσης είναι τα ακόλουθα:

- **Στάδιο 1**: Ο απομακρυσμένος χρήστης συνδέεται με τον LAC του ISP με χρήση του πρωτοκόλλου PPP. Ο LAC αυθεντικοποιεί τον χρήστη, με βάση το user name και password του. Στη συνέχεια, ο LAC προσδιορίζει την IP διεύθυνση του LNS που ανήκει στο LAN για το οποίο ο χρήστης αιτείται σύνδεση. Μεταξύ LAC και LNS, η σύνοδος L2TP ξεκινά.
- **Στάδιο 2**: Μετά την εκκίνηση της L2TP συνόδου, ξεκινά η αυθεντικοποίηση του χρήστη στον LNS. Μπορεί να χρησιμοποιηθεί οποιοσδήποτε τυποποιημένος αλγόριθμος αυθεντικοποίησης. Όπως στα πρωτόκολλα PPTP και L2F, το L2TP δε θέτει περιορισμό για αλγόριθμο αυθεντικοποίησης. Ωστόσο, στην πράξη, έχει προτιμηθεί κυρίως η αυθεντικοποίηση με χρήση του RADIUS.

- **Στάδιο 3**: Μετά από επιτυχή αυθεντικοποίηση, μπορεί να δημιουργηθεί μια προστατευμένη σήραγγα μεταξύ LAC και LNS. Το L2TP δεν προσδιορίζει ρητά μεθόδους για την κρυπτογράφηση (η οποία και

παρέχει την ασφάλεια). Ωστόσο, για συνδέσεις πάνω σε IP δίκτυα, μπορεί να χρησιμοποιηθεί το πρωτόκολλο IPSec. Τότε το L2TP ενθυλακώνεται σε UDP[6] πακέτα που μεταφέρονται μεταξύ LAC και LNS μέσω IPSec σήραγγας. Για αυτό χρησιμοποιείται ως βασική η UDP πόρτα 1701 – ωστόσο, μπορεί να χρησιμοποιηθεί εν γένει οποιαδήποτε άλλη UDP πόρτα.

Σε αναγκαστική σύνδεση, ο χρήστης στέλνει PPP πακέτα στον LAC[7] και η δημιουργία σύνδεσης μεταξύ του LAC και του LNS[8] του απομακρυσμένου δικτύου γίνεται ερήμην του – ο ίδιος ο χρήστης δεν κάνει καμία άλλη ενέργεια για τη δημιουργία αυτής. Το IPSec λοιπόν είναι η καλύτερη επιλογή για τον χρήστη, στέλνει απευθείας κρυπτογραφημένα (και άρα ασφαλή) τα δεδομένα. Το AH προστίθεται από τον LAC του ISP. Το ESP προστίθεται μόνο όταν ο LNS στον προορισμό υποστηρίζει IPSec. Για την ανταλλαγή του συμμετρικού κλειδιού κρυπτογράφησης χρησιμοποιείται το IKE.

Σε αυθόρμητη σύνδεση, το AH εφαρμόζεται στον υπολογιστή του χρήστη απευθείας (μια που ο υπολογιστής είναι το άκρο της σύνδεσης). Αν ο LNS στον προορισμό δεν υποστηρίζει IPSec, το ESP προστατεύει τα δεδομένα μόνο μέχρι να καταφτάσουν στον LNS.

Από τα παραπάνω γίνεται φανερό ότι οι κύριες λειτουργίες που πρέπει να μπορεί να κάνει ο LNS (εκτός βέβαια της βασικής, που είναι η προώθηση των L2TP πακέτων που λαμβάνει στον αντίστοιχο υπολογιστή του δικτύου) είναι εκείνες που τον κάνουν συμβατό με το IPSec: με άλλα λόγια, πρέπει να μπορεί να υποστηρίζει τόσο μια μεγάλη ποικιλία αλγορίθμων κρυπτογράφησης όσο και να μπορεί να επεξεργάζεται πακέτα που έχουν τις κεφαλίδες AH και ESP. Ένα χαρακτηριστικό του LNS είναι ότι δεν πραγματοποιεί φιλτράρισμα (σε αντίθεση με τον NAS στα PPTP δίκτυα).

Τέλος, θα πρέπει να σημειωθεί ότι το L2TP πρωτόκολλο μπορεί να χρησιμοποιηθεί και για σύνδεση δίκτυο-προς-δίκτυο (LAN-to-LAN tunneling): ειδική μέριμνα πρέπει να υπάρξει ώστε κάθε άκρο της σήραγγας να μπορεί να δρα ταυτόχρονα και σαν LAC αλλά και σαν LNS.

[6] Το πρωτόκολλο **User Datagram Protocol** (UDP) είναι ένα από τα βασικά πρωτόκολλα που χρησιμοποιούνται στο Διαδίκτυο για την αποστολή σύντομων μηνυμάτων (γνωστών και ως datagrams) από τον έναν υπολογιστή στον άλλον μέσα σε ένα δίκτυο υπολογιστών.
[7] **LCA** (local controller Access) τοπικός ελεγκτής πρόσβασης
[8] **LNS** (local network server) τοπικός δικτυακός server

2.2 Πρωτόκολλα Microsoft

Η Microsoft υλοποίησε τους δικούς της αλγόριθμους και πρωτόκολλα για να υποστηρίξει το PPTP . Αυτή η υλοποίηση, που ονομάζεται Microsoft PPTP, χρησιμοποιείται ευρέως ακριβώς επειδή είναι ήδη ενσωματωμένη στο λειτουργικό σύστημα Microsoft Windows . Παρακάτω παρουσιάζονται οι αλλαγές στη διαδικασία γένεσης κλειδιών αυθεντικοποίησης και κρυπτογράφησης και γίνεται λόγος για τις βελτιώσεις και τις απομένουσες αδυναμίες του μηχανισμού .

MS-CHAP

Το πρωτόκολλο αυθεντικοποίησης στο Microsoft PPTP είναι το MS-CHAP (**Microsoft Challenge/Reply Handshake Protocol**) και το πρωτόκολλο κρυπτογράφησης είναι το MPPE (Microsoft Point to Point Encryption) . Η Microsoft αναβάθμισε το πρωτόκολλο σε MS-CHAP version 2 (MS-CHAPv2) αφού σημαντικές αδυναμίες ασφάλειας του MS-CHAP version 1 (MS-CHAPv1) είδαν το φως της δημοσιότητας .

Οι πιο σημαντικές αλλαγές από το MS-CHAPv1 στο MS-CHAPv2 είναι :

- Εισάχθηκε μια διαδικασία αυθεντικοποίησης για τον διακομιστή (server), έτσι ώστε να εμποδιστούν οι παράνομοι διακομιστές να «προσποιούνται» (masquerading) τους νόμιμους διακομιστές.
- Τα πακέτα αλλαγής συνθηματικού από το MS-CHAPv1 έχουν αντικατασταθεί από ένα μοναδικό πακέτο αλλαγής συνθηματικού στο MS-CHAPv2 .
- Το MPPE χρησιμοποιεί μοναδικά κλειδιά προς κάθε κατεύθυνση .
- Η αδύναμη πλέον συνόψιση «LAN Manager» δεν στέλνεται μαζί με τις υπόλοιπες συνοψίσεις , αφού θεωρείται ότι εύκολα αποκωδικοποιείται .

Έτσι η Microsoft διόρθωσε ορισμένες αδυναμίες της στο κρυπτογραφικό σύστημα του PPTP και βελτίωσε την ποιότητα του κώδικα της . Η καινούρια έκδοση είναι πιο αποτελεσματική απέναντι σε επιθέσεις άρνησης εξυπηρέτησης και επιπλέον δεν διαρρέουν πληροφορίες για τον αριθμό των ενεργών συνεδριών VPN . Όμως υπάρχουν ακόμη σημαντικά προβλήματα ασφάλειας όπως το γεγονός ότι το κλειδί κρυπτογράφησης έχει τόση εντροπία πληροφορίας όση το συνθηματικό του χρήστη και το ότι περνά αρκετός όγκος δεδομένων από το κανάλι επικοινωνίας που επιτρέπει στους εισβολείς να εξαπολύσουν επιθέσεις κρυπτανάλυσης .

Ο μηχανισμός πρόκλησης/απόκρισης του MS-CHAPv1 περιγράφεται εν συντομία παρακάτω :

1. Ο πελάτης ζητά μία πρόκληση εισόδου από τον διακομιστή .

2. Ο διακομιστής απαντά με μία τυχαία πρόκληση μήκους 8 bytes .

3. Ο πελάτης χρησιμοποιεί την χειραψία «LAN Manager hash» του συνθηματικού του για να δημιουργήσει τρία κλειδιά DES . Καθένα από τα κλειδιά χρησιμοποιείται για να κρυπτογραφήσει την πρόκληση . Και τα τρία κωδικοποιημένα τμήματα ενώνονται σε μια απάντηση μήκους 24 bytes . Ο πελάτης δημιουργεί μια δεύτερη απάντηση μήκους 24 bytes χρησιμοποιώντας την συνόψιση «Windows NT hash» και την ίδια διαδικασία .

4. Ο εξυπηρετητής χρησιμοποιεί τη χειραψία (hash) του συνθηματικού του πελάτη , η οποία είναι αποθηκευμένη σε βάση δεδομένων, για να αποκρυπτογραφήσει τις αποκρίσεις. Εάν τα αποκρυπτογραφημένα τμήματα ταιριάζουν με την πρόκληση τότε η αυθεντικοποίηση ολοκληρώνεται και στέλνει πακέτο «επιτυχίας» πίσω στον πελάτη .

Αυτή η διαδικασία έχει αλλάξει στο MS-CHAPv2 όπως φαίνεται παρακάτω :

1. Ο πελάτης ζητά μία πρόκληση εισόδου από τον διακομιστή .

2. Ο διακομιστής απαντά με μία τυχαία πρόκληση μήκους 16 bytes

3.α Ο πελάτης δημιουργεί έναν τυχαίο αριθμό μήκους 16 bytes , που ονομάζεται "Peer Authenticator Challenge” .

β. Ο πελάτης δημιουργεί μία πρόκληση των 8 bytes συνοψίζοντας (hashing) την πρόκληση των 16 bytes που λήφθηκε στο βήμα (2) , το "Peer Authenticator Challenge” των 16 bytes που δημιουργήθηκε στο βήμα (3^{α}) και το όνομα χρήστη του πελάτη .

γ. Ο πελάτης δημιουργεί μια απάντηση των 24 bytes , χρησιμοποιώντας την συνόψιση «Windows NT hash» και την πρόκληση των 8 bytes που δημιουργήθηκε στο βήμα (β) . Αυτή η διαδικασία είναι ίδια με το MS-CHAPv1

δ. Ο πελάτης στέλνει στον διακομιστή τα αποτελέσματα των βημάτων (α) και (γ)

4.α Ο διακομιστής χρησιμοποιεί τη συνόψιση (hash) του συνθηματικού του πελάτη , η οποία είναι αποθηκευμένη σε βάση δεδομένων , για να αποκρυπτογραφήσει τις αποκρίσεις . Εάν τα αποκρυπτογραφημένα τμήματα ταιριάζουν με την πρόκληση τότε ο πελάτης αυθεντικοποιείται .

β. Ο διακομιστής χρησιμοποιεί την πρόκληση «Peer Authenticator Challenge» των 16 bytes του πελάτη και τη συνόψιση του συνθηματικού του πελάτη για να δημιουργήσει μια απόκριση των 20 bytes «Authenticator Response» .

5. Ο πελάτης υπολογίζει και ο ίδιος το «Authenticator Response» . Εάν ταιριάζει με την απόκριση που λήφθηκε τότε αυθεντικοποιείται και ο διακομιστής .

Αυτό το πρωτόκολλο λειτουργεί έτσι ώστε να εξαλείφει τις πιο σοβαρές αδυναμίες που υπήρχαν στο MS-CHAPv1 . Πιο αναλυτικά στο MS-CHAPv1 δύο παράλληλες συνοψίσεις μηνύματος (hash values) στέλνονταν από τον πελάτη στον διακομιστή : η συνόψιση LAN Manager και η συνόψιση Windows NT . Αυτές οι δύο συνοψίσεις ήταν δύο διαφορετικές εκδοχές συνόψισης του συνθηματικού του χρήστη. Η χειραψία LAN Manager είναι μια πολύ αδύναμη συνάρτηση χειραψία και διάφορα προγράμματα εύρεσης συνθηματικών όπως το L0 phtcrack μπορούσαν να «σπάσουν» αυτή τη χειραψία και μετά να χρησιμοποιήσουν αυτήν την πληροφορία για να σπάσουν την συνόψιση Windows NT . Αναιρώντας την συνόψιση LAN Manager στο MS-CHAPv2 , η Microsoft κατέστησε αυτού του είδους την επίθεση αδύνατη . Παρόλα αυτά η ασφάλεια του πρωτοκόλλου βασίζεται ακόμη στο συνθηματικό χρήστη που χρησιμοποιείται και το πρόγραμμα L0phtcrack μπορεί ακόμη να «σπάσει» αδύναμα συνθηματικά .

MPPE

Στον αρχικό μηχανισμό κρυπτογράφησης στο πρωτόκολλο MPPE (**Microsoft's Point to Point Encryption protocol**) χρησιμοποιούνται τα ίδια κλειδιά κρυπτογράφησης προς κάθε κατεύθυνση (πελάτη προς διακομιστή και διακομιστή προς πελάτη). Στην πιο πρόσφατη έκδοση τα κλειδιά του πρωτοκόλλου MPPE προέρχονται από το MS-CHAPv2 όπου ένα μοναδικό κλειδί χρησιμοποιείται προς κάθε κατεύθυνση . Τα κλειδιά για κάθε κατεύθυνση προέρχονται από την ίδια τιμή (τη συνόψιση του συνθηματικού χρήστη του πελάτη) , αλλά με διαφορετικό τρόπο ανάλογα με το από πού προέρχονται .

Συμπερασματικά η Microsoft έχει βελτιώσει το πρωτόκολλο PPTP ώστε να καλύψει αρκετές αδυναμίες του. Όμως το βασικό μειονέκτημα του είναι ότι είναι τόσο ασφαλές όσο ασφαλές είναι και το συνθηματικό χρήστη. Όσο η υπολογιστική δύναμη των ηλεκτρονικών υπολογιστών αυξάνεται τόσο μειώνεται η ασφάλεια που προσφέρει το συγκεκριμένο πρωτόκολλο και τόσο η χρήση άλλων πρωτοκόλλων πιο ασφαλών όπως το IPSec , πρέπει να γίνει πιο διαδεδομένη .

2.3 Πρωτόκολλο PPTP

Το PPTP είναι ένας συνδυασμός του PPP και του TCP/IP. Δύο ειδών πακέτα χρησιμοποιούνται στο PPTP: **πακέτα δεδομένων** (data packets) και **πακέτα ελέγχου**

(control packets). Τα πακέτα ελέγχου χρησιμοποιούνται για σηματοδοσία ενώ τα πακέτα δεδομένων για να μεταφέρουν τα δεδομένα του χρήστη. Τα πακέτα δεδομένων έχουν υποστεί την διαδικασία της ενθυλάκωσης χρησιμοποιώντας το GRE v2.

Το PPTP λειτουργεί ως εξής: αρχικά, χρησιμοποιεί αυτούσιο το PPP, από το οποίο εξασφαλίζει τα ακόλουθα:

- Εγκαθίδρυση της φυσικής ζεύξης
- Πιστοποίηση των χρηστών
- Δημιουργία PPP πλαισίων

Στη συνέχεια, τα PPP πλαίσια ενθυλακώνονται κατάλληλα σε μεγαλύτερα πακέτα, με στόχο τη μετάδοση δεδομένων μέσω μιας διόδου. Στην ουσία δημιουργούνται IP πακέτα, με χρήση του πρωτοκόλλου ενθυλάκωσης.

Οι συσκευές στον ISP που είναι υπεύθυνες για λειτουργίες του πρωτοκόλλου PPTP ονομάζονται είτε **Remote Access Servers** (RAS) είτε **Network Access Servers** (NAS) (το όνομα διαφοροποιείται ανάλογα με τον ακριβή ρόλο που έχει η συσκευή καθόλη τη διάρκεια υλοποίησης του πρωτοκόλλου). Πρακτικά, ένας NAS ή RAS δεν είναι τίποτα άλλο παρά συλλογή modems με κατάλληλο λογισμικό.

Μία από τις βασικές λειτουργίες του NAS είναι η πιστοποίηση ταυτότητας του χρήστη (δηλαδή ο έλεγχος του κατά πόσον ο χρήστης είναι εξουσιοδοτημένος στο να συνδεθεί στο δίκτυο). Αυτός ο έλεγχος ταυτότητας γίνεται μετά την αρχική αίτηση σύνδεσης στον ISP, κατά την οποία η ταυτότητα του χρήστη επικυρώθηκε με μηχανισμούς password που παρέχει το PPP (PAP ή CHAP). Με άλλα λόγια, η πιστοποίηση ταυτότητας του χρήστη που πραγματοποιεί ο NAS είναι η δεύτερη που λαμβάνει χώρα – έχει προηγηθεί είτε PAP είτε CHAP αυθεντικοποίηση. Ο RAS αυθεντικοποιεί τον χρήστη κυρίως με το πρωτόκολλο RADIUS και σπανιότερα με το TACACS.

Στο PPTP, οι ζεύξεις επικοινωνίας υλοποιούνται πάνω σε σήραγγες. Οι δυνατότητες του υπολογιστή του χρήστη καθορίζουν το άκρο της σήραγγας: αν ο υπολογιστής έχει PPTP λογισμικό, τότε αυτός είναι το άκρο της. Διαφορετικά, αν υποστηρίζει μόνο PPP και όχι PPTP, τότε το άκρο της βρίσκεται στον ISP και συγκεκριμένα στον RAS.

Υπάρχουν δύο ειδών σηράγγων όπως αναφέραμε και στο L2TP: οι **«αυθόρμητες»** (mandatory tunnels) και οι **«αναγκαστικές»** (compulsory ή

mandatory tunnels). Οι πρώτες δημιουργούνται μετά από αίτηση του χρήστη, ενώ οι αναγκαστικές δημιουργούνται αυτόματα, χωρίς καμία παρεμβολή από τον χρήστη.

Μία αναγκαστική σήραγγα έχει προκαθορισμένα ακραία σημεία (που είναι στην ουσία κάποιοι RAS), άρα ο έλεγχος πρόσβασης των χρηστών είναι πιο εύκολος. Δίνει επίσης τη δυνατότητα, αν η πολιτική της εταιρίας είναι τέτοια, οι εργαζόμενοι να μην έχουν πρόσβαση στο Internet, αλλά να χρησιμοποιούν τις Internet ζεύξεις αποκλειστικά και μόνο για το VPN. Επίσης στις αναγκαστικές σήραγγες μπορούν πολλαπλές συνδέσεις να υπάρχουν πάνω σε μία σήραγγα. Ένα μειονέκτημα των αναγκαστικών είναι το γεγονός ότι η σύνδεση του υπολογιστή του χρήστη με τον RAS πραγματοποιείται έξω από τη σήραγγα και, συνεπώς, είναι μη ασφαλής (αφού δεν πραγματοποιούνται οι μηχανισμοί κρυπτογράφησης που η σύνδεση επιβάλλει). Γενικά, οι αυθόρμητες σήραγγες προσφέρουν μεγαλύτερη ασφάλεια.

Οι αναγκαστικές χωρίζονται σε δύο υποκατηγορίες:

1. **Στατικές αναγκαστικές σήραγγες** (static compulsory tunnels):
    - *Realm-based*: ο RAS ελέγχει ένα τμήμα του ονόματος του χρήστη, τον *τομέα (realm)* και με βάση αυτό αποφασίζει τη δρομολόγηση της σήραγγας αυτού του χρήστη. Σε αυτές, όλοι οι χρήστες του ίδιου τομέα (π.χ. του ίδιου γραφείου) αντιμετωπίζονται με τον ίδιο τρόπο – δηλαδή, οι σήραγγες που δημιουργούνται προσφέρουν σε όλους την ίδια ποιότητα υπηρεσίας. Αυτό μειώνει την «ευλυγισία» του συστήματος.
    - *Automatic:* Υπάρχει προεγκατεστημένος εξοπλισμός – ο χρήστης καλεί ένα συγκεκριμένο τηλεφωνικό αριθμό για να έχει πρόσβαση στο VPN (να ξεκινήσει μία σήραγγα).

Γενικότερα, οι στατικές σήραγγες δεν προσφέρονται σε συστήματα όπου υπάρχει μεγάλο πλήθος χρηστών που αιτούνται πρόσβαση.

2. **Δυναμικές αναγκαστικές** (dynamic compulsory tunnels):
    - Με βάση την αίτηση κάθε χρήστη, γίνεται σύνδεσή του με τον RAS. Χρειάζεται ένας RADIUS server για την εξουσιοδότηση του χρήστη.

Τα PPTP VPNs μπορούν να υποστηρίξουν όλα τα παραπάνω είδη σηράγγων.

Η όλη λειτουργία του PPTP πραγματοποιείται σε τρεις φάσεις:

- Πρώτη φάση: Εδώ το πρωτόκολλο χρησιμοποιεί το γνωστό πρωτόκολλο PPP για τη σύνδεση του χρήστη με τον ISP .

- Δεύτερη φάση: Ανταλλάσσονται μηνύματα ελέγχου μεταξύ PPTP client και PPTP Server (RAS) για τη διατήρηση αλλά και τον τερματισμό της σύνδεσης. Τα μηνύματα αυτά ανταλλάσσονται με βάση τις IP διευθύνσεις τους, στην 1723 TCP θύρα του RAS. Τα PPTP μηνύματα ελέγχου ενθυλακώνονται σε TCP/IP πακέτα.

- Τρίτη φάση: Τα πακέτα δεδομένων μεταφέρονται μέσω της σήραγγας που έχει υλοποιηθεί από την προηγούμενη φάση. Τα πακέτα είναι κρυπτογραφημένα. Ο βασικός αλγόριθμος κρυπτογράφησης που έχει χρησιμοποιηθεί για την υλοποίηση του PPTP πρωτοκόλλου είναι ο RC4. Το κλειδί κρυπτογράφησης προκύπτει από εφαρμογή μιας συνάρτησης κατακερματισμού στο password του χρήστη (αφού το password το έχει, εκτός βέβαια από τον ίδιο το χρήστη, και το δίκτυο λόγω του RADIUS Server, δεν χρειάζεται ανταλλαγή κλειδιού). Η κρυπτογράφηση ξεκινά από τον υπολογιστή του χρήστη – κάτι που προσδίδει μεγαλύτερη ασφάλεια.

Μέχρι τώρα αναφερόμασταν, όσον αφορά τα Εικονικά Δίκτυα που βασίζονται στο PPTP, μόνο σε περιπτώσεις όπου ένας χρήστης συνδέεται με το PC του σε ένα δίκτυο. Αν και αυτό ήταν το αρχικό κίνητρο ανάπτυξης του PPTP, μπορεί παρόλα αυτά να εξυπηρετήσει και περιπτώσεις σύνδεσης δικτύου με δίκτυο (LAN-to-LAN tunneling) όπως και στο L2TP. Απλά ο server σε κάθε ένα από τα δύο δίκτυα που επικοινωνούν θα πρέπει να μπορεί να λειτουργεί άλλοτε ως server και άλλοτε ως client. Κατά τα άλλα, μία LAN-to-LAN PPTP υποδομή μοιάζει πολύ με μία LAN-to-LAN IPSec υποδομή, με εξαίρεση το ότι δεν υπάρχει το πρωτόκολλο ανταλλαγής κλειδιού IKE σε αντίθεση με το L2TP.

Οι PPTP servers προωθούν πακέτα από και προς το αντίστοιχο LAN, έχοντας επίσης τη δυνατότητα να «φιλτράρουν» τα εισερχόμενα πακέτα. Όταν ο ISP διαθέτει PPTP server δεν χρειάζεται ο υπολογιστής του χρήστη να είναι εφοδιασμένος με ειδικό PPTP software – διαφορετικά, κάτι τέτοιο είναι απαραίτητο (και σε αυτήν την τελευταία περίπτωση το άκρο της σήραγγας είναι ο υπολογιστής και όχι ο PPTP server).

Στα μειονεκτήματα του PPTP συγκαταλέγεται το γεγονός ότι οι PPTP servers δέχονται δεδομένα μόνο στην 1723 TCP θύρα – κάτι που αποτελεί σημαντική πληροφορία για κάποιον που θέλει να υποκλέψει την επικοινωνία. Επίσης, GRE πακέτα (που ενυπάρχουν στα PPTP πακέτα) δεν μπορούν να περάσουν από όλους τους τοίχους ασφαλείας (firewalls). Τέλος, τα VPNs που στηρίζονται στο PPTP εξαρτώνται πολύ από τα πρωτόκολλα που διαθέτει και μπορεί να υποστηρίξει ο ISP σε αντίθεση με το IPSec που αναλύεται σε επόμενο κεφάλαιο.

Συγκρίνοντας το L2TP με το PPTP, το πρώτο λειτουργεί γενικά καλύτερα σε περιπτώσεις όπου τα πακέτα περνάνε από «τοίχους ασφαλείας», μια που δεν υπάρχει GRE ενθυλάκωση η οποία είναι αυτή που δημιουργεί το αντίστοιχο πρόβλημα στο PPTP. Επίσης, παρέχει μεγαλύτερη ασφάλεια ως προς την ανάλυση κίνησης (traffic analysis), λόγω του ότι η επικοινωνία δεν γίνεται μόνο μέσω μιας συγκεκριμένης UDP θύρας στον LNS (αν και υπάρχει μια προκαθορισμένη θύρα ως βασική, η 1701): οι διαχειριστές δικτύου μπορούν να αλλάζουν αυτήν τη θύρα, δυσκολεύοντας έτσι το έργο ενός επιτιθέμενου.

2.4 Το Πρωτόκολλο RADIUS

Το πρωτόκολλο RADIUS έχει τη δομή μοντέλου «πελάτη-εξυπηρετητή» (client-server). Ο NAS δέχεται τις αιτήσεις των χρηστών, παίρνει ID και passwords από αυτούς, και τα προωθεί στον RADIUS server. Ο RADIUS Server ενημερώνει για το αν εγκρίνει την πρόσβαση ή όχι, μια που διατηρεί μία κεντρική βάση δεδομένων των χρηστών, τόσο με τα στοιχεία τους όσο και με τις αντίστοιχες υπηρεσίες που μπορεί να παρέχει σε καθέναν από αυτούς. Γενικότερα, ο RADIUS Server διατηρεί στη βάση του διάφορα στοιχεία, όπως τη διεύθυνση του NAS (για πληροφορίες στατιστικής φύσεως της χρήσης της ζεύξης) καθώς και πληροφορίες χρέωσης των χρηστών (αν κάτι τέτοιο είναι πολιτική του παρόχου του δικτύου).

Συχνά υπάρχουν και RADIUS proxy servers, οι οποίοι είναι εγκατεστημένοι στους ISPs και ενημερώνονται ανά περιοδικά διαστήματα από τον κεντρικό RADIUS server – διατηρούν δηλαδή οι ίδιοι ένα αντίγραφο της βάσης δεδομένων, με βάση την οποία αυθεντικοποιούν το χρήστη.

Το πρωτόκολλο RADIUS αναπτύχθηκε από την Livingston Enterprises ως ένας server πρόσβασης, πιστοποίησης και παρακολούθησης. Από τότε έχει υλοποιηθεί από διάφορους άλλους πωλητές και έχει κερδίσει ευρεία υποστήριξη ανάμεσα ακόμα και στους παροχείς υπηρεσιών (ISPs).

Η Λειτουργία Πρωτοκόλλου

Η επικοινωνία μεταξύ ενός NAS και ενός RADIUS server βασίζεται στο **User Datagram Protocol** (UDP).

Οι δημιουργοί του RADIUS επέλεξαν το UDP ως το πρωτόκολλο μεταφοράς για τεχνικούς λόγους. Γενικά το RADIUS θεωρείται μία υπηρεσία άνευ συνδέσεως.

Θέματα που σχετίζονται με τη διαθεσιμότητα του server, την επανεκπομπή και τα timeouts διαχειρίζονται από διάφορες συσκευές του RADIUS και όχι από το πρωτόκολλο μεταφοράς.

Τυπικά μία αίτηση για login αποτελείται από μία αίτηση από τον NAS server στον RADIUS server και μια απάντηση, θετική ή αρνητική, του τελευταίου (Access-Accept ή Access-Reject). Το πακέτο αίτησης που στέλνει ο NAS server περιέχει το username, το κρυπτογραφημένο password, την IP διεύθυνση του NAS server και τη πόρτα. Η μορφή της αίτησης παρέχει επιπλέον πληροφορίες για τον τύπο της σύνδεσης την οποία ο χρήστης θέλει να ξεκινήσει.

Όταν ο RADIUS server λαμβάνει μια αίτηση από κάποιον NAS, ψάχνει σε μια βάση δεδομένων για το username που υπάρχει στην αίτηση. Εάν το username δεν υπάρχει στη βάση δεδομένων τότε είτε ένα τυπικό προφίλ φορτώνεται και ο RADIUS server αποστέλλει μήνυμα αποδοχής, είτε αποστέλλει μήνυμα απόρριψης το οποίο μπορεί να συνοδεύεται και από κάποιο επεξηγηματικό μήνυμα του λόγου απόρριψης.

Στην περίπτωση που το username βρεθεί και το password είναι σωστό ο RADIUS server επιστρέφει μία Access-Accept απάντηση η οποία περιλαμβάνει μια λίστα των χαρακτηριστικών των ρυθμίσεων που πρέπει να χρησιμοποιηθούν από τη μεριά του NAS για τη σύνδεση. Τυπικές παράμετροι περιλαμβάνουν το τύπο της υπηρεσίας, το τύπο του πρωτοκόλλου, την IP διεύθυνση που θα δοθεί στο χρήστη (στατική ή δυναμική), την access list που πρέπει να εφαρμοστεί ή τη στατική διεύθυνση που πρέπει να εγκατασταθεί στον πίνακα δρομολογίων του NAS.

Για κάθε τύπο login που χρειάζεται πιστοποίηση και έγκριση, πρέπει να εισαχθεί μια γραμμή εντολών. Αυτή η γραμμή είναι η λίστα που χρησιμοποιείται για login μέσω του RADIUS εκτός αν υπάρχει κάποια άλλη λίστα που έχει ρυθμιστεί. Η παρακολούθηση μπορεί να χρησιμοποιηθεί ανεξάρτητα από τις άλλες διαδικασίες και επιτρέπει την αποστολή δεδομένων στην αρχή και στο τέλος των συνδέσεων καταδεικνύοντας τη ποσότητα των πόρων που χρησιμοποιήθηκαν κατά τη σύνδεση. Ένας ISP θα μπορούσε να χρησιμοποιήσει το RADIUS για να καλύψει ειδικές απαιτήσεις ασφάλειας και χρέωσης.

2.5 Το πρωτόκολλο TACACS+

Το TACACS+ επιτρέπει σε ένα ξεχωριστό server πρόσβασης (τον TACACS+ server) να παρέχει τις υπηρεσίες πιστοποίησης, έγκρισης και παρακολούθησης με

ανεξάρτητο τρόπο. Κάθε υπηρεσία μπορεί να συνδυαστεί με τη δική της βάση δεδομένων ή μπορεί να χρησιμοποιήσει τις άλλες υπηρεσίες που είναι διαθέσιμες στο δίκτυο.

Η φιλοσοφία σχεδίασης του TACACS+ είναι ο καθορισμός μιας μεθόδου για την διαχείριση όχι όμοιων server πρόσβασης (NAS) από ένα και μόνο σύνολο διαχειριστικών υπηρεσιών όπως μια βάση δεδομένων. Ένας NAS παρέχει πρόσβαση σε έναν χρήστη, σε ένα δίκτυο ή υποδίκτυο ή και σε διασυνδεδεμένα δίκτυα.

Το TACACS+ αποτελείται από τρία κύρια μέρη: την υποστήριξη του πρωτοκόλλου από servers πρόσβασης και δρομολογητές, τα χαρακτηριστικά του πρωτοκόλλου και την κεντρική βάση δεδομένων. Παρόμοια με μια εσωτερική βάση δεδομένων, το TACACS+ υποστηρίζει τα παρακάτω τρία απαιτούμενα χαρακτηριστικά ενός ασφαλούς συστήματος.

RADIUS	TACACS+
UDP: Separate timers	TCP: Automatically adjusts to network conditions
Hashes password only	Encrypts entire message
Authentication/authorization one element	Authentication/authorization distinct elements
Multivendor support	Cisco proprietary
Supports IP	Multiprotocol support

Κεφάλαιο 3ο

Σε όλα τα χρόνια της ανάπτυξης των τηλεπικοινωνιακών δικτύων δημιουργηθήκαν και δομηθήκαν διάφορα δίκτυα. Κανείς δεν μπορεί να πει επακριβώς ποιες οι διαφορές μεταξύ τους, γιατί όλα σχεδόν αναπτύσσονται ομοίως και αντιγράφουν το ένα το άλλο, άλλα πάλι αποτελούν εξέλιξη του ενός από το άλλο και άλλα δημιουργούνται με συνδυασμό τεχνολογιών από τα υπάρχοντα δίκτυα. Τέτοιου είδους δίκτυα είναι και τα VPNs.

Ένας τρόπος για να διαχωρίσει κάνεις τα δίκτυα είναι

1. με βάση την αρχιτεκτονική τους
2. με βάση των σκοπό και τις αποστάσεις που εξυπηρετούν
3. και με βάση την τεχνολογία που εφαρμόζουν.

Τα VPNs μπορούν να εφαρμοστούν σε όλες σχεδόν τις αρχιτεκτονικές, σκοπός τους είναι η ασφαλή μεταφορά πληροφοριών ανεξαρτήτως την απόσταση (αυτό θα αναληθή στο κεφάλαιο 5). Σε αυτό το κεφάλαιο θα εξετάσουμε την τεχνολογία των VPNs

Τα VPNs είναι μια τεχνολογία από μόνα τους που εφαρμόζονται πάνω σε υπάρχουσες τεχνολογίες αλλά και τροποποιούν την τεχνολογία τους ανάλογα με το σε πια εφαρμόζονται.

3.1 Τεχνολογίες δικτύων

Αν και υπάρχουν αρκετές τεχνολογίες δικτύων τρεις είναι οι σημαντικότερες και ενδιαφέρουσες.

1. IP τεχνολογία
2. ATM τεχνολογία
3. Frame Relay που αποτελεί εξέλιξη της X.25

Η IP είναι η συνηθέστερη και αυτή που χρησιμοποιείται περισσότερο στο Internet. Ανήκει στις Συγχρονισμένες τεχνολογίες μεταγωγής πακέτου και κυκλωμάτων. Σε αντίθεση με την ATM που ανήκει στην Ασυγχρόνιστες. Η Frame Relay έχει αναπτύξει τεχνολογίες και για τις δύο μορφές μεταγωγής πακέτου και

κυκλωμάτων. Αλλά και οι τρεις ακλουθούν τα μοντέλα των ομότιμων (**Peer-to-peer**) οντοτήτων και της επικάλυψης (**overlay**).

Με την σειρά τους εφαρμόζονται και αυτές στις υπάρχουσες τεχνολογίες που αναλύονται μερικώς στο κεφάλαιο 5.

- **ISDN** - Integrated Services Digital Network
- **BISDN**-Broadband Integrated Services Digital Network
- **Δίκτυα xDSL** - Digital subscriber line

3.1.1 IP Τεχνολογία

Τα VPN δομούνται σήμερα με διάφορους τρόπους. Ο δημοφιλέστερος τρόπος είναι η χρήση τεχνολογιών IP, οι οποίες προσφέρουν περισσότερες δυνατότητες αλλά και ευελιξία.

Μία φαινομενικά απλή ιδέα επιτρέπει στους υπολογιστές και στα δίκτυα σε όλο τον κόσμο να μοιράζονται πληροφορίες και μηνύματα στο Internet:

"Σπάστε κάθε πληροφορία και μήνυμα σε μικρά κομμάτια που ονομάζονται πακέτα, παραδώστε αυτά τα πακέτα στο σωστό προορισμό και εν συνεχεία συναρμολογήστε τα ξανά στην αρχική τους μορφή έτσι ώστε ο υπολογιστής να μπορεί να τα δει και να τα χρησιμοποιήσει."

Αυτό ακριβώς κάνουν δύο από τα σημαντικότερα επικοινωνιακά πρωτόκολλα που χρησιμοποιούνται στο Internet το **Transmission Control Protocol** (TCP) [9]και το **Internet Protocol** (IP)[10]. Τα πρωτόκολλα αυτά αναφέρονται συνήθως ως Μοντέλο Διαστρωμάτωσης TCP/IP. Το TCP διασπά και συναρμολογεί τα πακέτα, ενώ το IP διασφαλίζει ότι τα πακέτα στέλνονται στο σωστό προορισμό τους.

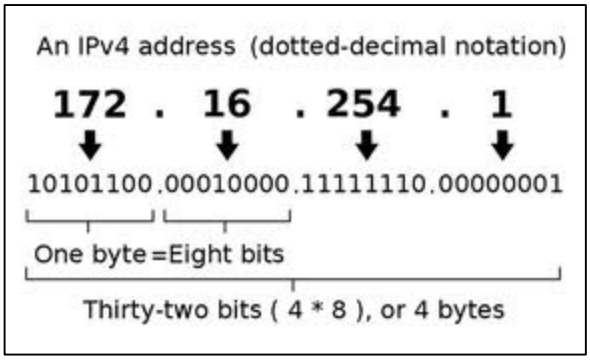
Το Internet αποτελεί ένα διανεμητικά διασυνδεδεμένο νοητό δίκτυο. Σε ένα τέτοιο δίκτυο δεν υπάρχει μία απλή, σχέση μεταξύ του αποστολέα και του παραλήπτη. Έτσι, όταν στέλνεται μια πληροφορία, αυτή σπάει σε μικρά πακέτα, στέλνεται μέσω πολλών διαφορετικών οδών την ίδια στιγμή και συναρμολογείται ξανά στο σημείο του παραλήπτη.

---

[9] Το **TCP *(Transmission Control Protocol - Πρωτόκολλο Ελέγχου Μεταφοράς)*** είναι ένα από τα κυριότερα πρωτόκολλα της Σουίτας Πρωτοκόλλων Διαδικτύου. Βρίσκεται πάνω από το *πρωτόκολλο IP*. Οι κύριοι στόχοι του πρωτοκόλλου TCP είναι να επιβεβαιώνεται η αξιόπιστη αποστολή και λήψη δεδομένων, επίσης να μεταφέρονται τα δεδομένα χωρίς λάθη μεταξύ του στρώματος δικτύου (network layer) και του στρώματος εφαρμογής (application layer) και, φτάνοντας στο πρόγραμμα του στρώματος εφαρμογής, να έχουν σωστή σειρά.

[10] **Το Πρωτόκολλο IP**, ανήκει στο Επίπεδο Δικτύου, στο Μοντέλο Διαστρωμάτωσης TCP/IP. Καθορίζει τη μορφή των πακέτων που στέλνονται μέσω ενός διαδικτύου, καθώς και τους μηχανισμούς που χρησιμοποιούνται για την προώθηση των πακέτων από έναν υπολογιστή προς έναν τελικό προορισμό μέσω ενός ή περισσότερων δρομολογητών. Εισήχθη από τους Vint Cerf και Bob Kahn το 1974.

Από την άλλη μεριά, το τηλεφωνικό σύστημα αποτελεί ένα υλικά διασυνδεδεμένο δίκτυο. Σε ένα τέτοιο δίκτυο, από τη στιγμή που επιτευχθεί μία σύνδεση (όπως μια τηλεφωνική κλήση για παράδειγμα) το συγκεκριμένο τμήμα του δικτύου εξυπηρετεί αποκλειστικά αυτή τη σύνδεση.



Το χαρακτηριστικότερο γνώρισμα του IP είναι η 32-bits διεύθυνσή του. Μια εικονική διεύθυνση δίνεται σε κάθε υπολογιστή και δρομολογητή του δικτύου. Η πραγματική φυσική διεύθυνση της συσκευής λαμβάνεται χρησιμοποιώντας μερικά πρωτόκολλα προσδιορισμού διεύθυνσης (address resolution protocol, ARP[11]). Τα μηχανήματα χρησιμοποιούν διαφορετικές μορφές για τις φυσικές διευθύνσεις. Οι μορφές αυτές βασίζονται στα πρότυπα που χρησιμοποιούνται. Για αυτό η IP διεύθυνση αναπτύχθηκε ως μορφή αναφοράς σε ένα επίπεδο διευθύνσεων κατανοητό από όλα τα μηχανήματα. Ένα χαρακτηριστικό όλων των IP δικτύων είναι ότι βασίζονται σε μηχανισμούς μετάδοσης πακέτων με την κατά το δυνατόν καλύτερη προσπάθεια. Δηλαδή το δίκτυο δεν εξυπακούεται πως εξασφαλίζει την ποιότητα υπηρεσίας (Quality of Service, QoS) ή την τάξη υπηρεσίας (Class of Service, CoS). Αυτό είναι ένα σημαντικό μειονέκτημα για πραγματικού χρόνου κίνηση πάνω από IP δίκτυα, που απαιτούν μια ορισμένη ποιότητα υπηρεσίας, QoS για να είναι αποδεκτή η υπηρεσία που παρέχουν. Κατά συνέπεια ξεχωριστά πρωτόκολλα χρειάζεται να αναπτυχθούν και να εφαρμοστούν προκειμένου να μεταφερθεί φωνή μέσω IP με μια αποδεκτή ποιότητα.

Για να μπορούν οι υπολογιστές να εκμεταλλεύονται τις δυνατότητες του Internet χρειάζονται ειδικό λογισμικό το οποίο κατανοεί και μεταφράζει τα πρωτόκολλα TCP/IP. Το εν λόγω λογισμικό αναφέρεται συχνά σαν socket (υποδοχή) ή TCP/IP stack. Για τα PCs το απαιτούμενο λογισμικό ονομάζεται Winsock.

[11] Το **Address Resolution Protocol** (**ARP**) (πρωτόκολλο επίλυσης διευθύνσεων) ορίστηκε στο RFC 826 και χρησιμοποιείται για να βρεθεί μια διεύθυνση του επιπέδου συνδέσμου (link layer) ή διεύθυνση υλικού (hardware address) ενός host με βάση μια διεύθυνση του επιπέδου επικοινωνίας (network layer). Αν και το συναντάμε κυρίως με τα πρωτόκολλα IPv4 και Ethernet (το RFC 826 το ονομάζει *πρωτόκολλο επίλυσης διευθύνσεων Ethernet* (Ethernet Address Resolution Protocol)), το ARP μπορεί να χρησιμοποιηθεί με το IP πάνω στο ATM ή το FDDI.

Υπάρχουν αρκετές διαφορετικές εκδόσεις του Winsock για το περιβάλλον του PC. Ενώ για τα συστήματα Macintosh, το λογισμικό ονομάζεται MacTCP. Και στις δύο περιπτώσεις το εν λόγω λογισμικό δρα σαν ενδιάμεσος μεταξύ του Internet και του προσωπικού υπολογιστή. Οι προσωπικοί υπολογιστές μπορούν πάντως να εκμεταλλευτούν τα απλούστερα και στοιχειώδη τμήματα του Internet χωρίς τη χρήση του Winsock ή MacTCP, αν και για την πλήρη πρόσβαση στο Δίκτυο είναι απαιτούμενα τα TCP/IP stacks.

Ο υπολογιστής συνδέεται σε ένα μικρό τοπικό δίκτυο (LAN) με τη χρήση μιας κάρτας δικτύου. Για την επικοινωνία με το δίκτυο η κάρτα δικτύου χρειάζεται έναν driver (πρόγραμμα οδηγό) – ένα λογισμικό δηλαδή που μεσολαβεί μεταξύ του δικτύου και της κάρτας. Αν ένας υπολογιστής δεν είναι φυσικά συνδεδεμένος σε ένα LAN με την κάρτα δικτύου μπορεί να συνδεθεί στο Internet με τη χρήση ενός modem.

Και σ' αυτήν την περίπτωση ο υπολογιστής χρειάζεται ένα TCP/IP stack προκειμένου να χρησιμοποιήσει τα πρωτόκολλα TCP/IP. Βέβαια σήμερα δεν χρειάζεται κάρτα δικτύου ή driver. Αντιθέτως, ο υπολογιστής χρειάζεται να χρησιμοποιήσει ένα ή δύο πρωτόκολλα λογισμικού: το **SLIP** (Serial Line Internet Protocol)[12] ή το **PPP** (Point-to-Point Protocol)[13].

Τα πρωτόκολλα SLIP και PPP έχουν σχεδιαστεί για υπολογιστές συνδεδεμένους στο Internet με σειριακή σύνδεση μέσω modem. Γενικά, το νεώτερο PPP προσφέρει μία σύνδεση με λιγότερα λάθη από αυτήν που προσφέρει το παλαιότερο SLIP.

Οι υπολογιστές μπορούν επίσης να συνδεθούν στο Internet χωρίς τη χρήση των TCP/IP stacks, SLIP ή PPP. Σε αυτή την περίπτωση πάντως δεν θα μπορούν να εκμεταλλευτούν την πλήρη δυναμική του Internet και ειδικότερα το WWW (παγκοσμίου ιστού). Για να εκμεταλλευτείτε πλήρως τις δυνατότητες που προσφέρει το Internet χρειάζεστε έναν υπολογιστή που να αποτελεί μέρος του

[12] Το **πρωτόκολλο SLIP** -(Serial Line IP) είναι το παλαιότερο πρωτόκολλο που χρησιμοποιήθηκε για τη μεταφορά πακέτων IP από τηλεφωνικές γραμμές. Είναι πολύ απλό στην υλοποίησή του και χρησιμοποιεί απλές τεχνικές ενθυλάκωσης. Δεν παρέχει διευθυνσιοδότηση, συμπίεση και τεχνικές ελέγχου-διόρθωσης σφαλμάτων.

[13] Το **πρωτόκολλο PPP**-(Point-to-Point Protocol) είναι το ευρύτερα αναπτυγμένο πρωτόκολλο για τη σύνδεση μέσω τηλεφώνου (dial up) Ουσιαστικά ενθυλακώνει τα TCP/IP πακέτα του υπολογιστή-πελάτη και τα προωθεί στον εξυπηρετητή μέσω της σειριακής γραμμής επικοινωνίας Ο εξυπηρετητής λαμβάνει τα πακέτα και τα προωθεί στο Internet. Είναι full-duplex και μπορεί να χρησιμοποιηθεί σε διάφορες τεχνολογίες φυσικού μέσου.

δικτύου, δηλαδή να διαθέτει ένα τουλάχιστον υπολογιστή με TCP/IP stack. Τα πρωτόκολλα SLIP και PPP πρέπει να χρησιμοποιούνται στην περίπτωση τηλεφωνικής κλήσης σε έναν Παροχέα Internet (ISP) για πρόσβαση στον Web.

Βασικές Λειτουργίες TCP/IP

Το **πρωτόκολλο IP** είναι υπεύθυνο για το πέρασμα του πακέτου από υπολογιστή σε υπολογιστή μέσα από το σύνολο των συνδέσεων. Καθώς το IP δρομολογεί το κάθε πακέτο μέσα στο δίκτυο, προσπαθεί να το παραδώσει, αλλά δεν μπορεί να εγγυηθεί ούτε ότι το πακέτο θα φτάσει στον προορισμό του ούτε ότι τα διάφορα πακέτα που αποτελούν τα αρχικά δεδομένα θα φτάσουν με τη σειρά με την οποία στάλθηκαν ούτε ότι το περιεχόμενο των πακέτων θα φτάσει αναλλοίωτο.

Το **πρωτόκολλο TCP** προσφέρει ένα αξιόπιστο πρωτόκολλο πάνω από το IP. Εγγυάται ότι τα πακέτα θα παραδοθούν στον προορισμό τους, ότι θα φτάσουν με τη σειρά με την οποία στάλθηκαν και ότι τα περιεχόμενα των πακέτων θα φτάσουν αναλλοίωτα (δηλ. όπως στάλθηκαν). Το TCP δουλεύει ως εξής: το κάθε πακέτο δεδομένων αριθμείται. Ο υπολογιστής - παραλήπτης και ο υπολογιστής - αποστολέας, αλλά όχι οι ενδιάμεσοι υπολογιστές, παρακολουθούν τους αριθμούς των πακέτων και ανταλλάσσουν μεταξύ τους πληροφορίες. Ο παραλήπτης λαμβάνει το πρώτο πακέτο, το δεύτερο, κλπ. Σε περίπτωση που παρουσιαστεί κάποιο πρόβλημα στο δίκτυο είτε χαθεί κάποιο πακέτο κατά τη διάρκεια της μετάδοσης, το ξαναζητάει και ο αποστολέας είναι υπεύθυνος για την αναμετάδοση του. Ο παραλήπτης ελέγχει επίσης αν το περιεχόμενο των πακέτων φτάνει σωστά .

3.1.2 ATM Τεχνολογία

Η κεντρική ιδέα πίσω από το ATM είναι αντί να αναγνωρίζει το σύστημα τον αριθμό της σύνδεσης από τη θέση του πακέτου σε μια στοίβα, απλά να φέρει το πακέτο τον αριθμό της σύνδεσης μαζί με τα δεδομένα, και ταυτόχρονα να κρατά τον συνολικό αριθμό των bytes σε ένα πακέτο μικρό, έτσι ώστε αν χαθεί κάποιο πακέτο λόγω συμφόρησης, να έχει ελάχιστη επιρροή στην ροή των δεδομένων και ίσως να μπορεί να ανακτηθεί με ειδικούς αλγορίθμους επαναληπτικότητας (redundancy).

Το όλο σχήμα φέρει από μεταγωγή πακέτου, οπότε και ονομάστηκε «Γρήγορη μεταγωγή πακέτου με μικρά σταθερού μεγέθους πακέτα». Το δε μέγεθος αυτό (53

bytes) προήλθε από την επιθυμία των εταιρειών να κρατήσουν σταθερή τη ποιότητα των φωνητικών επικοινωνιών όπως στα δίκτυα Συγχρονισμένης τεχνολογίας μεταγωγής πακέτου, γιατί σε συνδέσεις που ο χρόνος μεταφοράς πακέτου πρέπει να είναι μικρός (όπως στη κλασική τηλεφωνία), η πιθανότητα να χαθούν πακέτα αυξάνεται, αλλά αφού το μέγεθος του πακέτου είναι πολύ μικρό, αυτό δεν συνεπάγεται αισθητή απώλεια στη φυσική ροή της ομιλίας.

Έτσι στο ATM σε κάθε σύνδεση ανατίθεται ένα «εικονικό αναγνωριστικό κυκλώματος» (VCI - Virtual Circuit Identifier), το οποίο περιέχεται σε κάθε πακέτο και αναγνωρίζει με μοναδικό τρόπο τα δύο άκρα της σύνδεσης.

Υπάρχουν πολλές εφαρμογές στις οποίες η τεχνολογία ATM μπορεί να χρησιμοποιηθεί.

Οι κυριότερες από αυτές είναι:

- Τηλεσυνδιάσκεψη (Video Conferencing)
- Συνδιάσκεψη από γραφείο σε γραφείο (Desktop Conferencing)
- Εικονοτηλέφωνο (Videophone)
- Εικόνα / Ήχος κατά παραγγελία (Audio/Video On Demand)
- Εικονικά τοπικά δίκτυα (VLAN: Virtual LANs)
- Επικοινωνίες ATM μεγάλης χωρητικότητας με κινητούς κόμβους (συνήθως με δορυφορικές ζεύξεις).

Το ATM έχει σχεδιαστεί έτσι ώστε να μπορεί να χρησιμοποιηθεί με την ίδια ευκολία τόσο σε κοντινές αποστάσεις (π.χ. ένα γραφείο ή ένα κτίριο) όσο και σε μακρινές (διεθνείς και διηπειρωτικές συνδέσεις). Αυτό υπονοεί ότι μεγάλο μέρος της δουλειάς υποδομής που απαιτείται σήμερα για να συνεργάζονται αρμονικά τα τοπικά δίκτυα (LAN) με τα δίκτυα μεγάλων αποστάσεων (WAN) ή και τα μητροπολιτικά δίκτυα (MAN), μπορεί να εξαλειφθεί.

Ένα τελευταίο και πολύ σημαντικό επακόλουθο της ενοποίησης των δικτύων φωνής και δεδομένων είναι η λεγόμενη ενοποίηση τηλεφωνικών και δικτύων δεδομένων σε μεγάλες και μικρές επιχειρήσεις. Με τη δυνατότητα του ATM να χειρίζεται με την ίδια ευκολία το φορτίο που του αναθέτουν, είναι δυνατό να ενοποιηθούν τα συνήθως ανεξάρτητα δύο εσωτερικά δίκτυα των οργανισμών αυτών σε ένα, μειώνοντας το κόστος συντήρησης και επένδυσης. Η αναβαθμησιμότητα του ATM, όπως διαφάνηκε παραπάνω, αφήνει πολλά περιθώρια για επέκταση του ενιαίου δικτύου, τόσο σε χωρητικότητα, όσο και σε απόσταση.

Με το ATM μπορούμε είτε να μεταφέρουμε πακέτα (κελιά) δεδομένων απευθείας με την αρχιτεκτονική του ATM είτε τοποθετημένα διαδοχικά IP πακέτα

πάνω από επίπεδα μεταφοράς που ως βάση έχουν το ATM. Η τελευταία επιλογή είναι αναποτελεσματική εξαιτίας του υπερβολικού αριθμού πρωτοκόλλων που υπάρχει στα ανώτερα επίπεδα. Αυτό βέβαια έρχεται σε αντίθεση με το λόγο για τον οποίον αναπτύχθηκε το ATM : Μια αποδοτική αρχιτεκτονική με ενσωματωμένες πολλές χρήσεις. Αντίθετα με το IP ή το Frame relay το ATM δεν είναι μόνο ένα πρωτόκολλο. Δεν είναι περιορισμένο σε ένα μόνο επίπεδο σε κάποια αρχιτεκτονική. Είναι το ίδιο μια αρχιτεκτονική. Είναι μέρος του δικτύου ευρείας ζώνης (B-ISDN).

Το ATM έχει αυτό το όνομα επειδή δεν είναι συγχρονισμένο, δεν είναι δηλαδή συνδεδεμένο με ένα ρολόι. Η βασική ιδέα που στηρίζεται είναι να μεταφερθούν όλες οι πληροφορίες με μικρά, σταθερού μήκους πακέτα που ονομάζονται κελιά και έχουν μήκος 53 bytes. Στην περίπτωση της φωνής είναι 5 bytes για την επικεφαλίδα και 48 bytes για το φορτίο. Η υπηρεσία ATM ονομάζεται και cell relay.

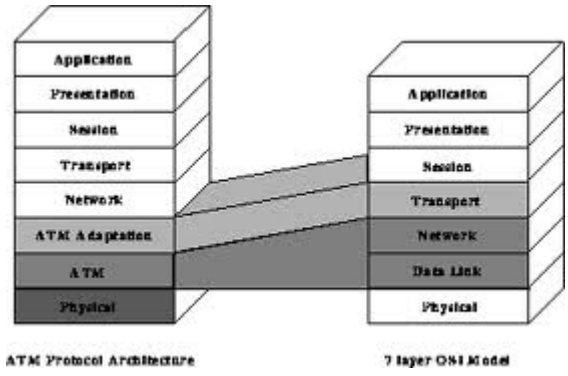
Η μεταγωγή κελιών (cell switching) είναι αρκετά εύκαμπτη και μπορεί να χειρισθεί εύκολα κίνηση σταθερού ρυθμού (ήχος, βίντεο) και μεταβλητού ρυθμού (δεδομένα). Σε πολύ υψηλές ταχύτητες η ψηφιακή μεταγωγή κυψελών είναι ευκολότερη από ότι με τη χρήση παραδοσιακών τεχνικών πολυπλεξίας, κυρίως χρησιμοποιώντας οπτικές ίνες. Η δημιουργία κλήσης απαιτεί αρχικά την αποστολή μηνύματος για την αποκατάσταση της σύνδεσης. Μετά από αυτό, τα επόμενα κελιά ακολουθούν την ίδια διαδρομή για να φτάσουν στον προορισμό. Όμοια με το frame relay, η διανομή των κελιών δεν είναι σίγουρη. Από την άλλη όμως, η τοποθέτησή τους σε σειρά είναι εγγυημένη.

Οι προοριζόμενες ταχύτητες για τα δίκτυα του ATM είναι 155.52MB/s (για συμβατότητα με SONET (Synchronous Optical Network, επιτρέπει τη μετάδοση διαφορετικών τύπων δεδομένων σε μία μόνο γραμμή, σε μια οπτική ίνα) και 622 MB/s (για τέσσερα 155MB/s κανάλια).

Η αρχιτεκτονική του ATM αποτελείται από δύο κύρια επίπεδα, το επίπεδο ATM (ATM layer) και το στρώμα προσαρμογής του ATM

ATM Reference Model

Higher Layers		
ATM Adaptation Layer (AAL)		Convergence Sublayer (CS) Segmentation and Reassembly (SAR) Sublayer
ATM Layer		Generic flow control (GFC) Cell header creation/verification Cell VPI/VCI translation Cell multiplex and demultiplex
Physical Layer	Tranmission Convergence (TC) Sublayer	HEC generation/verification Cell delineation Cell-rate decoupling Transmission adaption
	Physical Medium-Dependent (PMD) Sublayer	Bit timing (time recover) Line coding for physical medium



ATM Protocol Architecture 7 layer OSI Model

(ATM Adaptation Layer, AAL). Ακριβώς πάνω από το φυσικό επίπεδο είναι το επίπεδο ATM (ATM layer), που ασχολείται με τα κελιά και τη μεταφορά των κελιών. Καθορίζει τη μορφή των κελιών και τη σημασία της επικεφαλίδας. Ασχολείται ακόμα με τη διαχείριση των εικονικών κυκλωμάτων. Επίσης εδώ πραγματοποιείται ο έλεγχος συμφόρησης. Επειδή πολλές εφαρμογές δεν λειτουργούν διαφορετικά με τα κελιά από ότι με τα πακέτα, ένα επίπεδο πάνω από το επίπεδο ATM ορίστηκε να επιτρέπει στους χρήστες να στέλνουν πακέτα μεγαλύτερου μήκους από αυτό των κελιών. Αυτό ονομάζεται στρώμα προσαρμογής του ATM (ATM Adaptation Layer, AAL). Υπάρχουν πέντε τύποι του AALs που καθορίζονται για διαφορετικού τύπου υπηρεσίες. Το AAL 1 και το AAL 2 χρησιμοποιούνται για να μεταφέρουν τη φωνή άμεσα πάνω από ένα ATM. Εάν θέλουμε να χρησιμοποιήσουμε voice over IP over ATM τότε χρειάζεται να χρησιμοποιήσουμε το AAL 5.

Σύγκριση IP – ATM

Τα IP δίκτυα έχουν σχεδιαστεί, κυρίως, για να υποστηρίξουν μια υπηρεσία βασισμένη στο μηχανισμό μετάδοσης πακέτων με την κατά το δυνατόν καλύτερη προσπάθεια (best-effort υπηρεσία), που είναι κατάλληλη για δεδομένα. Όπως έχει αναφερθεί και παραπάνω, αντιμετωπίζουν ακόμα πολλά εμπόδια στην υποστήριξη υψηλής ποιότητας σε ένα περιβάλλον πολλών υπηρεσιών. Οι καινούριες αρχιτεκτονικές και τα καινούρια πρωτόκολλα που αναπτύσσονται πρέπει να περάσουν ακόμα από πολλά στάδια για να είναι ικανοποιήσουν αυτές τις ανάγκες.

Τα ATM πρωτόκολλα και πρότυπα για δίκτυα πολύ-υπηρεσιών έχουν καθορισθεί κατά ένα μεγάλο μέρος. Οι βασικές προκλήσεις που παραμένουν για τις υπηρεσίες συσχετίζονται με :

- την επιλογή των αλγορίθμων επεξεργασίας,
- ένα πρωτόκολλο μεταφοράς πάνω από το ATM επίπεδο δηλαδή, το AAL
- τη σωστή αρχιτεκτονική του δικτύου.

Το ATM επικοινωνεί με τα PSTN δίκτυα καλά. Επίσης ενσωματώνει καλά διαφορετικούς τύπους κίνησης περιλαμβάνοντας όλους τους τύπους με σταθερό και μεταβλητό ρυθμό (Constant Bit Rate, CBR και Variable Bit Rate, VBR).Υποστηρίζει ακόμα, την εγγυημένη ποιότητα εξυπηρέτησης (QoS) και την ενσωματωμένη διάκριση ποιότητας εξυπηρέτησης. Το ATM έχει πολύ καλή υποστήριξη από τα πρότυπα των φυσικών επίπεδων όπως το SONET. Έτσι παρουσιάζεται ως η τέλεια τεχνολογία για υποστήριξη φωνής. Ωστόσο, η πολύπλευρη ύπαρξή της έχει και μειονεκτήματα. Ο έλεγχος συμφόρησης, ο έλεγχος ροής και τα ζητήματα διαχείρισης παραμένουν άλυτα.

Ενώ τα IP δίκτυα επιφέρουν σημαντικά υψηλότερη καθυστέρηση που όμως μειώνεται καθώς η ταχύτητα συνδέσεως αυξάνει. Η συνεχής αύξηση της κίνησης δεδομένων θα δικαιολογήσει την υψηλότερη ταχύτητα συνδέσεως που χρειάζεται να υποστηρίξει η IP κίνηση δεδομένων. Η μεταφορά με υψηλή προτεραιότητα σε IP δίκτυα θα είναι στη συνέχεια πολύ ελκυστική. Ενώ τα IP πακέτα επιτρέπεται να είναι μήκους 64 KB, το μέγιστο μέγεθος για τα μεταφερόμενα πακέτα σήμερα στο Internet είναι 1536 bytes, με μέσο όρο γύρω στα 350 bytes.

Και τα δύο, IP και ATM, μπορούν να προσφέρουν υπηρεσίες με πολλές εφαρμογές VPNs. Η ικανότητα να προσφέρουν τέτοιες υπηρεσίες οφείλεται στα ATM πρότυπα και προϊόντα. Οι IP επιλογείς (switches) έχουν ευέλικτη και ιεραρχημένη διαχείριση εύρους ζώνης συχνοτήτων που συμβάλλει στη δημιουργία IP δικτύων όλο και πιο κατάλληλα να προσφέρουν τέτοιες υπηρεσίες. Η τυποποίηση των διαφοροποιημένων υπηρεσιών προσθέτει επιπλέον ευελιξία στα IP δίκτυα που παρέχουν υπηρεσίες με πολλές VPNs. Οι διαφοροποιημένες υπηρεσίες χρησιμοποιούνται για τον καθορισμό και τον έλεγχο τις κίνησης του δικτύου σε τάξεις. Με αυτόν τον τρόπο ορισμένες εφαρμογές παίρνουν προτεραιότητα. Οι διαφοροποιημένες υπηρεσίες είναι η πιο προηγμένη μέθοδος για τη διαχείριση της κίνησης από την άποψη της τάξης υπηρεσιών (Class of Service).

Το μεγαλύτερο εμπόδιο στην ανάπτυξη του ATM για ενοποιημένες υπηρεσίες φωνής και δεδομένων είναι το μεγάλο κόστος. Ο εξοπλισμός του ATM είναι πολύ ακριβός. Επίσης, τα IP δίκτυα είναι τα επικρατέστερα στον κόσμο σήμερα. Για την μετατροπή τους σε ATM απαιτείται μια πλήρη ανακαίνιση που είναι επίσης, πολύ ακριβή για τους περισσότερους. Η επιτυχία της μετάδοσης πάνω από στα δίκτυα πακέτων βασίζεται στο χαμηλότερο κόστος. Εάν σκεφτούμε αυτά τότε θα πρέπει να παραμείνουμε στα IP δίκτυα και να ενισχύσουμε τις ικανότητές τους.

3.1.3 Frame Relay τεχνολογία

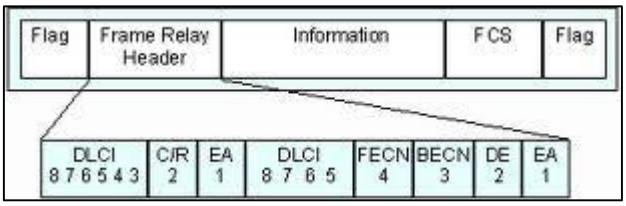
Το Frame Relay προσφέρει μια δυνατότητα ανταλλαγής δεδομένων μέσω δικτύων μεταγωγής πακέτων, η οποία χρησιμοποιείται ως συνδετικός κρίκος μεταξύ των συσκευών του χρήστη (π.χ. routers, bridges, host machines) και του εξοπλισμού του δικτύου (π.χ. κόμβοι μεταγωγής). Οι συσκευές του χρήστη συχνά αποκαλούνται και **DTE** (Data Terminal Equipment), ενώ οι συσκευές του δικτύου, που διασυνδέονται με τα DTE, συχνά αποκαλούνται και **DCE** (Data Circuit-terminating Equipment). Το δίκτυο το οποίο προσφέρει τη διασύνδεση Frame Relay μπορεί να είναι είτε ένα δημόσιο δίκτυο, είτε ένα ιδιωτικό, το οποίο εξυπηρετεί μια απλή επιχείρηση.

Στην ουσία η τεχνική δημιουργήθηκε για να αξιοποιήσει τις δυνατότητες που παρέχει το σύγχρονο τηλεπικοινωνιακό περιβάλλον με στόχο να ικανοποιήσει τις αυξημένες του ανάγκες για υψηλές ταχύτητες. Πιο συγκεκριμένα η τεχνική αξιοποίησε: αφενός την αύξηση της επεξεργαστικής ικανότητας των συσκευών που συνδέονται σήμερα στα δίκτυα, αναθέτοντας στους σταθμούς εργασίας την εκτέλεση εργασιών όπως η διαχείριση σφαλμάτων μετάδοσης και ο έλεγχος ροής και ακολουθίας πακέτων, και αφετέρου τον εκσυγχρονισμό της τηλεπικοινωνιακής υποδομής, που οδήγησε στη δημιουργία αξιόπιστων δικτύων οπτικών ινών ή ψηφιακών συστημάτων (SONET / SDH) με πολύ "καθαρές" γραμμές μετάδοσης.

Ως μια διασύνδεση σε ένα δίκτυο, το Frame Relay είναι ίδιο με το X.25(που αναλύετε στο κεφαλαίο 5). Ομως διαφέρει σημαντικά από το X.25 όσον αφορά τη λειτουργικότητά του και τη μορφή του. Πιο συγκεκριμένα το Frame Relay αυτό καθ' αυτό είναι ένα πρωτόκολλο δευτέρου επιπέδου για αποδοτική μεταφορά δεδομένων σε υψηλές ταχύτητες, που κυρίως έρχεται να καλύψει την ανάγκη διασύνδεσης τοπικών δικτύων (LAN) με δίκτυα WAN, ή LAN με LAN όπου παρατηρούνται σύντομες αλλά μεγάλου όγκου αιχμές στη μετάδοση δεδομένων. Η τεχνική είναι περισσότερο απλοποιημένη σε σχέση με το X.25, διευκολύνοντας έτσι την γρηγορότερη εκτέλεση και την υψηλότερη απόδοση.

Ως μια διασύνδεση μεταξύ των συσκευών του χρήστη και του δικτύου, παρέχει τα μέσα για στατιστική πολύπλεξη πολλών λογικών ζεύξεων δεδομένων

(νοητών κυκλωμάτων), πάνω σε μια απλή φυσική ζεύξη μετάδοσης. Στο Frame Relay δεν υπάρχουν λογικά κανάλια όπως στο X25, αλλά η πολύπλεξη πάνω στη φυσική σύνδεση γίνεται μέσω του πεδίου DLCI, το οποίο καθορίζει τον αριθμό ταυτότητας του κάθε νοητού κυκλώματος και δίνει σε κάθε κόμβο την πληροφορία δρομολόγησης του πλαισίου προς τον τελικό αποδέκτη. Σε αντίθεση με συστήματα τα οποία χρησιμοποιούν μόνο τεχνικές DTM για να υποστηρίξουν πολλαπλές γραμμές δεδομένων, η στατιστική πολύπλεξη (SDTM) που κάνει το Frame Realy προσφέρει μια πιο ευέλικτη και αποτελεσματική αξιοποίηση του εύρους ζώνης του μέσου μετάδοσης. Η στατιστική πολύπλεξη, πιο συγκεκριμένα, είναι μια βελτιωμένη μορφή της πολύπλεξης DTM. Βασικός περιορισμός της απλής DTM πολύπλεξης είναι το ότι η κεντρική αρτηρία πρέπει να μπορεί να υποστηρίξει ρυθμό μετάδοσης τουλάχιστον ίσο με το άθροισμα των μέγιστων ρυθμών μετάδοσης των νοητών κυκλωμάτων που διέρχονται μέσω αυτής. Η πολύπλεξη SDTM υπερέχει της DTM επειδή μπορεί και εκμεταλλεύεται τα νεκρά διαστήματα, κατά τα οποία δεν διακινούνται δεδομένα μέσω των νοητών κυκλωμάτων, και κατανέμει δυναμικά τη χωρητικότητα της κεντρικής αρτηρίας μόνον στα νοητά κυκλώματα που πράγματι διακινούν δεδομένα.



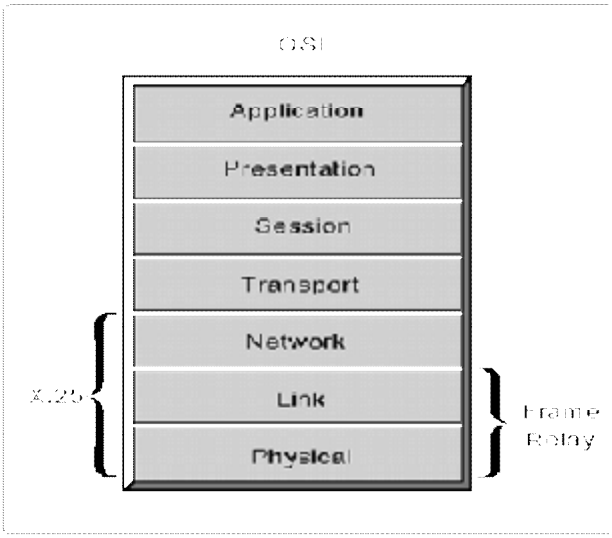
Με τον τρόπο αυτό, πολύ περισσότερα νοητά κυκλώματα μπορούν να εξυπηρετηθούν από την αρτηρία χωρίς να χρειάζεται να αυξηθεί η ταχύτητά της. Το πλήθος των νοητών κυκλωμάτων που μπορούν να εξυπηρετηθούν εξαρτάται κυρίως από το ποσοστό χρόνου πραγματικής μετάδοσης δεδομένων καθενός, δηλαδή τον "φόρτο" του. Ωστόσο για να λειτουργήσει αποτελεσματικά το σχήμα της στατιστικής πολύπλεξης απαιτείται η προσωρινή αποθήκευση των δεδομένων (buffering). Αυτό όμως δεν δημιουργεί κανένα απολύτως πρόβλημα στον αυξημένης υπολογιστικής ισχύος, δικτυακό εξοπλισμό που διαθέτουμε σήμερα.

Ενα άλλο σημαντικό χαρακτηριστικό, όπως αναφέρθηκε και παραπάνω, είναι ότι εκμεταλλεύεται τις τελευταίες εξελίξεις της τεχνολογίας μετάδοσης των δικτύων ευρείας περιοχής (WAN). Τα πρώτα πρωτόκολλα WAN, όπως το X.25, αναπτύχθηκαν όταν ακόμα δέσποζαν τα "θορυβώδη" συστήματα αναλογικής μετάδοσης και το μέσο μετάδοσης ήταν ο χαλκός. Αυτές οι ζεύξεις είναι πολύ λιγότερο αξιόπιστες από τα οπτικά μέσα και τις συνδέσεις ψηφιακής μετάδοσης που είναι διαθέσιμες σήμερα (οι ψηφιακοί ρυθμοί σφαλμάτων είναι μικρότεροι από ένα

σφάλμα σε κάθε 1.000.000 μεταδιδόμενα bit). Με συνδέσεις σαν αυτές, τα πρωτόκολλα επιπέδου ζεύξης μπορούν να παραλείψουν τους χρονοβόρους αλγορίθμους διόρθωσης λαθών και ελέγχου ροής, αφήνοντάς τους να εκτελεστούν από τα υψηλότερα επίπεδα του μοντέλου OSI, που διαθέτουν τέτοιες δυνατότητες (π.χ. TCP / IP). Αφού η εξακρίβωση των σφαλμάτων και το βάρος της διόρθωσης αφαιρείται απ' το δίκτυο και μεταβιβάζεται στις συσκευές πηγής και προορισμού, οι χρόνοι απόκρισης του δικτύου βελτιώνονται σημαντικά. Αυτοί οι βελτιωμένοι χρόνοι απόκρισης του δικτύου, βελτιώνουν και τους χρόνους απόκρισης των εφαρμογών που εξυπηρετούνται μέσω του δικτύου ευρείας περιοχής (WAN). Ετσι είναι πλέον δυνατό να έχουμε μεγαλύτερη απόδοση χωρίς να θυσιάζεται η ακεραιότητα των δεδομένων.

Το Frame Relay σχεδιάστηκε με αυτό το σκεπτικό. Περιλαμβάνει μεν ένα αλγόριθμο κυκλικού ελέγχου πλεονασμού CRC (cyclic redundancy check) για την ανίχνευση σφαλμάτων μετάδοσης (έτσι ώστε να απορρίπτονται τα αντίστοιχα πλαίσια), αλλά δεν περιλαμβάνει κανένα μηχανισμό πρωτοκόλλου για τη διόρθωση των σφαλμάτων (π.χ. με την επανεκπομπή των δεδομένων σ' αυτό το επίπεδο της σύνδεσης), ούτε μηχανισμούς ελέγχου ροής.

Μια άλλη διαφορά μεταξύ του Frame Relay και του X.25 είναι η απουσία σαφούς ελέγχου ροής ανά νοητό κύκλωμα. Τώρα, που πολλά πρωτόκολλα υψηλότερων επιπέδων εκτελούν αποτελεσματικά τους δικούς τους αλγόριθμους ελέγχου ροής, η ανάγκη εκτέλεσης αυτής της λειτουργίας στο επίπεδο δικτύου έχει ελαττωθεί. Γι' αυτό το λόγο το Frame Relay δεν περιλαμβάνει διαδικασίες σαφούς ελέγχου ροής, αφού αυτές υπάρχουν και σε υψηλότερα επίπεδα. Για την ακρίβεια η τεχνική έχει εξαλείψει εντελώς το τρίτο επίπεδο του OSI (επίπεδο πακέτων του X.25), αυξάνοντας έτσι την ταχύτητα μετάβασης μέσα από το δίκτυο και ελαχιστοποιώντας την επεξεργασία των δεδομένων στους κόμβους. Συνεπώς το δίκτυο απλοποιείται προσφέροντας στους χρήστες μόνο λειτουργίες πρώτου και δευτέρου επιπέδου. Αντιθέτως, παρέχονται πολύ απλοί μηχανισμοί επισήμανσης της συμφόρηση στο δίκτυο ώστε να επιτρέπεται



σ' αυτό να ενημερώνει τις συσκευές των χρηστών ότι οι πόροι του δικτύου πλησιάζουν σε κατάσταση συμφόρησης. Αυτή η επισήμανση μπορεί να προειδοποιήσει τα πρωτόκολλα υψηλότερων επιπέδων ότι ίσως χρειάζεται έλεγχος ροής των δεδομένων.

Οι παραπάνω τεχνολογίες αναφέρονται ξανά στο κεφάλαια αλλά αυτή την φορά σε μια σύγκριση μεταξύ τους ως προς την ασφάλεια

3.2 Μορφές και Μοντέλα VPNs

Τα σημερινά WAN είναι τυπικά χτισμένα με τη χρήση ιδιωτικών γραμμών ή ιδιωτικού Frame Relay και ATM. Το μέρος της απομακρυσμένης σύνδεσης στο δίκτυο είναι επίσης μια ιδιωτική λύση με τις εταιρίες να αναπτύσσουν και να διαχειρίζονται τα δικά τους συστήματα απομακρυσμένης πρόσβασης. Εφαρμογές extranet συνήθως δεν υποστηρίζονται ή πραγματοποιούνται σαν μία ακριβή υπηρεσία σε συγκεκριμένες περιπτώσεις που απαιτείται.

Ένα τέτοιο ιδιωτικό δίκτυο περιορίζει την επεκτασιμότητα του σε απομακρυσμένους χρήστες και συνεργάτες, είναι δύσκολο στη διαχείριση και επιπλέον ακριβό στο εύρος ζώνης και στη διαχείριση του. Η μετανάστευση από ένα ιδιωτικό δίκτυο σε VPN επικεντρώνεται στο κάθε ξεχωριστό τμήμα του δικτύου-intranet και απομακρυσμένης πρόσβασης και επεκτείνει το δίκτυο στους συνεργάτες της επιχείρησης.

3.2.1 Overlay και P-P Μοντέλα

Το Επικαλυπτόμενο (Overlay) VPN

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. Ο πελάτης εγκαθιστά μια router-to-

router επικοινωνία ανάμεσα στις CPE[14] συσκευές στα VCs που είναι εφοδιασμένος από τον πάροχο υπηρεσίας.

Στη συνέχεια το πρωτόκολλο δρομολόγησης δεδομένων ανταλλάσσει πληροφορία μεταξύ των συσκευών του παρόχου και έτσι 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 δεσμευμένο εγγυημένο εύρος ζώνης εξαρτάται από την στρατηγική δέσμευσης 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 VPNs μπορούν να υλοποιηθούν με χρήση διαφόρων διασυνδεδεμένων WAN τεχνολογιών επιπέδου 2, συμπεριλαμβανομένων των X.25, frame relay 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 Internet. Οι πιο κοινές IP-to-IP Tunneling τεχνολογίες είναι το Generic Route Encapsulation (GRE) και το IP Encryption(Αναλύετε στο κεφάλαιο 5).

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 συνδέσεων με λίγες κεντρικές τοποθεσίες και πολλές απομακρυσμένες, αλλά γίνεται υπερβολικά δύσκολο στη διαχείριση σε μια περισσότερο πολύπλοκη & σύνθετη διάταξη.
- **Μερική γνώση & πρόβλεψη κίνησης**. Η σωστή δημιουργία των VC με τις απαραίτητες χωρητικότητες, απαιτεί λεπτομερή γνώση της site-to-site κίνησης που είναι 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.

[14] **CPE** - Customer Premises Equipment - Συνδρομητικός εξοπλισμός για της τηλεφωνικές κλήσης.

- **Υποστήριξη πολύπλοκη επιχειρηματικού μοντέλου** από τους παροχείς δικτυακών υπηρεσιών. Τέλος αλλά όχι λιγότερα σημαντικό αποτελεί το γεγονός ότι το Overlay VPN μοντέλο, όταν εφαρμόζεται με επιπέδου 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.

Το Μοντέλο των ομότιμων (Peer-to-Peer) οντοτήτων P-P VPN

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.(βλέπε SSL 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.

Διαμοιραζόμενο P-P VPN

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 διεπαφή 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.

Αφιερωμένο P-P VPN

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[15] «τρέχει» μεταξύ του PE και του PO 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

[15] Ορισμένα πολύ γνωστά πρωτόκολλα δρομολόγησης είναι τα: BGP RIP OSPF

- 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

3.2.2 Μορφές VPNs

Τα VPN χωρίζονται σε τρεις κατηγορίες: απομακρυσμένης πρόσβασης, intranets και extranets. Κάθε τύπος VPN έχει διαφορετικά θέματα ασφάλειας και ποιότητας παρεχόμενων υπηρεσιών να αντιμετωπίσει

Απομακρυσμένης Πρόσβασης (Remote Access) ή VDPN

Τα VPNs αυτού του τύπου επεκτείνουν το δίκτυο σε τηλεργαζόμενους, κινούμενους χρήστες ή ακόμα και μικρότερα απομακρυσμένα γραφεία με περιορισμένη κίνηση από και προς το δίκτυο της επιχείρησης και των συλλογικών υπολογιστικών της πόρων. Επιτρέπουν στους χρήστες να συνδεθούν στα intranets και extranets των συνεργατών τους όταν, από όπου και όπως αυτοί θέλουν.

Τα VPNs απομακρυσμένης πρόσβασης παρέχουν σύνδεση και δίνουν δυνατότητα σύνδεσης μέσα από μία διαμοιρασμένη μορφή με τις ίδιες πολιτικές, με το ιδιωτικό δίκτυο. Οι μέθοδοι πρόσβασης είναι ευέλικτες ασύγχρονες κλήσεις, ISDN, xDSL, κινητό IP και καλωδιακές τεχνολογίες. Τα πλεονεκτήματα της μετάβασης στα VPN είναι:

- Μειωμένα κεφάλαια για απόκτηση modem και αναγκαίου εξοπλισμού υλοποίησης του VPN
- Δυνατότητα χρήσης τοπικών τηλεφωνικών γραμμών και όχι υπεραστικών, ελαχιστοποιώντας έτσι σε μεγάλο βαθμό το κόστος σύνδεσης.
- Μεγαλύτερη διαβάθμιση και ευκολία ανάπτυξης για νέους χρήστες.
- Επιστροφή της επιχείρησης στο σκοπό της και όχι στη συντήρηση του μέσου επίτευξής του.

Κατά την υλοποίηση ενός VPN σημαντική είναι απόφαση για το που θα ξεκινάει η διαδικασία της σήραγγας και της κρυπτογράφησης στον dialup χρηστή ή στον Διακομιστή Πρόσβασης Δικτύου (Network Access Server-NAS). Στο μοντέλο λειτουργίας όπου έχουμε έναρξη σύνδεσης από dialup χρηστή η κρυπτογραφημένη σήραγγα εγκαθιδρύεται στον dialup χρηστή χρησιμοποιώντας IPSec, L2TP,

PPTP κάνοντας έτσι το δίκτυο του παροχέα υπηρεσιών απλά ένα μέσο μεταφοράς στο δίκτυο των συνεργατών.

Ένα πλεονέκτημα του μοντέλου αυτού είναι το ότι η χρήση του πρωτοκόλλου **POP**[16] για την κλήση στον παροχέα υπηρεσιών είναι ασφαλισμένη. Ένα ζήτημα που πρέπει να προσεχθεί στην περίπτωση αυτή είναι το αν θα ενεργοποιηθεί το λογισμικό ασφάλειας του συστήματος ή θα προτιμηθεί κάποιο συμπληρωματικό πακέτο ασφάλειας. Η επιλογή της δεύτερης λύσης έχει μεν όλα τα θετικά στοιχεία που απορρέουν από την εφαρμογή ειδικού πακέτου ασφάλειας αλλά έχει και το αρνητικό της ανάγκης εγκατάστασης και συντήρησής του.

Εάν το μοντέλο, τώρα, είναι ότι κάποιος δικομιστής (NAS) ξεκινά τη σύνδεση τότε τα θέματα που αφορούν το λογισμικό που τρέχει στον dialup χρηστή περιορίζονται αισθητά. Ο απομακρυσμένος χρήστης επικοινωνεί με τον POP δικομιστής του παροχέα υπηρεσιών χρησιμοποιώντας μία PPP/SLIP σύνδεση, πιστοποιείται από τον παροχέα υπηρεσιών ο οποίος σε απάντηση ξεκινά ένα ασφαλές κρυπτογραφημένο τούνελ με την επιχείρηση από το POP κάνοντας χρήση των L2TP ή L2F. Με την αρχιτεκτονική αυτή όλη η "εξυπνάδα" του VPN βρίσκεται στη πλευρά του δικομιστής του παροχέα υπηρεσιών δεν υπάρχει λογισμικό τελικού χρήστη στην επιχείρηση που να χρειάζεται συντήρηση μειώνοντας έτσι την ανάγκη διαχείρισης των απομακρυσμένων συνδέσεων.

Το μειονέκτημα, ωστόσο, αυτού του σεναρίου είναι η ανυπαρξία ασφάλειας στο τοπικό δίκτυο που ενώνει τον dialup χρηστή με το δίκτυο του παροχέα υπηρεσιών. Για την επιλογή του τελικού μοντέλου που ταιριάζει σε μια επιχείρηση πρέπει να γίνει στάθμιση όλων αυτών των παραγόντων.

Intranet VPNs

Τα Intranet VPNs είναι η εναλλακτική λύση στη δομή WAN αφού μπορούν να αυξήσουν ή να αντικαταστήσουν τις ιδιωτικές γραμμές ή άλλες ιδιωτικές WAN υποδομές ενεργοποιώντας διαμοιρασμένες υποδομές που παρέχονται από τους παροχείς υπηρεσιών.

Τα Intranet VPNs χτίζονται πάνω στο Internet ή σε IP, Frame Relay ή ATM του δικτύου του παροχέα υπηρεσιών.

[16] Το **Post Office Protocol (POP)**, επίσης γνωστό και ως **POP3** είναι ένα πρωτόκολλο που χρησιμοποιείται για την παραλαβή των ηλεκτρονικών μηνυμάτων (email) από έναν απομακρυσμένο εξυπηρετητή (server) χρησιμοποιώντας σύνδεση TCP/IP.

Τα Intranet VPNs που χτίζονται πάνω σε IP WAN υποδομή χρησιμοποιούν IPSec ή GRE για τη δημιουργία ασφαλών τούνελ για τη μεταφορά της κίνησης του WAN. Όταν συνδυάζονται με τους μηχανισμούς QoS (WFQ, WRED, GTS, CAR) του παροχέα υπηρεσιών, τότε διασφαλίζεται η αποδοτικότερη χρήση του εύρους ζώνης και αξιόπιστη διασύνδεση. Τα πλεονεκτήματα των Intranet είναι:

- Μειωμένο κόστος WAN εύρους ζώνης
- Εύκολη σύνδεση απομακρυσμένων sites
- Αυξημένο χρόνο λειτουργίας(uptime) με την ενεργοποίηση της υπηρεσίας πλεοναζόντων WAN διασυνδέσεων στους παροχείς υπηρεσιών.

Το στήσιμο ενός Intranet VPN χρησιμοποιώντας το Internet είναι η πιο αποδοτική, για τα χρήματα που διατίθενται και τα αποτελέσματα που έχουμε, τεχνολογία υλοποίησης των VPN. Τα επίπεδα των υπηρεσιών, ωστόσο, δεν εγγυώνται την πλήρη ασφάλεια στο Internet. Όταν υλοποιούμε ένα intranet VPN, πρέπει να σταθμίζουμε ποία τα υπέρ και ποία τα κατά των διαφόρων λύσεων.

Εάν για παράδειγμα θέλαμε εγγυημένη ποιότητα διασύνδεσης τότε θα ήταν καλύτερα να στήναμε το VPN πάνω από κάποιο IP, Frame Relay, ATM δίκτυο ενός παροχέα υπηρεσιών.

Extranets VPNs

Το να επεκτείνει μια επιχείρηση τη σύνδεσή της με τους συνεργάτες και προμηθευτές της είναι ακριβή και δύσκολη υπόθεση σε ένα περιβάλλον ιδιωτικού δικτύου. Ακριβές αφιερωμένες συνδέσεις πρέπει να φτάσουν μέχρι τους συνεργάτες, πολιτικές διαχείρισης και πρόσβασης θα πρέπει να επιλεχθούν και να συντηρηθούν και συχνά υπάρχει η ανάγκη εγκατάστασης συμβατού εξοπλισμού στον χώρο του συνεργάτη. Όταν επιπλέον υπεισέρχεται και ο παράγοντας "κλήση" τότε τα πράγματα μπλέκονται ακόμα περισσότερο διότι κάθε ξεχωριστό domain πρέπει να διαχειρίζεται ξεχωριστά. Χάρη σε αυτήν τη πολυπλοκότητα πολλές εταιρίες δεν επεκτείνουν τη σύνδεσή τους στους συνεργάτες τους και υπόκεινται σε ότι αυτό συνεπάγεται. Ένα από τα πλεονεκτήματα της VPN WAN αρχιτεκτονικής είναι η ευκολία της ανάπτυξης και διαχείρισης των extranet.

Η extranet σύνδεση επιτυγχάνεται χρησιμοποιώντας την ίδια αρχιτεκτονική και πρωτοκολλά με αυτά των intranet και απομακρυσμένων VPN δικτύων. Η κύρια διαφορά είναι το ότι η άδεια πρόσβασης στους χρήστες δίδεται μια φορά κατά τη σύνδεση στο δίκτυο του συνεργάτη τους.

3.3 Οι τεχνολογίες που χρησιμοποιούν τα VPNs

3.3.1 IPSec VPN

Το IPSec σχεδιάστηκε να υποστηρίζει δύο λειτουργίες κωδικοποίησης . Η λειτουργία «μεταφοράς» (Transport mode) προστατεύει μόνο το «φορτίο δεδομένων» του κάθε πακέτου , ενώ η λειτουργία «σηράγγων» (tunnel mode) κωδικοποιεί και την κεφαλή, αλλά και το φορτίο δεδομένων του κάθε πακέτου . Όπως λογικά είναι φανερό η λειτουργία «σηράγγων» είναι πιο ασφαλής από την απλούστερη λειτουργία «μεταφοράς», αφού προστατεύει τις ταυτότητες του αποστολέα και του παραλήπτη, καθώς επίσης και άλλα πεδία της διεύθυνσης IP που μπορεί να δώσουν πληροφορίες σε κάποιον «εισβολέα». Απαραίτητη προϋπόθεση για να λειτουργήσει σωστά το πρωτόκολλο IPSec είναι όλες οι επικοινωνούντες συσκευές να μοιράζονται ένα κοινό μυστικό κλειδί . Η διαδικασία ανταλλαγής μυστικών κλειδιών χρησιμοποιεί δημόσια ψηφιακά πιστοποιητικά και βασίζεται στα πρωτόκολλα ISAKMP/Oakley/IKE (αναλύονται στο κεφάλαιο 5) και στο πρότυπο πιστοποίησης X.509 .

Για να δημιουργηθεί μία διασύνδεση τύπου “σήραγγας” ανάμεσα σε δύο υπολογιστικά συστήματα χρησιμοποιώντας ένα πρωτόκολλο VPN θα πρέπει και οι δύο εμπλεκόμενες μεριές να έχουν εφαρμόσει παρόμοιες πολιτικές ασφάλειας στο σύστημα. Διαφορετικές αρχιτεκτονικές ασφάλειας θα μπορούσαν να οδηγήσουν σε μία κατάσταση όπου το ένα σύστημα είναι λιγότερο ασφαλές από το άλλο με συνέπεια να είναι και πιο ευάλωτο . Έτσι κάποιος πιθανός «εισβολέας» , έχοντας τον έλεγχο του αδύναμου συστήματος θα μπορεί να «επιτεθεί» και στο άλλο σύστημα χρησιμοποιώντας διάφορες τεχνικές τύπου «masquerading[17]»

Τα VPNs με IPSec τεχνολογία έχουν ως βάση την ασφάλεια με την χρήση πρωτοκόλλων που βοηθούν στην δημιουργία εικονικών σηράγγων και όχι τειχών προστασίας.

Η IPSec διασφαλίζει την εμπιστευτικότητα, την ακεραιότητα και την αυθεντικότητα των επικοινωνιών δεδομένων σε ένα IP δίκτυο. Η IPSec παρέχει τον απαραίτητο μηχανισμό για την ανάπτυξη ευκίνητων λύσεων ασφάλειας σε ένα δίκτυο.

[17] Πλαστογράφηση δεδομένων/σηματοδοσίας και υπόδηση κόμβων

Η IPSec υλοποιεί κρυπτογράφηση και πιστοποίηση επιπέδου δικτύου, παρέχοντας μια λύση ασφαλείας μέσα στην ίδια την αρχιτεκτονική του δικτύου. Έτσι τα συστήματα και οι εφαρμογές που βρίσκονται στις άκρες δεν χρειάζονται αλλαγές ή ρυθμίσεις για να έχουν το πλεονέκτημα της ισχυρής ασφάλειας. Επειδή τα κρυπτογραφημένα πακέτα μοιάζουν με κανονικά IP πακέτα μπορούν εύκολα να δρομολογηθούν μέσα από οποιοδήποτε IP δίκτυο, όπως το Internet, χωρίς καμία αλλαγή στον ενδιάμεσο δικτυακό εξοπλισμό. Οι μόνες συσκευές οι οποίες γνωρίζουν για την κρυπτογράφηση είναι αυτές στα ακραία σημεία. Αυτό το χαρακτηριστικό μειώνει δραστικά τόσο το κόστος της υλοποίησης όσο και το κόστος της διαχείρισης.

Έλεγχοι κρυπτογράφησης και πιστοποίησης ταυτότητας μπορούν να εφαρμοσθούν σε διάφορα επίπεδα στην δικτυακή υποδομή

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 λειτουργικότητα).
- Να είναι συμβατό με τα υπάρχοντα πρωτόκολλα.

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

Συνήθως οι υλοποιήσεις έχουν μία ξεχωριστή πολιτική για κάθε δικτυακή διασύνδεση (network interface) που έχει ενεργοποιημένο το IPSec η οποία έχει εγγραφές για εισερχόμενη και εξερχόμενη κίνηση. 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 που θα αναφέρει πως θα επεξεργαστεί το πακέτο. Τα πακέτα ταιριάζουν στις πολιτικές με βάση τους selectors[18]. Αν για ένα πακέτο δεν βρεθεί εγγραφή τότε το πακέτο απορρίπτεται και το γεγονός αναφέρεται στο σύστημα.

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.

Το IPSec συνδυάζει ένα ολοκληρωμένο σύστημα το οποίο παρέχει εμπιστευτικότητα , ακεραιότητα και πιστοποίηση της ταυτότητας των IP πακέτων. Το IPSec αναφέρεται σε μια σειρά πρωτοκόλλων όπως ορίζεται στα RFC 2401-2411 και RFC 2451. Αυτά τα πρωτόκολλα χωρίζονται σε δύο κύριες κατηγορίες:

- ***Πρωτόκολλα σχετικά με την ασφάλεια***, τα οποία καθορίζουν την πληροφορία που πρέπει να προστεθεί σε ένα IP πακέτο για να ενεργοποιηθούν οι έλεγχοι εμπιστευτικότητας, ακεραιότητας και πιστοποίησης ταυτότητας. Επίσης καθορίζεται και το πως πρέπει να γίνει η κρυπτογράφηση των δεδομένων του πακέτου.

- ***Πρωτόκολλα σχετικά με την ανταλλαγή κλειδιών***, τα οποία διαπραγματεύονται το συσχετισμό ασφάλειας μεταξύ των δυο υποψήφιων προς επικοινωνίας οντοτήτων

[18] Οι **selectors** είναι πεδία στα πακέτα με βάση τα οποία γίνεται η αντιστοίχηση των πακέτων ορισμένες από την πολιτική της βάσης

Πακέτα IPSec

Η IPSec ορίζει ένα νέο σετ επικεφαλίδων το οποίο προστίθεται στα IP διαγράμματα. Αυτές οι νέες επικεφαλίδες τοποθετούνται μετά την επικεφαλίδα IP και πριν το πρωτόκολλο επιπέδου 4 (τυπικά το TCP ή το UDP[19]). Αυτές οι νέες επικεφαλίδες παρέχουν πληροφορίες για την ασφάλεια του φορτίου των IP πακέτων όπως αναλύεται παρακάτω:

- **Επικεφαλίδα πιστοποίησης ταυτότητας** (AH Authentication Header). Αυτή η επικεφαλίδα όταν προστίθεται σε ένα IP διάγραμμα διασφαλίζει την ακεραιότητα και την ταυτότητα των δεδομένων. Δεν παρέχει ασφάλεια πιστότητας. Η επικεφαλίδα αυτή χρησιμοποιεί μια keyed-hash συνάρτηση αντί ψηφιακών υπογραφών διότι η τεχνολογία ψηφιακών υπογραφών είναι πολύ αργή και θα μείωνε την απόδοση του δικτύου.
- **Φορτίο ασφαλείας ενθυλάκωσης** (ESP Encapsulating Security Payload). Αυτή η επικεφαλίδα όταν προστίθεται σε ένα IP διάγραμμα προστατεύει την ακεραιότητα και την ταυτότητα των δεδομένων. Αν η ESP χρησιμοποιείται για την επικύρωση της ακεραιότητας των δεδομένων δεν περιλαμβάνει τα αμετάβλητα πεδία της IP επικεφαλίδας.

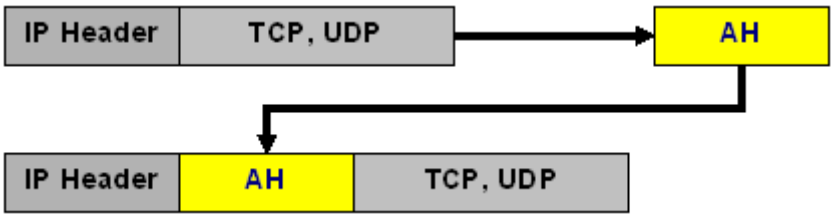
[19] **User Datagram Protocol** (UDP) είναι ένα από τα βασικά πρωτόκολλα που χρησιμοποιούνται στο Διαδίκτυο ανάλογο του TCP

Οι AH και οι ESP μπορούν να χρησιμοποιηθούν ανεξάρτητα ή μαζί, αν και για τις περισσότερες εφαρμογές μια από τις δυο είναι αρκετή. Και για τα δυο αυτά πρωτόκολλα οι IPSec δεν καθορίζει συγκεκριμένους αλγόριθμους που πρέπει να χρησιμοποιηθούν αλλά παρέχει ένα ανοικτό πλαίσιο για βιομηχανική υλοποίηση με παραγωγή ανεξάρτητων αλγορίθμων. Αρχικά οι περισσότερες υλοποιήσεις της IPSec θα περιλαμβάνουν υποστήριξη για το MD5[20] ή για το SHA (Secure Hash Algorithm) όπως ορίζεται από την κυβέρνηση των Η. Π. Α. για την ακεραιότητα και την πιστοποίηση της ταυτότητας. Το DES (Data Encryption Standard) είναι προς το παρόν ο πιο κοινά προσφερόμενος αλγόριθμος κρυπτογράφησης αν και υπάρχουν και άλλοι όπως οι IDEA, Blowfish και RC4.

Η επικεφαλίδα AH

Η επικεφαλίδα αυθεντικοποίησης (AH Authentication Header) 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.

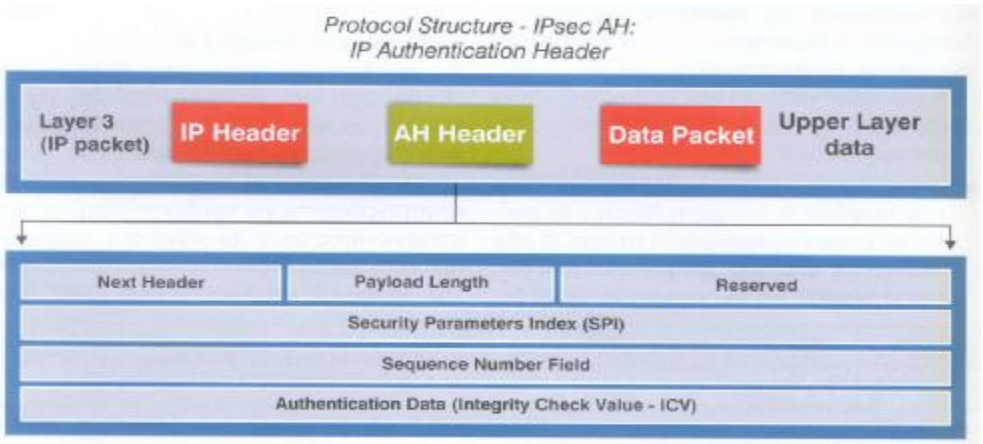
Σε σύγκριση με το ESP το AH δεν παρέχει κρυπτογράφηση των δεδομένων, αλλά προστατεύει τις επικεφαλίδες των πακέτων παρέχοντας αυθεντικοποίηση, κάτι που δεν κάνει από μόνο του το ESP, εκτός αν και αυτά τα πεδία εμπεριέχονται στη κρυπτογράφηση.



Το γεγονός αυτό καθ' αυτό της χρησιμοποίησης ενός κοινού μυστικού κλειδιού που είναι γνωστό και στα δύο μέρη (αποστολέας-δέκτης) εγγυάται την πιστοποίηση της ταυτότητας των συμβαλλομένων.

[20] Διάσημες συναρτήσεις κατατεμαχισμού είναι η MD5 και η SHA

- Πεδίο επόμενης κεφαλίδας (Next Header field), όπου προσδιορίζει ποια είναι η επόμενη κεφαλίδα που είναι παρούσα στο IP πακέτο (π.χ. TCP, UDP κ.ο.κ.)
- Μέγεθος του φορτίου (Payload length)
- Δείκτης παραμέτρων ασφαλείας (Security Parameter Index (SPI)) – προσδιορίζει στον παραλήπτη ποια πρωτόκολλα ασφαλείας χρησιμοποιήθηκαν από τον αποστολέα
- Ακολουθιακός αριθμός (Sequence number): αυξάνεται κατά ένα για κάθε νέο πακέτο που καταφτάνει στον δέκτη από τον ίδιο αποστολέα και με το ίδιο SPI.
- Δεδομένα πιστοποίησης ταυτότητας (Authentication data) – το τμήμα εκείνο που εξασφαλίζει την πιστοποίηση ταυτότητας. Όπως ήδη αναφέρθηκε, είναι το αποτέλεσμα μίας συνάρτησης κατακερματισμού (Integration Check Value – ICV).
- Σε ολόκληρο το IP πακέτο, εκτός από εκείνα τα πεδία (IP header fields) που αλλάζουν κατά τη μεταφορά του όπως παραδείγματος χάριν το πεδίο TTL, που αλλάζει από τους δρομολογητές των διάφορων δικτύων (μειώνεται), κατά μήκος της πορείας που ακολουθεί το IP πακέτο.
- Σε όλο το AH header πλην του πεδίου του “Authentication Data” .
- Σε όλα τα δεδομένα των πάνω στρωμάτων της στοίβας πρωτοκόλλου (δεδομένα του IP πακέτου).



Ένα πακέτο υπόκειται στον AH μόνο όταν το IPSec καθορίσει ότι το πακέτο ταυτίζεται με μια ασφαλή διασύνδεση. Όταν ένα πακέτο που περιέχει ένα AH φτάσει στον προορισμό του, ο δέκτης καθορίζει πολίτικη ασφαλείας βασισμένη στη IP διεύθυνση του προορισμού, στο πρωτόκολλο ασφάλειας (AH) και το SPI. Η πολίτικη ασφαλείας 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.

Αν χρειαστεί κατάτμηση θα γίνει μετά την ολοκλήρωση του AH στο IPSec. Για αυτό στο επίπεδο μεταφοράς το AH εφαρμόζεται μόνο σε ολόκληρα πλαίσια δεδομένων του IP και όχι σε κομμάτια. Ο παραλήπτης υπολογίζει την τιμή ελέγχου γνησιότητας με βάση μερικά χαρακτηριστικά του πακέτου. 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.
- Το 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 32bit 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.

Ο μετρητής του αποστολέα μηδενίζεται όταν δημιουργείται ένα σύνολο πακέτων, 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 σύνολο πακέτων 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 σύνολο πακέτων. 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 σύνολο πακέτων. Αυτό θα πρέπει να γίνεται στην αρχή του ελέγχου για να αποφεύγονται περιττοί έλεγχοι και να επιταχύνεται η όλη διαδικασία. Τα διπλά πακέτα απορρίπτονται.

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 τείχους προστασίας.

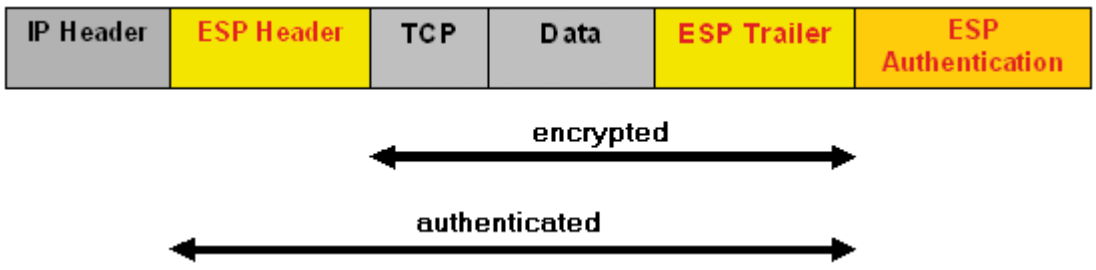
Οι υπηρεσίες ασφάλειας που προσφέρει η επικεφαλίδα ESP είναι:

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

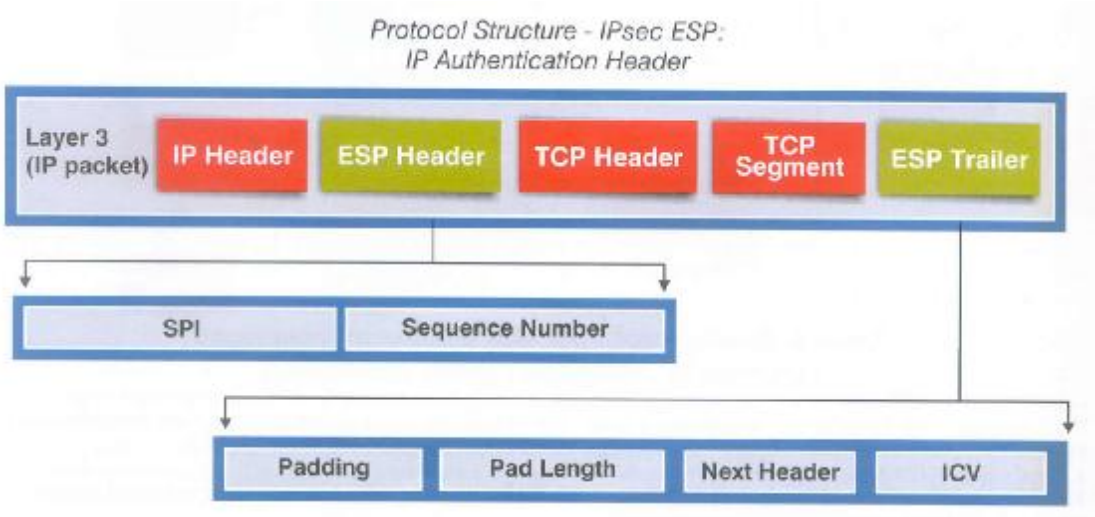
Το ποιες από αυτές τις υπηρεσίες θα χρησιμοποιηθούν κατά την διάρκεια μιας σύνδεσης, εξαρτάται από τις παραμέτρους που θα οριστούν κατά την δημιουργία του **συνδέσμου ασφάλειας** (Security association) για την σύνδεση αυτή. Η εμπιστευτικότητα μπορεί να χρησιμοποιηθεί αυτόνομα. ωστόσο κάτι τέτοιο δεν 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 και είναι αποτελεσματική μόνο αν εφαρμοστεί κατά την επικοινωνία ενός τείχους προστασίας και ενός σταθμού, ή μεταξύ δύο αντιπυρικών ζωνών



Τα πεδία της κεφαλίδας ESP είναι 6 – δύο από αυτά τοποθετούνται πριν το φορτίο του IP πακέτου (ESP Header) και τα υπόλοιπα τέσσερα μετά από αυτό (ESP Trailer). Τα πεδία SPI και Sequence Number του ESP Header έχουν την ίδια λειτουργία όπως στο AH. Το ίδιο ισχύει για τα πεδία Pad Length, Next Header και ICV (το οποίο είναι προαιρετικό) του ESP Trailer. Το πεδίο Συμπλήρωσης (Padding) έχει μέγεθος το πολύ 255 bytes και χρειάζεται για να προσαρμόζεται το μέγεθος του IP πακέτου, ανάλογα με τον αλγόριθμο κρυπτογράφησης που χρησιμοποιείται (αν αναλογιστούμε ότι κάποιοι αλγόριθμοι κρυπτογράφησης απαιτούν τα δεδομένα να



είναι μήκους πολλαπλάσιου κάποιου συγκεκριμένου αριθμού bytes).

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.

Οι βασικές λειτουργίες του πρωτοκόλλου είναι οι εξής:

- **Διαδικασία εύρεσης σε ποιο σύνδεσμο ασφάλειας ανήκει το πακέτο**. Για την διαδικασία αυτή χρησιμοποιείται το πεδίο δείκτη παραμέτρων ασφάλειας (SPI). Για κάθε σύνδεσμο ασφάλειας καθορίζεται (συνήθως από των 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 που έχει αποφασιστεί κατά την δημιουργία του συνδέσμου ασφάλειας. Ως είσοδος σε αυτήν την συνάρτηση 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

IKE (Internet Key Exchange)

Η IPSec μπορεί να θεωρήσει ότι ένας συσχετισμός ασφάλειας υπάρχει αλλά δεν έχει το μηχανισμό να τον δημιουργήσει. Η IETF επέλεξε να σπάσει τη διαδικασία αυτή σε δύο μέρη : η IPSec παρέχει την επεξεργασία των πακέτων επιπέδου IP και το πρωτόκολλο διαχείρισης κλειδιών Internet *(IKMP Internet Key Management Protocol)*, ασχολείται με ότι έχει να κάνει με τους συσχετισμούς ασφάλειας. Μετά από εξέταση πολλών εναλλακτικών λύσεων συμπεριλαμβανομένων και των SKIP (Simple Key Management Protocol) και Photouris, η IETF επέλεξε το IKE σαν το τρόπο ρύθμισης των συσχετισμών ασφάλειας για την IPSec.(το IKE αναλύεται στο κεφάλαιο 5)

3.3.2 SSL VPN

Τα Εικονικά Ιδιωτικά Δίκτυα Επιπέδου 4 (Μεταφοράς) υλοποιούνται μέσω του πρωτοκόλλου SSL (**Secure Sockets Layer**). Το SSL είναι ένα πρωτόκολλο που ανήκει στην κατηγορία αυτή και ολοκληρώνει την ασφάλεια πάνω από το TCP/IP πρωτόκολλο . Το SSL διαχειρίζεται την εμπιστευτικότητα και την ακεραιότητα του καναλιού μετάδοσης (με κατάλληλη κρυπτογράφηση των δεδομένων), καθώς και την αυθεντικοποίηση του εξυπηρετητή, αλλά και του πελάτη όταν αυτό είναι απαραίτητο

Οι υπηρεσίες που παρέχει είναι οι εξής :

- Κρυπτογράφηση δεδομένων
- Αυθεντικοποίηση εξυπηρετητή
- Ακεραιότητα των μηνυμάτων που μεταδίδονται στο διαδίκτυο

Η κρυπτογράφηση γίνεται χωρίς να απαιτείται αλληλεπίδραση με τον χρήστη. Η έκδοση SSL 2.0 υποστηρίζει μόνο αυθεντικοποίηση εξυπηρετητή (server

authentication) , ενώ η έκδοση SSL 3.0 παρέχει επιπλέον αυθεντικοποίηση πελάτη (client authentication). Το πρωτόκολλο SSL χρησιμοποιεί το TCP/IP για την μεταφορά των δεδομένων και είναι ανεξάρτητο από την εφαρμογή που χρησιμοποιείται από τον τελικό χρήστη.

Το πρωτόκολλο SSL χρησιμοποιεί την RSA κρυπτογράφηση δημόσιου κλειδιού για να εξασφαλίσει την ασφαλή μετάδοση. Αυτού του είδους η κρυπτογράφηση χρησιμοποιεί ένα ζεύγος κλειδιών, το δημόσιο και το ιδιωτικό κλειδί για κρυπτογράφηση και αποκρυπτογράφηση. Οποιαδήποτε πληροφορία κρυπτογραφείται με το ένα κλειδί, μπορεί να αποκρυπτογραφηθεί μόνο με το άλλο.

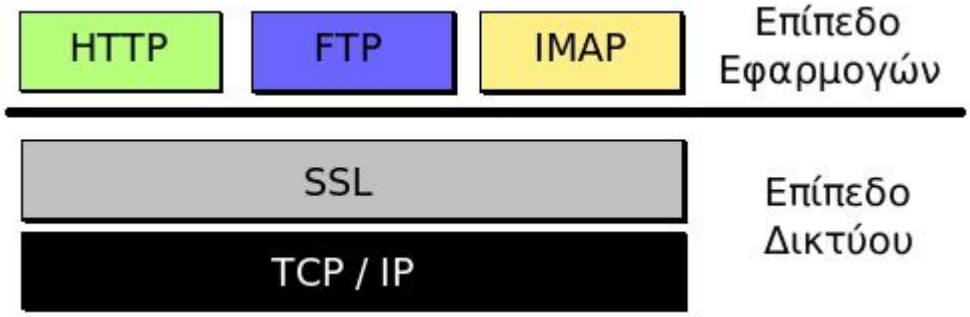
Ένα διαφορετικό κλειδί συνεδρίας (session key) χρησιμοποιείται σε κάθε σύνδεση πελάτη/εξυπηρετητή . Το κλειδί κάθε συνόδου λήγει με την συμπλήρωση 24 ωρών ζωής. Το SSL χρησιμοποιεί τη κρυπτογραφία δημόσιου κλειδιού για την ανταλλαγή αυτού του κλειδιού και για αμοιβαία ταυτοποίηση των συναλλασσόμενων μερών. Για την κρυπτογράφηση της συνόδου χρησιμοποιείται η συμμετρική κρυπτογραφία που είναι σαφώς γρηγορότερη .

Κατά την εφαρμογή του πρωτοκόλλου γίνεται μια ανταλλαγή πληροφοριών ως εξής :

- Ο πελάτης ξεκινά την σύνδεση
- Ο εξυπηρετητής απαντά , στέλνοντας στον πελάτη το digital ID του. Μπορεί να ζητήσει και το digital ID του πελάτη για ταυτοποίηση
- Ο πελάτης επιβεβαιώνει το digital ID του εξυπηρετητή . Αν χρειαστεί στέλνει το δικό του digital ID στον εξυπηρετητή για ταυτοποίηση
- Ολοκληρώνεται η διαδικασία ταυτοποίησης . Ο πελάτης στέλνει το κλειδί συνεδρίας κρυπτογραφημένο με το δημόσιο κλειδί του εξυπηρετητή .
- Εγκαθίσταται ένα ασφαλές κανάλι επικοινωνίας μεταξύ πελάτη και εξυπηρετητή

Η επόμενη έκδοση του SSL ονομάστηκε TLS 1.0 (Transport Layer Security) η οποία περιλαμβάνει βελτιώσεις και επεκτάσεις του πρωτοκόλλου SSL 3.0 .

Το SSL προστατεύει την πιστότητα των δεδομένων που στέλνονται από κάθε εφαρμογή που το χρησιμοποιεί, αλλά δεν προστατεύει τα δεδομένα που αποστέλλονται από άλλες εφαρμογές. Κάθε σύστημα και εφαρμογή πρέπει να είναι προστατεμένη από το SSL για να του παρέχει το τελευταίο την προστασία.



Λειτουργία του SSL

Η ασφαλής σύνδεση που παρέχεται με το πρωτόκολλο SSL επιτυγχάνεται μέσω:

α) της πιστοποίησης της ταυτότητας των πλευρών που επικοινωνούν και

β) της κρυπτογράφησης της κίνησης που πραγματοποιείται μεταξύ τους.

Βάση αυτών το SSL χωρίζεται σε δύο μέρη ή υποπρωτόκολλα , το **SSL Handshake Protocol** (SSLHP) και το **SSL Record Protocol** (SSLRP).

Το SSLHP διαπραγματεύεται τους αλγόριθμους κρυπτογράφησης που θα χρησιμοποιηθούν και πραγματοποιεί την πιστοποίηση της ταυτότητας του server και εάν ζητηθεί και του client. Ενώ το SSLRP συλλέγει τα δεδομένα σε πακέτα και αφού τα κρυπτογραφήσει τα μεταδίδει και αποκρυπτογραφεί τα παραλαμβανόμενα πακέτα.

SSL Record Protocol

Ένα πακέτο SSL αποτελείται από δύο μέρη, την επικεφαλίδα και τα δεδομένα. Η επικεφαλίδα μπορεί να είναι είτε 3 bytes είτε 2 bytes, από τις οποίες περιπτώσεις η δεύτερη χρησιμοποιείται όταν τα δεδομένα χρειάζονται συμπλήρωμα. Το πεδίο escape-bit στην περίπτωση των 3 bytes υπάρχει μόνο σε εκδόσεις μετά το SSL 2.0 και προβλέπεται για ρύθμιση πληροφοριών. Για την επικεφαλίδα των 2 bytes το μέγεθος του πακέτου είναι 32767 bytes, ενώ για την επικεφαλίδα των 3 bytes το μέγεθος είναι 16383 bytes.

Το κομμάτι των δεδομένων αποτελείται από ένα Message Authentication Code (MAC), τα πραγματικά δεδομένα και δεδομένα συμπλήρωσης, εάν χρειάζονται. Αυτό το κομμάτι είναι που κρυπτογραφείται κατά την μετάδοση. Τα συμπληρωματικά δεδομένα απαιτούνται όταν οι αλγόριθμοι κρυπτογράφησης εν

χρήση είναι τύπου block ciphers[21] και ο ρόλος τους είναι να συμπληρώνουν τα πραγματικά δεδομένα ώστε το μέγεθος τους είναι πολλαπλάσιου του μεγέθους που δέχεται σαν είσοδο ο block cipher. Εάν χρησιμοποιούνται stream ciphers[22] τότε δεν απαιτείται συμπλήρωμα και μπορεί αν χρησιμοποιηθεί η επικεφαλίδα των 2 bytes.

Το MAC είναι κρυπτογραφικού αλγορίθμου digest ή hash value των δημοσιών-κρυφών κλειδιών του αποστολέα του πακέτου, των πραγματικών δεδομένων, των συμπληρωματικών δεδομένων και ενός αριθμού ακολουθίας, στην σειρά που δίνονται.

Προβλέπεται και η συμπίεση των δεδομένων με κατάλληλους μηχανισμούς που επιλέγονται κατά το handshake[23], ενώ δεν αποκλείεται να χρειαστεί και τεμαχισμός της πληροφορίας σε πολλά πακέτα.

SSL Handshake Protocol

Το πρωτόκολλο SSL Handshake διαχωρίζεται σε δύο επιμέρους φάσεις: η πρώτη φάση αφορά την επιλογή των αλγόριθμων, την ανταλλαγή ενός πρωτεύοντος κλειδιού και την πιστοποίηση της ταυτότητας του server. Η δεύτερη φάση διαχειρίζεται την πιστοποίηση της ταυτότητας του χρήστη (εάν ζητηθεί) και ολοκληρώνει την διαδικασία του handshaking. Όταν ολοκληρωθούν και οι δύο φάσεις, το στάδιο του handshake τελειώνει και η μεταφορά μεταξύ των δύο άκρων αρχίζει. Όλα τα μηνύματα κατά την διάρκεια του handshaking και μετά στέλνονται σύμφωνα με το SSL Record Protocol.

Το πακέτο των αλγορίθμων κρυπτογράφησης περιλαμβάνει την μέθοδο για την ανταλλαγή των κλειδιών, τον αλγόριθμο κρυπτογράφησης και τον μηχανισμό για την παραγωγή του MAC.

---

[21] Οι **κρυπτογραφικοί αλγόριθμοι δέσμης (block ciphers)** τεμαχίζουν σε τμήματα (blocks) το αρχικό κείμενο που πρόκειται να κρυπτογραφηθεί και κρυπτογραφούν κάθε τμήμα ξεχωριστά. Συνηθισμένα μεγέθη ενός τμήματος δεδομένων είναι τα 64 ή 128 bits. Η κρυπτογράφηση κάθε ενός τμήματος γίνεται χρησιμοποιώντας μία μαθηματική συνάρτηση κρυπτογράφησης και το μυστικό κλειδί. Το αποτέλεσμα της διαδικασίας κρυπτογράφησης είναι η παραγωγή ενός κρυπτογραφημένου τμήματος το οποίο στην πλειοψηφία των περιπτώσεων έχει το ίδιο μήκος με το αντίστοιχο τμήμα του αρχικού κειμένου.

[22] Οι **κρυπτογραφικοί αλγόριθμοι ροής (stream ciphers)** χρησιμοποιούνται για την κρυπτογράφηση μίας συνεχούς ροής δεδομένων (data stream). Για την κρυπτογράφηση επιλέγεται αρχικά μία *γεννήτρια κλειδοροής (keystream generator)*, η οποία δέχεται ως είσοδο το μυστικό κλειδί και παράγει στην έξοδό της μία ψευδοτυχαία ακολουθία bits, η οποία ονομάζεται κλειδοροή (keystream). Στην συνέχεια εφαρμόζεται η συνάρτηση XOR ανάμεσα στο αρχικό κείμενο και στην κλειδοροή και το αποτέλεσμα της συνάρτησης είναι η τελική κρυπτογραφημένη ροή δεδομένων.

[23] Κάθε σύνδεση SSL ξεκινά πάντα με την ανταλλαγή μηνυμάτων από τον server και τον client έως ότου επιτευχθεί η ασφαλής σύνδεση, πράγμα που ονομάζεται χειραψία (handshake).

Τα βήματα της διαδικασίας SSL Handshake είναι τα ακόλουθα:

Βήμα 1: Ο SSL client συνδέεται με τον SSL server και ζητά να τον πιστοποιήσει. Επίσης ο client ενημερώνει για το ποιους αλγορίθμους κρυπτογράφησης υποστηρίζει. Ο server από την πλευρά του επιβεβαιώνει το αν μπορεί να υποστηρίξει τους αλγορίθμους αυτούς, ενώ επίσης αποδίδει και έναν μοναδικό αριθμό (connection id) στη σύνδεση που έχει δημιουργηθεί.

Βήμα 2: Ο server αποδεικνύει την ταυτότητά του με την αποστολή του ψηφιακού του πιστοποιητικού. Τα πιστοποιητικά επαληθεύονται με τον έλεγχο των ημερομηνιών εγκυρότητας, καθώς και από το γεγονός ότι το πιστοποιητικό φέρει την υπογραφή μίας διαπιστευμένης αρχής πιστοποιητικού. Υπάρχει η δυνατότητα, προαιρετικά, ο server να ζητήσει πιστοποίηση ταυτότητας από τον client.

Βήμα 3: Εάν ο server έχει ζητήσει πιστοποιητικό γνησιότητας από τον client, αυτός το αποστέλλει. Επίσης πραγματοποιείται η διαπραγμάτευση για τον αλγόριθμο κρυπτογράφησης μηνύματος, καθώς και για τη συνάρτηση κατακερματισμού. Συνήθως ο server επιλέγει την πιο ισχυρή κρυπτογραφική μέθοδο από αυτές που του πρότεινε ο client. Ταυτόχρονα, ο client και ο server παράγουν τα κλειδιά συνόδου σύμφωνα με τα ακόλουθα βήματα:

α) Ο client παράγει έναν τυχαίο αριθμό τον οποίο στέλνει στο server, κρυπτογραφημένο με το δημόσιο κλειδί του server (που έχει αποκτηθεί από το πιστοποιητικό του server).

β) Ο server απαντά με περισσότερα τυχαία δεδομένα (κρυπτογραφημένα με το δημόσιο κλειδί του client, αν είναι διαθέσιμο. Αλλιώς, στέλνει τα δεδομένα μη κρυπτογραφημένα - clear text).

γ) Τα κλειδιά κρυπτογράφησης παράγονται από όλα αυτά τα τυχαία δεδομένα με τη χρήση των συναρτήσεων κατακερματισμού.

Βήμα 4: Ανταλλάσσονται μηνύματα τερματισμού των διαδικασιών του Handshake Protocol.

Σήμερα, το πρωτόκολλο SSL είναι το πιο διαδεδομένο πρωτόκολλο ασφάλειας για το Internet. Μειονέκτημα της χρήσης του αποτελεί το γεγονός ότι επιβραδύνεται η επικοινωνία του browser του client με τον HTTPS server. Η καθυστέρηση οφείλεται στις λειτουργίες κρυπτογράφησης και αποκρυπτογράφησης με ασύμμετρο κρυπτοσύστημα κατά την αρχικοποίησης της SSL συνόδου. Πρακτικά, οι χρήστες αντιλαμβάνονται μικρή καθυστέρηση λίγων δευτερολέπτων μεταξύ της έναρξης σύνδεσης με το HTTPS εξυπηρετητή και της ανάκτησης της πρώτης HTML σελίδας από αυτόν. Επειδή κατά τη σχεδίαση του SSL αποθηκεύεται το κύριο μυστικό κλειδί, η καθυστέρηση επηρεάζει μόνον την πρώτη SSL επικοινωνία μεταξύ browser και HTTPS server. Συγκριτικά με την εγκατάσταση συνόδου, ο επιπλέον φόρτος από τη λειτουργία αλγορίθμων όπως οι DES, RC2, RC4, είναι πρακτικά ασήμαντος.

3.3.3 Τεχνολογία MPLS

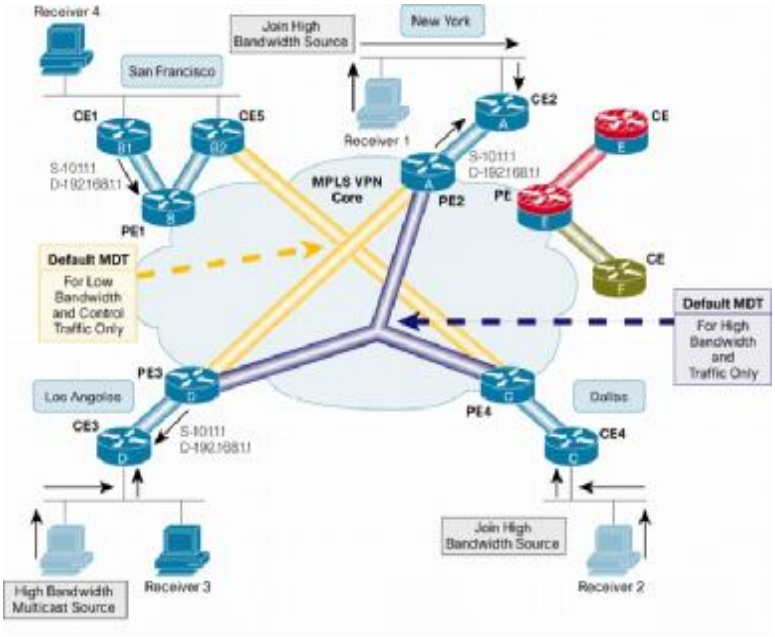
Η TCP/IP ακολουθία πρωτοκόλλων (και ειδικότερα το IP πρωτόκολλο) αποτελεί τη βάση για πολλά δημόσια και ιδιωτικά δίκτυα δεδομένων. Η ενοποίηση των δικτύων φωνής, δεδομένων και πολυμέσων βασίζεται κυρίως σε IP-based πρωτόκολλα, οδηγώντας έτσι στην ανάγκη για τεχνικές και λειτουργικές βελτιώσεις. Η τεχνολογία μεταγωγής ετικέτας (Label Switching) είναι μία από τις απαντήσεις που δίνουν οι εταιρείες σε αυτήν την πρόκληση.

Έτσι, το MPLS είναι μια τεχνολογία που αρχικά προτάθηκε σαν ένα μέσο για τη βελτίωση της ταχύτητας προώθησης και της απόδοσης των IP (Internet Protocol) δρομολογητών, και τώρα αναδύεται σαν μια τεχνολογία κρίσιμης σημασίας για IP δίκτυα μεγάλης κλίμακας. Το MPLS έχει τις ρίζες του στην εκρηκτική εξάπλωση της κυκλοφορίας που παράγεται από το Internet. Η αύξηση του πλήθους των χρηστών και η κλιμάκωση των απαιτήσεων σε εύρος ζώνης οδήγησαν σε μεγάλη ζήτηση στα δίκτυα. Καθώς δημιουργούν IP δίκτυα, οι Service Providers αναζητούν ένα μέσο για να βελτιστοποιήσουν τις επενδύσεις του δικτύου κορμού, στοχεύοντας ταυτόχρονα στην αποτελεσματική διαχείριση του διαθέσιμου εύρους ζώνης, στην παροχή ποιότητας υπηρεσίας, και στην ύπαρξη δυνατότητας καθορισμού του τρόπου με τον οποίο η κυκλοφορία ταξιδεύει μέσα σε ένα δίκτυο με στόχο τη διαχείριση του δικτύου έτσι ώστε να χρησιμοποιούνται αποδοτικά όλοι οι δικτυακοί σύνδεσμοι και να επιτυγχάνεται η όσο το δυνατόν καλύτερη απόδοση. Ωστόσο, τα παραδοσιακά δίκτυα IP δρομολόγησης στερούνται των παραπάνω δυνατοτήτων.

Παρόλα αυτά, η IP δρομολόγηση έχει άλλα πλεονεκτήματα που αντιπαραβάλλονται στα παραπάνω ή και τα συμπληρώνουν. Η IP δρομολόγηση χρησιμοποιεί ευέλικτα, γρήγορης σύγκλισης, αυτόματα πρωτόκολλα δρομολόγησης τα οποία παρέχουν ευελιξία και ένα δυναμισμό αυτοανάρρωσης στη διαχείριση της τοπολογίας. Τα πλεονεκτήματα αυτά συμβαδίζουν με την ταχεία εξάπλωση του Internet, όπου χιλιάδες νέοι hosts προστίθενται επί καθημερινής βάσης.

Μια πρώτη πρόταση για την υποστήριξη των παραπάνω δυνατοτήτων από IP δίκτυα ήταν η δημιουργία IP δικτύων πάνω από τα δίκτυα δευτέρου επιπέδου. Τα δίκτυα δευτέρου επιπέδου, όπως το ATM, χαρακτηρίζονται από προβλέψιμα μονοπάτια και παροχή ποιότητας υπηρεσίας. Ωστόσο, παρουσιάζουν ένα πλήθος μειονεκτημάτων δύο από τα σημαντικότερα είναι τα εξής:

- Η διαχείριση της ATM τοπολογίας είναι πολύπλοκη. Για τη δημιουργία σύνδεσης μεταξύ πολλαπλών τοποθεσιών, απαιτείται η σαφής σχεδίαση ενός πλέγματος συνδέσμων.
- Η διαχείριση δύο ξεχωριστών δικτύων δημιουργεί ένα μεγαλύτερο λειτουργικό φορτίο.



Για την ικανοποίηση των παραπάνω αναγκών χωρίς τα μειονεκτήματα των IP/ATM δικτύων, αρκετές εταιρείες έχουν κάνει προτάσεις για συνδυασμό της IP δρομολόγησης και της ATM μεταγωγής. Τελικά, η IETF (Internet Engineering Task Force) ανέπτυξε μια βασική (standards-based) αρχιτεκτονική και ένα σύνολο πρωτοκόλλων με όνομα MPLS.

Το MPLS δεν ελέγχεται από τις εφαρμογές και δεν έχει κανένα στοιχείο πρωτοκόλλου τελικού χρήστη . Σε αντίθεση με τα άλλα πρωτόκολλα, το MPLS ανήκει μόνο στους δρομολογητές. Επιπλέον, το MPLS είναι ανεξάρτητο από τα πρωτόκολλα (multi-protocol), κι έτσι μπορεί να χρησιμοποιηθεί και με άλλα δικτυακά πρωτόκολλα εκτός από το IP (ATM, PPP, Frame-Relay, Ethernet και token ring) ή ακόμα και πάνω από το επίπεδο σύνδεσης δεδομένων. Συνδυάζει τη τεχνολογία μεταγωγής δευτέρου επιπέδου με τις δικτυακές υπηρεσίες τρίτου επιπέδου, ενώ παράλληλα μειώνει την πολυπλοκότητα και τα λειτουργικά κόστη.

Αποτελεί μια τεχνολογία κλειδί για τα δίκτυα κορμού. Δίνει στους παροχείς υπηρεσιών τη δυνατότητα να προσφέρουν διαφοροποιημένες IP υπηρεσίες από άκρη

σε άκρη απαιτώντας ταυτόχρονα απλούστερη διαμόρφωση και διαχείριση τόσο για τους παροχείς υπηρεσιών όσο και για τους πελάτες. Το MPLS δεν αντικαθιστά την IP δρομολόγηση, αλλά μπορεί να λειτουργήσει παράλληλα με υπάρχουσες και μελλοντικές τεχνολογίες δρομολόγησης με στόχο την προώθηση δεδομένων με υψηλή ταχύτητα και τη δέσμευση του εύρους ζώνης για ροές κυκλοφορίας με διαφορετικές απαιτήσεις.

Η σημασία του MPLS έγκειται στο γεγονός ότι δίνει στα σύγχρονα δίκτυα τη δυνατότητα να αντιμετωπίσουν τις μεγάλες προκλήσεις που συναντούν στα ακόλουθα πεδία:

- Λειτουργικότητα: Παράδειγμα αποτελεί η ρητή δρομολόγηση (explicit routing)
- Κλιμάκωση (Scalability)
- Εξέλιξη: Δυνατότητα αλλαγής και επέκτασης των δικτύων αποφεύγοντας τη μεγάλη αποδιοργάνωση ή διακοπή τους.
- Ολοκλήρωση

Υπάρχει ένα πλήθος απαιτήσεων που θα πρέπει να ικανοποιούνται έτσι ώστε το MPLS να λειτουργεί αποδοτικά και να επιφέρει τα επιθυμητά οφέλη:

- Οι MPLS τεχνολογίες κορμού πρέπει να είναι συμβατές με μια ευρεία σειρά πρωτοκόλλων δρομολόγησης, και να μπορούν να λειτουργούν ανεξάρτητα από υποκείμενα πρωτόκολλα δρομολόγησης.
- Το MPLS πρέπει να παρέχει μηχανισμούς πρωτοκόλλων που είτε να μπορούν να εμποδίσουν το σχηματισμό των βρόχων και/ή να περιέχουν την ποσότητα των δικτυακών πόρων που απαιτείται λόγω της παρουσίας των βρόχων.
- Η MPLS προώθηση πρέπει να επιτρέπει ‘προώθηση συνόλων’ (aggregate forwarding) των δεδομένων του χρήστη. Δηλαδή, πρέπει να επιτρέπει τη μεταφορά πολλαπλών ροών δεδομένων σα μια μονάδα και να εξασφαλίζει ότι το συγκεκριμένο σύνολο ροών θα ακολουθεί ένα μόνο μονοπάτι..
- Το MPLS πρέπει να υποστηρίζει διαχείριση και διατήρηση τουλάχιστον των δυνατοτήτων και των λειτουργιών που υποστηρίζονται στα τυπικά IP δίκτυα. Τα σύγχρονα εργαλεία δικτυακής διαχείρισης και διάγνωσης πρέπει να συνεχίσουν να λειτουργούν έτσι ώστε να παρέχεται κάποια συμβατότητα.

- Οι MPLS τεχνολογίες κορμού πρέπει να μπορούν να λειτουργούν με unicast και multicast ροές. Κατά τον καθορισμό του MPLS πρέπει να μελετηθούν και να αναλυθούν θέματα σχετικά με την κλιμάκωση (scalability).
- Οι MPLS τεχνολογίες πρέπει να μπορούν να λειτουργούν με ροές για να μεταφέρουν όλη την best-effort κυκλοφορία, όπου n είναι το πλήθος των κόμβων ενός MPLS τομέα. Τα MPLS πρωτόκολλα πρέπει να έχουν τη δυνατότητα να εκμεταλλεύονται το hardware που υποστηρίζει συνένωση των ροών όπου κρίνεται κατάλληλο.
- Τα πρότυπα του MPLS, καθώς και τα Internet πρότυπα, πρέπει να είναι μια αυτόνομη λύση που δεν πρέπει να απαιτεί ειδικά hardware χαρακτηριστικά που δεν υπάρχουν στον εξοπλισμό ενός. Ωστόσο, η λύση μπορεί να χρησιμοποιήσει ορισμένα επιπρόσθετα hardware χαρακτηριστικά επιλογής (π.χ., για τη βελτιστοποίηση της απόδοσης).
- Το MPLS πρέπει να είναι συμβατό με το μοντέλο των Ολοκληρωμένων Υπηρεσιών (Integrated Services), συμπεριλαμβανομένου και του RSVP (Resource Reser Vation Protocol).
- Τα MPLS switches θα πρέπει να είναι δυνατό να συνυπάρχουν με non-MPLS switches στο ίδιο δίκτυο, χωρίς να τους προσθέτουν απαίτηση για επιπλέον διαμόρφωση.
- Το MPLS πρέπει να μπορεί να χρησιμοποιηθεί στο ίδιο δίκτυο στο οποίο λειτουργούν ταυτόχρονα πρωτόκολλα επιπέδου διασύνδεσης δεδομένων.
- Το MPLS πρέπει να υποστηρίζει ανάθεση των ετικετών τόσο βάση της τοπολογίας όσο και βάση της κυκλοφορίας και των αιτήσεων.

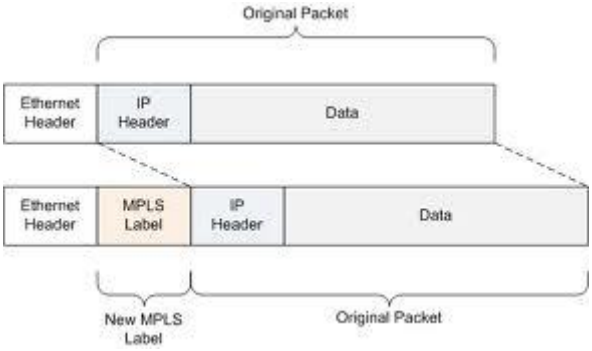
MPLS Πρωτόκολλο

Το MPLS (**Multiprotocol Label Switching**) είναι ένα πρωτόκολλο το οποίο δημιουργήθηκε από την IETF με στόχο να αυξήσει την ευελιξία και την απόδοση του παραδοσιακού IP και ταυτόχρονα να δώσει την δυνατότητα για την παροχή νέων υπηρεσιών στο Διαδίκτυο. Το MPLS συνδυάζει την μεταγωγή με ετικέτα (label) και την παραδοσιακή δρομολόγηση του πρωτοκόλλου IP. Η τεχνική αυτή χρησιμοποιεί, εν γένει, ‘ετικέτες’ που κατασκευάζονται και τοποθετούνται κατά την εισαγωγή των πακέτων στο Δίκτυο Μεταγωγής / Κορμού, για την προώθηση τους στον τελικό

προορισμό. Οι ετικέτες υποδεικνύουν τόσο τη δρομολόγηση των πακέτων όσο και τα χαρακτηριστικά ποιότητας των υπηρεσιών που παρέχονται από το δίκτυο.

Τα κύρια συστατικά της τεχνολογίας MPLS είναι τα εξής:

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



Ενθυλάκωση MPLS Ετικέτας

Δρομολογητής ετικέτας (Label Switch Router (LSR)): Αποτελεί την συσκευή κορμού του δικτύου που μετάγει πακέτα εφοδιασμένα με την κατάλληλη ετικέτα, σύμφωνα με τους προϋπολογισμένους πίνακες μεταγωγής.

Δρομολογητής ετικέτας άκρου (Edge Label Switch Router (Edge LSR)): Είναι η συσκευή που τοποθετείται στο άκρο του κυρίως δικτύου, η οποία εκτελεί την αρχική επεξεργασία και κατηγοριοποίηση του κάθε πακέτου και του αναθέτει την πρώτη ετικέτα.

Μονοπάτι ετικέτας (Label Switched Path (LSP)): Είναι το "μονοπάτι" που ορίζεται από τις ετικέτες που δημιουργούνται και ανατίθενται στο κάθε πακέτο, μεταξύ των τελικών σημείων του δικτύου. Ένα LSP μπορεί να είναι ορισμένο είτε στατικά είτε δυναμικά. Το τελευταίο προσδιορίζεται αυτόματα χρησιμοποιώντας πληροφορίες δρομολόγησης. Τα στατικά LSPs χρησιμοποιούνται σπανιότερα.

Πρωτόκολλο διανομής ετικετών (Label Distribution Protocol (LDP)): Είναι το πρωτόκολλο που έχει σαν ρόλο την απόδοση ετικετών στα πακέτα, καθώς και τη μετάφραση των πληροφοριών τους από τους LSRs. Αναθέτει ετικέτες στα πακέτα από τις δικτυακές συσκευές στις άκρες και στον πυρήνα του δικτύου, έτσι

ώστε να καθοριστούν τα αναγκαία LSPs. Η απόδοση των ετικετών γίνεται σε συνδυασμό με κάποια πρωτόκολλα δρομολόγησης, όπως τα Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS), Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP) ή Border Gateway Protocol (BGP).

Ο ρόλος του Edge LSR

Ο edge LSR διαδραματίζει έναν από τους σημαντικότερους ρόλους στη λειτουργία του MPLS. Αποτελεί ευθύνη του edge LSR να κατηγοριοποιεί την κυκλοφορία και να τοποθετεί και να αφαιρεί ετικέτες σε/από τα πακέτα. Όπως προαναφέρθηκε, οι ετικέτες μπορεί να ανατίθενται βάση και άλλων παραγόντων εκτός από τη διεύθυνση προορισμού. Ο edge LSR καθορίζει αν η κυκλοφορία είναι μια ροή μεγάλης διάρκειας, υλοποιεί πολιτικές διαχείρισης και ελέγχους πρόσβασης, και συναθροίζει την κυκλοφορία σε μεγαλύτερες ροές όταν αυτό είναι δυνατό. Όλες αυτές είναι λειτουργίες που πρέπει να πραγματοποιούνται στο όριο μεταξύ των IP και MPLS «κόσμων». Έτσι, οι δυνατότητες των edge LSRs αποτελούν το κλειδί για την επιτυχία ενός περιβάλλοντος μεταγωγής ετικέτας, καθώς και ένα σημείο ελέγχου και διαχείρισης για τον παροχέα υπηρεσιών.

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.

Λειτουργία LSR

Για την ανταλλαγή των labels μεταξύ των LSRs αναπτύχθηκε ένα νέο πρωτόκολλο γνωστό ως LDP (Label Distribution Protocol). Το LDP εφαρμόζεται μεταξύ δύο διαδοχικών LSRs 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 Α σε ένα κόμβο Β όπου έχει γίνει δέσμευση μιας ετικέτας Ε ο Α καλείται Upstream και ο Β Downstream κόμβος.

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 ο ίδιος θα τα προωθεί.

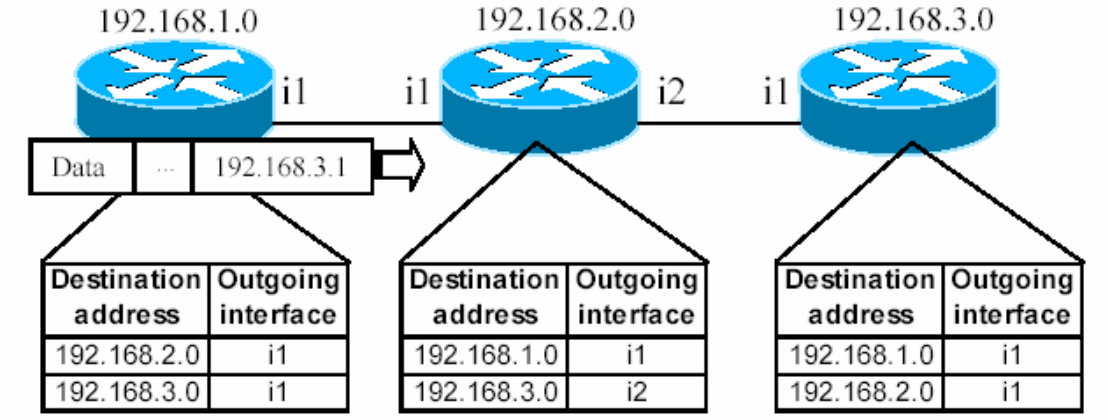
Οι LSRs έχουν δύο σημαντικές διαφορές από τους παραδοσιακούς δρομολογητές. Πρώτον η πληροφορία που ανταλλάσσουν μεταξύ τους δεν αφορά μόνο την δρομολόγηση αλλά επιπλέον και πληροφορία σχετικά με τον τρόπο προώθησης των πακέτων (δηλαδή τα labels). Δεύτερον, ενώ οι παραδοσιακοί δρομολογητές εφαρμόζουν 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.

Προώθηση MPLS Πακέτων

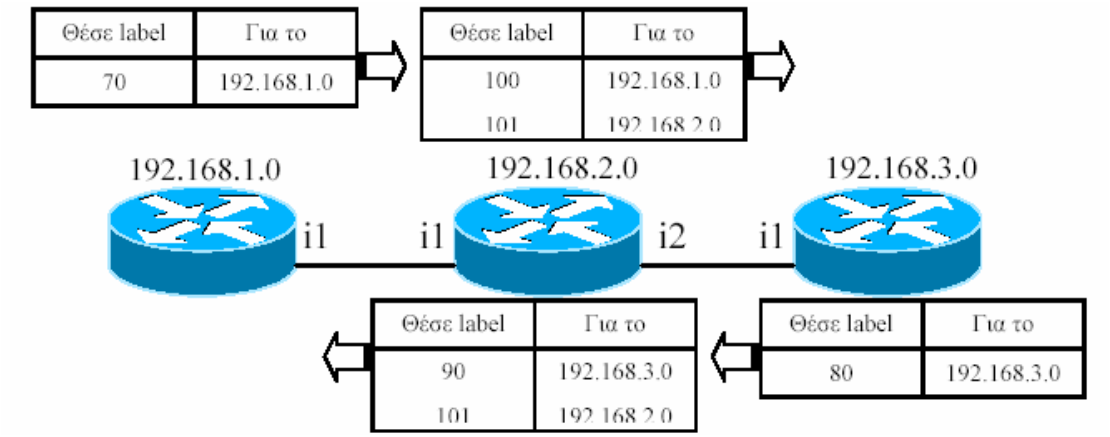
Η διαδικασία προώθησης σε ένα δίκτυο MPLS χωρίζεται σε δύο μέρη. Στο πρώτο μέρος εκτελούνται τα παραδοσιακά πρωτόκολλα δρομολόγησης και δημιουργούνται οι γνωστοί πίνακες δρομολόγησης. Στην συνέχεια, οι LSRs για κάθε εγγραφή του πίνακα δρομολόγησης επικοινωνούν με τους γειτονικούς τους κόμβους (σύμφωνα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



Η δρομολόγηση στους παραδοσιακούς IP δρομολογητές

Σύμφωνα με τον παραδοσιακό τρόπο δρομολόγησης , 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.

Στην ακόλουθη εικόνα, 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.



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**). Στην ακόλουθη εικόνα 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

Local tag	Outgoing tag	Prefix	Outgoing interface
100	70	192.168.1.0/24	i1
90	80	192.168.3.0/24	i2
101		192.168.2.0/24	

Local tag	Outgoing tag	Prefix	Outgoing interface
	90	192.168.3.0/24	i1
	101	192.168.2.0/24	i1
70		192.168.1.0/24	

Local tag	Outgoing tag	Prefix	Outgoing interface
	100	192.168.1.0/24	i1
	101	192.168.2.0/24	i1
80		192.168.3.0/24	

Η λειτουργία προώθησης στο MPLS

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 προκείμενη 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.

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 πάνω σε 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.

L3 MPLS VPNs

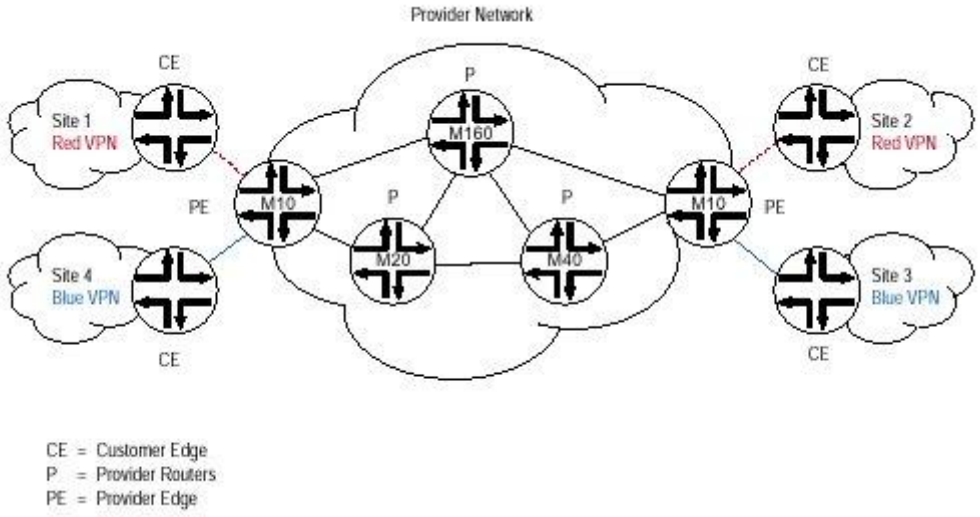
Τα Εικονικά Ιδιωτικά Δίκτυα Επιπέδου Δικτύου που βασίζονται στην τεχνολογία **MPLS** (L3 MPLS VPNs) επιτρέπουν τη δημιουργία VPNs κάνοντας χρήση του δικτύου κορμού MPLS του ISP. Τα VPNs αυτά είναι σε επίπεδο IP και επομένως η μεταφορά της πληροφορίας γίνεται με τη χρήση αποκλειστικά του πρωτοκόλλου IP.

Τρία διαφορετικά είδη δρομολογητών συναντάμε στα MPLS VPNs:

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

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

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



Οι PE δρομολογητές διαμοιράζονται τις πληροφορίες δρομολόγησης και ενημερώνουν τους πίνακες δρομολόγησης που ανήκουν σε κάθε VPN. Οι P δρομολογητές δε συμμετέχουν στην δρομολόγηση της κυκλοφορίας του πελάτη, αλλά πραγματοποιούν την προώθηση για τα MPLS LSPs που μεταφέρουν αυτήν την κυκλοφορία. Οι P δρομολογητές χρησιμοποιούν, ωστόσο, ένα IGP για τη διατήρηση των πινάκων δρομολόγησης του παροχέα.

Ένα MPLS VPN σχηματίζεται όταν ο παροχέας συσχετίζει τους ατομικούς πίνακες δρομολόγησης στους PE δρομολογητές με τα MPLS LSPs που οδηγούν από εκείνον το PE δρομολογητή σε άλλους PE δρομολογητές που παρέχουν υπηρεσία σε άλλους CE δρομολογητές στο ίδιο VPN. Ένας μόνο PE δρομολογητής μπορεί να εξυπηρετήσει πολλούς διαφορετικούς CE δρομολογητές και αντίστοιχα πολλά VPNs.

Ο παροχέας, και όχι ο πελάτης, συσχετίζει ένα συγκεκριμένο VPN με κάθε interface όταν παρέχεται το VPN. Εντός του δικτύου του παροχέα, οι RDs συσχετίζονται με κάθε πακέτο, κι έτσι το VPN δεν μπορεί να χρησιμοποιηθεί από τρίτους προσπαθώντας να ξεγελάσουν μια ροή ή ένα πακέτο. Οι χρήστες μπορούν να συμμετάσχουν σε ένα Intranet ή Extranet μόνο αν ανήκουν στο σωστό φυσικό port και έχουν τον κατάλληλο RD. Αυτή η ιδιότητα καθιστά την είσοδο στα MPLS VPNs θεωρητικά αδύνατη, και παρέχει στους χρήστες τα ίδια επίπεδα ασφάλειας με μια Frame Relay, μισθωμένης γραμμής ή ATM υπηρεσία.

Οι VPN-IP πίνακες προώθησης περιέχουν ετικέτες που αντιστοιχούν σε IP διευθύνσεις. Αυτές οι ετικέτες δρομολογούν την κυκλοφορία σε κάθε τοποθεσία ενός VPN. Αφού χρησιμοποιούνται οι ετικέτες αντί για τις IP διευθύνσεις, οι πελάτες μπορούν να διατηρήσουν τα σχήματα των ιδιωτικών τους διευθύνσεων, χωρίς να

απαιτείται μετάφραση της δικτυακής διεύθυνσης για να μεταδοθεί η κυκλοφορία μέσω του δικτύου του παροχέα. Η κυκλοφορία διαχωρίζεται ανάμεσα στα VPNs χρησιμοποιώντας ένα λογικά ξεχωριστό πίνακα προώθησης για κάθε VPN. Βάσει του εισερχόμενου interface, το switch επιλέγει ένα συγκεκριμένο πίνακα προώθησης, ο οποίος περιέχει μόνο έγκυρους προορισμούς στο VPN. Για τη δημιουργία Extranets, ένας παροχέας διαμορφώνει ρητά την επικοινωνία μεταξύ των VPNs.

Σύμφωνα με αυτήν την προσέγγιση οι παροχείς μπορούν να χρησιμοποιούν την ίδια υποδομή για την υποστήριξη πολλών VPNs, χωρίς να απαιτείται να δημιουργήσουν ξεχωριστά δίκτυα για κάθε πελάτη. Επιπλέον, αυτή η λύση υποστηρίζει IP VPN δυνατότητες μέσα στο ίδιο το δίκτυο, κι έτσι οι παροχείς μπορούν να διαμορφώσουν ένα δίκτυο για όλους τους συνδρομητές το οποίο θα παρέχει ιδιωτικές IP δικτυακές υπηρεσίες, όπως Intranets και Extranets, χωρίς πολύπλοκη διαχείριση, σήραγγες ή VC πλέγματα.

Τα IP VPN δίκτυα που βασίζονται στο MPLS είναι πιο εύκολο να ενοποιηθούν με τα δίκτυα των πελατών που βασίζονται σε IP. Οι συνδρομητές μπορούν να διασυνδεθούν με την υπηρεσία ενός παροχέα χωρίς να μεταβάλλουν τις Internet εφαρμογές τους, διότι αυτά τα δίκτυα έχουν μια έμφυτη ενημερότητα σχετικά με τις εφαρμογές, για παροχή μυστικότητας και ποιότητας υπηρεσίας.

Ολοένα και περισσότερες εταιρίες ζητούν διασύνδεση των εταιρικών παραρτημάτων τους, χρησιμοποιώντας την υποδομή που ήδη διαθέτουν (π.χ. Frame Relay switches, ATM switches, Ethernet switches). Από την άλλη πλευρά υπάρχει ο ISP επιθυμεί να διατηρεί ένα δίκτυο κορμού με ενιαία αρχιτεκτονική και όχι να είναι ένα συνονθύλευμα από διαφορετικές τεχνολογίες. Σε αυτήν την περίπτωση η τεχνολογία MPLS είναι άκρως δελεαστική. Έτσι «γεννήθηκαν» τα L2 MPLS VPNs.

L2 MPLS VPN

Η δυνατότητα δημιουργίας Layer 2 MPLS VPNs βασίζεται στην δυνατότητα ενθυλάκωσης (encapsulation) και μεταφοράς (transport) των **protocol data units** PDUs, για διάφορα πρωτόκολλα του επιπέδου 2, πάνω από ένα MPLS δίκτυο. Μέχρι σχετικά πρόσφατα δεν υπήρχε σχετική προτυποποίηση, αλλά σήμερα γίνεται προσπάθεια δημιουργίας κάποιων κανόνων. Η σχετική διαδικασία είναι σε εξέλιξη, αλλά ήδη έχουν παραχθεί κάποιες προτάσεις με μορφή Internet drafts (draft kompella, draft martini).

Η ενθυλάκωση πλαισίων του επιπέδου 2 για μετάδοση πάνω από IP και MPLS δίκτυα επιτυγχάνεται με τη μέθοδο της εξομοίωσης εικονικών κυκλωμάτων για τη μετάδοση των PDUs των πρωτοκόλλων του επιπέδου 2, κατά μήκος ενός IP/MPLS δικτύου.

Ένα σύνολο από τέτοια εικονικά κυκλώματα μπορούν να μεταφερθούν μέσα από μια σήραγγα . Για να επιτευχθεί αυτό θα πρέπει οι PDUs των πρωτοκόλλων του επιπέδου 2 να ενθυλακωθούν. Διακρίνονται τρία επίπεδα ενθυλάκωσης:

- Η επικεφαλίδα του tunnel (header), που περιέχει τις πληροφορίες που απαιτούνται για τη μετάδοση της PDU πάνω από το IP ή το MPLS δίκτυο. Αυτή η επικεφαλίδα καθορίζεται από το πρωτόκολλο που χρησιμοποιείται για το μηχανισμό των σηράγγων, π.χ. MPLS, GRE, L2TP κ.λπ.
- Το πεδίο αποπολυπλεξίας (demultiplexer field), που χρησιμοποιείται για τον διαχωρισμό των ξεχωριστών εξομοιούμενων εικονικών κυκλωμάτων μέσα σε ένα τούνελ. Το πεδίο αυτό πρέπει, επίσης, να γίνεται κατανοητό από το πρωτόκολλο που χρησιμοποιείται για το μηχανισμό των τούνελ, π.χ. μπορεί να είναι μία MPLS ετικέτα (MPLS label), ένα πεδίο-κλειδί του GRE (GRE key field) κ.λπ.
- Η ενθυλάκωση του εξομοιούμενου εικονικού κυκλώματος (emulated VC encapsulation), που περιέχει πληροφορία για την ενθυλακωμένη PDU και η οποία είναι απαραίτητη για την σωστή εξομοίωση του αντίστοιχου πρωτοκόλλου του επιπέδου 2. Αν και τα διάφορα πρωτόκολλα του επιπέδου 2 απαιτούν την τοποθέτηση διαφορετικής πληροφορίας σε αυτή τη θέση, η προτεινόμενη προτυποποίηση κάνει την ενθυλάκωση όσο πιο κοινή γίνεται. Για το λόγο αυτό η πληροφορία χωρίζεται σε δύο τμήματα:
    - τη λέξη ελέγχου (control word) που έχει κοινή δομή για κάθε πρωτόκολλο
    - επιπέδου 2 που υποστηρίζεται και πληροφορία που διαφοροποιείται ανάλογα με το πρωτόκολλο (protocol specific)

Η είσοδος της εκάστοτε PDU στο IP/MPLS δίκτυο και η ενθυλάκωσή της γίνεται στον ingress router. Η ενθυλακωμένη PDU μεταδίδεται πάνω από το δίκτυο και μέχρι τον egress router. Εκεί αφαιρούνται οι πληροφορίες ενθυλάκωσης και η PDU μεταδίδεται εκτός του IP/MPLS δικτύου.

Σε αρκετές περιπτώσεις δεν είναι απαραίτητο να μεταδίδεται η επικεφαλίδα της PDU του επιπέδου 2 (layer 2 header) πάνω από το IP/MPLS δίκτυο. Αυτό γίνεται χρησιμοποιώντας πληροφορίες που υπάρχουν στη λέξη ελέγχου (control word) ή έχουν ήδη γίνει γνωστές στους δύο δρομολογητές (ingress και egress) με κατάλληλη σηματοδοσία. Έτσι είναι δυνατόν η επικεφαλίδα αυτή να αφαιρείται από τον ingress δρομολογητή και να ανακατασκευάζεται στον egress δρομολογητή.

Η λέξη ελέγχου (control word) χρησιμοποιείται για:

- την διατήρηση της ορθής σειράς των PDUs
- το "γέμισμα" (padding) των μικρών PDUs, ώστε να έχουν μέγεθος κατάλληλο για μετάδοση
- την μετάδοση πληροφοριών της επικεφαλίδας των PDUs του επιπέδου 2

Η λέξη ελέγχου (control word) αποτελείται από:

- 4 bits, που είναι δεσμευμένα για μελλοντική χρήση και πρέπει να είναι 0
- 4 bits, που είναι διαθέσιμα για τη μετάδοση flags που εξαρτώνται από το πρωτόκολλο του επιπέδου 2 που ενθυλακώνεται
- bits, που πρέπει να είναι 0
- 6 bits, που δηλώνουν αν η μεταδιδόμενη πληροφορία έχει μέγεθος μικρότερο από 64 και το επιπλέον padding πρέπει να αφαιρεθεί, και
- 4 bits, που είναι δεσμευμένα για μελλοντική χρήση και πρέπει να είναι 0
- 16 bits, που δηλώνουν έναν αύξοντα αριθμό της εκάστοτε PDU, ώστε αυτές να παραδίδονται με σωστή σειρά.

Το νόημα των 4 bits που χρησιμοποιούνται για τη μετάδοση flags διαφοροποιείται ανάλογα με το πρωτόκολλο του επιπέδου 2 το οποίο ενθυλακώνεται. Τα πρωτόκολλα που υποστηρίζονται μέχρι σήμερα είναι:

- Frame Relay
- ATM
    - ATM AAL5 CPCS-SDU mode
    - ATM cell mode
- Ethernet VLAN
- Ethernet
- HDLC
- PPP

Για τον διαχωρισμό των ξεχωριστών εξομοιούμενων εικονικών κυκλωμάτων μέσα σε μια σήραγγα, στην περίπτωση μετάδοσης πάνω από MPLS δίκτυο, ως πεδίο αποπολυπλεξίας χρησιμοποιείται ένα MPLS label. Το label αυτό βρίσκεται στο τέλος της στοίβας των labels και αποκαλείται VC label. Η τιμή του συμφωνείται ανάμεσα στους ingress και egress routers είτε με σηματοδοσία είτα με απευθείας ρύθμιση τους. Εάν είναι επιθυμητό να μεταφέρεται και πληροφορία σχετικά με την ποιότητα υπηρεσίας που θα πρέπει να είχε το πακέτο, αυτή τοποθετείτε στο πεδίο EXP του label. Η ίδια τιμή πρέπει να υπάρχει και σε όλα τα labels που τοποθετούνται πιο ψηλά στη στοίβα.

Για να μεταδοθεί μία PDU ενός πρωτοκόλλου του επιπέδου 2 από τον ingress router στον egress router θα πρέπει να υπάρχει εγκατεστημένο μεταξύ τους ένα LSP. Ο ingress router μπορεί λοιπόν να προκαλέσει τη μεταφορά της ενθυλακωμένης PDU, τοποθετώντας στην αρχή του πακέτου ένα label και στέλνοντας στον κατάλληλο γειτονικό router. Αυτό το label ονομάζεται tunnel label και το αντίστοιχο LSP ονομάζεται tunnel LSP. Το tunnel LSP απλά μεταφέρει τα πακέτα από τον ingress router στον egress router. Το tunnel label δεν μπορεί να χρησιμοποιηθεί από τον egress router για να αποφασίσει τι θα κάνει με το πακέτο (και μάλιστα αν χρησιμοποιείται penultimate hop popping, ο egress router δεν βλέπει καν το tunnel label). Επομένως, αν το payload δεν είναι ένα IP πακέτο (όπως στην περίπτωση μετάδοσης μιας PDU ενός πρωτοκόλλου του επιπέδου 2) πρέπει να υπάρχει ένα ακόμη label το οποίο θα γίνει ορατό στον egress router και το οποίο θα χρησιμοποιηθεί για να αποφασίσει ο egress router τι θα κάνει με το πακέτο. Αυτό το label ονομάζεται VC label.

Έτσι, όταν ένας ingress router στέλνει μία PDU ενός πρωτοκόλλου του επιπέδου 2 σε κάποιον egress router, πρώτα εισάγει το κατάλληλο VC label στη στοίβα των labels και μετά εισάγει το tunnel label. Το tunnel label είναι αρκετό για να μεταφερθεί το πακέτο μέχρι τον egress router. Το VC label δεν είναι ορατό κατά τη διέλευση του πακέτου μέσα από το MPLS δίκτυο. Γίνεται ορατό μόνο στον egress router που το χρησιμοποιεί για να αποφασίσει τον τρόπο χειρισμού του πακέτου.

Να σημειωθεί ότι το VC label πρέπει να είναι πάντα στον πάτο της στοίβας των labels, ενώ το tunnel label πρέπει να είναι αμέσως από πάνω του. Φυσικά κατά τη μετάδοση του πακέτου μέσα από το MPLS δίκτυο είναι δυνατόν να εισαχθούν στη στοίβα επιπλέον labels (τα οποία κάποια στιγμή θα αφαιρεθούν).

Η διανομή (distribution) του tunnel label (όπως και των άλλων επιπλέον labels) μπορεί να γίνει με οποιαδήποτε αποδεκτή μέθοδο για διανομή MPLS labels. Για τα VC labels μπορεί να χρησιμοποιηθεί στατική ανάθεση των labels, αλλά και διανομή μέσω από σηματοδοσία. Σε αυτή την περίπτωση το VC label θα πρέπει να διανεμηθεί από τον egress router στον ingress router χρησιμοποιώντας το πρωτόκολλο LDP σε downstream unsolicited mode.

Αυτή η τεχνική επιτρέπει την μετάδοση απεριόριστου αριθμού από "VCs" του επιπέδου 2 μέσα από το ίδιο τούνελ. Έτσι δεν υπάρχουν προβλήματα κλιμάκωσης στον κορμό του δικτύου.

Συμπερασματικά πλέον, χρησιμοποιώντας τους παραπάνω μηχανισμούς για ενθυλάκωση και μετάδοση PDUs ενός πρωτοκόλλου επιπέδου 2 είναι δυνατόν ένα MPLS δίκτυο να παρέχει εικονικά κυκλώματα του εν λόγω πρωτοκόλλου. Τα εικονικά αυτά κυκλώματα μπορούν να χρησιμοποιηθούν για την δημιουργία VPNs του επιπέδου 2. Για την υλοποίηση αυτών των VPNs γίνεται ρύθμιση των CE routers και στη συνέχεια ρύθμιση των αντίστοιχων PE routers. Στη συνέχεια γίνεται ανταλλαγή πληροφοριών ανάμεσα στους PE routers. Αυτό συμβαίνει και κάθε φορά που υπάρχει κάποια αλλαγή.

Σε αντίθεση με τα Layer 3 MPLS VPNs, στα Layer 2 MPLS VPNs ο δρομολογητής CE δεν είναι γειτονικός στο επίπεδο 3 με τον PE, αλλά με τους άλλους CE δρομολογητές του VPN. Ο δρομολογητής PE παραλαμβάνει PDUs του επιπέδου 2 και τις προωθεί μέσω του MPLS δικτύου χωρίς να εξετάζει τα PDUs του επιπέδου 3. Η προώθηση είναι διάφανη και οι δρομολογητές CE δεν αντιλαμβάνονται ότι μεταξύ τους υπάρχει ένα MPLS δίκτυο. Έτσι οι δρομολογητές PE δεν συμμετέχουν στη δρομολόγηση μέσα στο VPN, και δεν διατηρούν τις σχετικές πληροφορίες.

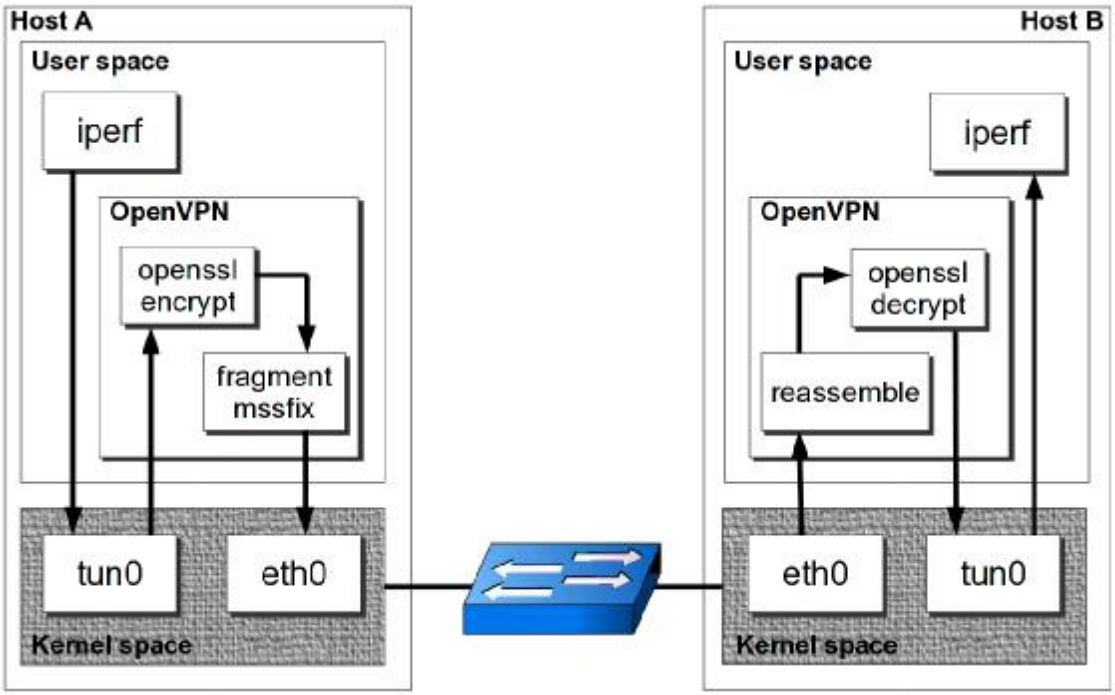
3.3.4 OpenVPN

Το OpenVPN είναι μια υλοποίηση VPN που βασίζεται σε SSL/TLS υποδομή, που διαχειρίζεται την δημιουργία σηράγγων και την διαδικασία κρυπτογράφησης, και δημιουργεί την ίδια διασύνδεση δύο άκρων που εφαρμόζεται και από το IPSec.

Το πρωτόκολλο OpenVPN προορίζεται για απλούς χρήστες , αφού δεν απαιτεί εξεζητημένες αλλαγές στον πυρήνα του λειτουργικού συστήματος (ΛΣ) για να λειτουργήσει . Συνήθως μια εφαρμογή για να εφαρμόσει κρυπτογράφηση σε μια

διασύνδεση , πρέπει να επικοινωνήσει με τον πυρήνα του ΛΣ για να επιτύχει πρόσβαση χαμηλού επιπέδου με το υλικό μέσω του οποίου έγινε η διασύνδεση .

Στο OpenVPN χρησιμοποιείται μία εικονική διασύνδεση (virtual interface) , η οποία είναι προσβάσιμη και ελεγχόμενη από τον χρήστη , δίχως την εξάρτηση από τον πυρήνα του ΛΣ . Έτσι το πρωτόκολλο αυτό είναι πιο ασφαλές σε σχέση με το IPSec και παρέχει μεγαλύτερη ευελιξία στην εγκατάσταση σε συστήματα διαφορετικών αρχιτεκτονικών και ευκολία στην διαχείριση . Ακόμη είναι δυνατόν να συνυπάρχει στο ίδιο σύστημα με το πρωτόκολλο IPSec .Το πρωτόκολλο SSL/TLS έχει εφαρμοστεί ευρέως και επομένως έχουν εντοπιστεί τα μειονεκτήματα του . Ένα σημαντικό αρνητικό στοιχείο είναι το ότι ένα πακέτο θα ληφθεί σε υψηλότερο επίπεδο σε σχέση με το IPSec και η επεξεργασία του θα κρατήσει περισσότερο χρόνο.



Μετάδοση σε OPEN VPN

Το OpenVPN προσφέρει κρυπτογράφηση των σηράγγων με δύο τρόπους. Είτε χρησιμοποιώντας ένα σταθερό κλειδί το οποίο γνωρίζουν και οι τα δύο άκρα της σήραγγας, το οποίο έχουν ανταλλάξει με κάποιο ασφαλή τρόπο . Είτε χρησιμοποιώντας κρυπτογράφηση δημόσιου και ιδιωτικού κλειδιού και τη δημιουργία πιστοποιητικών ασφαλείας για τον server και τους clients. Φυσικά η δεύτερη μέθοδος είναι και η πιο δυνατή κρυπτογράφηση παρέχοντας ένα πολύ μεγάλο βαθμό ασφάλειας , ωστόσο δεν παρέχει την απλότητα του σταθερού κλειδιού.

Εφόσον λοιπόν υπάρχει κάποιος εύκολος και ασφαλής τρόπος να μοιραστούνε τα δύο άκρα το ίδιο κλειδί προτιμάται η κρυπτογράφηση σταθερού κλειδιού. Σε κάθε περίπτωση μεγαλύτερη ασφάλεια σημαίνει και μεγαλύτερη πολυπλοκότητα και η επιλογή γίνεται συνήθως ανάλογα το περιεχόμενο και την σημαντικότητα αυτών που θέλουμε να διαφυλάξουμε.

Η δημιουργία της σήραγγας μπορεί να γίνει είτε με χρήση του TCP πρωτοκόλλου , είτε του UDP. Χρησιμοποιούμε UDP πακέτα και όχι TCP συνδέσεις καθώς υπάρχει πρόβλημα όταν κάνουμε σήραγγα TCP συνδέσεων πάνω σε TCP. Πιο συγκεκριμένα το TCP παρακολουθεί τη συνέχεια των πακέτων και αυτών που χάνονται και ζητάει αυτά τα χαμένα πακέτα να σταλούν πάλι , κάτι το οποίο είναι καλό όταν έχουμε μόνο ένα στρώμα (layer) TCP. Διαθέτει επίσης προσαρμοστικούς χρόνους για το πόσο να περιμένει μέχρι να ζητήσει νέα αίτηση για να σταλθεί το πακέτο. Το χρονικό αυτό διάστημα αλλάζει και αυξάνει εκθετικά όταν τα πακέτα συνεχίζουν να αποτυγχάνουν.

Εάν έχουμε TCP πάνω από TCP , τότε έχουμε 2 επίπεδα ελέγχου ροής των πακέτων με διαφορετικούς χρόνους αιτήσεων. Εάν οι χρόνοι αυτοί έχουν μεγάλη διαφορά μεταξύ τους αυτό μπορεί να έχει ως αποτέλεσμα την ραγδαία μείωση της απόδοσης του συστήματος επιβραδύνοντας σημαντικά την TCP σύνδεση.

Το OpenVPN μπορεί να δουλέψει με δύο τρόπους. Είτε χρησιμοποιώντας τον οδηγό TAP γεφυρώνοντας (bridge) δίκτυα μεταξύ τους , είτε με τον οδηγό TUN δρομολογώντας (routing) τα δύο δίκτυα μεταξύ τους.

Κάνοντας bridge των δικτύων ενώνουμε τα δύο δίκτυα σε ένα κοινό subnet .

Δεν χρειάζονται επιπλέον δηλώσεις των routes , ενώ τα broadcasts μεταδίδονται μέσα από το VPN , επιτρέποντας έτσι σε εφαρμογές που εξαρτώνται από τα LAN broadcasts να δουλέψουν . Τέτοιες εφαρμογές πχ είναι το Windows NetBIOS file sharing και το network neighbourhood browsing. Επίσης με το bridge μπορεί να γίνει χρήση οποιουδήποτε πρωτοκόλλου μέσω Ethernet όπως το IPv4 , IPv6 , Netware IPX, AppleTalk , κτλ.

Ωστόσο το bridge δεν έχει την αποδοτικότητα και την μεταβλητότητα που παρέχουν τα routed δίκτυα , γι αυτό και τις περισσότερες φορές εφόσον δεν είναι απαραίτητο προτιμάται η δρομολόγηση μεταξύ των δικτύων .

Το OpenVPN αποτελεί σήμερα ένας από τους πιο ασφαλείς τρόπους δημιουργίας σηράγγων και VPNs και σε συνδυασμό με την εύκολη προσαρμοστικότητα του στα λειτουργικά συστήματα , αλλά και το γεγονός ότι είναι

ένα πρόγραμμα ανοιχτού κώδικα (open source) , αποτελεί μια πολύ καλή λύση που γίνεται όλο και πιο δημοφιλής.

Το λογότυπο του Open VPN

Κεφάλαιο 4ο

Ένα δίκτυο VPN έχει ως βασικό σκοπό να εξασφαλίσει την επικοινωνία κάθε απομακρυσμένου γραφείου/καταστήματος, ή ακόμα και με κάθε στέλεχος της εταιρίας που βρίσκεται εκτός γραφείου, με τα κεντρικά γραφεία της επιχείρησης ή οποιοδήποτε άλλο σημείο ανήκει στο εν λόγω δίκτυο (επικοινωνία any-to-any). Η επικοινωνία αυτή συνήθως αφορά στη λειτουργία επιχειρηματικών εφαρμογών, τη μεταφορά αρχείων, την τηλεφωνική επικοινωνία μεταξύ των σημείων, την πρόσβαση στο Διαδίκτυο και το ηλεκτρονικό ταχυδρομείο αλλά και οποιαδήποτε άλλη ανάγκη επιθυμεί να καλύψει η επιχείρηση.

Η συνηθέστερη περιγραφή ενός VPN είναι αυτή μιας υποδομής που επιτρέπει τη σύνδεση δύο ή περισσότερων ιδιωτικών δικτύων με το Internet μέσα από ένα ασφαλές κανάλι. Στην πραγματικότητα, τα VPN προσφέρουν πρόσβαση στο Internet και επικοινωνία ανάμεσα σε γραφεία/καταστήματα μιας επιχείρησης που βρίσκονται σε διαφορετικές γεωγραφικές τοποθεσίες χρησιμοποιώντας το ήδη υπάρχον δημόσιο δίκτυο και όχι ακριβές μισθωμένες γραμμές. Την ίδια στιγμή, τα VPN παρέχουν τον ίδιο βαθμό ασφαλείας με τα ιδιωτικά δίκτυα, ενώ εκμεταλλεύονται αποτελεσματικά τις οικονομίες κλίμακος που δημιουργούνται.

4.1 Χαρακτηριστικά των VPN

Το VPN αποτελεί επίσης έναν ιδιαίτερα αποτελεσματικό τρόπο ανταλλαγής σημαντικών πληροφοριών και δεδομένων, ανάμεσα σε υπαλλήλους που βρίσκονται σε διαφορετικές τοποθεσίες, όπως σε πελάτες, προμηθευτές και γενικότερα συνεργάτες εκτός γραφείου. Καθώς οι επιχειρήσεις δεν είναι πλέον αναγκασμένες να επενδύσουν στην απαραίτητη υποδομή, μπορούν να μειώσουν ακόμη περισσότερο το λειτουργικό τους κόστος με το να αναθέτουν τις υπηρεσίες δικτύου σε παρόχους τέτοιων υπηρεσιών (ψηφιακό outsourcing).

Εξάλλου, τα VPN μειώνουν ακόμη περισσότερο τα κόστη της επιχείρησης, καθώς εξαλείφουν την ανάγκη για υπεραστικά τηλεφωνήματα είτε για σύνδεση στο διαδίκτυο, είτε για επικοινωνία ανάμεσα σε διαφορετικά γραφεία της επιχείρησης, καθώς η σύνδεση (κλήση) πραγματοποιείται με τον πλησιέστερο κόμβο του παρόχου.

Τα VPN δομούνται σήμερα με διάφορους τρόπους. Ο δημοφιλέστερος τρόπος είναι η χρήση τεχνολογιών IP, οι οποίες προσφέρουν περισσότερες δυνατότητες αλλά και ευελιξία. Επίσης οι IP δίνουν τη δυνατότητα παροχής πληθώρας υπηρεσιών προστιθέμενης αξίας στην επιχείρηση.

Η ασφάλεια και η προστασία των δεδομένων είναι παράγοντας πρωταρχικής σημασίας όταν γίνεται ανάπτυξη υπηρεσιών μέσω διαδικτύου, γεγονός που τις καθιστά ευάλωτες σε επιθέσεις και πρόσβαση από ανεπιθύμητα μέρη. Τα ασφαλή IP-VPN (IPSec) δίκτυα προσφέρουν υψηλότατο βαθμό ασφαλείας από τέτοιες απειλές.

Τα δεδομένα που διακινούνται μέσω των VPN είναι εμπιστευτικά, και απαιτείται πιστοποίηση με κωδικούς για την πρόσβαση σε αυτά. Συχνά εταιρίες επιλέγουν να αναπτύσσουν extranets πάνω σε Ιδεατά Ιδιωτικά Δίκτυα, προκειμένου να δώσουν συγκεκριμένα δικαιώματα πρόσβασης σε πελάτες, συνεργάτες και εμπορικούς εταίρους. Επίσης, η λύση αυτή επιτρέπει και τον έλεγχο της πρόσβασης, με διαφορετικά δικαιώματα για διαφορετικές ομάδες εργαζομένων. Αυτή η μέθοδος είναι πολύ πιο απλή και οικονομική από "παραδοσιακές" μεθόδους που εφαρμόζουν σήμερα διευθυντές τεχνολογίας.

Τα VPN χωρίζονται σε τρεις γενικές κατηγορίες: αυτά που βασίζονται στον **εξοπλισμό**, αυτά που βασίζονται στα **τείχη προστασίας** και όσα χρησιμοποιούν **ανεξάρτητες εφαρμογές**. Απλούστερα είναι τα VPN που βασίζονται στον εξοπλισμό, ωστόσο συχνά δεν είναι τόσο ευέλικτα όσο τα VPN που χρησιμοποιούν λογισμικό. Ασφαλέστερα όλων θεωρούνται τα δίκτυα που βασίζονται σε τείχος προστασίας. Ωστόσο, αν γίνει υπερ-φόρτωση του τείχους, ενδέχεται να προκύψουν ζητήματα απόδοσης.

Καθώς η αγορά των VPN ωριμάζει και εξελίσσεται ταχύτατα, όλο και συχνότερα τα διαφορετικά μοντέλα δόμησης VPN δανείζονται το ένα χαρακτηριστικά από το άλλο.

Τα VPN πρώτης γενιάς

Τα VPN πρώτης γενιάς, δηλαδή τα **IPsec VPNs**, προσέφεραν λύσεις απομακρυσμένης πρόσβασης για χρήστες καθώς και site-to-site συνδεσιμότητα για

πάνω από μία δεκαετία. Παρόλα αυτά, τα IPsec VPNs έχουν μία λογική πρόσβασης στο δίκτυο του τύπου “όλα ή τίποτα”, με δυσκολίες στη διαχείριση του λογισμικού VPN client, κάτι που συνεπάγεται αντίστοιχα αυξημένα κόστη.

Τα VPN δεύτερης γενιάς

Τα **SSL VPN** είναι τα VPN δεύτερης γενιάς, τα οποία έδωσαν λύσεις στους περιορισμούς των IPsec VPN, προσφέροντας αυξημένη ασφάλεια και μειωμένα λειτουργικά έξοδα, μια που δεν απαιτείται διαχείριση client λογισμικού. Παρόλα αυτά τα SSL VPN δεν έχουν καταφέρει να ανταποκριθούν στις απαιτήσεις και να αντικαταστήσουν τις λύσεις IPsec VPN. Μέχρι σήμερα όλα τα προϊόντα SSL VPN που χρησιμοποιήθηκαν προς αντικατάσταση των IPsec VPN είχαν σημαντικά προβλήματα ταχύτητας και απώλειας παραγωγικότητας των χρηστών, με αποτέλεσμα να μην μπορούν οι επιχειρήσεις να ωφεληθούν πραγματικά από τα πλεονεκτήματα των SSL VPNs, δηλαδή την αυξημένη ασφάλεια και τα χαμηλά λειτουργικά κόστη.

Τα VPN τρίτης γενιάς

Σήμερα, το **SSL VPN-Plus** και **MPLS** είναι VPN τρίτης γενιάς, που συνδυάζει όλα τα πλεονεκτήματα των SSL VPN – αυξημένη ασφάλεια και υψηλό ρυθμό μετάδοσης, ενώ ταυτόχρονα εκμηδενίζει τα προβλήματα επιδόσεων από τα οποία υποφέρουν οι λύσεις VPN δεύτερης γενιάς. Το SSL VPN-Plus είναι πιο γρήγορο, πιο εύκολο και πιο οικονομικό στην υλοποίησή του από τα IPSec VPNs, ενώ μειώνει το συνολικό κόστος και αυξάνει τον έλεγχο του IT, πρακτικά εξαφανίζοντας την πολυπλοκότητα των διαδικασιών παραμετροποίησης, διαχείρισης και υποστήριξης των IPSec VPN clients. Με δυνατότητες λειτουργίας τόσο σε μορφή client-to-site όσο και site-to-site, το SSL VPN-Plus μπορεί πλήρως να αντικαταστήσει το IPsec VPN για ασφαλή απομακρυσμένη πρόσβαση στο εταιρικό δίκτυο.

4.2 Διαχείριση της Δρομολόγησης και της Διασύνδεσης

Ένα ουσιώδες μέρος των χαρακτηριστικών λειτουργίας των VPN είναι η όσο το δυνατόν αποδοτικότερη χρήση του πολυτίμου εύρους ζώνης των WAN και η αξιόπιστη διασύνδεση κρίσιμων δεδομένων κατά την παροχή παραδοσιακών υπηρεσιών δρομολόγησης. Η φύση της δικτυακής κίνησης είναι τέτοια που

δημιουργεί συμφορήσεις στο δίκτυο και κάνει κακή χρήση του διαθέσιμου εύρους ζώνης. Το τι αποκομίζουμε από αυτή τη κατάσταση είναι προφανές: οι διασυνδέσεις WAN υπολειτουργούν την ίδια στιγμή που η συμφόρηση του δικτύου, ιδιαίτερα τις ώρες αιχμής ,περιορίζει τη διακίνηση σημαντικών πληροφοριών.

Για τους παραπάνω λόγους αναπτύχθηκε και εφαρμόζεται η έννοια της ποιότητας των παρεχόμενων υπηρεσιών (Quality of Service-**QoS**). Το QoS καθορίζει την ικανότητα του δικτύου να κατανέμει τους πόρους του συστήματος με σειρά προτεραιότητας σε κρίσιμες ή ευαίσθητες στην καθυστέρηση πληροφορίες και να ελαχιστοποιεί τους πόρους που προορίζονται για χρήση από μικρής προτεραιότητας πληροφορία. Το QoS θέτει δύο βασικές απαιτήσεις στις εφαρμογές που τρέχουν στα VPN:

1. ***Απόδοση***
2. ***Εφαρμογή Πολιτικής***. Οι πολιτικές καθορίζονται για την κατανομή δικτυακών πόρων σε συγκεκριμένους χρήστες , εφαρμογές και project groups ή σε servers με υψηλό βαθμό προτεραιότητας. Τα συστατικά μέρη του QoS όπως αυτά εφαρμόζονται στα επίπεδα 2 και 3 των VPN είναι:

- Κατηγοριοποίηση πακέτων καθορίζει τη προτεραιότητα των πακέτων σύμφωνα με τις επιταγές της δικτυακής πολιτικής
- Διασφαλισμένος Ρυθμός Πρόσβασης (Committed Access Rate-**CAR**) διασφαλίζει ένα ελάχιστο βαθμό διασύνδεσης σε συγκεκριμένες εφαρμογές και χρήστες σύμφωνα με τις επιταγές της δικτυακής πολιτικής
- Σταθμισμένο Σύστημα Δίκαιης Πρόσβασης (Weighted Fair Queing-**WFQ**) ορίζει τη διασύνδεση των πακέτων βάση της δικτυακής πολιτικής

- Σταθμισμένη Υπηρεσία Τυχούσας Ανίχνευσης Καθυστερήσεων (Weighted Random Early Detection-**WRED**) συμπληρώνει το TCP στη πρόβλεψη και διαχείριση της δικτυακής συμφόρησης στο VPN backbone, διασφαλίζοντας προβλέψιμους ρυθμούς διασύνδεσης
- Γενικό Σύστημα μορφοποίησης Δικτυακής Κίνησης (Generic Traffic Shaping-**GTS**) ομαλοποιεί τη κίνηση για να διασφαλίσει τη καλύτερη δυνατή απόδοση των VPN WAN διασυνδέσεων
- Αναπαραγωγή του Border Gateway Protocol (**BGP**) επιτρέπει στο QoS να επεκταθεί και στις δύο κατευθύνσεις μιας VPN σύνδεσης

Αυτοί οι μηχανισμοί του QoS αλληλοσυμπληρώνονται δουλεύοντας παράλληλα σε διαφορετικά σημεία του VPN και παράγοντας μία ολοκληρωμένη απ' άκρη-σ' άκρη QoS πρόταση. Το **QoS** πρέπει να εφαρμόζεται σε όλα τα μέρη των VPN για να είναι αποτελεσματικό διότι η αποσπασματική χρήση του δεν είναι ικανή να διασφαλίσει απόλυτα προβλέψιμα επίπεδα απόδοσης. Η απόδοση του δικτύου μπορεί να μετρηθεί με το **Cisco Response Time Reporter** (**RTR**), ένα χαρακτηριστικό παρακολούθησης του δικτύου από το Cisco IOS. Το RTR μετράει το χρόνο λειτουργίας του δικτύου, την καθυστέρηση και άλλα χαρακτηριστικά που βοηθούν στον καθορισμό πολιτικής και έλεγχο της εφαρμογής της.

4.3 Διαχείριση Δικτύου: Λειτουργώντας το VPN

Τα VPN περιλαμβάνουν πολλές υπηρεσίες ασφάλειας και QoS επιπρόσθετα αυτών των δικτυακών συσκευών. Οι επιχειρήσεις πρέπει να είναι σε θέση να διαχειρίζονται την VPN υποδομή συμπεριλαμβανομένων και των απομακρυσμένων χρηστών και των extranets. Λαμβάνοντας υπόψη όλα αυτά καταλαβαίνουμε τη σημασία της σωστής διαχείρισης των VPN. Ωστόσο μία VPN WAN αρχιτεκτονική είναι αρκετά ευέλικτη στη διαχείριση της και αντίθετα με οποιαδήποτε άλλη αρχιτεκτονική ιδιωτικού δικτύου προσφέρει τη δυνατότητα στις επιχειρήσεις να καθορίσουν το βαθμό του ελέγχου που θέλουν να έχουν πάνω στο δίκτυο οι ίδιες και να επιλέξουν λιγότερο ευαίσθητες υπηρεσίες που θα τις προωθήσουν σε παροχείς υπηρεσιών για να τις συντηρούν.

Πολλές επιχειρήσεις επιλέγουν την καθημερινή παρακολούθηση του VPN τους έχοντας έτσι την ανάγκη ενός συστήματος διαχείρισης και χάραξης

πολιτικής. Ένα τέτοιο σύστημα επεκτείνει το υπάρχον πλαίσιο έτσι ώστε αυτό να συμπεριλάβει WAN κανόνες διαχείρισης.

Όπως το WAN επεκτείνεται με τη τεχνολογία VPN, ένα συγκεκριμένο πλαίσιο απαιτήσεων πρέπει να ικανοποιείται για να είναι επιτυχής η αποστολή του διαχειριστή του συστήματος. Αυτό είναι:

- Ø Ελαχιστοποίηση του κινδύνου η μετάβαση από μία "αφιερωμένη" δομή σε μία διανεμημένη που χρησιμοποιεί μηχανισμούς μεταφοράς ,όπως το Internet, οδηγεί στην εμφάνιση νέων προκλήσεων ασφάλειας και παρακολούθησης: οι διαχειριστές πρέπει να μπορούν να επεκτείνουν τη πρόσβαση στο VPN από διαφορετικά sites, συνεταίρους και τηλεργαζόμενους και συγχρόνως να διασφαλίζουν την ακεραιότητα των δεδομένων
- Ø Κλιμάκωση η ραγδαία πρόσθεση και νέων χρηστών στο VPN απαιτεί επέκταση του δικτύου, αναβάθμιση του hardware και του software, διαχείριση του εύρους ζώνης και διατήρηση μιας πολιτικής με ακρίβεια και ταχύτητα
- Ø Κόστος για να συνειδητοποιήσουνε πλήρως οι διαχειριστές τα πλεονεκτήματα ,στο κόστος, από τη λειτουργία των VPN θα πρέπει να είναι σε θέση να εφαρμόζουν νέες VPN τεχνολογίες και να εξυπηρετούν νέους χρήστες χωρίς να αυξάνουν παράλληλα και το προσωπικό του συστήματος, με αντίστοιχους τουλάχιστον ρυθμούς

Η ικανοποίηση αυτών των απαιτήσεων μέσα από μία διαδικασία βημάτων: κλιμακωτή διαχείριση συσκευών, υποστήριξη υβριδικών συστημάτων και αναβάθμιση των δικτύων που έχουν σαν βάση πλατφόρμες της Cisco.

1. Κλιμακωτή Διαχείριση Συσκευών. Εργαλεία που επιτρέπουν τη διαχείριση μιας συσκευής κάθε φορά δεν δίνουν τη δυνατότητα στους διαχειριστές να εφαρμόσουν πολιτική ευρείας κλίμακας όπως απαιτείται από τις επιχειρήσεις. Το δίκτυο πρέπει να διαχειρίζεται από κάποια πολιτική, ενιαία και όχι σαν μεμονωμένες συσκευές. Έτσι είναι δυνατή η διαχείριση των πόρων του δικτύου μαζικά.
2. Υποστήριξη Υβριδικών Δικτυακών Αρχιτεκτονικών. Σε ένα υβριδικό περιβάλλον λειτουργίας η διαχείριση του VPN θα πρέπει να γίνεται μέσα στην υπάρχουσα διαχειριστική αρχιτεκτονική. Τα διάφορα εργαλεία θα πρέπει να

προσαρμοστούν και στις ανάγκες του VPN για να υπάρχει ομοιόμορφη διαχείριση.

4.4 Εφαρμογές των VPN

Αποτελεί γεγονός πως οι VPN λύσεις ορίζονται από το εύρος των προσφερόμενων χαρακτηριστικών. Μια VPN πλατφόρμα πρέπει να είναι ασφαλής από εισβολή και κακομεταχείριση, να μπορεί να παραδίδει κρίσιμα δεδομένα στο χρόνο που πρέπει και με αξιοπιστία και να είναι διαχειρίσιμο από κάθε σημείο της επιχείρησης. Αν κάποια από τις παραπάνω απαιτήσεις δεν εφαρμόζεται στην πράξη, η VPN λύση δεν είναι ολοκληρωμένη.

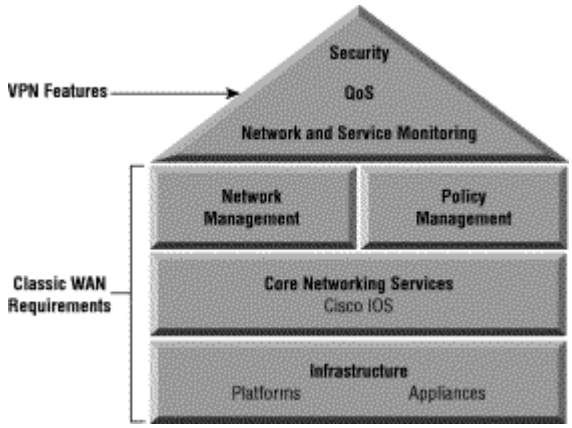
Τα ουσιαστικά στοιχεία ενός VPN μπορούν να χωριστούν σε πέντε αρκετά ανοιχτές κατηγορίες ως ακολούθως:

1. *Διαβαθμισιμότητα Πλατφόρμας*. Κάθε ένα από αυτά τα στοιχεία θα πρέπει να είναι διαβαθμισμένα σε όλες τις VPN πλατφόρμες, από μία διάταξη μικρού γραφείου έως την εφαρμογή τους σε μεγάλες επιχειρήσεις: Η ικανότητα προσαρμογής των VPN στις ανάγκες της σύνδεσης και του εύρους ζώνης είναι κρίσιμη εάν είναι να επιλεγεί αυτή η λύση.
2. *Ασφαλείς Τεχνικές*. Σήραγγες κρυπτογράφησης, πιστοποίησης πακέτων και χρηστών όπως επίσης και έλεγχος πρόσβασης.
3. *Υπηρεσίες VPN*. Λειτουργίες Ποιότητας Υπηρεσιών (Quality of Service QoS) όπως έρευνα, αποφυγή συμφορήσεων στο δίκτυο, έλεγχος κίνησης, κατηγοριοποίηση πακέτων όπως επίσης και VPN υπηρεσίες δρομολόγησης που κάνουν χρήση αλγορίθμων.
4. *Προστασία*. Ανίχνευση εισβολών και ενεργή παρακολούθηση ασφάλειας των τοίχων προστασίας.
5. *Διαχείριση*. Επιβολή πολιτικών ασφάλειας και ποιότητας υπηρεσιών κατά μήκος του VPN και παρακολούθηση του δικτύου.

Αυτά τα πέντε συστατικά μέρη κλειδιά δίδονται στο πλαίσιο του χαρακτηριστικού της διαβάθμισης των ανοιχτών συστημάτων παρέχοντας δυνατότητες από άκρη-σε-άκρη.

Η ικανοποίηση αυτών των απαιτήσεων δεν συνιστά απαραίτητα την αντικατάσταση μιας υπάρχουσας δικτυακής υποδομής WAN. Οι VPN λύσεις της

συγκεκριμένης επιχείρησης επαυξάνουν τις υπάρχουσες δικτυακές υποδομές και τους δίνουν επιπλέον ασφάλεια, αξιοπιστία και δυνατότητα διαχείρισης, χαρακτηριστικά υπαρκτά σε ένα VPN περιβάλλον.



Σε μερικές περιπτώσεις τοπολογιών WAN όπου το ζητούμενο είναι υψηλή απόδοση κρυπτογράφησης και ασφάλειας συνίσταται η χρήση των "VPN-optimized" δρομολογητών, οι οποίοι προσφέρουν επιπλέον ασφάλεια μέσο καθαρά μηχανισμών hardware. Η εφαρμογή VPN λύσεων σε κάθε σύνολο από VPN routers δίνει τη δυνατότητα εύρωστης ανάπτυξης του VPN δικτύου μέσα από τις υπάρχουσες δικτυακές υποδομές χωρίς να υπάρχει η ανάγκη επενδύσεων σε νέες δομές από μέρους της επιχείρησης.

Τα VPN χρησιμοποιούν τα **Firewalls της Cisco** (IOS Firewall και PIX που θα δούμε στο κεφάλαιο 6), το σύστημα **NetRanger** για ανίχνευση εισβολών, το σύστημα **NetSonar** για καταγραφή δεδομένων ασφάλειας και ανίχνευση πιθανών ελλείψεων σε αυτήν, και τα συστήματα πρωτοκόλλων **RADIUS** και **TACACS+** (που αναφέραμε στο κεφάλαιο 2) για πιστοποίηση χρηστών. Για όλα αυτά τα συστήματα υπάρχουν ειδικά κεφάλαια όπου αναλύονται διεξοδικά οι δυνατότητές τους και τα χαρακτηριστικά λειτουργίας τους.

Ένα ουσιώδες μέρος των χαρακτηριστικών λειτουργίας των VPN είναι η όσο το δυνατόν αποδοτικότερη χρήση του πολυτίμου εύρους ζώνης των WAN και η αξιόπιστη διασύνδεση κρίσιμων δεδομένων κατά την παροχή παραδοσιακών υπηρεσιών δρομολόγησης. Η φύση της δικτυακής κίνησης είναι τέτοια που δημιουργεί συμφορήσεις στο δίκτυο και κάνει κακή χρήση του διαθέσιμου εύρους ζώνης. Το τι αποκομίζουμε από αυτή τη κατάσταση είναι προφανές: οι διασυνδέσεις WAN υπολειτουργούν την ίδια στιγμή που η συμφόρηση του δικτύου, ιδιαίτερα τις ώρες αιχμής, περιορίζει τη διακίνηση σημαντικών πληροφοριών.

Ένα VPN μπορεί να χρησιμοποιήσει ένα ή περισσότερους από δύο μηχανισμούς. Ο ένας είναι να χρησιμοποιούν ιδιωτικά μισθωμένα κυκλώματα από έναν πάροχο επικοινωνίας, αυτό ονομάζεται ***αξιόπιστο VPN*** . ο άλλος είναι να στείλει κρυπτογραφημένα δεδομένα μέσω του δημόσιου δικτύου, αυτό ονομάζεται ***ασφαλές VPN*** . Χρησιμοποιώντας ένα ασφαλές VPN πάνω από έαν αξιόπιστό VPN λέγεται **υβριδικό VPN**. Συνδυάζοντας τα δύο είδη του ασφαλούς VPN σε μια πύλη, για παράδειγμα, IPsec και Secure Sockets Layer (SSL), καλείται, επίσης, *υβριδικό VPN* .

Αξιόπιστα VPNs

Με τα χρόνια, οι αξιόπιστες εφαρμογές VPNs έχουν μετακινηθεί από τα πρώτα ιδιωτικά κυκλώματα που μισθώνονται από τους προμηθευτές του ιδιωτικού τομέα των τηλεπικοινωνιών κυκλωμάτων IP δικτύων, σε μισθωμένα κυκλώματα από παρόχους υπηρεσιών Διαδικτύου. Οι κύριες τεχνολογίες που χρησιμοποιούνται για την εφαρμογή αξιόπιστων VPNs πάνω από IP δίκτυα είναι τα κυκλώματα **ATM**, **frame-relay** κυκλώματα και **Multiprotocol Label Switching** (MPLS).

Τα ATM και Frame Relay λειτουργούν στο στρώμα ζεύξης δεδομένων, τα οποία είναι Layer 2 του μοντέλου OSI. (Επίπεδο 1 είναι το φυσικό επίπεδο. Layer 3 είναι το στρώμα δικτύου). Το MPLS μιμείται μερικές ιδιότητες ενός κυκλώματος μεταγωγής του δικτύου κατά τη διάρκεια μεταγωγής πακέτων του δικτύου, και λειτουργεί σε ένα στρώμα που συχνά αναφέρεται ως "2,5" που είναι ενδιάμεση μεταξύ της ζεύξης δεδομένων και το δίκτυο. Το MPLS έχει αρχίζει να αντικαταστήσει το ATM και Frame Relay για την εφαρμογή αξιόπιστων VPNs.

Ασφαλής VPNs

Ασφαλή VPNs μπορούν να χρησιμοποιήσουν το IPsec με κρυπτογράφηση **IPSec**, με Layer 2 Tunneling Protocol (**L2TP**), **SSL 3.0** ή Transport Layer Security (**TLS**) με κρυπτογράφηση, Layer 2 Forwarding (**L2F**) ή Point-to-Point Tunneling Protocol (**PPTP**).

Το IPsec ή IP Security, είναι ένα πρότυπο για την κρυπτογράφηση και επικύρωση πακέτων IP στο επίπεδο δικτύου. Το IPsec έχει μια σειρά από πρωτόκολλα κρυπτογράφησης για δύο λόγους: για εξασφάλιση πακέτων δικτύου και την ανταλλαγή των κλειδιών κρυπτογράφησης. Ορισμένοι ειδικοί σε θέματα ασφάλειας, για παράδειγμα, του Bruce Schneier Counterpane Internet Security Inc, έχουν θεωρησει το IPsec ως το προτιμώτερο πρωτόκολλο για VPNs από τα τέλη της

δεκαετίας του 90. Το IPsec υποστηρίζεται στα Windows XP, 2000, 2003 και Vista. Στο Linux 2.6 και αργότερα, στο Mac OS X, NetBSD, FreeBSD και το OpenBSD. Στο Solaris, AIX και HP-UX . Πολλοί προμηθευτές παρέχουν IPsec VPN servers και τους πελάτες.

Η Microsoft έχει συμπεριλάβει PPTP πελάτες σε όλες τις εκδόσεις των Windows από τα Windows 95 OSR2 PPTP οι πελάτες βρίσκονται σε Linux, Mac OS X, Palm συσκευές PDA και Mobile 2003 windows συσκευές. Η εταιρεία έχει επίσης συμπεριλάβει PPTP server σε όλα τα προϊόντα της από το διακομιστή των Windows NT 4.0.

4.5 Πλεονεκτήματα και οφέλη

Ένα VPN - Virtual Private Network - είναι μια λύση μεγάλων αποστάσεων με ασφαλείς συνδέσεις δικτύου. Τα VPNs συνήθως υλοποιούνται (αναπτυχθεί) από επιχειρήσεις ή οργανισμούς και όχι από μεμονωμένα άτομα, αν και ένα εικονικό δικτύό μπορεί να επιτευχθεί μέσα από ένα οικιακό δίκτυο. Σε σύγκριση με άλλες τεχνολογίες, το VPN προσφέρει πολλά πλεονεκτήματα, ιδιαίτερα οφέλη για ασύρματο τοπικό δίκτυο περιοχής.

Για μια οργάνωση που κοιτάζει να παρέχει ένα ασφαλές δίκτυο υποδομής για την πελατειακή της βάση, ένα VPN προσφέρει δύο βασικά πλεονεκτήματα έναντι εναλλακτικών τεχνολογιών: μείωση του κόστους, και την επεκτασιμότητα του δικτύου. Στους πελάτες της πρόσβαση σε αυτά τα δίκτυα, το VPN φέρει επίσης κάποια οφέλη από την ευκολία στη χρήση.

Εξοικονόμηση κόστους με VPN

Ένα VPN μπορεί να σώσει μια οργάνωση χρήματα σε διάφορες καταστάσεις:

- εξαλείφοντας την ανάγκη για τις ακριβές μισθωμένες υπεραστικές γραμμές
- μείωση υπεραστικές τηλεφωνικές χρεώσεις
- εκφόρτωση κόστος υποστήριξης

VPNs vs μισθωμένες γραμμές – ένας οργανισμός ιστορικά χρειάζεται να μισθώσει χωρητικότητα δικτύου, όπως η T1 γραμμές για να επιτευχθεί η πλήρης, εξασφάλιση στη σύνδεση μεταξύ των διαφόρων εγκαταστάσεων του γραφείου τους. Με ένα VPN, που χρησιμοποιεί τα μέσα μαζικής υποδομής δικτύου,

συμπεριλαμβανομένου του διαδικτύου πολύ φθηνότερα από της τοπικές μισθωμένες γραμμές ή ακόμα και από ευρυζωνικές συνδέσεις σε ένα κοντινό υπηρεσία παροχής Internet (ISP) .

Τηλεφωνικές χρεώσεις ανά απόσταση - Ένα VPN μπορεί επίσης να αντικαταστήσει διακομιστές απομακρυσμένης πρόσβασης και υπεραστικές dialup συνδέσεις δικτύου που χρησιμοποιούνταν συνήθως στο παρελθόν από όσους ταξιδεύουν για επαγγελματικούς λόγους χρειάζεται να έχουν πρόσβαση στην εταιρεία τους intranet . Για παράδειγμα, με Internet VPN, οι πελάτες χρειάζονται μόνο σύνδεση στο σημείο πρόσβασης στο πλησιέστερο φορέα παροχής υπηρεσιών που είναι συνήθως τοπικά.

Το κόστος υποστήριξης - Με VPNs, το κόστος της διατήρησης servers τείνει να είναι λιγότερο από άλλες προσεγγίσεις λόγω ότι οι οργανισμοί μπορούν να αναθέτουν σε τρίτους την αναγκαία υποστήριξη από επαγγελματίες τρίτους παροχείς υπηρεσιών.

VPN επεκτασιμότητα

Το κόστος για μια οργάνωση της οικοδόμησης ενός ειδικού ιδιωτικου δίκτυου μπορεί να είναι λογικό στην αρχή, αλλά αυξάνει εκθετικά την οργάνωση μεγαλώνει. Μια εταιρεία με δύο υποκαταστήματα, για παράδειγμα, μπορούν να αναπτύξουν μία μόνο ειδική γραμμή για τη σύνδεση των δύο τοποθεσιών, αλλά 4 υποκαταστήματα απαιτούν 6 γραμμές για να συνδεθούν απ 'ευθείας μεταξύ τους, 6 υποκαταστήματα χρειάζονται 15 γραμμές, και ούτω καθεξής.

Ένα VPN που βασίζεται στο Διαδίκτυο αποφεύγει αυτό το πρόβλημα επεκτασιμότητας. Ειδικά για τις απομακρυσμένες και τις διεθνείς τοποθεσίες, ενα διαδικτυακό VPN προσφέρει ανώτερη ποιότητα των υπηρεσιών.

Χρησιμοποιώντας ένα VPN

Για να χρησιμοποιήθεί ένα VPN, κάθε πελάτης πρέπει να διαθέτει το κατάλληλο λογισμικό δικτύωσης ή υποστήριξη υλικού σε τοπικό δίκτυο και τους υπολογιστές τους. Όταν ρυθμιστεί σωστά, οι VPN λύσεις είναι εύκολες στη χρήση και μερικές φορές μπορεί να λειτουργήγουν αυτόματα ως μέρος της διαδικασίας εισόδου στο δικτύο.

Η VPN τεχνολογία λειτουργεί επίσης καλά με Wi-Fi τοπικής δικτύωσης περιοχής. Ορισμένοι οργανισμοί χρησιμοποιούν VPNs για να εξασφαλίσουν ασύρματες συνδέσεις σε τοπικά σημεία πρόσβασης όταν εργάζονται μέσα στο

γραφείο. Αυτές οι λύσεις παρέχουν ισχυρή προστασία χωρίς να επηρεάζει την απόδοση υπερβολικά.

Περιορισμοί του VPN

Παρά τη δημοτικότητά τους, τα VPN δεν είναι τέλεια και οι περιορισμοί υπάρχουν, όπως ισχύει και για κάθε τεχνολογία. Κάθε Οργανισμός θα πρέπει να εξετάσει θέματα όπως τα παρακάτω κατά την ανάπτυξη και τη χρήση εικονικών ιδιωτικών δικτύων στις λειτουργίες τους:

1. Τα VPNs απαιτούν λεπτομερή κατανόηση των ζητημάτων ασφάλειας του δικτύου και την ασφαλή εγκατάσταση / παραμετροποίηση για την εξασφάλιση επαρκούς προστασίας σε ένα δημόσιο δίκτυο όπως το Internet.

2. Η αξιοπιστία και η απόδοση του βασιζόμενου στο διαδίκτυο, VPN δεν είναι υπό τον άμεσο έλεγχο ενός οργανισμού. Αντ 'αυτού, η λύση θα βασίζεται σε έναν ISP και την ποιότητα των υπηρεσιών τους.

3. Ιστορικά, VPN προϊόντα και λύσεις από διάφορους προμηθευτές δεν ήταν πάντα συμβατά λόγω των ζητημάτων με τα πρότυπα της τεχνολογίας VPN. Προσπαθώντας να συνδυάσουν εξοπλισμό αυτό μπορεί να προκαλέσει τεχνικά προβλήματα, και χρησιμοποιώντας εξοπλισμό από έναν προμηθευτή δεν μπορεί να δώσει τόσο μεγάλη εξοικονόμηση κόστους.

Οφέλη και κίνδυνοι για την ασφάλεια των VPN

Ένα VPN μπορεί να διαγράψει τα γεωγραφικά εμπόδια για μια εταιρεία, επιτρέπει στους υπαλλήλους να εργάζονται αποτελεσματικά από το σπίτι και επιτρέπει σε μια επιχείρηση να συνδεθεί με ασφάλεια με τους προμηθευτές και τους εταίρους της. Ένα VPN είναι συνήθως πολύ φθηνότερο από ιδιωτικές γραμμές.

Από την άλλη πλευρά, η χρήστες του VPN μπορεί να εκθέσουν μιαν εταιρεία σε πιθανούς κινδύνους. Ενώ τα περισσότερα VPNs που χρησιμοποιούνται σήμερα είναι αρκετά ασφαλής, εναπόκειται στους διαχειριστές του δικτύου να εφαρμόζουν τα ίδια πρότυπα ασφαλείας για υπολογιστές που συνδέονται στο δίκτυο μέσω VPN ή υπολογιστές που συνδέονται άμεσα με το τοπικό δίκτυο.

Αξιοπιστία, επεκτασιμότητα και την απόδοση των VPN

Επειδή ασφαλώς τα VPNs βασίζονται στην κρυπτογράφηση και μερικές από τις λειτουργίες κρυπτογράφησης που χρησιμοποιούνται είναι υπολογιστικά ακριβές, οι διαχειριστές συνήθως διαχειρίζονται το φόρτο εργασίας του server με τον περιορισμό του αριθμού των ταυτόχρονων συνδέσεων σε αυτό το server. Όταν ο

αριθμός των ανθρώπων που προσπαθούν να συνδεθούν ξαφνικά κορυφώνεται, διαταράσσεται η μεταφορά δεδομένων, οι εργαζόμενοι μπορούν να βρεθούν σε θέση να μην έχουν την δυνατότητα να συνδεθούν επειδή όλοι οι server είναι απασχολημένοι. Αυτό δίνει στους διαχειριστές κίνητρο να παρέχουν πρόσβαση σε βασικές εφαρμογές χωρίς να απαιτείται η σύνδεση μέσω VPN. Για παράδειγμα, με τη δημιουργία διακομιστών μεσολάβησης ή διακομιστές στο Διαδίκτυο επιτρέπουν στους υπαλλήλους έχουν πρόσβαση στο ηλεκτρονικό ταχυδρομείο από το σπίτι ή από το δρόμο χώρις να χρειάζεται να συνδεθούν μέσα από το δίκτυο VPN της επιχείρησης

Η επιλογή μεταξύ IPsec και SSL / TLS για ένα σενάριο μπορεί να είναι περίπλοκη. Μια εκτίμηση είναι ότι το SSL / TLS μπορεί να λειτουργήσει με βάση το NAT-firewall ενώ το IPsec δεν μπορεί, αλλά και τα δύο πρωτόκολλα μέσω firewalls δεν χρειάζονται να μεταφράζουν τις διευθύνσεις. Το IPsec κρυπτογραφεί όλες τις IP κίνησης μεταξύ δύο υπολογιστών. Το SSL / TLS χρησιμοποιεί ασύμμετρη λειτουργία κρυπτογράφησης για να δημιουργήσει μια σύνδεση, και πιο αποτελεσματική συμμετρική λειτουργίες κρυπτογράφησης για να εξασφαλίσει μια συνεδρία.

Οι διαχειριστές μπορούν να αποφασίσουν να αναμίξουν τα πρωτόκολλα για την βέλτιστη ισορροπία μεταξύ απόδοσης και ασφάλειας. Για παράδειγμα, οι πελάτες μπορεί να συνδεθεί σε ένα Web server από ένα firewall χρησιμοποιώντας ένα πρόγραμμα περιήγησης που προστατεύεται από το SSL / TLS, ο web server μπορεί να συνδεθεί με ένα server κάποιας εφαρμογής χρησιμοποιώντας το IPsec Και ο server της εφαρμογή μπορεί να συνδεθεί με ένα διακομιστή βάσης δεδομένων σε ένα άλλο τείχος προστασίας χρησιμοποιώντας SSL.

Η κλιμάκωση των VPNs μπορεί μερικές φορές να βελτιωθεί με τη χρήση των ειδικών συσκευών διαχείρισης πόρων.

Τα VPN και σε ποιες επιχειρήσεις απευθύνονται

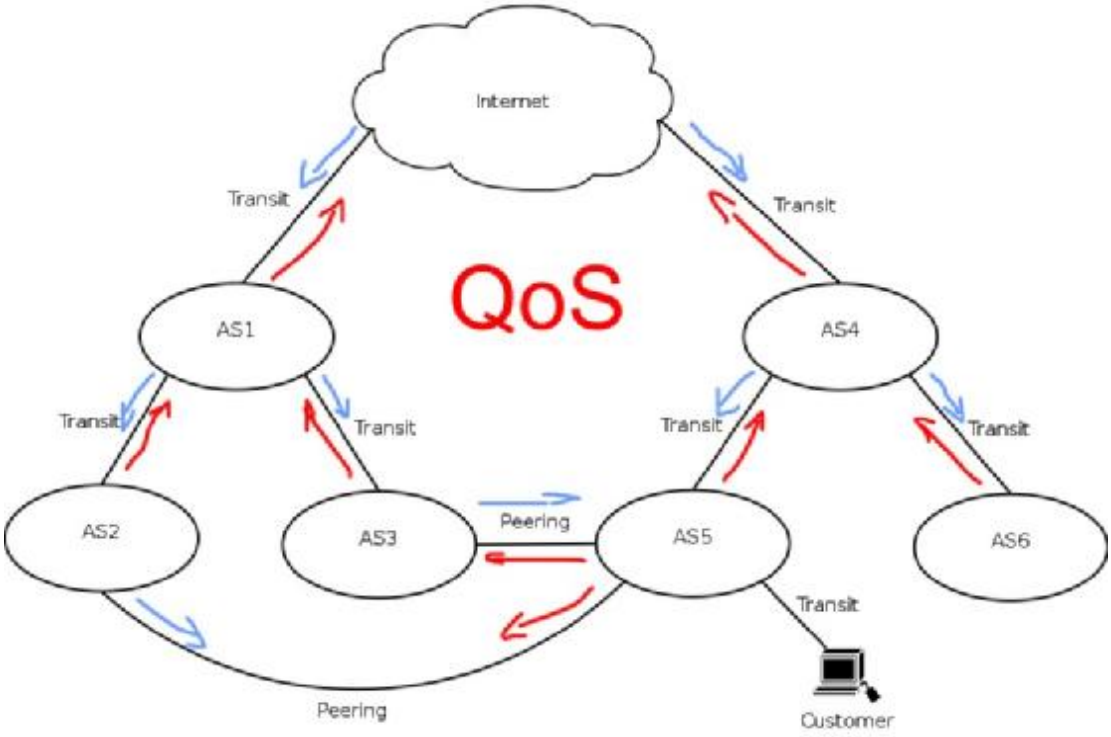
Επιχειρήσεις με περισσότερα από ένα σημεία παρουσίας (καταστήματα, γραφεία) πολύ συχνά αντιμετωπίζουν προβλήματα επικοινωνίας ή λειτουργίας που απορρέουν από τη γεωγραφική απόσταση που χωρίζει αυτά τα σημεία. Σε αυτές ακριβώς τις επιχειρήσεις απευθύνεται ένα Ιδεατό Ιδιωτικό Δίκτυο (Virtual Private Network, VPN), το οποίο μπορεί να προσφέρει λύσεις σε θέματα επικοινωνίας, οργάνωσης, διαχείρισης και κατανομής πληροφοριών σε όλα τα τμήματα ή τα

υποκαταστήματα μιας επιχείρησης, όπου κι αν βρίσκονται, και κυρίως με συγκεκριμένες εγγυήσεις.

Οι **VPN** υπηρεσίες κάνουν χρήση διαφόρων τεχνολογιών, καθώς και QoS (**Q**uality **o**f **S**ervice) μηχανισμών, για την παροχή λύσεων σε επιχειρήσεις πάνω από το δίκτυο του παρόχου. Οι τεχνολογίες έχουν δημιουργηθεί ειδικά για να προσφέρου μεγάλες δυνατότητες κλιμάκωσης στην κατασκευή Ιδεατών Ιδιωτικών Δικτύων (VPN), με συνέπεια να επιτρέπει τη δημιουργία ιδεατών συνδέσεων που αποτελούνται από αρκετές εκατοντάδες σημεία, με μειωμένο διαχειριστικό κόστος. Παράλληλα προσφέρουν μία σειρά από σημαντικά πλεονεκτήματα, τα οποία είναι απαραίτητα για την απρόσκοπτη λειτουργία του ιδιωτικού δικτύου δεδομένων των σημερινών επιχειρήσεων:

- Τα Ιδεατά Ιδιωτικά Δίκτυα παρέχουν αυξημένη προστασία κατά τη διακίνηση των δεδομένων μεταξύ των σημείων παρουσίας της εταιρείας, μειώνοντας έτσι τον κίνδυνο υποκλοπής, καθώς η κίνηση ανάμεσα στα σημεία που ανήκουν στο VPN είναι παντελώς απομονωμένη από την κίνηση των άλλων VPN του παροχου.
- Η υπηρεσία των VPN της δίνει τη δυνατότητα δημιουργίας κλειστών ιδιωτικών δικτύων, των οποίων τα μέλη μπορούν να συνδέονται μεταξύ τους με οποιαδήποτε επιθυμητή λογική τοπολογία. Με την ευελιξία αυτή διευκολύνεται η εξυπηρέτηση διαφορετικών επιχειρησιακών διαδικασιών πάνω από το ίδιο δίκτυο. Π.χ. η εξυπηρέτηση της φωνητικής επικοινωνίας των σημείων παρουσίας μίας εταιρείας απαιτεί άμεση διασυνδεσιμότητα ενός σημείου με οποιοδήποτε άλλο σημείο της εταιρείας (full mesh λογική τοπολογία). Κάτι τέτοιο δεν είναι επιθυμητό για τα δίκτυα δεδομένων κάποιων επιχειρήσεων οι οποίες μπορούν να επιλέξουν τοπολογία αστέρα ή partial mesh. Με τη χρήση συγκεκριμένα της τεχνολογίας MPLS και οι δύο λύσεις μπορούν να συνυπάρξουν πάνω από ένα ενιαίο δίκτυο. Η ευελιξία των υπηρεσιών VPN δίνει τη δυνατότητα ενσωμάτωσης των μελλοντικών απαιτήσεων που μπορεί να προκύψουν από το δυναμικά εξελισσόμενο επιχειρησιακό περιβάλλον, σε μικρό χρόνο και με ελεγχόμενο κόστος.
- Με τη χρήση των υπηρεσιών VPN παρέχεται η δυνατότητα διατήρησης του σχήματος διευθυνσιοδότησης το οποίο έχει υιοθετήσει εσωτερικά μια εταιρεία, μειώνοντας με αυτόν τον τρόπο σημαντικά το κόστος υιοθέτησης της νέας τεχνολογίας.

- Οι υπηρεσίες VPN δίνουν τη δυνατότητα δημιουργίας πολιτικής επιπέδου υπηρεσιών από άκρο σε άκρο, διασφαλίζοντας με αυτόν τον τρόπο την προνομιακή μεταχείριση των ευαίσθητων επιχειρησιακών δεδομένων σε όλα τα στάδια της μετάβασής τους στο δίκτυο.
- Με τη χρήση των υπηρεσιών VPN δίνεται η δυνατότητα στις επιχειρήσεις να δημιουργούν Ιδεατά Ιδιωτικά Δίκτυα χρησιμοποιώντας μία πληθώρα τεχνολογιών διασύνδεσης, όπως κυκλώματα οπτικών ινών, ψηφιακές γραμμές, ADSL, SDSL, Dial up, ώστε να επεκτείνουν το δίκτυο τους με αποτελεσματικό και αποδοτικό τρόπο.



Μια μορφή QoS

Κεφάλαιο 5ο

Η ανάπτυξη ενός διαμοιραζόμενου δικτύου, θέτει σοβαρά ζητήματα όσον αφορά την ασφάλειά του. Οι διάφοροι χρήστες θέλουν να είναι σίγουροι για την ασφάλεια που παρέχει το δίκτυο απέναντι σε εισβολείς και χρήστες που κερδίζουν παράνομα, πρόσβαση στους πόρους του δικτύου, παρακολουθούν ή αλλοιώνουν τα κρίσιμα για αυτούς δεδομένα, που μετακινούνται σε αυτό.

5.1 Ασφάλεια

Από τη στιγμή της ύπαρξης του INTEPNET, ποιος ο λόγος να πληρώνει κάποιος τεράστια πόσα για την ανάπτυξη VPN δικτύων και συστημάτων; Η απάντηση είναι απλή. Το INTEPNET δεν προσφέρει ασφάλεια.

Η δουλειά που κάνει το Ίντερνετ είναι να μεταφέρει παντού ότι δεδομένα που του δίνεις ή ζητάς. Αν κάποιος στείλει δεδομένα είναι πολύ εύκολο, να τα διαβάσει ο οποιοσδήποτε είναι συνδεδεμένος στο Ίντερνετ.

Αυτός είναι και ο λόγος ανάπτυξης των VPN (Virtual Private Networks) δικτύων. Αναλύοντας και μόνο τον όρο “Private” - «Ιδιωτικά» - αντιλαμβανόμαστε την σημασία της ασφάλειας που παρέχουν τα VPN δίκτυα. Τα τρία βασικά χαρακτηριστικά της ασφάλειας που παρέχουν είναι:

- **Integrity:** «Ακεραιότητα»· εξασφάλιση της διαμεταγωγής των σωστών και μόνο δεδομένων.
- **Encryption**: «Κρυπτογράφηση» · εξασφάλιση της μη δυνατότητας ανάγνωσης από τρίτους
- **Authentication**: «Πιστοποίηση» · εξασφάλιση της ταυτότητας του εκάστοτε client.

Η επίτευξη των παραπάνω χαρακτηριστικών επιτυγχάνεται μέσω των δυο συστατικών στοιχείων ασφάλειας ενός VPN δικτύου, τα οποία είναι:

- **Tunneling**: «Σήραγγες»· Εγγυημένη μεταφορά δεδομένων μέσω συγκεκριμένης δρομολόγησης.
- **Firewall**: «Τοίχος Προστασίας»· Εγγυημένη πρόσβαση σε αποθήκες δεδομένων.

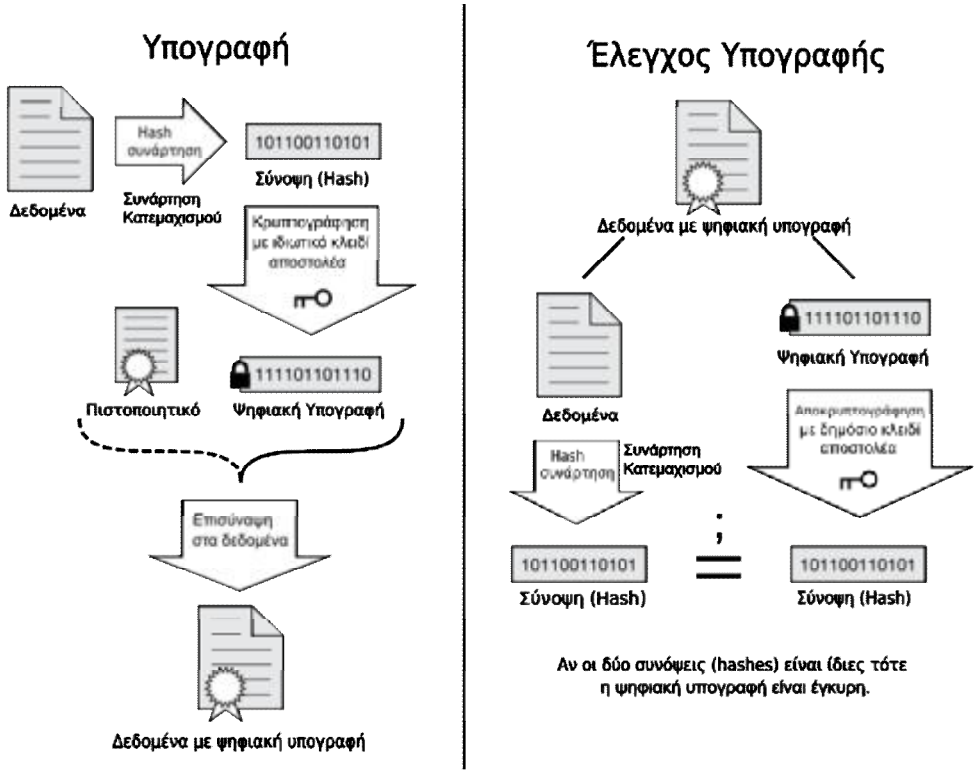
Αυτοί οι δυο μηχανισμοί αλληλοσυμπληρώνονται παρέχοντας ασφάλεια σε διαφορετικά σημεία του δικτύου.

5.1.1 Authentication: «Πιστοποίηση»

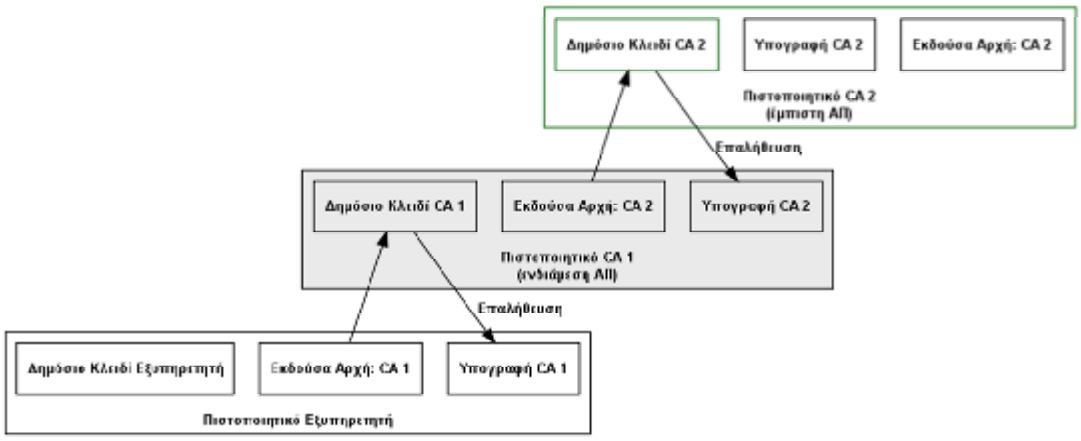
Μεγάλη σημασία για την ασφάλεια της δικτυακά διακινούμενης πληροφορίας έχει η ακεραιότητά της. Σε ένα ανασφαλές δίκτυο, τα πακέτα μπορεί να υποκλαπούν, να αλλοιωθούν τα δεδομένα τους και να επαναπροωθηθούν στον προορισμό τους με λανθασμένες πληροφορίες.

Αυτό αποφεύγετε με την έκδοση ένα πιστοποιητικού. Ένα πιστοποιητικό είναι μια δήλωση με ψηφιακή υπογραφή, η οποία συνδέει την τιμή ενός δημόσιου κλειδιού με την ταυτότητα του ατόμου, της συσκευής ή της υπηρεσίας που διαθέτει το αντίστοιχο ιδιωτικό κλειδί. Δηλαδή, επιτρέπουν την επαλήθευση του ισχυρισμού ότι ένα συγκεκριμένο δημόσιο κλειδί ανήκει σε μια συγκεκριμένη οντότητα. Τα πιστοποιητικά αποτρέπουν κάποιον να υποδυθεί κάποιον άλλο με την χρήση ψεύτικου κλειδιού.

Μπορούν να εκδοθούν πιστοποιητικά για ποικίλες λειτουργίες, όπως ο έλεγχος ταυτότητας χρήστη του Web, ο έλεγχος ταυτότητας διακομιστή Web, το ασφαλές ηλεκτρονικό ταχυδρομείο, η ασφάλεια πρωτοκόλλου Internet (IPSec), η ασφάλεια **TLS** (**Transport Layer Security**) και η προσθήκη υπογραφής σε κώδικα.



Εκδίδονται επίσης πιστοποιητικά από μία αρχή έκδοσης πιστοποιητικών (CA) σε άλλη, προκειμένου να δημιουργηθεί μια ιεραρχία πιστοποιητικών. Σ' αυτήν της ιεραρχία, οι οργανισμοί κάθε επιπέδου πιστοποιούν δημόσια κλειδιά. Έτσι, πολλές φορές το πιστοποιητικό για έναν χρήστη μπορεί να συνοδεύεται από μία αλυσίδα πιστοποιητικών που φθάνουν ως την κορυφή της ιεραρχίας. Σε κάθε πιστοποιητικό περιέχεται η υπογραφή του ανώτερου εκδοτικού οργανισμού που έχει δημιουργηθεί με το ιδιωτικό κλειδί. Δηλαδή μια CA πιστοποιεί μια άλλη CA, με μία σειρά ιεραρχίας από πάνω προς τα κάτω. Το δημόσιο κλειδί του εκδοτικού οργανισμού που είναι στην κορυφή της ιεραρχίας δεν πιστοποιείτε από κανέναν. Γι' αυτό ο οργανισμός εκδίδει πιστοποιητικό για τον εαυτό του. Αυτονόητο είναι, λοιπόν, ότι αυτός ο οργανισμός πρέπει να είναι απόλυτα έμπιστος. Το πιστοποιητικό εκδίδει ονομάζετε **«πιστοποιητικό ρίζας»** και περιέχει το δημόσιο κλειδί, την υπογραφή και το ιδιωτικό του κλειδί.



Ο χρήστης που επιθυμεί να αποκτήσει ένα πιστοποιητικό, θα δημιουργήσει πρώτα ένα ζεύγος ιδιωτικού δημόσιου κλειδιού και θα αποστείλει σε μία CA το δημόσιο κλειδί μαζί με πληροφορίες που προσδιορίζουν την ταυτότητα του χρήστη. Η CA αφού επαληθεύσει την ταυτότητα του χρήστη και σιγουρευτεί ότι η αίτηση έκδοσης πιστοποιητικού προέρχεται από τον πραγματικό χρήστη, απαντά στον χρήστη με χρήστη το πιστοποιητικό του μαζί με τα ιεραρχικά δεμένα πιστοποιητικά που επιβεβαιώνουν την αυθεντικότητα την δημόσιου κλειδιού της CA.

Συνήθως, τα πιστοποιητικά περιέχουν τις εξής πληροφορίες:

- Το **όνομα του κατόχου**
- Την **τιμή δημόσιου κλειδιού**

- Τις **πληροφορίες αναγνώρισης** του, όπως το όνομα και η διεύθυνση ηλεκτρονικού ταχυδρομείου
- Την **περίοδο ισχύος** (τη χρονική διάρκεια κατά την οποία το πιστοποιητικό θεωρείται έγκυρο)
- **Πληροφορίες αναγνώρισης εκδότη**
- Την **ψηφιακή υπογραφή του εκδότη**, η οποία πιστοποιεί την εγκυρότητα της σύνδεσης μεταξύ του δημόσιου κλειδιού και των πληροφοριών αναγνώρισης του αντικειμένου.

Ένα πιστοποιητικό είναι έγκυρο μόνο για το χρονικό διάστημα που καθορίζεται σε αυτό, έτσι κάθε πιστοποιητικό περιέχει τις ημερομηνίες οι οποίες είναι τα όρια της περιόδου ισχύος. Μετά την πάροδο του διαστήματος ισχύος ενός πιστοποιητικού, θα πρέπει να γίνει αίτηση για νέο πιστοποιητικό από τον εκδότη του πιστοποιητικού που μόλις έληξε.

Υπάρχουν και πιστοποιητικά που ακυρώνονται πριν την λήξη τους. Αυτά αποθηκεύονται σε μία **λίστα ανάκλησης πιστοποιητικών** (Certificate Revocation Lists). Είναι πολλοί οι λόγοι που ένα πιστοποιητικό μπορεί να ανακληθεί. Π.χ Εάν ενας υπάλληλος απολυθεί, η εταιρεία θα ακυρώσει το πιστοποιητικό, ώστε να μην έχει την δυνατότητα να υπογράφει έγγραφα με το κλειδί του.

Επειδή τα πιστοποιητικά χρησιμοποιούνται γενικά για την εδραίωση ταυτότητας και την δημιουργία αξιοπιστίας για την ασφαλή ανταλλαγή πληροφοριών, οι CA μπορούν να εκδώσουν πιστοποιητικά σε άτομα, συσκευές (όπως υπολογιστές) και υπηρεσίες που εκτελούνται σε υπολογιστές (όπως η ασφάλεια IPSec).

Στις περιπτώσεις όπου δύο οντότητες όπως συσκευές, άτομα, εφαρμογές ή υπηρεσίες—επιχειρούν να εδραιώσουν ταυτότητα και αξιοπιστία, το γεγονός ότι και οι δύο οντότητες θεωρούν αξιόπιστη την ίδια αρχή έκδοσης πιστοποιητικών, επιτρέπει την εδραίωση δεσμού ταυτότητας και αξιοπιστίας μεταξύ τους. Μόλις ένα αντικείμενο πιστοποιητικού υποβάλλει ένα πιστοποιητικό που εκδόθηκε από αξιόπιστη CA, η οντότητα που επιχειρεί να εδραιώσει αξιοπιστία μπορεί να προχωρήσει στην ανταλλαγή πληροφοριών, αποθηκεύοντας το πιστοποιητικό του αντικειμένου του πιστοποιητικού στον δικό της χώρο αποθήκευσης και, εφόσον υπάρχει, το δημόσιο κλειδί που περιέχεται στο πιστοποιητικό, να κρυπτογραφήσει ένα κλειδί περιόδου λειτουργίας, έτσι ώστε να είναι ασφαλείς όλες οι επόμενες

επικοινωνίες. Το πιστοποιητικό δεν χρειάζεται να αποστέλλεται κάθε φορά που ξεκινά μία συναλλαγή. Αρκεί να σταλεί μία φορά κατά την έναρξη της σύνδεσης.

Για παράδειγμα, όταν χρησιμοποιείτε το Internet για ηλεκτρονικές τραπεζικές εργασίες, είναι σημαντικό να γνωρίζετε ότι το πρόγραμμα περιήγησης στο Web επικοινωνεί απευθείας και με ασφάλεια με το διακομιστή Web της τράπεζάς. Το πρόγραμμα περιήγησης στο Web πρέπει να έχει τη δυνατότητα να εκτελεί έλεγχο ταυτότητας του διακομιστή Web, προτού λάβει χώρα μια ασφαλής συναλλαγή. Δηλαδή, ο διακομιστής Web πρέπει να έχει τη δυνατότητα να αποδεικνύει την ταυτότητά του στο πρόγραμμα περιήγησης στο Web, προτού προχωρήσει η συναλλαγή.

Πολλές εταιρείες εγκαθιστούν δικές τους αρχές έκδοσης πιστοποιητικών και εκδίδουν πιστοποιητικά σε εσωτερικές συσκευές, υπηρεσίες και υπαλλήλους, για να δημιουργήσουν ασφαλέστερο περιβάλλον υπολογιστών. Οι μεγάλες εταιρίες ενδέχεται να έχουν πολλές αρχές έκδοσης πιστοποιητικών, οργανωμένες σε μια ιεραρχία (όπως αναλύσαμε και παραπάνω), η οποία οδηγεί σε μια αρχή έκδοσης πιστοποιητικών ρίζας. Έτσι, ο υπάλληλος μιας εταιρείας ενδέχεται να έχει πολυάριθμα πιστοποιητικά στο χώρο αποθήκευσης πιστοποιητικών, τα οποία έχουν εκδοθεί από ποικίλες εσωτερικές αρχές έκδοσης πιστοποιητικών, που κάνουν κοινή χρήση μιας αξιόπιστης σύνδεσης, μέσω της διαδρομής πιστοποίησης προς την αρχή έκδοσης πιστοποιητικών ρίζας.

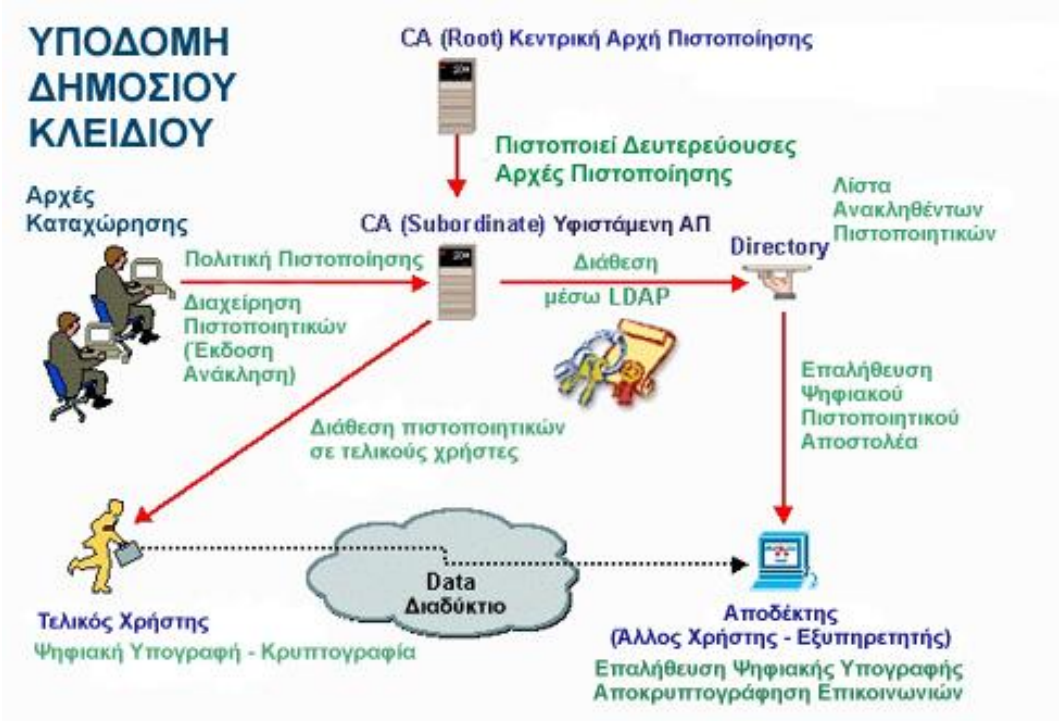
Όταν ένας υπάλληλος συνδέεται με το δίκτυο της εταιρείας από το σπίτι του, χρησιμοποιώντας ένα εικονικό ιδιωτικό δίκτυο (VPN), ο διακομιστής VPN μπορεί να παρουσιάσει ένα πιστοποιητικό διακομιστή για να αποδείξει την ταυτότητά του. Επειδή το πιστοποιητικό ρίζας της εταιρείας είναι αξιόπιστο και επειδή το πιστοποιητικό του διακομιστή VPN εκδόθηκε από την εταιρική αρχή έκδοσης πιστοποιητικών ρίζας, ο υπολογιστής-πελάτης (client) μπορεί να προχωρήσει στη σύνδεση και ο υπάλληλος γνωρίζει ότι ο υπολογιστής του είναι στην πραγματικότητα συνδεδεμένος με το διακομιστή VPN της εταιρείας του.

Ο διακομιστής VPN πρέπει να έχει επίσης τη δυνατότητα ελέγχου της ταυτότητας του υπολογιστή-πελάτη VPN πριν από την ανταλλαγή δεδομένων μέσω της σύνδεσης VPN. Ο έλεγχος της ταυτότητας οποιουδήποτε επιπέδου του υπολογιστή γίνεται είτε με την ανταλλαγή πιστοποιητικών υπολογιστή είτε με τον έλεγχο ταυτότητας σε επιπέδο χρήστη, με τη χρήση μιας μεθόδου ελέγχου ταυτότητας μέσω πρωτοκόλλου **Point-to-Point** (PPP). Για συνδέσεις L2TP (**Layer 2 Tunneling Protocol**)/IPSec,

απαιτούνται πιστοποιητικά υπολογιστή τόσο για τον υπολογιστή-πελάτη όσο και για το διακομιστή.

Το πιστοποιητικό του υπολογιστή-πελάτη ενδέχεται να εξυπηρετεί πολλές χρήσεις, οι περισσότερες από τις οποίες βασίζονται στον έλεγχο ταυτότητας, επιτρέποντας στον υπολογιστή-πελάτη να χρησιμοποιεί πολλούς εταιρικούς πόρους, χωρίς να χρειάζονται μεμονωμένα πιστοποιητικά για κάθε πόρο. Για παράδειγμα, το πιστοποιητικό του υπολογιστή-πελάτη ενδέχεται να επιτρέπει δυνατότητα σύνδεσης VPN, καθώς επίσης πρόσβαση στην τοποθεσία intranet του εταιρικού χώρου αποθήκευσης, σε διακομιστές προϊόντων και στη βάση δεδομένων ανθρώπινου δυναμικού, όπου έχουν αποθηκευτεί τα δεδομένα των υπαλλήλων.

Όπως το πιστοποιητικό του υπολογιστή-πελάτη έτσι και το πιστοποιητικό του διακομιστή VPN ενδέχεται επίσης να εξυπηρετεί πολλές χρήσεις. Το ίδιο πιστοποιητικό ενδέχεται να χρησιμοποιείται στην επαλήθευση της ταυτότητας διακομιστών ηλεκτρονικού ταχυδρομείου, διακομιστών Web ή διακομιστών εφαρμογών. Η αρχή έκδοσης πιστοποιητικών προσδιορίζει τον αριθμό των χρήσεων για κάθε πιστοποιητικό που εκδίδει.

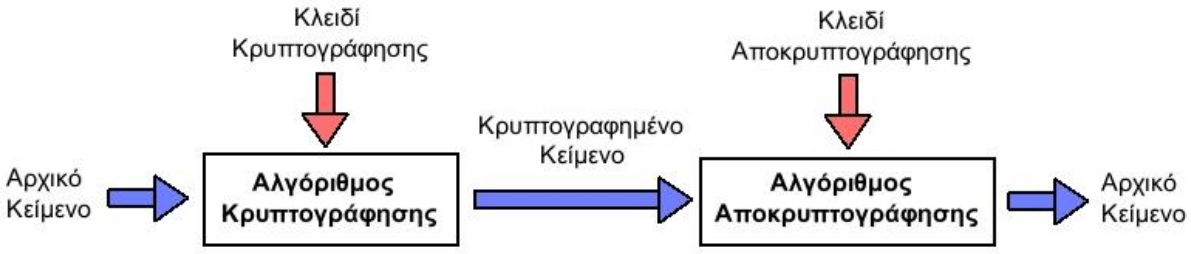


5.1.2 Encryption: «Κρυπτογράφηση»

Κρυπτογράφηση είναι ο μετασχηματισμός δεδομένων σε μορφή που να είναι αδύνατον να διαβαστεί χωρίς την γνώση της σωστής ακολουθίας bit. {Μπορείτε να φανταστείτε την κρυπτογράφηση σαν την ασφάλιση ενός πολύτιμου αντικειμένου σε ένα γερό κιβώτιο με ένα κλειδί}. Τα ευαίσθητα δεδομένα κρυπτογραφούνται με έναν αλγόριθμο κλειδιού, που καθιστά αδύνατη την ανάγνωσή τους χωρίς γνώση του κλειδιού.

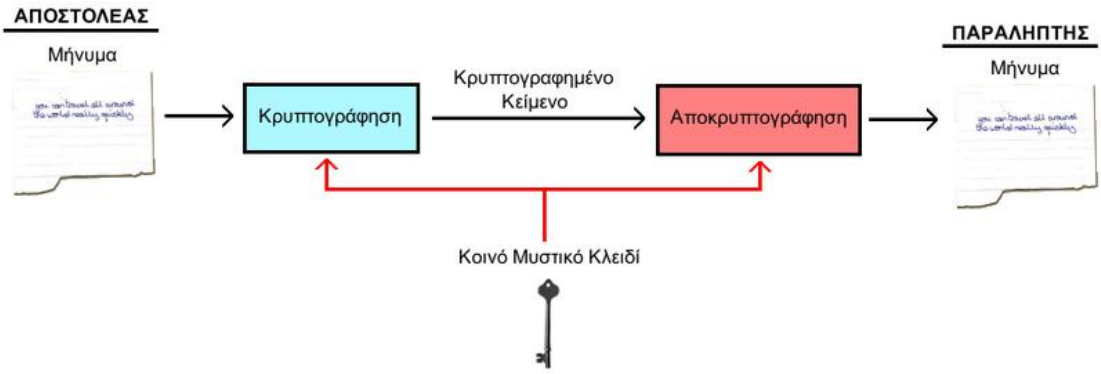
"Κλειδί" καλείται η ακολουθία bit και χρησιμοποιείται σε συνδυασμό με κατάλληλο αλγόριθμο / συνάρτηση.

Τα κλειδιά κρυπτογράφησης δεδομένων καθορίζονται την ώρα που πραγματοποιείται η σύνδεση με τον υπολογιστή του άλλου άκρου. Η χρήση της κρυπτογράφησης δεδομένων μπορεί να αρχίσει από τον υπολογιστή σας ή από το διακομιστή στον οποίο συνδέεστε. Είναι μια διαδικασία που μπορεί να εκτελεστεί τόσο σε hardware όσο και σε software.

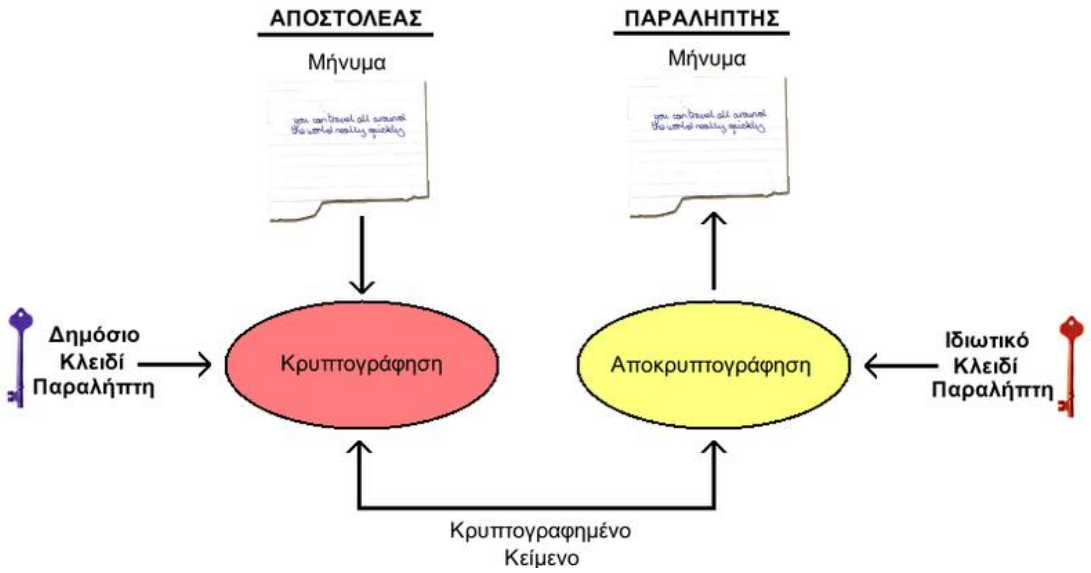


Η αντίστροφη διαδικασία είναι η αποκρυπτογράφηση και απαιτεί γνώση του κλειδιού. Η κρυπτογράφηση και η αποκρυπτογράφηση απαιτούν, το κλειδί. Σε μερικούς μηχανισμούς χρησιμοποιείται το ίδιο κλειδί και για την κρυπτογράφηση και για την αποκρυπτογράφηση, για άλλους όμως τα κλειδιά διαφέρουν. Με βάση αυτό έχουμε δύο είδη κρυπτογράφησης.

Α: **Ασύμμετρη Κρυπτογραφία*(Public-Key Cryptography)***



Β: **Συμμετρική Κρυπτογραφία(*Secret-Key Cryptography*)**



Η **ασύμμετρη κρυπτογραφία** χρησιμοποιεί δύο διαφορετικά κλειδιά για την κρυπτογράφηση και αποκρυπτογράφηση. Κάθε χρήστης έχει στην κατοχή του ένα ζεύγος κλειδιών, το ένα λέγεται δημόσιο κλειδί και το άλλο ιδιωτικό κλειδί. Το δημόσιο κλειδί δημοσιοποιείται, ενώ το ιδιωτικό κλειδί κρατείται μυστικό. Το ιδιωτικό κλειδί δεν μεταδίδεται ποτέ στο δίκτυο και όλες οι επικοινωνίες βασίζονται στα δημόσια κλειδιά. Η μόνη απαίτηση της ασύμμετρης κρυπτογραφίας είναι η εξακρίβωση και επιβεβαιωμένη συσχέτιση των δημόσιων κλείδων με τους κατόχους τους ώστε να μην είναι δυνατή πλαστή αντιγραφή. Η ασύμμετρη κρυπτογράφηση μπορεί να χρησιμοποιηθεί όχι μόνο για κρυπτογράφηση, αλλά και για παραγωγή ψηφιακών υπογραφών.

Στην **συμμετρική κρυπτογραφία**, ο αποστολέας και ο παραλήπτης ενός μηνύματος γνωρίζουν και χρησιμοποιούν το ίδιο μυστικό κλειδί. Ο αποστολέας χρησιμοποιεί το μυστικό κλειδί για να κρυπτογραφήσει το μήνυμα και ο παραλήπτης χρησιμοποιεί το ίδιο κλειδί για να αποκρυπτογραφήσει το μήνυμα. Η συμμετρική κρυπτογραφία χρησιμοποιείται όχι μόνο για κρυπτογράφηση, άλλα και για πιστοποίηση ταυτότητας. Μία τέτοια τεχνική είναι η ***Message Authentication Code (MAC)***.

Το κύριο πρόβλημα της συμμετρικής κρυπτογραφίας είναι η συνεννόηση του αποστολέα και του παραλήπτη στο κοινό μυστικό κλειδί που θα κρυπτογραφεί και αποκρυπτογραφεί όλη την διακινούμενη πληροφορία, χωρίς κάποιον άλλο να λάβει

γνώση αυτού. Πλεονέκτημα της είναι ότι είναι ταχύτερη από την ασύμμετρη κρυπτογραφία.

Τα VPN εφαρμόζουν κύριος ασύμμετρη κρυπτογράφηση με την τεχνική των κρυπτογραφημένων τούνελ για να προστατέψουν τα δεδομένα από το να αλλοιωθούν και να παρακολουθηθούν από παράνομες οντότητες και για να πραγματοποιήσουν, εάν είναι αναγκαίο, ενθυλάκωση πολλαπλών πρωτοκόλλων. Τα Τούνελ παρέχουν λογική από point-to-point σύνδεση σε ένα δίκτυο IP χωρίς μόνιμες συνδέσεις δίνοντας τη δυνατότητα εφαρμογής ανεπτυγμένων χαρακτηριστικών ασφάλειας σε ένα τέτοιο περιβάλλον. Η Κρυπτογράφηση εφαρμόζεται στη σύνδεση με τη διαδικασία των τούνελ με σκοπό το μπέρδεμα των δεδομένων κάνοντάς τα έτσι επεξεργάσιμα μόνο σε αυτούς για τους οποίους προορίζονται και από αυτούς που έχουν το δικαίωμα να τα στείλουν.

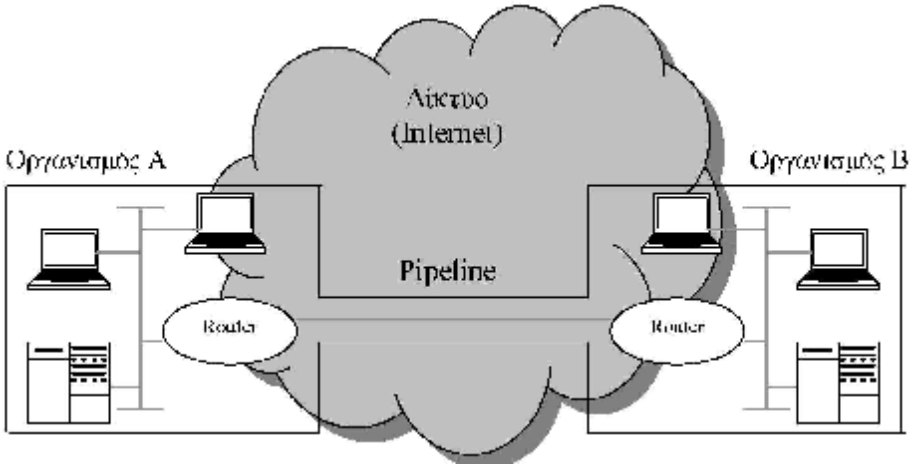
Σε εφαρμογές όπου η ασφάλεια έρχεται σε δεύτερο λόγο, μπορεί να γίνει εφαρμογή της μεθόδου των τούνελ χωρίς τη χρήση κρυπτογράφησης για την παροχή υποστήριξης πολλαπλών πρωτοκόλλων χωρίς εξασφάλιση του απόρρητου.

Τα VPN δίκτυα χρησιμοποιούν την IPSec, δευτέρου επιπέδου πρωτόκολλο σηραγγοποίησης (L2TP), το επίσης δευτέρου επιπέδου πρωτόκολλο προώθησης (L2F), το (GRE) πρωτόκολλο γενικής ενθυλάκωσης με υποστήριξη για τούνελ και τέλος τις πιο ισχυρές τεχνολογίες κρυπτογράφησης DES και 3DES. Επιπλέον τα VPN χρησιμοποιούν μεγάλους διανομείς ηλεκτρονικών πιστοποιητικών όπως VeriSign, Entrust, Netscape, Cisco και άλλες για τη διαχείριση της ασφάλειας/κρυπτογράφησης

Οι Συνδέσεις δικτύου υποστηρίζουν κυρίως δύο τύπους κρυπτογράφησης: Τη Microsoft MPPE, που χρησιμοποιεί την κρυπτογράφηση RSA RC4, καθώς και μια υλοποίηση της ασφάλειας IPSec (Internet Protocol security), που χρησιμοποιεί την κρυπτογράφηση **DES** (**Data Encryption Standard**) και τους αλγόριθμους κρυπτογράφησης Triple DES. Τόσο η MPPE όσο και η IPSec υποστηρίζουν πολλαπλά επίπεδα κρυπτογράφησης.

Επίπεδα κρυπτογράφησης

- **MPPE τυπική** (40 bit, 56 bit)
- **MPPE ισχυρή** (128 bit)
- **IPSec DES** (56 bit)
- **IPSec Triple DES** (3DES, 168-bit)



Με απλά λόγια: αν υποθέσουμε ότι ένας υπολογιστής τις Χ εταιρίας Α.Ε με έδρα την Αθήνα θέλει να επικοινωνήσει με ένας υπολογιστή στο υποκατάστημα της εταιρίας στην Θεσσαλονίκη.

Ο υπολογιστής Α της Αθήνας δημιουργεί ένα αυτοδύναμο πακέτο και το προωθεί στον vpn δρομολογητή ΑΧ (που βρίσκετε στα γραφεία της Αθήνας και συνδέετε με το Ιντερνέτ). Ο δρομολογητή με το λογισμικό vpn (που έχει από την ανάλογη εταιρία vpn δικτύων και παροχής CA) κρυπτογραφεί το αυτοδύναμο πακέτο και το ενθυλακώνει σε ένα νέο πακέτο που το προωθεί στον δρομολογητή ΒΧ μέσω του Ιντερνέτ και της σήραγγας.

Ο δρομολογητής ΒΧ των γραφείων την Θεσσαλονίκης, αποκρυπτογραφεί το πακέτο με το ιδιωτικό κλειδί που έχει σε αντιστοιχία με το δημόσιο κλειδί και ελέγχοντας το πιστοποιητικό για την εδραίωση της σύνδεσης προωθεί το αρχικό αυτοδύναμο πακέτο στο υπολογιστή Β της Θεσσαλονίκης.

5.1.3. Integrity: «Ακεραιότητα»

Ακεραιότητα δεν είναι κάτι παραπάνω από αυτό που λέει και η ίδια η λέξη. Στην ουσία είναι ο σκοπός των δύο προηγουμένων τεχνικών αλλά και των δικτύων VPN. Να παραδίδεται στον παραλήπτη το μεταβιβαζόμενο πακέτο, χωρίς αυτό να έχει αλλοιωθεί ή σε περίπτωση που αυτό έχει υποστεί κάποια αλλοίωση να είναι δυνατή η επιδιόρθωση του.

Ο λόγος που εξετάζεται σαν ανεξάρτητο κομμάτι τις ασφάλειας είναι ότι, είναι η ίδια η ασφάλεια. Η κρυπτογράφηση και η πιστοποίηση έχει να κάνει, με εξωγενείς κινδύνους. Υπάρχουν και άλλοι λόγοι, πού μπορεί να οδηγήσουν σε αλλοίωση της

πληροφορίας που μεταβιβάζεται ή της κακής χρήσης αυτής. Για την διασφάλιση της ακεραιότητας πρέπει να τηρούνται και κάποιοι εσωτερικοί μηχανισμοί του δικτύου.

1. ***Εσωτερική Εμπιστευτικότητα*** δηλαδή η διασφάλιση της πληροφορίας από οποιονδήποτε δεν έχει το δικαίωμα να την δει ή να κρατήσει αντίγραφό της. Είτε με την κωδικών κλειδώματος ενός αρχείου, είτε με την επιλεκτική άδεια πρόσβασης. Αυτός ο τύπος ασφάλειας περιλαμβάνει τόσο την προστασία του συνόλου της πληροφορίας όσο και μέρους της το οποίο από μόνο του μπορεί να δείχνει άκακο αλλά που μπορεί να οδηγήσει στην αποκάλυψη άλλων σημαντικών πληροφοριών.
2. ***Καταγραφή*** ο διαχειριστής ενός δικτύου δεν πρέπει να ανησυχεί μόνο για τους χρήστες χωρίς άδεια πρόσβασης αλλά και για εκείνους που αν και νόμιμοι κάνουν λάθη ή προκαλούν σκόπιμα κάποιο πρόβλημα. Σε τέτοιες περιπτώσεις πρέπει να καθορισθεί τι έχει γίνει, από ποιόν και τι επηρεάστηκε. Ο μόνος τρόπος να επιτύχουμε όλα τα παραπάνω είναι να κάνουμε χρήση κάποιων αρχείων καταγραφής της δραστηριότητας στο σύστημα το οποίο να είναι ικανό να μας δώσει πληροφορίες για το ποιος και τι έκανε.
3. ***Διαθεσιμότητα*** Αφορά την προστασία των υπηρεσιών έτσι ώστε να μην υποβαθμιστεί η δυνατότητα παροχής τους. Εάν κάποια στιγμή ζητηθεί μια συγκεκριμένη υπηρεσία από νόμιμο χρήστη και δεν του δοθεί, αυτό ισοδυναμεί με την απώλεια της πληροφορίας που βρίσκεται στο σύστημα.
4. ***Έλεγχος*** πρόσβασης στο σύστημα. Αν και όλες οι παραπάνω μορφές / υπηρεσίες ασφάλειας είναι εξίσου σημαντικές, διαφορετικοί οργανισμοί δίνουν διαφορετική προτεραιότητα στη καθεμία διότι αντιμετωπίζουν διαφορετικού είδους απειλές.

Γι’ αυτό και η ακεραιότητα έχει να κάνει με το είδος της πληροφορίας που μεταφέρεται στο δίκτυο. Για παράδειγμα σε ένα πανεπιστημιακό περιβάλλον πιο σημαντικά θεωρούνται η ακεραιότητα και η διαθεσιμότητα της πληροφορίας, ενώ σε ένα περιβάλλον σχετιζόμενο με την εθνική ασφάλεια το οποίο επεξεργάζεται απόρρητες πληροφορίες, η εμπιστευτικότητα έρχεται πρώτη και η διαθεσιμότητα τελευταία

Πολιτική ασφαλείας

Οι πολιτικές ασφάλειας είναι ένα θεμελιώδες μέρος της ασφάλειας, και τα VPNs δεν αποτελούν εξαίρεση. Πέραν αυτού τα VPNs αντιπροσωπεύουν μια τεράστια αλλαγή στην μέχρι τώρα φιλοσοφία της ασφάλειας, λόγω του ότι η διακίνηση πληροφοριών γίνετε μέσω διαδικτύου.

Η έννοια, «πολιτικές ασφάλειας» είναι κάτι που ξεκίνησε με την δημιουργία των πρώτων δικτύων και η ανάγκη ύπαρξης της περιγράφηκε και αναλύθηκε από πολλούς. Κυρίως όμως σε μικρά και κλειστά δίκτυα, που απλά συνδέονται στο διαδίκτυο και δεν έχουν ως βάση τους το ίδιο το διαδίκτυο. Εντούτοις, το ζήτημα της ασφάλειας εξ' αποστάσεως πρόσβασης μέσω διαδικτύου δεν έχει αντιμετωπιστεί ποτέ, σε αναλογία με τον ογκώδη αριθμό ευαίσθητων πληροφοριών που διακινούν τα VPNs μέσω Διαδικτύου.

5.1.4 Tunneling: Σήραγγες και Firewall: Τοίχος Προστασίας

Με βάση τον τρόπο που λειτουργούν τα Ιδεατά Ιδιωτικά Δίκτυα, μπορούν να χωριστούν σε δύο κατηγορίες. Στα **Ασφαλή Ιδεατά Ιδιωτικά Δίκτυα** (SVPN) και στα **Έμπιστα**(TVPN). Τα ασφαλή VPN χρησιμοποιούν πρωτόκολλα κρυπτογράφησης και μεταφέρουν τα δεδομένα μέσω «σηράγγων», που σημαίνει ότι τα πακέτα ενθυλακώνονται μέσα σε άλλα πακέτα και στέλνονται έτσι μέσα στο δίκτυο με σκοπό την απόκρυψη του περιεχομένου τους και την επίτευξη της ιδιωτικότητας. Μερικά από αυτά τα πρωτόκολλα είναι τα **IPsec** (IP security), **SSL** (Secure Sockets Layer), **PPTP** (point-to-point tunneling protocol), **L2TP** (Layer 2 Tunnelling Protocol), **L2TPv3** (Layer 2 Tunnelling Protocol version 3) τα οποία υιοθετούν διαφορετικές τεχνικές για την ασφαλή μεταφορά των δεδομένων. Απώτερος σκοπός όλων όμως είναι η παροχή αξιόπιστων μεταδόσεων πάνω από αναξιόπιστα δίκτυα, όπως το Internet. Από την άλλη πλευρά τα Έμπιστα VPN δεν χρησιμοποιούν κρυπτογράφηση και τεχνικές με σήραγγες, αλλά εμπιστεύονται την άμυνά τους στη χρησιμοποίηση του δικτύου ενός μόνο παρόχου για να προστατέψουν τις επικοινωνίες τους. Τέτοια δίκτυα είναι τα **MPLS VPN** και το **L2F** (Layer 2 Forwarding).

MPLS VPN δίκτυο παρέχει στην Ελλάδα ο ΟΤΕ . Ένα τέτοιο δίκτυο έχει ως βασικό σκοπό να εξασφαλίσει την επικοινωνία κάθε απομακρυσμένου

γραφείου/καταστήματος ή ακόμα και μετακινούμενου στελέχους με τα κεντρικά γραφεία της επιχείρησης ή οποιοδήποτε άλλο σημείο ανήκει στο εν λόγω δίκτυο (any to any επικοινωνία), σύμφωνα με τις συγκεκριμένες προδιαγραφές που έχει θέσει ο πελάτης. Η επικοινωνία αυτή συνήθως αφορά τη λειτουργία επιχειρησιακών εφαρμογών, τη μεταφορά αρχείων, την τηλεφωνική επικοινωνία μεταξύ των σημείων, τη πρόσβαση στο διαδίκτυο και στο ηλεκτρονικό ταχυδρομείο αλλά και οποιαδήποτε άλλη ανάγκη θέλει να καλύψει ο πελάτης.

Με την ραγδαία ανάπτυξη των VPNs, έχει υπάρξει ένα τεράστιο ζήτημα ως αναφορά την εφαρμογή της ασφάλειας και τη προστασία των εταιρικών απορρήτων. Η βιομηχανία ασφάλειας πρέπει να δει ακόμα μια φορά την ευπάθεια των VPNs.

Η έκθεση σε πληροφορίες είναι τόσο μεγάλη που πολλοί έχουν αγνοήσει τα προφανή. Σε μερικές περιπτώσεις, οι άνθρωποι βλέπουν ότι υπάρχει ένα θεμελιώδες ζήτημα με την ασφάλεια των πληροφοριών πέρα από την προφανή επικοινωνία που παρέχεται από το IPSec, αλλά είναι τοποθετημένο σε χαμηλή προτεραιότητα.

Ένα παράδειγμα είναι ο διαχωρισμός των σηράγγων επικοινωνίας εναντίον των ενιαίων σηράγγων. Αρκετοί θεωρούν ότι η υιοθέτηση ενιαίων σηράγγων θα αποτρέψει την πειρατεία Όταν μια ενιαία σήραγγα υποστηρίζεται, πολλοί ξεχνάνε ότι ακόμα παραμένει μια σύνδεση IP με το Internet. Εάν το επίπεδο που εφαρμόζεται (OSI) η ασφάλεια που απαιτείται για να υποκλαπεί ένα IPSec VPN είναι διαθέσιμο σε έναν υποκλοπέα, η αλληλεπίδραση με την IP σύνδεση ενός συστήματος είναι πολύ λιγότερο περίπλοκη. Έτσι η απόπειρα υποκλοπής γίνεται με την χρήση μιας εφαρμογής και αυτό δίνει την δυνατότητα στον υποκλοπέα να καθοδηγηθεί μέσω του πελάτη (απομακρυσμένο χρηστή) στο εσωτερικό δίκτυο.

Στην περίπτωση της ενιαίας σήραγγας ο υποκλοπέας αντιμετωπίζει μια μεγαλύτερη πρόκληση στο να μπορέσει να χωρίσει τη σήραγγα. Με αυτό τον τρόπο, μπαίνοντας μέσω ενός μακρινού συστήματος και με την χρήση ενιαίας σήραγγας δεν μπορεί να γίνει λήψη και εγκατάσταση μιας **Trojan**[24] εφαρμογή υποκλοπής, που μπορεί κρύβεται πίσω από τα μεταφερόμενα δεδομένα. Αυτό ώμος δεν είναι αληθές γιατί ένα Trojan μπορεί να εκτελεστεί σε πολλούς στόχους και επιτρέπει στον εισβολέα να αναμιχθεί μόνο όταν χρειάζεται - μειώνοντας την έκθεση του στο σύστημα και διατηρήσει την ανωνυμία του.

[24] **Trojan**: είναι ένα κακόβουλο πρόγραμμα που ξεγελάει τον χρήστη και τον κάνει να πιστεύει ότι εκτελεί κάποια χρήσιμη λειτουργία ενώ στα κρυφά εγκαθιστά στον υπολογιστή του άλλα κακόβουλα προγράμματα.

Απλά λοιπόν τίθεται ζήτημα , αν υπάρχει ένα επίπεδο στο οποίο οι διάφορες επιθέσεις μπορούν να συγκριθούν ενάντια στο πραγματικό επίπεδο αποδεκτού κινδύνου.

Οι σήραγγες VPN είναι εδραιωμένη σύνδεση ασφαλών γραμμών στης οποίες μπορείς να στέλνεις και να λαμβάνεις δεδομένα μέσω ενός δημόσιου δικτύου ή του internet. Η σήραγγα λειτουργεί όπως το μετρό, μεταφέρει από ένα σημείο σε άλλο.

Τα πρωτόκολλα διαχείρισης που περιλαμβάνονται στο λογισμικό εδραίωσης της σήραγγας, λειτουργούν ως πύλη για τον χρήστη. Ελέγχουν το άνοιγμα και κλείσιμο της σήραγγας μετά από αίτηση του χρηστή, για μεταφορά δεδομένων στην σήραγγα.

Η αποστολή πληροφοριών μέσω της σήραγγας, απαιτεί ένα datagram[25] με βάση το πρωτόκολλο, εξασφαλίζοντας ότι τα δύο τελικά σημεία έχουν τις ίδιες παραμέτρους (διεύθυνση IP παρόμοια, κρυπτογράφηση δεδομένων και συμπίεση). Για τη ασφαλή θέσπιση την εικονική σύνδεση, τα δεδομένα είναι κωδικοποιημένα όταν αποστέλλονται ή κρυπτογραφούνται πριν μεταδοθούν μέσω της σήραγγας..

Η σήραγγα γίνεται από τον μεταγωγέα του δικτύου. Αυτός θεσπίζει τη σειρά, του ελέγχου ταυτότητας και εδραιώνει την σύνδεση των διακομιστώ του VPN.

Υπάρχουν κύρια 3 πρωτοκόλλα απομακρυσμένης πρόσβασης μέσω σηράγγων VPN. Το πρώτο είναι το PPTP , το δεύτερο το L2TP και το τρίτο το L2F όπως αναφέραμε και παραπάνω.

Το τείχος προστασίας από την άλλη είναι ένα σημαντικό κομμάτι του εξοπλισμού σε μια επιχείρηση που συνδέει τον οποιαδήποτε στον δίκτυο της μέσω Internet. Μερικά από τα τείχη προστασίας παρέχουν ικανοποιητική πρόσβαση μέσω VPN, ενώ άλλα βασίζονται στις VPN πύλες που λειτουργούν παράλληλα και παρέχουν την πρόσβαση στο εσωτερικό δίκτυο.

Το τείχος προστασίας είναι λογισμικό ή υλικό και ελέγχει τις πληροφορίες, οι οποίες έρχονται η φεύγουν σε έναν υπολογιστή από το Internet ή ένα δίκτυο. Το τείχος προστασίας παρεμβάλλεται ανάμεσα σε δύο δίκτυα που έχουν διαφορετικό επίπεδο εμπιστοσύνης. Το Διαδίκτυο έχει μικρό βαθμό εμπιστοσύνης, ενώ το εταιρικό δίκτυο διαθέτει μεγάλο βαθμό εμπιστοσύνης. Ο σκοπός της τοποθέτησης

[25] **Δεδομενόγραμμα (datagram)** (ή *αυτοδύναμο πακέτο*), αναφέρεται ειδικά στα πακέτα που ενθυλακώνονται από μια “αναξιόπιστη” (ασυνδεσμική) υπηρεσία. Μια “αξιόπιστη υπηρεσία” είναι αυτή η οποία ειδοποιεί το χρήστη σε περίπτωση απώλειας κατά τη μεταφορά ενός πακέτου, ενώ μια “αναξιόπιστη” υπηρεσία δεν ειδοποιεί σε περίπτωση απώλειας. Ο όρος αυτός, χρησιμοποιείται κυρίως για να περιγράψει τα πακέτα των πρωτοκόλλων του Επιπέδου Δικτύου (π.χ. IP datagram, UDP datagram).

ενός τείχους προστασίας είναι είτε να αποκλείει είτε να επιτρέπει να περάσουν αρχεία και δεδομένα στον υπολογιστή, ανάλογα με τις ρυθμίσεις του. Ακόμη κι αν πιστεύουμε ότι δεν υπάρχει τίποτα στον έναν υπολογιστή που θα ενδιέφερε κάποιον, ένας ιός τύπου worm[26] θα μπορούσε να θέσει εκτός λειτουργίας τον υπολογιστή ή κάποιος άλλος θα μπορούσε να χρησιμοποιήσει τον υπολογιστή για να εξαπλώσει ιούς σε άλλους υπολογιστές χωρίς να το αντιλαμβανόμαστε.

Παρόλα αυτά όμως, ένα τείχος προστασίας μπορεί να αποδειχθεί άχρηστο εάν δεν ρυθμιστεί σωστά. Η σωστή πρακτική είναι να ρυθμίζεται ούτως ώστε να απορρίπτει όλες τις συνδέσεις που δεν ικανοποιούν τα κριτήρια εμπιστοσύνης του VPN δικτυού χωρίς όμως να απορρίπτει και πακέτα που έχουν μικρότερη σημασία με χαμηλότερο επίπεδο σε ασφάλεια.. Για να ρυθμιστεί σωστά θα πρέπει ο διαχειριστής του δικτύου να έχει μία ολοκληρωμένη εικόνα για τις ανάγκες του δικτύου.

Υπάρχουν τριών ειδών τοίχοι ασφαλείας:

- **Φίλτρα πακέτων** (Packet filters)

  Ένα φίλτρο πακέτων εξετάζει στα εισερχόμενα πακέτα τις IP διευθύνσεις πηγής και προορισμού και επιτρέπουν τη διέλευση, με βάση τους κανόνες που έχει θέσει ο διαχειριστής του VPN δικτύου.

- **Πύλες ασφαλείας** (security gateways (proxies))

  Οι πύλες ασφαλείας επιτρέπουν στους χρήστες να χρησιμοποιούν έναν proxy server[27] προκειμένου να επικοινωνήσουν με ασφαλή συστήματα.

- **Έξυπνα φίλτρα** (Smart filters ή stateful inspections firewalls)

  Αυτά βασίζονται στην τεχνική **Stateful Multi-Layer Inspection** (SMLI).

Στόχος τους εκτός της μέγιστης δυνατής ασφάλειας, είναι και η βέλτιστη δυνατή απόδοση. Τα έξυπνα φίλτρα μοιάζουν με πύλες ασφαλείας, υπό την έννοια ότι

[26] **Worm**: είναι ένα αυτοαναπαραγόμενο και κακόβουλο πρόγραμμα υπολογιστή, το οποίο χρησιμοποιεί δίκτυο υπολογιστών για να στείλει αντίγραφα του εαυτού του σε άλλους κόμβους (υπολογιστές του δικτύου) και μπορεί να το πράξει χωρίς την παρέμβαση του χρήστη. Το γεγονός αυτό οφείλεται σε κενά ασφαλείας του υπολογιστή προορισμού.

[27] **Proxy server**: είναι ένας διακομιστής που έχει στόχο να βελτιώσει την ταχύτητα πλοήγησης στο διαδίκτυο και παράλληλα να μειώσει την κίνηση του δικτύου προς το διαδίκτυο. Τοποθετείται ενδιάμεσα των χρηστών και του διαδικτύου. Λαμβάνει τα αιτήματα ιστοσελίδων από έναν χρήστη, προσκομίζει τη σελίδα από το Διαδίκτυο, και έπειτα την δίνει στον υπολογιστή που την ζήτησε. Ο proxy server μπορεί να είναι και μέρος ενός τείχους προστασίας και μπορεί να αποτρέπει τους χάκερς από το να χρησιμοποιήσουν το διαδίκτυο για να αποκτήσουν πρόσβαση σε υπολογιστές ενός ιδιωτικού δικτύου.

εξετάζουν όλο το πακέτο, χρησιμοποιούν όμως ειδικούς αλγορίθμους για να καθορίζουν τη διέλευση των εισερχόμενων πακέτων. Ένα έξυπνο φίλτρο κλείνει όλες τις TCP θύρες και τις ανοίγει δυναμικά, όταν κάποιες συνδέσεις τις χρειάζονται. Λόγω της μεγάλης ασφάλειας που παρέχουν χρησιμοποιούνται κατά κόρον στα VPN – αν και συνδυάζονται και με πύλες ασφαλείας, για αυθεντικοποίηση.

5.1.5 Πρωτόκολλο Διαχείρισης Κλειδιών Internet IKE

Το IKE δημιουργεί ένα πιστοποιημένο και ασφαλές κανάλι σήραγγα μεταξύ δύο οντοτήτων και κατόπιν διαπραγματεύεται τους συσχετισμούς ασφάλειας για την IPSec. Αυτή η διαδικασία απαιτεί από τις δύο οντότητες να πιστοποιήσουν η μία την άλλη και να μοιράσουν κλειδιά.

Πιστοποίηση Ταυτότητας

Τα δύο μέρη πρέπει να πιστοποιήσουν το ένα το άλλο. Το IKE είναι πολύ ευέλικτο και υποστηρίζει πολλές διαφορετικές μεθόδους πιστοποίησης της ταυτότητας. Οι δύο οντότητες πρέπει να συμφωνήσουν σε ένα κοινό πρωτόκολλο πιστοποίησης μέσω μιας κατάλληλης διαδικασίας. Σε αυτή τη φάση υλοποιούνται συνήθως οι παρακάτω μηχανισμοί :

- Προ-Μοιρασμένα Κλειδιά. Το ίδιο κλειδί προ-εγκαθίσταται και στις δύο μηχανές. Κατά την πιστοποίηση αποστέλλεται από τη μία μηχανή στην άλλη μία επεξεργασμένη μορφή (με τη βοήθεια μιας hash συνάρτησης) του ίδιου κλειδιού. Εάν αυτή η μορφή συμπίπτει με αυτήν που υπολογίζεται τοπικά σε κάθε μηχανή, τότε η διαδικασία πιστοποίησης έχει θετικό αποτέλεσμα.
- Κρυπτογράφηση Δημοσίων Κλειδιών. Κάθε μηχανή "γεννάει" έναν ψευδο-τυχαίο αριθμό τον οποίο και κρυπτογραφεί με το δημόσιο κλειδί της άλλης μηχανής. Η πιστοποίηση επιτυγχάνεται μέσω της ικανότητας των μηχανών να υπολογίσουν μια hash συνάρτηση του τυχαίου αριθμού αποκρυπτογραφώντας με τα private keys (ιδιωτικά κλειδιά) ότι λαμβάνουν από το συνομιλητή τους. Το σύστημα παρέχει ακόμα και δυνατότητα άρνησης συμμετοχής σε οποιαδήποτε διαδικασία πιστοποίησης. Προς το παρόν μόνο ο αλγόριθμος δημοσίων κλειδιών της RSA υποστηρίζεται.

- Ψηφιακές Υπογραφές**.** Κάθε συσκευή υπογράφει ψηφιακά ένα σύνολο δεδομένων και τα στέλνει στην άλλη. Αυτή η μέθοδος είναι παρόμοια με την προηγούμενη μόνο που δεν παρέχει μηχανισμό άρνησης της εμπλοκής της σε κάποια προσπάθεια πιστοποίησης. Προς το παρόν υποστηρίζονται τόσο ο αλγόριθμος δημοσίων κλειδιών της RSA όσο και οι προδιαγραφές ψηφιακών υπογραφών (DSS).

Τόσο η διαδικασία κρυπτογράφησης όσο και αυτή των ψηφιακών υπογραφών απαιτεί τη χρήση ψηφιακών πιστοποιητικών για την επικύρωση της δημόσιας σε ιδιωτική αντιστοίχησης. Το IKE επιτρέπει την ανεξάρτητη ανταλλαγή των ψηφιακών πιστοποιητικών με τη χρήση για παράδειγμα του DNSSEC ή την ανταλλαγή τους σαν μέρος του IKE.

Ανταλλαγή Κλειδιών

Τα δύο μέρη πρέπει να έχουν ένα κοινό, έστω προσωρινό, κλειδί έτσι ώστε να κρυπτογραφήσουν το IKE τούνελ. Το πρωτόκολλο **Diffie-Helman** χρησιμοποιείται για τη συμφωνία σε ένα κοινό κλειδί. Η ανταλλαγή πιστοποιείται όπως περιγράφηκε παραπάνω για τη αποφυγή επιθέσεων παρεμβολών.

Το IPSec περιλαμβάνει, εκτός από την επεξεργασία των πακέτων μέσω των κεφαλίδων AH και ESP, και πρωτόκολλα ανταλλαγής του κλειδιού. Μετά από εξέταση πολλών εναλλακτικών λύσεων για τη διαχείριση του κλειδιού, η IETF επέλεξε το **IKE (Internet Key Exchange)** σαν τον τρόπο ρύθμισης των συσχετίσεων ασφάλειας για το IPSec.

Το IKE (επέκταση του προϋπάρχοντος ISAKMP/Oakley πρωτοκόλλου) δημιουργεί ένα πιστοποιημένο και ασφαλές κανάλι (tunnel) μεταξύ δύο οντοτήτων και κατόπιν διαπραγματεύεται τις συσχετίσεις ασφάλειας για το IPSec. Αυτή η διαδικασία απαιτεί από τις δύο οντότητες να πιστοποιήσουν η μία την άλλη και να μοιράσουν κλειδιά. Οι δύο οντότητες πρέπει να συμφωνήσουν σε ένα κοινό πρωτόκολλο πιστοποίησης μέσω μιας κατάλληλης διαδικασίας. Σε αυτή τη φάση υλοποιούνται συνήθως οι παρακάτω μηχανισμοί :

- **Προ-Μοιρασμένα Κλειδιά**—Το ίδιο κλειδί προ-εγκαθίσταται και στις δύο μηχανές. Κατά την πιστοποίηση αποστέλλεται από τη μία μηχανή στην άλλη μία επεξεργασμένη μορφή (με τη βοήθεια μιας συνάρτησης

κατακερματισμο) του ίδιου κλειδιού. Εάν αυτή η μορφή συμπίπτει με αυτήν που υπολογίζεται τοπικά σε κάθε μηχανή, τότε η διαδικασία πιστοποίησης έχει θετικό αποτέλεσμα.

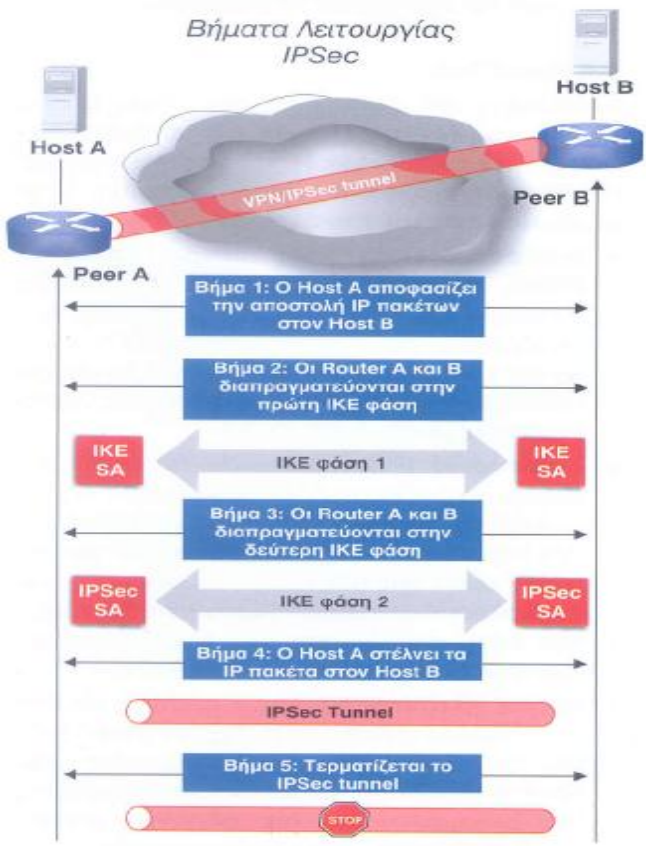
- **Κρυπτογράφηση Δημοσίων Κλειδιών**—Κάθε μηχανή παράγει έναν ψευδο-τυχαίο αριθμό τον οποίο και κρυπτογραφεί με το δημόσιο κλειδί (public key) της άλλης μηχανής. Η πιστοποίηση επιτυγχάνεται μέσω της ικανότητας των μηχανών να υπολογίσουν μια συνάρτηση κατακερματισμού του τυχαίου αριθμού, αποκρυπτογραφώντας με τα ιδιωτικά κλειδιά (private keys) ότι λαμβάνουν από το συνομιλητή τους. Υποστηρίζεται μόνο ο αλγόριθμος δημοσίων κλειδιών RSA.
- **Ψηφιακές Υπογραφές**—Κάθε συσκευή υπογράφει ψηφιακά ένα σύνολο δεδομένων και τα στέλνει στην άλλη. Ο αποστολέας χρησιμοποιεί το κρυφό του ιδιωτικό κλειδί για να υπογράψει ηλεκτρονικά τα δεδομένα του. Ο αποδέκτης του κειμένου χρησιμοποιεί το public key του αποστολέα, το οποίο έτσι και αλλιώς γνωρίζει αφού είναι δημόσιο, για να ελέγξει την υπογραφή του αποστολέα. Αν αυτός ο έλεγχος είναι επιτυχής, αυτό σημαίνει ότι το κείμενο δεν έχει αλλαχθεί και έχει πιστοποιηθεί η ταυτότητα του αποστολέα υποστηρίζονται τόσο ο αλγόριθμος δημοσίων κλειδιών της RSA όσο και οι προδιαγραφές ψηφιακών υπογραφών (DSS).

Μετά την πιστοποίηση της ταυτότητας του κάθε χρήστη, πρέπει να υπάρξει η ανταλλαγή του κλειδιού που θα χρησιμοποιηθεί για την κρυπτογράφηση των δεδομένων που θα σταλούν μετέπειτα, κατά την επικοινωνία των δύο χρηστών. Ως βασικό αλγόριθμο ανταλλαγής κλειδιού το IKE υποστηρίζει τον Diffie-Hellman, αν και μπορεί να υπάρξουν και άλλοι.

Diffie-Hellman: Μηχανισμός ανταλλαγής κλειδιών που αναπτύχθηκε από τους Diffie και Hellman το 1976. Επιτρέπει σε δύο χρήστες να ανταλλάσσουν ένα μυστικό κλειδί μέσα από ένα μη ασφαλές κανάλι. Είναι ένας κρυπτογραφικός αλγόριθμος δημοσίου κλειδιού. Το πρωτόκολλο έχει δύο παραμέτρους (αριθμούς): p και g. Το p είναι ένας πολύ μεγάλος πρώτος αριθμός και το g είναι ένας αριθμός με την ιδιότητα $g^k \neq 1 \bmod p$ για όλους τους k από 1 μέχρι p-2 (δηλαδή, στοιχείο-γεννήτορας (generator) στο σώμα των ακεραίων Modulo p). Τα p,g τα γνωρίζουν όλοι

– είναι δημοσίως γνωστά. Ας υποθέσουμε τώρα ότι δύο χρήστες, ο Α και ο Β, θέλουν να συμφωνήσουν για ένα μυστικό κλειδί. Πρώτα, ο Α παράγει μία τυχαία τιμή x και ο Β μία τυχαία τιμή y (όπου τα x,y είναι μικρότερα του p). Τα x,y κρατούνται μυστικά – μόνο ο Α δηλαδή γνωρίζει το x και μόνο ο Β το y. Στη συνέχεια ο Α υπολογίζει τον αριθμό $x' = g^x \bmod p$ και ο Β τον αριθμό $y' = g^y \bmod p$. Κατόπιν, ο ένας στέλνει στον άλλον τις τιμές αυτές. Τέλος, ο Α κάνει τον υπολογισμό $(y')^x = g^{xy} \bmod p$ και ο Β κάνει με την σειρά του τον υπολογισμό $(x')^y = g^{xy} \bmod p$. Συνεπώς και οι δύο υπολογίζουν τον ίδιο αριθμό – ο οποίος θα είναι το μυστικό κλειδί που θα χρησιμοποιήσουν. Η ασφάλεια του πρωτοκόλλου αυτού βασίζεται στο γεγονός ότι ένας επιτιθέμενος, ο οποίος παρακολουθεί το τι ανταλλάσσουν οι Α και Β, δεν μπορεί από τα x', y' να υπολογίσει το μυστικό κλειδί: για να το κάνει αυτό θα πρέπει να ξέρει είτε το x είτε το y. Όμως, όταν τα p και g είναι πολύ μεγάλα, το να ξέρει κανείς το x' ή το y' δεν του αρκεί για να βρει το x ή το y.

Ο ακριβής ρόλος του IKE για τη διεκπαιρέωση μίας IPSec επικοινωνίας μεταξύ δυο ή περισσότερων συσκευών αντικατοπτρίζεται στην ακόλουθη διαδοχή βημάτων που λαμβάνουν χώρα σε μία IPSec ανταλλαγή δεδομένων



- **Ενεργοποίηση μιας IPSec συνόδου**. Στο βήμα αυτό καθορίζεται το σύνολο των IP πακέτων που πρόκειται να προστατευθούν μέσω του IPSec.
- **IKE - Πρώτη φάση**. Δημιουργία και λειτουργία της IKE Συσχέτισης Ασφαλείας.
- **IKE – Δεύτερη φάση**. Δημιουργία και λειτουργία της AH/ESP Συσχέτισης Ασφαλείας
- **Μεταφορά Δεδομένων**. Τα IP πακέτα που επιλέχθηκαν από το πρώτο βήμα μεταφέρονται.
- **Τερματισμός της IPSec συνόδου**. Εφόσον ολοκληρωθεί η μεταφορά των IP πακέτων και δεν χρησιμοποιείται η παραπάνω σύνοδος, η τελευταία τερματίζεται.

Στην **πρώτη φάση IKE** μέσω των IKE SAs προετοιμάζεται το έδαφος για την επόμενη διαπραγμάτευση των άλλων πρωτοκόλλων ασφάλειας του IPSec (όπως το AH και το ESP πρωτόκολλο). Στην πραγματικότητα υλοποιείται η διαχείριση των κλειδιών μέσω του IKE.

Οι κυριότερες λειτουργίες που συναντάμε στη πρώτη φάση του IKE είναι οι εξής:

- **Πιστοποίηση των μελών** που συμμετέχουν σε μια IPSec επικοινωνία.
- **Ανάπτυξη μιας ή περισσότερων πολιτικών ασφάλειας** IKE βασισμένες στη γενική πολιτική ασφάλειας ενός οργανισμού. Κάθε πολιτική απαιτεί την λήψη αποφάσεων για πέντε βασικές επιλογές ασφάλειας: *μέθοδος πιστοποίησης, αλγόριθμος κρυπτογράφησης, αλγόριθμος κατακερματισμού (για έλεγχο της ακεραιότητας δεδομένων),* παράμετροι του *Diffie - Hellman αλγορίθμου (που προσδιορίζει το μέγεθος κλειδιού) και διάρκεια ζωής μίας SA*. Οι διαφορετικές πολιτικές μπορεί να απαιτούνται παραδείγματος χάριν στη περίπτωση που ένα IPSec συμβαλλόμενο μέρος δεν υποστηρίζει κάποια από τις παραπάνω μεθόδους ή αλγόριθμους.
- **Εκτέλεση αλγόριθμου** Diffie-Hellman για την δημιουργία ενός ή περισσοτέρων κοινών μυστικών κλειδιών.
- **Δημιουργία ασφαλούς «διόδου»** (tunneling) για την ολοκλήρωση της επόμενης (δεύτερης) IKE φάσης.

Η πρώτη φάση του IKE μπορεί να πραγματοποιηθεί με δυο τρόπους: είτε τον κύριο τρόπο (main) είτε τον επιθετικό (aggressive). Με τον πρώτο τρόπο έχουμε συνολικά τρεις ανταλλαγές μηνυμάτων και προς τις δυο κατευθύνσεις μεταξύ των συμβαλλόμενων μερών μιας IPSec επικοινωνίας (σχήμα 17), ενώ με τον δεύτερο τρόπο οι παραπάνω ανταλλαγές συμπτύσσονται σε μια μόνο ανταλλαγή με τρία στάδια (αποστολέας - δέκτης, δέκτης - αποστολέας, αποστολέας - δέκτης).

Οι ανταλλαγές μηνυμάτων που λαμβάνουν χώρα στην πρώτη φάση του IKE είναι οι εξής:

Πρώτη Ανταλλαγή. Σε αυτή καθορίζονται οι αλγόριθμοι ασφάλειας (κρυπτογράφησης) και πιστοποίησης ταυτότητας οι οποίοι πρόκειται να χρησιμοποιηθούν στα επόμενα βήματα. Για κάθε μια κατεύθυνση μία ξεχωριστή Συσχέτιση Ασφαλείας (SA) δημιουργείται με πληροφορίες που περιλαμβάνουν τους αλγόριθμους κρυπτογράφησης και πιστοποίησης που υποστηρίζονται από το κάθε άκρο της συνομιλίας, τον αλγόριθμο παραγωγής κοινού μυστικού κλειδιού (συμφωνία αρχικών παραμέτρων του Diffie-Hellman αλγορίθμου), τον χρόνο διάρκειας της πρώτης IKE φάσης, τον τρόπο πιστοποίησης που θα χρησιμοποιηθεί (π.χ. προμοιρασμένα κλειδιά) κ.ο.κ. Στο τέλος της παραπάνω διαδικασίας καθένας από τα IPSec «συνομιλούντες» διαθέτει μία κοινή IKE SA.

Δεύτερη Ανταλλαγή. Εφόσον επέλθει συμφωνία με τις προτεινόμενες παραμέτρους, εκτελείται ο αλγόριθμος παραγωγής κοινού μυστικού κλειδιού (Diffie-Hellman) μέσω του οποίου παράγεται ένα κλειδί που είναι κοινό και στα δύο μέρη. Ο εν λόγω αλγόριθμος είναι κρίσιμος στις διαδικασίες που αφορούν το IPSec πρωτόκολλο επειδή το κοινό μυστικό κλειδί χρησιμοποιείται για να κρυπτογραφήσει τα δεδομένα χρησιμοποιώντας τους βασικούς αλγορίθμους κρυπτογράφησης που διευκρινίζονται στα IPSec SA (π.χ. στον DES).

Τρίτη Ανταλλαγή. Κάθε συμβαλλόμενο μέρος ταυτοποιεί το άλλο με χρήση των κατάλληλων αλγόριθμων (που έχουν οριστεί νωρίτερα).

Η **δεύτερη φάση IKE** πραγματοποιείται αμέσως μετά την ολοκλήρωση της πρώτης φάσης. Στην φάση αυτή εκτελούνται τα εξής:

- **Διαπραγμάτευση μιας κοινής πολιτικής IPSec**. Καθορίζονται οι τρόποι χρήσης των αλγόριθμων κρυπτογράφησης (π.χ. αν θα είναι τρόπος μεταφοράς ή σήραγγας, αν θα χρησιμοποιηθεί AH ή ESP κ.ο.κ.)

- **Δημιουργία IPSec Συσχέτισης Ασφαλείας).** Στην δεύτερη ΙΚΕ φάση κάθε στιγμή μπορεί να δημιουργηθεί ένα νέο IPSec SA στη περίπτωση που το προηγούμενο τερματιστεί, είτε λόγω αδυναμίας συμφωνίας των συμβαλλομένων μερών για τις παραμέτρους επικοινωνίας είτε λόγω παρέλευσης του προκαθορισμένου χρόνου λειτουργίας ενός IPSec SA.
- **Χρήση Κλειδιών**. Τα κοινά μυστικά κλειδιά που δημιουργήθηκαν στη πρώτη φάση χρησιμοποιούνται για τις λειτουργίες της κρυπτογράφησης και αποκρυπτογράφησης των δεδομένων που μεταφέρονται μεταξύ των δύο IPSec συμβαλλομένων μερών.

Αυτά τα δύο βήματα, πιστοποίηση και ανταλλαγή κλειδιών, δημιουργούν το IKE SA ένα ασφαλές κανάλι μεταξύ των δύο συσκευών. Το ένα μέρος του τούνελ προσφέρει ένα σύνολο αλγορίθμων ενώ το άλλο πρέπει να κάνει αποδεκτή μία από τις προσφορές ή να απορρίψει ολόκληρη τη σύνδεση. Όταν πλέον τα δύο μέρη συμφωνήσουν στη χρήση συγκεκριμένων αλγορίθμων αντλούν το υλικό των κλειδιών για χρήση από την IPSec μαζί με μία ή και τις δύο επικεφαλίδες (AH και ESP).

Η IPSec χρησιμοποιεί διαφορετικό κλειδί από αυτό του IKE. Το κλειδί της IPSec μπορεί να προέλθει από την επαναχρησιμοποίηση της ανταλλαγής Diffie-Helman για την επίτευξη υψηλού βαθμού ασφάλειας, ή με την χρησιμοποίηση της αρχικής ανταλλαγής Diffie-Helman η οποία και παρήγαγε το IKE SA, αφού αυτή πρώτα συσχετισθεί μέσω μιας hash συνάρτησης με κάποιους τυχαίους αριθμούς.

Η πρώτη μέθοδος παρέχει μεγαλύτερη ασφάλεια αλλά είναι πολύ πιο αργή. Αφού όλα τα παραπάνω τελειώσουν το IPSec SA έχει εγκαθιδρυθεί.

Παράδειγμα Ο Bob προσπαθεί να επικοινωνήσει με ασφάλεια, με την Alice. Οι κινήσεις που γίνονται είναι οι παρακάτω:

1. Ο Bob στέλνει τα δεδομένα του προς την Alice
2. Όταν ο δρομολογητής του Bob δει τα πακέτα ελέγχει τη πολιτική ασφάλειάς τους και αντιλαμβάνεται ότι αυτά πρέπει να είναι κρυπτογραφημένα.
3. Η προ-ρυθμισμένη πολιτική ασφάλειας λέει επιπλέον ότι ο δρομολογητής της Alice πρέπει να είναι το τελικό σημείο του IPSec τούνελ.
4. Ο δρομολογητής του Bob κοιτάει να δει εάν έχει εγκαθιδρυμένη μια IPSec SA με το δρομολογητή της Alice.
5. Σε περίπτωση που μια τέτοια δεν υπάρχει, τότε ζητάει μία από το IKE.

Εάν οι δύο δρομολογητές έχουν έτοιμη μια IKE SA τότε μπορεί γρήγορα να ξεκινήσει μια IPSec SA. Εάν δεν έχουν, τότε πρέπει να περιμένουν να δημιουργηθεί μία πρώτα. Σαν μέρος αυτής της διαδικασίας, οι δύο δρομολογητές ανταλλάσσουν ψηφιακά πιστοποιητικά. Αυτά θα πρέπει να είναι υπογεγραμμένα από πριν από κάποιον τρίτο τον οποίο εμπιστεύεται τόσο oBob όσο και η Alice (οι δρομολογητές αυτών). Όταν ενεργοποιηθεί το IKE κανάλι οι δρομολογητές μπορούν να ξεκινήσουν τις διαπραγματεύσεις για την IPSec SA. Όταν αυτή πια,ενεργοποιηθεί τότε θα έχει συμφωνηθεί ένας αλγόριθμος κρυπτογράφησης (για παράδειγμα ο DES) και ένας αλγόριθμος πιστοποίησης (για παράδειγμα ο MD5) και θα έχει επιπλέον γίνει και η ανταλλαγή κάποιου κλειδιού. Τώρα πλέον ο δρομολογητής του Bob μπορεί να κρυπτογραφήσει τα IP πακέτα του και να τα τοποθετήσει σε νέα IPSec πακέτα για να τα στείλει στο δρομολογητή της Alice. Όταν ο τελευταίος τα λαμβάνει, κοιτάει την IPSec SA και κατόπιν αποθυλακώνει και επεξεργάζεται κατάλληλα το αρχικό πακέτο το οποίο και προωθεί στην Alice.Όσο και σύνθετα αν ακούγονται όλα αυτά, στην πραγματικότητα συμβαίνουν εντελώς αυτόματα και χωρίς να φαίνεται το παραμικρό στα μάτια τόσο του Bob όσο και της Alice.

5.2 Σύγκριση στα Δίκτυα εφαρμογής των VPN’s

Υπάρχουν δύο ειδών VPN. Τα πρώτα είναι τα **Απομακρυσμένης Πρόσβασης** (remote access VPN), που επιτρέπουν σε μεμονωμένους χρήστες να συνδέονται στο τοπικό δίκτυο της εταιρείας (LAN) από απόσταση με ασφαλείς και κρυπτογραφημένες συνδέσεις. Τα άλλα είναι τα **Σημείο-προς-Σημείο** Ιδεατά Ιδιωτικά Δίκτυα (site-to-site VPN) στα οποία μια εταιρεία μπορεί να συνδέσει πολλαπλά σημεία της με άλλα σημεία, όπως ένα δημόσιο δίκτυο σαν το Διαδίκτυο ή άλλα τοποικά δίκτυα. Υπάρχουν δύο τύποι site-to-site VPN συνδέσεων. Οι **Intranet-based**, όπου η εταιρεία μπορεί να συνδέσει δύο δικά της απομακρυσμένα δίκτυα μεταξύ τους, ώστε να δημιουργήσουν ένα μοναδικό VPN και οι **Extranet-based**, όπου δύο διαφορετικές εταιρείες μπορούν να συνδέσουν τα τοπικά τους δίκτυα για να έχουν ένα κοινό περιβάλλον εργασίας.

Στην ενότητα αυτή θα γνωρίσουμε τις τεχνολογίες μετάδοσης, που μπορεί να είναι κλασσικές ή και αρκετά προηγμένες, καθώς και τα βασικά χαρακτηριστικά τους.

Για την ανάπτυξη των δικτύων χρησιμοποιούνται δίκτυα μεταγωγής (κυκλώματος, πακέτου), δορυφορικές συνδέσεις, μικροκυματικές συνδέσεις, οπτικές ίνες, ακόμα και συστήματα καλωδιακής τηλεόρασης. Ο σχηματισμός δικτύων επιτυγχάνεται με τη χρήση κατάλληλων γραμμών σύνδεσης και στοιχείων.

Πάνω σε αυτό βασίζεται και η τεχνολογία VPN, για να κάνει πραγματικά ως προς το χρήστη, ένα ευρύ δίκτυο να εμφανίζεται και να λειτουργεί κατά τον ίδιο ακριβώς τρόπο με το τοπικό δίκτυο την εκάστοτε επιχείρησης.

Επειδή είναι αρκετά δύσκολο, για μια εταιρεία να εγκαταστήσει και να διαχειριστεί από μόνη της τις γραμμές σε ένα εύρη δικτύου πολλών χιλιομέτρων, συνήθως τις νοικιάζει από κάποιο τηλεπικοινωνιακό φορέα, ο οποίος μπορεί να έχει αναπτύξει την απαραίτητη σε εξοπλισμό αλλά και γεωγραφική εξάπλωση υποδομή. Από την άλλη μεριά κάνεις απλά χρήση του Ιντερνέτ.

Συνεχής πρόσβασης ή Dial-Up Ασφάλεια

Η σύνδεση στο εσωτερικό δίκτυο ενός μακρινού χρήστη μέσω της χρήσης modem, δημιουργεί διάφορα, πιθανά σενάρια ως προς την ασφάλεια της επικοινωνίας. Θα ήταν πολύ δύσκολο να υποκλαπεί μια σύνοδος με την χρήση modem εάν τα άκρα της επικοινωνίας δεν είναι προσιτά στον υποκλοπέα.

Όταν ο μακρινός χρήστης συνδέεται, πρέπει να είναι σίγουρος ότι δεν υπάρχει κανένας ανεπιθύμητος που αλληλεπιδρά με το σύστημα ή τη μετάδοση του χρήστη. Αν και αυτό είναι μόνο μια υπόθεση! όταν συγκρίνεται με το Διαδίκτυο, οι λύσεις dial-up μειώνουν την πιθανότητα υποκλοπής στα άκρα. Όταν ένας χρήστης συνδέεται με ένα συγκεκριμένο modem, συνδέεται με μόνο σκοπό στο εσωτερικό δίκτυο. Εάν πάλι θέλει να συνδεθεί στο Διαδίκτυο και αυτό επιτρέπεται, ο χρήστης λαμβάνει τους πιο αργούς χρόνους πρόσβασης και περιορισμένου πόρους εάν του διατίθεται η υπηρεσία Διαδικτύου.

Παλαιοτέρα, πριν από την εξάπλωση του Διαδικτύου και την αυξανόμενη ανάγκη για αυτό, η δυνατότητα πρόσβασης των υπάλληλων, τουλάχιστον με τον εταιρικό εξοπλισμό, ήταν σχετικά απλή. Η Πρόσβαση στο Διαδίκτυο ήταν μόνο dial-up και οι επιχειρήσεις δεν προσπαθούσαν να πάρουν τους υπαλλήλους τους το εύρος του Διαδικτύου. Εν ολίγοις, η έκθεση σε πιθανή υποκλοπή στο χρήστη, το σύστημα,

και η κυκλοφορία με τις μακρινές λύσεις dial-up είναι περιορισμένη. Προσθέστε στην ασφάλεια όταν συνδέονται με άμεσης πρόσβασης dial-up και το γεγονός ότι μερικοί άνθρωποι απλά δεν ενδιαφέρονται να πληρώσουν για μια αργή σύνδεση Διαδικτύου μέσω modem. Οι εταιρίες είχαν επίσης τη δύναμη να δηλώσουν μια πολιτική ασφάλειας, ότι κανένας εξοπλισμός της επιχείρησης δεν επρόκειτο να χρησιμοποιηθεί για την πρόσβαση Διαδικτύου.

5.2.1 Σύγκριση στα δίκτυα μεταγωγής πακέτων των VPN

Τα Ιδεατά Ιδιωτικά Δίκτυα επιτυγχάνουν σημαντικές μειώσεις στα τηλεπικοινωνιακά κόστη μίας εταιρείας, σε σχέση με τις παραδοσιακές λύσεις διασύνδεσης, ενώ παράλληλα μπορούν να εγγυηθούν τόσο την ασφάλεια επικοινωνίας όσο και το ποιοτικό επίπεδο της παρεχόμενης υπηρεσίας (Service Level Agreement) κάτι που δεν είναι εύκολο με τις κλασικές μεθόδους διασύνδεσης.
Τα Ιδεατά Ιδιωτικά Δίκτυα απευθύνονται συνήθως σε μεσαίες και μεγάλες επιχειρήσεις που:

- Διαθέτουν περισσότερα από ένα υποκαταστήματα στην Ελλάδα ή το εξωτερικό και υπάρχει ανάγκη επικοινωνίας μεταξύ τους για μεταφορά δεδομένων ή φωνής
- Διαθέτουν μετακινούμενα στελέχη για τα οποία υπάρχει ανάγκη επικοινωνίας με τα κεντρικά γραφεία για μεταφορά δεδομένων ή για πρόσβαση σε πληροφορίες
- Θέλουν να δημιουργήσουν ένα ασφαλές και αξιόπιστο περιβάλλον επικοινωνίας με συνεργάτες ή προμηθευτές τους
- Λειτουργούν σήμερα ένα παραδοσιακό τηλεπικοινωνιακό δίκτυο και ενδιαφέρονται να μειώσουν τα τηλεπικοινωνιακά τέλη

Επειδή όμως τα VPN’s δεν είναι από μόνα τους δίκτυα . Για να ικανοποιηθεί η διαρκώς αυξανόμενη ανάγκη για επικοινωνία σε ευρύτερες γεωγραφικές εκτάσεις, έχουν αναπτυχθεί διάφορα δίκτυα εδώ και πολλά χρονιά. Τα VPN χρησιμοποιούν αυτά τα δίκτυα για να εφαρμοστούν. Κάποια από αυτά εξελίσσονται ταυτόχρονα μετά την τεχνολογία των VPN και κάποια παράλληλα, αποτελώντας άλλες τεχνολογίες.

Οι τεχνολογίες, που χρησιμοποιούνται στις υπηρεσίες δικτύων ευρείας περιοχής (υπηρεσίες WAN) παρέχονται ως υπηρεσίες από τους διάφορους τηλεπικοινωνιακούς φορείς, είναι οι παραδοσιακές

- Επιλεγόμενες Τηλεφωνικές Γραμμές
- Μόνιμες ή Μισθωμένες Γραμμές
- X.25 : Τεχνολογία μεταγωγής πακέτου

Πάνω στη X.25 έχουν αναπτυχτεί και αυτές που κάνουν και χρήση του Ιντερνέτ, σε αυτές συγκαταλέγετε και η VPN.

- Δίκτυα Frame Relay
- ISDN - Intergrated Services Digital Network
- BISDN-Broadband Integrated Services Digital Network
- Δίκτυα ATM. (Ασύγχρονος τρόπος μεταφοράς δεδομένων)
- Δίκτυα xDSL

5.2.1.1 Παραδοσιακές τεχνολογίες

Σε αυτές τις τεχνολογίες δεν χρησιμοποιούνται πολύπλοκα πρωτόκολλα και συστήματα ασφαλείας. Είναι σαν να έχεις ένα τεράστιο καλώδιο, συνδεδεμένο στα άκρα με δύο υπολογιστές που κάνουν ανταλλαγή πακέτων. Τα πακέτα μεταφέρονται στο καλώδιο χωρίς να κυκλοφορούν ξένα πακέτα ή να εισέρχεται κανείς άλλος στην γραμμή.

Επιλεγόμενες Τηλεφωνικές Γραμμές

Στο ίδιο δίκτυο, που χρησιμοποιείται για την επικοινωνία μέσω τηλεφωνικών συσκευών, είναι δυνατό να χρησιμοποιηθεί και για την επικοινωνία υπολογιστών. Το παγκόσμια εκτεταμένο αυτό δίκτυο είναι γνωστό σαν δημόσιο τηλεφωνικό δίκτυο μεταγωγής (**Public Switched Telephone Network, PSTN**). Για το χώρο των υπολογιστών, το PSTN, προσφέρει μέσω των επιλεγόμενων τηλεφωνικών γραμμών, τις γραμμές σύνδεσης, που απαιτούνται για το σχηματισμό δικτύου.

Επειδή ο αρχικός σχεδιασμός του PSTN έγινε για τη μετάδοση φωνής και όχι για τη μετάδοση ψηφιακών δεδομένων, απαιτούνται ειδικές συσκευές, τα modems, για τη διαμόρφωση των ψηφιακών σημάτων, που παράγουν οι υπολογιστές σε αναλογικά και αντίστροφα.

Οι επιλεγόμενες τηλεφωνικές γραμμές προσφέρουν σχετικά μικρούς ρυθμούς μετάδοσης. Η ποιότητα τους δεν είναι σταθερή και εξαρτάται από την ποιότητα των γραμμών, που συμμετέχουν στη δημιουργία της σύνδεσης. Σήμερα, η ταχύτητα ροής δεδομένων μπορεί να φθάσει σε αυτές τις γραμμές και τα 56 Kbps.

Η επιλεγόμενη τηλεφωνική γραμμή είναι πολύ διαδεδομένη υπηρεσία και χρησιμοποιείται για συνδέσεις περιορισμένης διάρκειας, όταν δεν δικαιολογείται το επιπλέον κόστος αφιερωμένης γραμμής. Μερικές τυπικές εφαρμογές της είναι η πρόσβαση στο Διαδίκτυο ή σε άλλες online υπηρεσίες χαμηλής ταχύτητας, η σύνδεση απομακρυσμένου κόμβου με το τοπικό δίκτυο, η τηλεργασία. Επίσης χρησιμοποιείται σαν εφεδρική γραμμή σε περίπτωση βλάβης μιας μόνιμης γραμμής.

Μόνιμες ή Μισθωμένες Γραμμές

Αντίθετα από τις επιλεγόμενες γραμμές, που πρέπει να δημιουργούνται κάθε φορά, που απαιτείται σύνδεση μεταξύ δύο σημείων, οι μισθωμένες ή μόνιμες γραμμές παρέχουν μια επικοινωνιακή γραμμή έτοιμη να χρησιμοποιηθεί ανά πάσα στιγμή. Υπάρχουν αναλογικές και ψηφιακές μισθωμένες γραμμές, οι οποίες προσφέρονται από τους διάφορους τηλεπικοινωνιακούς φορείς.

Η αναλογική μισθωμένη γραμμή είναι περισσότερο γρήγορη και αξιόπιστη από την επιλεγόμενη γραμμή. Επίσης είναι σχετικά ακριβή, γιατί ο τηλεπικοινωνιακός φορέας δεσμεύει πολύτιμους πόρους του δικτύου του για τη μισθωμένη γραμμή, είτε αυτή χρησιμοποιείται είτε όχι. Οι αναλογικές μισθωμένες γραμμές, όπως και οι αναλογικές επιλεγόμενες γραμμές, απαιτούν τη χρήση modem, ενώ θέτουν όρια στην ποιότητα και στην ταχύτητα μετάδοσης. Οι μισθωμένες γραμμές είναι διαθέσιμες 24 ώρες το 24ωρο, 7 ημέρες την εβδομάδα ,και γι' αυτό είναι κατάλληλες, πχ για την μόνιμη σύνδεση μεταξύ των υποκαταστημάτων μιας εταιρίας, για την σύνδεση εταιριών με το διαδίκτυο, προκειμένου να παρέχουν υπηρεσίες πληροφόρησης διαρκώς διαθέσιμες

Όταν απαιτείται υψηλότερη ποιότητα επικοινωνίας και ευκολότερη διαχείριση, χρησιμοποιούνται οι ψηφιακές μισθωμένες γραμμές. Οι ταχύτητες των ψηφιακών γραμμών κυμαίνονται από 19,2 Kbps μέχρι 45 Mbps. Πολύ συχνά χρησιμοποιούμενη επιλογή είναι οι γραμμές E1 στα 2,048 Mbps (για την Ευρώπη) ή οι γραμμές TI στα 1,544 Mbps (για τη Β. Αμερική και την Ιαπωνία). Σε

περιπτώσεις, που επαρκούν μικρότερες ταχύτητες, είναι δυνατό να χρησιμοποιηθεί ποσοστό των γραμμών E1 ή T1 σε πολλαπλάσια των 64 Kbps.

Η ψηφιακή γραμμή E1 επιτρέπει την μετάδοση 32 καναλιών δεδομένων μέσα από μια δισύρματη τηλεφωνική γραμμή. Κάθε κανάλι δειγματοληπτείται 8000 φορές/sec και κάθε δείγμα, που παράγεται, κωδικοποιείται σε σειρά των 8 bits. Έτσι καθένα από τα 32 κανάλια μπορεί να μεταδίδει δεδομένα με ρυθμό 64kbps. Η γραμμή E1 μπορεί να μεταδίδει συνολικά δεδομένα με ρυθμό 2,048 Mbps.

Επειδή η μετάδοση είναι από άκρη σε άκρη ψηφιακή, για τη σύνδεση του δικτύου με τη γραμμή δεν χρησιμοποιείται modem αλλά άλλη συσκευή που ονομάζεται **μονάδα εξυπηρέτησης καναλιού-δεδομένων** (Channel Service Unit/Data Service Unit, CSU/DSU). Αυτή, αφενός, μετατρέπει το ψηφιακό σήμα, που παράγουν οι διάφοροι σταθμοί του δικτύου, σε ψηφιακό σήμα κατάλληλης μορφής (διπολικό), ώστε να μπορεί να μεταδοθεί στη γραμμή, αφετέρου περιέχει ειδικά ηλεκτρονικά κυκλώματα προστασίας των εγκαταστάσεων του παροχέα της υπηρεσίας.

Βασικό μειονέκτημα των ψηφιακών μισθωμένων γραμμών είναι ότι, αν παρουσιάσουν πρόβλημα, διακόπτεται η λειτουργία τους. Δεν υπάρχει, δηλαδή, η δυνατότητα να κρατηθεί η σύνδεση ανοιχτή σε χαμηλότερη ταχύτητα (κάτι που μπορεί να γίνει σε αναλογική γραμμή).

Η τιμολόγηση μισθωμένης γραμμής είναι συνάρτηση της ταχύτητας και της απόστασης μεταξύ των δύο ακραίων σημείων, κι όχι του όγκου των δεδομένων, που διακινούνται μέσα από αυτή. Αν πρόκειται να συνδέσουμε με αφιερωμένες γραμμές μικρό αριθμό σημείων και οι συνδέσεις να χρησιμοποιούνται πολλές ώρες την ημέρα, μπορεί η επιλογή τους να αποτελεί την πιο συμφέρουσα λύση από άποψη κόστους.

5.2.1.2 Τεχνολογία μεταγωγής πακέτου

X.25

Το X.25 είναι τεχνολογία μεταγωγής πακέτου, όπου τα δεδομένα μεταδίδονται στο δίκτυο μεταγωγής σε μικρά κομμάτια, τα πακέτα. Το δίκτυο X.25 αποτελείται, ουσιαστικά, από κόμβους μεταγωγής πακέτων (**Packet Switching Nodes, PSNs**), οι οποίοι δρομολογούν κατάλληλα τα πακέτα, ώστε να φθάσουν στον προορισμό τους.

Η διεπαφή μεταξύ του εξοπλισμού του χρήστη και του δικτύου μεταγωγής πακέτων περιγράφεται από το πρότυπο X.25, που αφορά τα τρία κατώτερα επίπεδα του μοντέλου αναφοράς του OSI.

Στο πρότυπο X25, ο ακραίος εξοπλισμός του χρήστη αναφέρεται σαν **τερματικός εξοπλισμός δεδομένων** (Data Terminal Equipment, **DTE**), και ο κόμβος μεταγωγής πακέτων, με τον οποίο συνδέεται ένα DTE, αναφέρεται σαν εξοπλισμός επικοινωνίας δεδομένων (Data Communication Equipment, DCE). Αν κάποιες από τις συσκευές του χρήστη δεν έχουν τη δυνατότητα διαχείρισης πακέτων X.25 (π.χ. ασύγχρονα τερματικά), υπάρχει δυνατότητα σύνδεσης τους σε τέτοιο δίκτυο μέσω της μονάδας συναρμολόγησης - αποσυναρμολόγησης πακέτων (Packet Assembler - Disassembler, PAD)

Τα πρώτα δίκτυα X.25 χρησιμοποιούσαν απλές τηλεφωνικές γραμμές για τη μετάδοση δεδομένων, που αποτελούσαν αρκετά αναξιόπιστο μέσο μετάδοσης και επέτρεπαν την εμφάνιση αρκετών λαθών. Για το λόγο αυτό το X.25 χρησιμοποιούσε ειδικές μεθόδους ανίχνευσης λαθών και επαναμετάδοσης δεδομένων. Με τις σημερινές τηλεπικοινωνιακές γραμμές, που εμφανίζουν πολύ μικρότερη πιθανότητα σφαλμάτων και είναι πολύ περισσότερο αξιόπιστες, ο εκτεταμένος έλεγχος λαθών του X.25 δεν είναι πια απαραίτητος και επιπλέον επιδρά αρνητικά στη ταχύτητα μετάδοσης των δεδομένων. Τα δίκτυα X.25 παρέχουν στους χρήστες υπηρεσίες νοητού κυκλώματος με σύνδεση (connection oriented services). Συγκεκριμένα μπορεί να παρέχουν νοητά κυκλώματα προσωρινά (SVSs) ή μόνιμα (PVCs).

Κάθε νοητό κύκλωμα προσδιορίζεται από ένα μοναδικό αριθμό **VCI** (**Virtual Channel Identifier**), κι έτσι μπορεί να εξυπηρετεί μια διαφορετική σύνδεση. Πολλά νοητά κυκλώματα είναι δυνατόν να πολυπλέκονται χρονικά μέσα στην ίδια φυσική σύνδεση και για το λόγο αυτό γίνεται πολύ καλύτερη εκμετάλλευση του διαθέσιμου εύρους ζώνης.

Τα **SVSs** είναι προσωρινές συνδέσεις, που δημιουργούνται όταν υπάρξει αίτηση σύνδεσης και τερματίζεται μόλις τελειώσει η μετάδοση δεδομένων. Κάθε τερματική συσκευή DTE του δικτύου παίρνει μια μοναδική διεύθυνση, που χρησιμοποιείται όπως ένας τηλεφωνικός αριθμός. Τα PVCs είναι μόνιμα διαθέσιμα κυκλώματα και δεν απαιτείται η κλήση για την δημιουργία τους, αλλά δημιουργούνται από το φορέα του δικτύου και παραμένουν μόνιμα στη διάθεση των χρηστών (όπως συμβαίνει και με τις μόνιμες μισθωμένες γραμμές)

Το κόστος της υπηρεσίας X.25 είναι πολύ προσιτό. Η τιμολόγηση γίνεται ανάλογα με το ποσό δεδομένων, που διακινήθηκε, κάνοντας αρκετά ελκυστική τη χρήση της στην περίπτωση μετάδοσης μικρού ποσού δεδομένων σποραδικά.

Αν και έχουν εμφανισθεί καινούργιες τεχνολογίες, όπως το ISDN και το Frame Relay, σε αρκετά μέρη του κόσμου χρησιμοποιείται η τεχνολογία X.25, γιατί είναι η πιο φθηνή ή ακόμη και η μόνη διαθέσιμη.

Δίκτυα Frame Relay

Καθώς η ανάπτυξη δικτύων βασίζεται όλο και περισσότερο στη χρήση ψηφιακών μεθόδων μετάδοσης, εμφανίστηκαν νέες τεχνολογίες μεταγωγής πακέτων, όπως για παράδειγμα το **Frame Relay**, που απαιτούν πολύ λιγότερο έλεγχο σφαλμάτων απ' ότι οι παλαιότερες τεχνολογίες. Το Frame Relay είναι σύγχρονη τεχνολογία γρήγορης μεταγωγής πακέτων (Fast Packet Switching), μεταβλητού μεγέθους.

Σε αυτή την τεχνολογία έχουν αφαιρεθεί αρκετές λειτουργίες ελέγχου οι οποίες δεν είναι απαραίτητες σε ένα αξιόπιστό και ασφαλές ψηφιακό περιβάλλον. Επίσης έχει προδιαγραφεί η ζεύξη μεταξύ της τερματικής συσκευής (DTE) και δικτύου (DCE).

Το δίκτυο Frame Relay προσφέρει στους χρήστες υπηρεσίες μόνο πρώτου και δεύτερου επιπέδου. Πρόκειται, ουσιαστικά, για συνδέσεις από σημείο σε σημείο, όπου ένα μόνιμο νοητό κύκλωμα (PVC) χρησιμοποιείται για τη μετάδοση πακέτων μεταβλητού μεγέθους στο επίπεδο σύνδεσης δεδομένων. Για την επικοινωνία δύο απομακρυσμένων τοπικών δικτύων, τα δεδομένα από το δίκτυο Α οδηγούνται μέσω ψηφιακής μισθωμένης γραμμής στον πλησιέστερο κόμβο μεταγωγής του δικτύου Frame Relay. Μετά προωθούνται κατάλληλα μέσω του δικτύου Frame Relay και τελικά φθάνουν στο δίκτυο προορισμού Β.

Τα δίκτυα τεχνολογίας Frame Relay είναι αρκετά δημοφιλή, γιατί εκτελούν πολύ πιο γρήγορα από άλλα συστήματα μεταγωγής βασικές λειτουργίες προώθησης πακέτων. Αυτό συμβαίνει, επειδή είναι εκ των προτέρων καθορισμένη η διαδρομή, που θα ακολουθήσουν τα πακέτα μιας σύνδεσης από άκρη σε άκρη. Δεν είναι ανάγκη να υπάρχουν συσκευές, που να τεμαχίζουν και να επανασυναρμολογούν τα πακέτα ή να αποφασίζουν για τη καλύτερη διαδρομή.

Όταν ο κόμβος του δικτύου Frame Relay λάβει ένα σήμα, διαβάζει την διεύθυνση προορισμού, που επιγράφεται στην επικεφαλίδα του σήματος και αμέσως μετά από έναν απλό έλεγχο προωθεί το σήμα χωρίς να περιμένει να το λάβει ολόκληρο. Το σήμα ακολουθώντας το PVC, φθάνει στον προορισμό, όπου τοποθετείται στην σωστή σειρά και επανασυναρμολογείται το πακέτο. Αν διαπιστωθεί ότι το πακέτο χάθηκε ή αλλοιώθηκε, η ακραία συσκευή λήψης ζητά την επαναμετάδοσή του από την συσκευή εκπομπής.

Ένα δίκτυο Frame Relay είναι σύστημα από σημείο σε σημείο αφού χρησιμοποιεί μόνιμα νοητά κυκλώματα. Επίσης τα δίκτυα Frame Relay είναι δυνατό να παρέχουν στους χρήστες τους εύρος ζώνης ανάλογα με τις ανάγκες τους. Υποστηρίζουν ταχύτητες από 64 Kbps έως 2,048Mbps (56 Kbps έως 1,544 Mbps αντίστοιχα για την Αμερική). Σε ανάπτυξη βρίσκονται προδιαγραφές για 34 Mbps (45 Mbps για την Αμερική).

Η τιμολόγηση της χρήσης του δικτύου Frame Relay εξαρτάται από το επιθυμητό εύρος ζώνης. Για την πρόσβαση του τοπικού δικτύου σε δίκτυο Frame Relay απαιτείται μισθωμένη ψηφιακή γραμμή για την σύνδεση με τον πλησιέστερο κόμβο, δρομολογητής με κάρτα Frame Relay και συσκευή CSU/OSU για τον μετασχηματισμό του ψηφιακού σήματος.

Με τη βελτίωση της τεχνολογίας των συσκευών μεταγωγής Frame Relay έγινε δυνατό οι παροχείς αυτής της υπηρεσίας να μπορούν να παρέχουν εγγύηση για την ελάχιστη χωρητικότητα κάθε καναλιού PVC μέσω του δεσμευμένου ρυθμού πληροφορίας (**Committed Information Rate**, **CIR**)**.** Φυσικά, όταν στο δίκτυο υπάρχει διαθέσιμο εύρος ζώνης, μπορούν να επιτευχθούν και υψηλότεροι ρυθμοί από τον CIR.

Η υπηρεσία είναι οικονομικότερη από τη χρήση αφιερωμένων γραμμών, όταν πρόκειται να διασυνδεθούν αρκετά τοπικά δίκτυα σε πολλές απομακρυσμένες περιοχές. Απαιτείται λιγότερο υλικό στα κεντρικά γραφεία του χρήστη - πελάτη της υπηρεσίας, αφού αρκεί μια μόνο γραμμή E1/T1 (μεταξύ του πελάτη και του παροχέα της υπηρεσίας) για το σύνολο των απαιτούμενων γραμμών. Ακόμη ο φορέας της υπηρεσίας είναι υπεύθυνος για τη διαχείριση και καλή λειτουργία του δικτύου Frame Relay, αντίθετα με τις αφιερωμένες γραμμές, όπου υπεύθυνος είναι ο χρήστης - πελάτης.

Ουσιαστικά το Frame Relay είναι μια επέκταση του X.25, που δεν αναλαμβάνει τα θέματα έλεγχου παρόλο που είναι πιο ευάλωτο στην συμφόρηση πακέτων. Τις οποίες αντιμετωπίζει με κάποιες δικές του τεχνικές.

ISDN - Intergrated Services Digital Network

Τα τελευταία χρόνια εμφανίζεται μεγάλη ζήτηση για παροχή υπηρεσιών ήχου, εικόνας, video, δεδομένων. Οι διάφοροι τηλεπικοινωνιακοί φορείς προσπαθώντας να ικανοποιήσουν τη ζήτηση αυτή δημιούργησαν εκτός από το τηλεφωνικό δίκτυο για τις υπηρεσίες φωνής, αρκετά ακόμη εξειδικευμένα δίκτυα, όπως δίκτυα δεδομένων για επικοινωνίες υπολογιστών (π.χ. το δίκτυο Hellaspac και το δίκτυο Hellascom, που δημιούργησε παλιότερα ο ΟΤΕ αλλά και το Σύζευξης που αναπτύχτηκε στα πλαίσια τις ηλεκτρονικής διακυβέρνησης), δίκτυα telex για επικοινωνίες κειμένου, δίκτυα καλωδιακής τηλεόρασης, κα. Η ανάπτυξη ξεχωριστών δικτύων για κάθε υπηρεσία έχει μειονεκτήματα, όπως μεγάλο διαχειριστικό κόστος για το τηλεπικοινωνιακό φορέα, αυξημένο κόστος για το χρήστη, λόγω του ποικίλου και διαφορετικού εξοπλισμού, που χρησιμοποιεί η κάθε τεχνολογία, αποθάρρυνση της εμπορικής ανάπτυξης. Τα παραπάνω προβλήματα έρχεται να λύσει το **Ψηφιακό Δίκτυο Ενοποιημένων Υπηρεσιών** (Integrated Services Digital Network, **ISDN**).

Το ISDN επιτρέπει στους χρήστες να μεταδίδουν φωνή, εικόνα και δεδομένα, σε ψηφιακή μορφή μέσα από την υπάρχουσα υποδομή δισύρματων τηλεφωνικών καλωδίων. Τα δισύρματα τηλεφωνικά καλώδια είναι μια μεγάλη εγκατεστημένη υποδομή, που δημιουργήθηκε κατά την ανάπτυξη του κλασσικού τηλεφωνικού δικτύου (Plain Old Telephone System, POTS) για την υποστήριξη της αναλογικής τηλεφωνίας. Το ISDN έδωσε τη δυνατότητα η μεγάλη αυτή υποδομή να χρησιμοποιηθεί για τη μετάδοση καθαρά ψηφιακού σήματος, με όλα τα πλεονεκτήματα, που αυτό συνεπάγεται...

Με το ISDN αποσυσχετίζεται το τηλεπικοινωνιακό δίκτυο από το είδος της πληροφορίας, που διακινεί, και τυποποιείται η διεπαφή συσκευών διαφόρων κατασκευαοτών στο δίκτυο, χωρίς να χρειάζεται ειδικός και πιθανά ακριβός εξοπλισμός προσαρμογής. Τα βασικά στοιχεία, που χαρακτηρίζουν το ISDN, είναι:

- **Η ψηφιακή μετάδοση**. Όλα τα σήματα μεταδίδονται σε ψηφιακή μορφή απ' άκρη σ' άκρη του δικτύου, δηλαδή από τη μια τερματική γραμμή έως την άλλη.

- **Η σηματοδοσία**, που γίνεται μέσω ιδιαίτερου καναλιού (common channel signaling). Με τον όρο σηματοδοσία ορίζουμε όλα εκείνα τα βοηθητικά σήματα με τα οποία διαχειριζόμαστε μια επικοινωνία (έναρξη, κλήση, κουδούνισμα κλπ).
- **Η ενιαία και πολλαπλού σκοπού διασύνδεση** των χρηστών στο δίκτυο. Ένας χρήστης μπορεί να απολαμβάνει τις διάφορες υπηρεσίες του δικτύου με μια και μόνο σύνδεση μέσω της ίδιας πρίζας.

Το δίκτυο ISDN παρέχει δύο τύπους πρόσβασης, τη διεπαφή βασικού ρυθμού και τη διεπαφή πρωτεύοντος ρυθμού.

Η **διεπαφή βασικού ρυθμού** (Basic Rate Interface, **BRI),** παρέχει δύο κανάλια φορείς (2 κανάλια-Β) κι ένα κανάλι σηματοδοσίας (1 κανάλι-D). Κάθε κανάλι-Β έχει ρυθμό μετάδοσης 64 Kbps και χρησιμοποιείται για τη μεταφορά ψηφιοποιημένης φωνής και δεδομένων. Το κανάλι-D έχει ρυθμό μετάδοσης 16 Kbps και χρησιμοποιείται για την εγκαθίδρυση και διαχείριση της σύνδεσης. Οι τηλεπικοινωνιακοί φορείς δίνουν τη δυνατότητα στους χρήστες-πελάτες τους να χρησιμοποιούν το ένα ή και τα δύο κανάλια-Β, πράγμα που σημαίνει, ότι η σύνδεση βασικού ρυθμού μπορεί να παρέχει ρυθμό μετάδοσης μέχρι 144 Kbps (2B+D)

Η **διεπαφή πρωτεύοντος ρυθμού** (Primary Rate Interface, **PRI**) παρέχει 30 κανάλια των 64 Kbps (30 Β-κανάλια) κι ένα κανάλι των 64 Kbps (1 D-κανάλι). Το εύρος ζώνης ενός ακόμη καναλιού των 64 Kbps χρησιμοποιείται για πλαισίωση (framing) και συντήρηση του δικτύου. Έχουμε, έτσι, συνολικό ρυθμό μετάδοσης 2,048Mbps, που άλλωστε είναι και η ταχύτητα που υποστηρίζει μια ψηφιακή γραμμή Ε1. Στη Β. Αμερική και Ιαπωνία έχουμε 23Β+1D κανάλια (όλα των 64 Kbps) και άλλα 8Kbps πλεονασμό, άρα, συνολικό ρυθμό 1,544 Mbps (μια ψηφιακή γραμμή Τ1).

Το ISDN χρησιμοποιεί την υπάρχουσα τηλεπικοινωνιακή υποδομή, απαιτεί, όμως, την εγκατάσταση ειδικής συσκευής στη μεριά του χρήστη, της συσκευής τερματισμού δικτύου **NT1** (Netmod). Ο τηλεπικοινωνιακός φορέας τοποθετεί τη συσκευή αυτή στο χώρο του χρήστη-συνδρομητή και μετά τη συνδέει με τον κόμβο ISDN στο τηλεφωνικό κέντρο, αρκετά χιλιόμετρα μακριά, χρησιμοποιώντας το συνεστραμμένο ζεύγος καλωδίων, που παλιότερα χρησιμοποιείτο στη σύνδεση με το τηλέφωνο του συνδρομητή.

Μετά η κίνηση δρομολογείται από το δίκτυο του τηλεπικοινωνιακού φορέα. Στη συσκευή τερματισμού NT1 είναι δυνατό να συνδεθούν μέχρι 8 συσκευές σε απόσταση 150 μέτρα. Μπορεί να είναι συσκευές ειδικά σχεδιασμένες για το

δίκτυο ISDN, όπως ψηφιακή τηλεφωνική συσκευή, Fax ομάδας 4, εικονοτηλέφωνο, δρομολογητής, ή απλές συσκευές, όπως η αναλογική τηλεφωνική συσκευή, κοινό τερματικό κ.α. Τα κανάλια B και D είναι λογικά κανάλια και όχι φυσικά. Έτσι στη συσκευή NT1 κατλήγει πάντα μια απλή δισύρματη γραμμή και όχι περισσότερα καλώδια. Ο συνδυασμός βασικού και πρωτεύοντος ρυθμού είναι ιδανικός για τη δημιουργία ενός δικτύου με μια κεντρική θέση και πολλές περιφερειακές. Χρησιμοποιώντας σύνδεση πρωτεύοντος ρυθμού στην κεντρική θέση και συνδέσεις βασικού ρυθμού στις περιφερειακές θέσεις, η κεντρική θέση - υπολογιστής μπορεί να επικοινωνεί ταυτόχρονα με 30 διαφορετικές απομακρυσμένες θέσεις - υπολογιστές (23 αντίστοιχα για την Αμερική).

Η υπηρεσία ISDN είναι χρήσιμη, όταν η μετάδοση δεδομένων δεν είναι συνεχής και οι ανάγκες σε ταχύτητα κυμαίνονται. Ο χρήστης πληρώνει όσο διαρκεί η κλήση, γι' αυτό είναι αρκετά συνηθισμένο να χρησιμοποιείται σαν εφεδρική σύνδεση αφιερωμένων γραμμών.

Το ISDN, που περιγράψαμε, αναφέρεται και ως **ISDN στενής ζώνης** (Narrowband ISDN), ενώ αναπτύσσονται και πρότυπα για το **ISDN ευρείας ζώνης** (Broadband ISDN), το οποίο απαιτεί τη χρήση οπτικής ίνας.

BISDN-Broadband Integrated Services Digital Network

Ο όρος **BISDN** σημαίνει **Broadband Integrated Services Digital Network** το οποίο μεταφράζεται ως ψηφιακό δίκτυο ενοποιημένων (ολοκληρωμένων) υπηρεσιών ευρέος φάσματος. Βασικός στόχος του BISDN είναι - όπως φαίνεται και από την ονομασία του - η κατασκευή ενός ψηφιακού δικτύου που θα ενοποιήσει τους διάφορους τύπους υπηρεσιών ευρέος φάσματος παρέχοντάς τους ένα κοινό για όλες πλαίσιο υποστήριξης. Μπορεί δηλαδή να θεωρηθεί ως επέκταση του ISDN, εξοπλισμένο όμως με δυνατότητες εξυπηρέτησης σημάτων ευρέος φάσματος.

Η διαφορά όμως μεταξύ του ISDN και του BISDN είναι ότι το πρώτο μπορεί να θεωρηθεί ως ένα δίκτυο μεταγωγής κυκλώματος που όμως έχει τη δυνατότητα να υλοποιήσει μετάδοση μεταγωγής πακέτων, ενώ το BISDN είναι ένα δίκτυο μεταγωγής πακέτων που έχει τη δυνατότητα να υλοποιήσει μετάδοση μεταγωγής κυκλώματος .

Οι βασικές υπηρεσίες που θα προσφέρει το BISDN είναι αυτές που θα εμφανισθούν στο άμεσο αλλά και στο απώτερο μέλλον. Ήδη, καθώς οι κοινωνικές και επαγγελματικές δραστηριότητες γίνονται όλο και πιο απαιτητικές, η ζήτηση για υπηρεσίες πολυμέσων (multimedia) και ευρέος φάσματος (π.χ. συνεδρίαση μέσω βίντεο – τηλεχειρουργική κ.α) γίνεται όλο και πιο έντονη.

Οι υπηρεσίες του μπορούν να ταξινομηθούν σε υπηρεσίες αλληλεπίδρασης και υπηρεσίες διανομής σήματος, σύμφωνα με τη διεύθυνση ροής της πληροφορίας.

Τα BISDN δίκτυα προσφέρουν ενοποίηση των υπηρεσιών, με άμεση συνέπεια την συνύπαρξη πολλών και διαφορετικών υπηρεσιών στα πλαίσια ενός τέτοιου δικτύου. Αυτό άλλωστε είναι και το κύριο χαρακτηριστικό: η ποικιλία των υπηρεσιών που αυτό υποστηρίζει.

- *Παροχή υπηρεσιών πολυμέσων (multimedia)*
- *Συνύπαρξη υπηρεσιών διανομής σήματος και υπηρεσιών αλληλεπίδρασης*
- *Μεγάλη διασπορά του φάσματος και της διάρκειας των υπηρεσιών*
- *Συνύπαρξη υπηρεσιών συνεχούς και μη συνεχούς τύπου*

Λόγω της μεγάλης ποικιλίας των υπηρεσιών (αλλά και της ποικιλίας των χαρακτηριστικών τους) που το BISDN πρέπει να υποστηρίξει, είναι απαραίτητη η ωρίμανση πολλών διαφορετικών κλάδων της τεχνολογίας για την υλοποίηση του.

Κατ’ αρχήν, εφόσον τα υψηλών ταχυτήτων σήματα ευρέος φάσματος αποτελούν το βασικό άξονα του BISDN, είναι αναπόφευκτο να συμβαδίζει η εξέλιξη του με την εξέλιξη στον τομέα μετάδοσης σημάτων υψηλής ταχύτητας, επεξεργασίας σημάτων υψηλής ταχύτητας και την εξέλιξη στην τεχνολογία διακοπτών υψηλής ταχύτητας.

Επίσης, σημαντικό ρόλο παίζουν οι εξελίξεις σε υλικό (hardware) και λογισμικό (software), στην τεχνολογία ημιαγωγών και την τεχνολογία τηλεπικοινωνιακών δικτύων (π.χ. ήδη οι οπτικές ίνες προκαλούν εξασθένηση του σήματος που δεν υπερβαίνει τα 0.5 db/km, ενώ οι τιμές των συσκευών εκπομπής και ανίχνευσης φωτός έχουν μειωθεί δραστικά).

Δίκτυα ATM. (Ασύγχρονος τρόπος μεταφοράς δεδομένων)

Ο **ασύγχρονος τρόπος μεταφοράς** (Asynchronous Transfer Mode, **ATM**) είναι σύγχρονη και πολλά υποσχόμενη εφαρμογή της τεχνικής της μεταγωγής.

Συνδυάζει την αποδοτικότητα της μεταγωγής πακέτων με την αξιοπιστία της μεταγωγής κυκλώματος. Για τη μετάδοση των δεδομένων, χρησιμοποιεί σταθερού μεγέθους πακέτα των 53 bytes. Από αυτά, τα 5 πρώτα bytes αποτελούν την ATM επικεφαλίδα (header) και τα υπόλοιπα 48 bytes την ωφέλιμη πληροφορία του χρήστη (payload).

Το γεγονός, ότι χρησιμοποιούνται πακέτα σταθερού μεγέθους, επιβαρύνει πολύ λιγότερο τις διεργασίες μεταγωγής και δρομολόγησης, που εκτελούνται σε κάθε κόμβο του δικτύου ATM. Έτσι, μπορούν να επιτευχθούν πολύ υψηλές ταχύτητες μεταγωγής των δεδομένων, που μπορούν να φθάσουν και τα 622 Mbps.

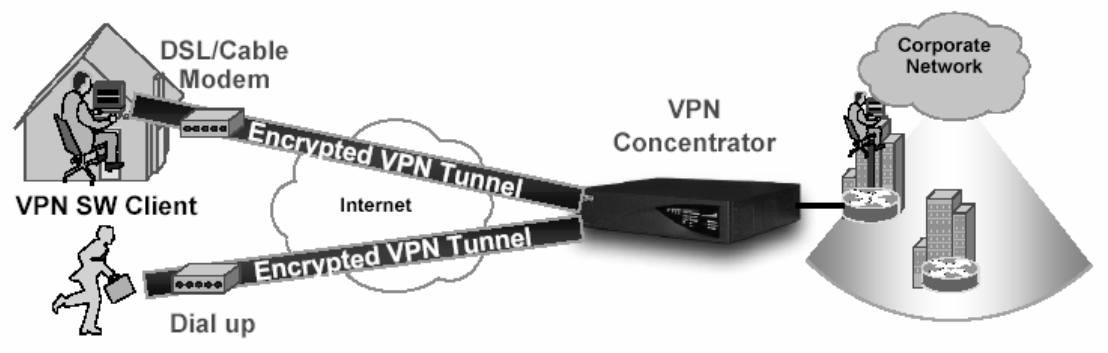
Με σύνδεση ATM 622 Mbps είναι δυνατόν να μεταδώσουμε την εγκυκλοπαίδεια Britannica, μαζί με τα γραφικά σε κάτι λιγότερο από ένα δευτερόλεπτο. Εάν χρησιμοποιούσαμε modem 56K θα χρειαζόμασταν τουλάχιστο 18 ώρες!

Η τεχνολογία ATM προδιαγράφτηκε αρχικά για τη δημιουργία του ISDN ευρείας ζώνης (Broadband ISDN), και παίζει πολύ σημαντικό ρόλο στο μέλλον των επικοινωνιών υψηλής ταχύτητας. Χρησιμοποιώντας μεθόδους στατιστικής πολυπλεξίας, κάνει δυναμική διάθεση του εύρους ζώνης ανάλογα με τη ζήτηση και μπορεί να υποστηρίξει τη μεταφορά κάθε κατηγορίας δεδομένων ακόμη και πραγματικού χρόνου, όπως φωνής, δεδομένων, fax, κινούμενης εικόνας, ήχου ποιότητας CD κ.α.

Ένα δίκτυο ATM αποτελείται από μεταγωγείς ATM υψηλής ταχύτητας, οι οποίοι δρομολογούν χωρίς καθόλου καθυστέρηση τα εισερχόμενα πακέτα. Έτσι, η τεχνολογία ATM προσφέρει πολύ υψηλές ταχύτητες ακόμη και κάτω από συνθήκες ιδιαίτερα αυξημένης κίνησης στο δίκτυο.

Σα μέσο μετάδοσης μπορεί να χρησιμοποιηθεί οποιοδήποτε από τα διαθέσιμα μέσα, όπως συνεστραμμένο ζεύγος καλωδίων, ομοαξονικό καλώδιο, οπτική ίνα. Ο εξοπλισμός, που απαιτείται στο ATM, προσφέρεται σήμερα από περιορισμένο αριθμό κατασκευαστών. Η μετατροπή της υπάρχουσας δικτυακής υποδομής σε καθαρά ATM περιβάλλον απαιτεί σε μεγάλο βαθμό αντικατάσταση του εξοπλισμού, κάτι που αποτελεί ανασταλτικό παράγοντα στην ταχεία και σε μεγάλη κλίμακα εξάπλωση της τεχνολογίας ATM. Έχει όμως ήδη αρχίσει να αποτελεί κύρια επιλογή στην ανάπτυξη δικτύων κορμού. Για παράδειγμα, ο ΟΤΕ αναπτύσσει δημόσιο δίκτυο ATM με 7 διαβιβαστικούς κόμβους και 32 κόμβους πρόσβασης, ενώ πολλά

πανεπιστημιακά ιδρύματα της χώρας μας βασίζουν την ανάπτυξη των δικτύων τους σε δίκτυο κορμού τεχνολογίας ATM.



Δίκτυα xDSL

Η **τεχνολογία xDSL** (x Digital Subscriber Line) κάνει δυνατή την επίτευξη πολύ υψηλών ταχυτήτων μεταφοράς δεδομένων μέσα από την υπάρχουσα τηλεφωνική καλωδιακή υποδομή και συγκεκριμένα μέσα από τα χάλκινα συνεστραμμένα ζεύγη καλωδίων, τα οποία χρησιμοποιούνται για να συνδέουν κάθε σπίτι με τον τηλεπικοινωνιακό. Το γράμμα «x» αφορά το σύνολο των διαφορετικών τεχνολογιών ADSL, R-ADSL, HDSL, SDSL και VDSL, που συμπεριλαμβάνονται στην ευρύτερη οικογένεια xDSL και είναι ουσιαστικά παραλλαγές της ψηφιακής συνδρομητικής γραμμής, δηλαδή της τεχνολογίας ISDN-BRI (2 κανάλια των 64 Kbps και ένα των 16 Kbps).

Σε πολλές περιπτώσεις το κόστος εγκατάστασης οπτικής ίνας μέχρι το σπίτι είναι απαγορευτικό. Με τη ραγδαία ανάπτυξη του Διαδικτύου και εφαρμογών απαιτητικών σε εύρος ζώνης, όπως πολυμέσα, τηλεδιάσκεψη, video κατά παραγγελία, έγινε φανερό, ότι ο συνδρομητικός βρόγχος αποτελεί τον κυριότερο περιοριστικό παράγοντα στη ταχύτητα πρόσβασης.

Η τεχνολογία xDSL μπορεί να προσφέρει ταχύτητες της τάξης των Mbps μέσα από αφόρτιστες μισθωμένες γραμμές και μάλιστα χωρίς τη χρήση ενισχυτών ή επαναληπτών. Υποστηρίζει τα πρότυπα E1 (2,048 Mbps) και T1 (1,544 Mbps) για τη μετάδοση δεδομένων, ενώ παράλληλα υποστηρίζει και τη μετάδοση φωνής. Χρησιμοποιεί συσκευή τερματισμού σε κάθε άκρο της σύνδεσης. Αυτή η συσκευή λειτουργεί όπως το modem, αφού λαμβάνει ροή ψηφιακού σήματος,

που στη συνέχεια το μεταδίδει στην τηλεφωνική γραμμή με τη μορφή αναλογικού σήματος υψηλού ρυθμού (λέγεται για baseband modem).

Χρησιμοποιούνται διάφορες τεχνολογίες διαμόρφωσης, οι οποίες χωρίζουν το διαθέσιμο εύρος ζώνης της γραμμής σε τρία κανάλια: ένα για τη μετάδοση της φωνής, ένα για τη μετάδοση δεδομένων προς τα πάνω (upstream) κι ένα για τη μετάδοση των δεδομένων προς τα κάτω (downstream).

Πρόσβαση τοπικού δικτύου σε δίκτυο ευρείας ζώνης περιοχής με την τεχνολογία DSL

Οι διάφορες παραλλαγές xDSL υποστηρίζουν συμμετρική ή ασύμμετρη μετάδοση δεδομένων. Αυτό σημαίνει, ότι τα δεδομένα μπορεί να μεταδίδονται με την ίδια ή διαφορετική ταχύτητα προς τις δύο κατευθύνσεις (downstream και upstream). Έτσι, κάθε παραλλαγή μπορεί να είναι κατάλληλη για χρήση σε εφαρμογές, όπου απαιτείται υψηλότερη ταχύτητα στην κατεύθυνση μετάδοσης προς το χρήστη (π.χ. πρόσβαση σε ιστοσελίδες) ή ίδια ταχύτητα και προς τις δύο κατευθύνσεις (π.χ. υποκατάστατο για γραμμές E1, τηλεδιάσκεψη).

Οι ταχύτητες που επιτυγχάνονται σε συνδέσεις xDSL, εξαρτώνται από την απόσταση και τη διατομή των καλωδίων που χρησιμοποιούνται στο τηλεφωνικό δίκτυο. Από τα χαρακτηριστικά των τεχνολογιών xDSL, βλέπουμε, ότι για πρόσβαση στο Ιντερνέτ μπορεί να χρησιμοποιηθεί τεχνολογία ADSL ή ADSL Lite. Αν οι απαιτήσεις σε ταχύτητα είναι πολύ μεγάλες, όπως στην περίπτωση πολυμεσικών εφαρμογών Internet ή τηλεόρασης υψηλής ευκρίνειας, μπορεί να χρησιμοποιηθεί τεχνολογία VDSL. Αντίθετα, στην περίπτωση διασύνδεσης τοπικών δικτύων, αντί για τις κλασικές ψηφιακές γραμμές E1/T1, μπορεί να χρησιμοποιηθεί κάποια από τις συμμετρικές τεχνολογίες HDSL, SDSL. Εξαιτίας του εξαιρετικά χαμηλού κόστους εγκατάστασης και λειτουργίας της απαιτουμένης υποδομής η τεχνολογία xDSL θα αποτελέσει στα χρόνια μία όλο και περισσότερο διαδεδομένη τεχνολογική λύση για την παροχή υπηρεσιών, αλλά και την χρήση των VPN τεχνολογιών για ασφαλέστερη επικοινωνία μεταξύ σημαντικών δικτύων.

Τα VPN μπορούν να εφαρμοστούν σε όλα σχεδόν τα παραπάνω δίκτυα χωρίς να αυξάνουν πολύ το κόστος, πέρα από αυτό που ήδη έχουν. Το κατά πόσο θα αυξηθεί τελικά το κόστος, επηρεάζεται και από την τεχνολογία του VPN που θέλει κανείς να εφαρμόσει. Αν εφαρμοστεί μια τεχνολογία που απαιτεί υλικό εξοπλισμό τοίχου προστασίας, θα αυξηθεί πολύ το κόστος σε σχέση με το λογισμικό τοίχος προστασίας του server δικτύου.

Το κύριο κριτήριο κόστους δεν είναι το VPN αλλά η τεχνολογία δικτύου που θα εφαρμοστεί.

Στους παρακάτω πίνακες φαίνονται οι συγκρίσεις των δικτύων.

ΠΛΕΟΝΕΚΤΗΜΑΤΑ

Επιλεγόμενες Τηλεφωνικές Γραμμές	***Μόνιμες ή Μισθωμένες Γραμμές***	***X.25 : Τεχνολογία μεταγωγής πακέτου***
Υψηλή διαθεσιμότητα	Υψηλή διαθεσιμότητα	Αξιοπιστία
Μικρό κόστος	Ασφάλεια	Μικρό κόστος
-	Μικρό κόστος σε σχέση με την ποσότητα των δεδομένων που μεταδίδονται.	Διαθέσιμη παντού
-	-	Διαχείριση του WAN από το φορέα

ΜΕΙΟΝΕΚΤΗΜΑΤΑ

Επιλεγόμενες Τηλεφωνικές Γραμμές	***Μόνιμες ή Μισθωμένες Γραμμές***	***X.25 : Τεχνολογία μεταγωγής πακέτου***
Μικρή ταχύτητα	Μεγάλο μηνιαίο πάγιο	Μικρή ταχύτητα
Μεταβλητή ποιότητα και αξιοπιστία	Αν η γραμμή είναι ψηφιακή τότε δύσκολη η εφεδρεία σε περίπτωση προβλήματος	Αργή απόκριση
-	-	Μόνο για δεδομένα

ΙΔΙΑΙΤΕΡΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ

Επιλεγόμενες Τηλεφωνικές Γραμμές	***Μόνιμες ή Μισθωμένες Γραμμές***	***X.25 : Τεχνολογία μεταγωγής πακέτου***
Απομακρυσμένη πρόσβαση	Διασύνδεση τοπικών δικτύων, που βρίσκονται σε μεγάλη απόσταση	Εφαρμογές τερματικού προς κεντρικό υπολογιστή
Εφαρμογές χωρίς απαιτήσεις για ταχύτητα	Μόνιμη σύνδεση στο Internet	-

ΠΛΕΟΝΕΚΤΗΜΑΤΑ

Frame Relay	***ISDN***	***ATM***
Υψηλές ταχύτητες και μικρότερες καθυστερήσεις λόγω περιορισμένου ελέγχου ροής και σφαλμάτων	Κόστος ικανοποιητικό για λογική χρήση	Πολύ υψηλές ταχύτητες (έως και 2,4Gbps)
Αξιοποίηση σύγχρονων μεθόδων ψηφιακής μετάδοσης	Ικανότητα μετάδοσης φωνής, εικόνας, δεδομένων	Μεταφορά φωνής, εικόνας και δεδομένων ακόμη και σε πραγματικό χρόνο!
Διαχείριση του WAN από τον φορέα και όχι από τον χρήστη	Χρήση υπάρχουσας υποδομής	Βέλτιστη αξιοποίηση του διαθέσιμου εύρους ζώνης
Φθηνότερη μόνιμη σύνδεση σε σχέση με την αφιερωμένη γραμμή	Ιδανική για χρήση σαν εφεδρικής γραμμής	-

ΜΕΙΟΝΕΚΤΗΜΑΤΑ

Frame Relay	***ISDN***	***ATM***
Σχετικά υψηλό αρχικό κόστος	Δεν επαρκεί για μεταφορά μεγάλης ποσότητας δεδομένων	Πρότυπα που ακόμη αναπτύσσονται
-	Ακριβό για συνεχή μεταφορά δεδομένων	Όχι ευρεία διάθεση
-	-	Όχι οικονομική

ΙΔΙΑΙΤΕΡΑ ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ

Frame Relay	***ISDN***	***ATM***
Διασύνδεση πολλών απομακρυσμένων τοπικών δικτύων	Ικανότητα μετάδοσης φωνής, εικόνας, δεδομένων	Κίνηση μεγάλου όγκου φωνή, εικόνας και δεδομένων
Η καλύτερη εναλλακτική λύση ως προς τις ψηφιακές αφιερωμένες γραμμές	Σαν εφεδρική γραμμή μαζί με ασύγχρονες επιλεγόμενες τηλεφωνικές γραμμές	-

Τα βασικά οφέλη για το VPN’s συνοψίζονται στα εξής:

Σύνδεση όλων των υποκαταστημάτων της εταιρείας : Το MPLS VPN θα επιτρέψει στην εταιρεία, να συνδέσει όλα τα σημεία παρουσίας της μεταξύ τους, επιτρέποντας έτσι την ανταλλαγή πληροφοριών μεταξύ υπολογιστών και εφαρμογών ή ακόμα και μεταφορά φωνής μεταξύ υπαλλήλων που βρίσκονται σε διαφορετικές πόλεις.

Προμήθεια ολοκληρωμένου αλλά και ευέλικτου πακέτου υπηρεσιών : Όλες οι λύσεις ιδεατών ιδιωτικών δικτύων παρέχουν όλα τα απαραίτητα δομικά συστατικά και πόρους που απαιτούνται για να λειτουργήσουν, χωρίς να αναγκάζουν το τελικό πελάτη να προβεί σε προμήθειες ή επενδύσεις – Είναι λύσεις “με το κλειδί στο χέρι”.

Προτεραιότητα φωνής, δεδομένων, Internet (QoS) : Στις περιπτώσεις αυτές των δικτύων όπου υπάρχει η ανάγκη μεταφοράς πολλών τύπων δεδομένων (φωνή, δεδομένα, Internet), το δίκτυο του παρόχου της υπηρεσίας ανάλογα με το διαθέσιμο εύρος ζώνης και τις προτεραιότητες του πελάτη, είναι δυνατόν να ορίσει τις προτεραιότητες των τύπων των δεδομένων με τέτοιο τρόπο ώστε οι κρίσιμες εφαρμογές να μην παρουσιάσουν σε καμία περίπτωση πρόβλημα επικοινωνίας.

Ελαχιστοποίηση του κόστους: Η εγκατάσταση και παροχή του VPN είναι μόνο ένα κλάσμα του κόστους που θα επένδυε σε διαφορετική περίπτωση η επιχείρηση για την

δημιουργία ενός συμβατικού δικτύου με μίσθωση γραμμών διασύνδεσης των απομακρυσμένων σημείων.

Βέλτιστη ασφάλεια : Η ασφάλεια κατά την ανταλλαγή ευαίσθητων δεδομένων μεταξύ των σημείων παρουσίας της εταιρείας είναι συνήθως ένα θέμα που απασχολεί τους διαχειριστές του δικτύου. Η σύνδεση VPN και κυρίως η τεχνολογία υλοποίησης MPLS που χρησιμοποιείται δημιουργεί ένα ασφαλές κανάλι μεταφοράς δεδομένων μέσα από το δίκτυο IP. Επιπλέον, η επιλογή προστασίας από firewall περιορίζει την πρόσβαση από και προς άλλα δίκτυα.

Μηδενικό κόστος διαχείρισης : Η διαχείριση του δικτύου γίνεται εξ' ολοκλήρου από το Network Operation Center του παρόχου της υπηρεσίας.

Το θέμα των VPNs είναι συνεχώς σε εξέλιξη. Το πιο ενδιαφέρον των VPNs είναι η διαθεσιμότητα των IP-sec-στάνταρ. Αυτό που μπορεί να φρενάρει κάποιον σχετικά με τα VPNs είναι το μεγάλο κόστος της επένδυσης και οι μεγάλες υποσχέσεις που δίνουν οι κατασκευαστές. Από τη στιγμή που τα VPNs αναγνωρίστηκαν ως τα πιο ασφαλή, πολλές επιχειρήσεις επένδυσαν πάνω σε αυτά. Πολλές επιχειρήσεις πλέον στο εξωτερικό αρχίζουν να αντικαθιστούν τα παλαιότερα δίκτυα με IP-VPNs.

Με απλά λόγια (Επίλογος)

Το να μπορέσει κάνει να πει με ακρίβεια τι είναι ένα ιδεατό ιδιωτικό δίκτυο είναι δύσκολο, μια και ο καθένας θα έλεγε κάτι διαφορετικό. Με απλά λόγια ένα VPN είναι η συνεργασία πολλών πρωτοκόλλων και δικτύων. Με τέτοιο τρόπο που οι πληροφορίες και τα δεδομένα να μεταφέρονται με ασφάλεια από τον αποστολέα στον παραλήπτη χωρίς να μπορεί κανείς άλλος να τις αναγνώσει ή ακόμα και να τις αλλοιώσει. Δίνοντας απλώς την αίσθηση στους χρήστες ότι το μόνο δίκτυο που υπάρχει είναι αυτό που συναλλάσσονται.

Πιο συγκεκριμένα, ο ακριβής ορισμός που θα μπορούσε κανείς να δώσει για εικονικό ιδιωτικό δίκτυο είναι ο εξής. Μια τεχνολογία που χρησιμοποιεί κρυπτογράφηση και σήραγγα IP για να μπορεί ένας οργανισμός με πολλές τοποθεσίες να χρησιμοποιεί συνδέσεις internet χαμηλού κόστους μεταξύ των τοποθεσιών, αλλά και να διατηρεί τα δεδομένα εμπιστευτικά.

Οι αντίστοιχες λοιπόν ορολογίες εμφανίζονται :

- **“virtual”** : Σημαίνει ότι ενώ από την πλευρά του χρηστή φαίνεται σαν να μιλάμε για ένα απλό σύστημα δικτυού, στην πραγματικότητα πίσω από ένα VPN βρίσκονται πολλά κομμάτια από συστήματα άλλων δικτύων.
- **“private”** :Σημαίνει ότι η επικοινωνία γίνεται εμπιστευτικά και όχι δημόσια εφόσον αποτελείτε από ασφαλή δίαυλο επικοινωνίας μεταξύ ενός απομακρυσμένου χρήστη και των συστημάτων της επιχείρησης, επομένως ο κίνδυνος για διάφορες επιπλοκές ελαχιστοποιείται.
- **“network”** : Σημαίνει ότι μια καλά επιλεγμένη ομάδα από υπολογιστικά συστήματα ενώνονται μεταξύ τους και με τη βοήθεια ενός πρωτοκόλλου (TCP/IP οικογένεια πρωτοκόλλων) μπορούν να επικοινωνούν.

Και τελος το σημαντικό είναι ότι το κάνουν καλά και οικονομικά σχέση με τα παλιά παραδοσιακά δίκτυα.

- Μικρότερο κόστος από αυτό των ιδιωτικών δικτύων.
- Μειωμένα έξοδα διαχείρισης συγκρινόμενα, αυτά της ιδιοκτησίας και λειτουργίας ιδιωτικού δικτύου.
- Απλοποίηση των δικτυακών τοπολογιών μειώνοντας έτσι το φόρτο διαχείρισης.

Βιβλιογραφία

1. Dave Kosiur, “Building and Managing Virtual Private Networks”, John Wiley & Sons, 1998.
2. Gordon Chaffee , “Διαλέξεις από το Πανεπιστήμιο του Berkeley” (2005)
3. Charlie Scott, Paul Wolfe and Mike Erwin, “Virtual Private Networks – Second Edition”, O’Reilly, 1999.
4. G. Montenegro. “Reverse Tunneling for Mobile IP, revised”. IETF RFC: 3024, January 2001.
5. C. Retsas. “DSL Technology, DLS Service Models, and Charging DSL Services”. MSc Thesis (in Greek), Computer Science Department, University of Crete, Greece, November 2000.
6. Joseph Steinberg - Timonth Speed, "SSL VPN Understandig, evaluating, and planning secure, web-based remote access", Packt Publishing 2005
7. James s, Tiller, "A Technical Guaide to IPSec Virtula Private Networks", Auerbach Publications 2001
8. IPSec VPN Design By Vijay Bollapragada, Mohamed Khalid, Scott Wainner ,Cisco Press 2005
9. Virtual Private Networks, Second Edition Charlie Scott, Paul Wolfe, Mike Erwin, O'Reilly 1999
10. Implementing Virtual Private Networks, Brown, Steven. McGraw-Hill Professional 1999
11. Comer, Douglas E. Διαδίκτυα με TCP/IP. Κλειδάριθμος 2001
12. Διαδίκτυο http://www.vpnc.org/
    http://www.cisco.com/
    http://conta.uom.gr/
    http://el.wikipedia.org/
    http://www.it.uom.gr/

ΠΕΡΙΛΗΨΗ

Στην παρούσα εργασία αναπτύσσονται τα βασικά πράγματα που χρειαζόμαστε για την δημιουργία ενός ιδεατού ιδιωτικού δικτυού και η βασικές γνώσεις δικτύων που τα απαρτίζουν.

Στο κεφάλαιο 1 υπάρχουν μερικά γενικά στοιχεία για την δημιουργία των VPNs και βασικές γνώσεις που πρέπει να ξέρει κάνει για να μπορέσει να κατανοήσει την λειτουργία τους (ενθυλάκωση, μοντέλο OSI, δίκτυα μεταφοράς δεδομένων).

Στο κεφαλαίο 2 αναπτύσσονται θέματα γύρο από τα βασικά πρωτοκολλά που χρησιμοποιούν τα VPNs (PPTP, IPSec, P2F,P2TP,MPPE, CHAP KAI GRE).

Στο κεφάλαιο 3 αναφέρονται θέματα γύρο από την τεχνολογία δικτύων IP, ATM, Frame relay και τις τεχνολογίες που χρησιμοποιούν τα VPNs IPSec, SSL, MPLS και OpenVPN. Αναφέρονται επίσης και οι μορφές των VPNs.

Στο κεφαλαίο 4 εξετάζονται θέματα γύρο από την χρησιμότητα ,τις παροχές των VPNs , τον σκοπό τους και την ολοκλήρωση τους. Γίνεται λόγος επίσης για την QoS ποιότητα υπηρεσιών.

Στο κεφάλαιο 5 θα δούμε τα θέματα ασφάλεια που δομούν τα VPN και θα εξετάσουμε διάφορες έννοιες γύρο από τους μηχανισμούς ασφαλείας