ΤΕΙ ΜΕΣΟΛΟΓΓΙΟΥ
ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑ
ΤΜΗΜΑ ΕΦΑΡΜΟΓΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΣΤΗΝ ΔΙΟΙΚΗΣΗ ΚΑΙ ΤΗΝ ΟΙΚΟΝΟΜΙΑ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ TCP/IP ΚΑΙ Η ΔΙΑΧΕΙΡΙΣΗ ΤΗΣ

ΓΕΩΡΓΙΑ ΖΑΧΑΡΙΑΔΟΥ
Α.Μ :8719

ΚΑΤΕΡΙΝΑ ΖΑΦΕΙΡΟΠΟΥΛΟΥ
ΑΜ :8718

Επιβλέπων καθηγητής :
Επιστημονικός συνεργάτης Γεώργιος Αλεξανδρής

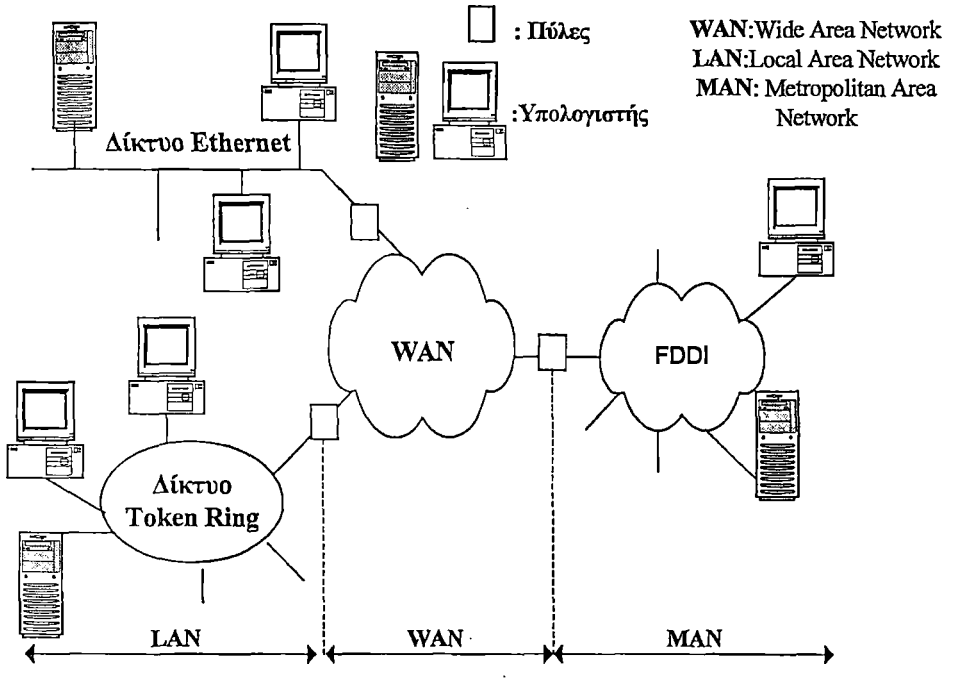
ΠΕΡΙΕΧΟΜΕΝΑ

1. ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ

1.1 Γενικά

Είναι σε όλους πλέον γνωστό , ότι η κοινωνία έχει ξεφύγει από τα όρια της λεγόμενης «βιομηχανικής εποχής» και έχει εισέλθει σε μια νέα, πολλά υποσχόμενη εποχή, αυτή της πληροφορίας και της διακίνησής της από άκρο σε άκρο σε όλο τον πλανήτη. Παρόλο όμως που βρισκόμαστε ακόμα, τουλάχιστον χρονικά, στην αρχή αυτής της νέας εποχής, η ταχύτατη ανάπτυξη της τεχνολογίας, έδωσε όλα τα απαραίτητα εργαλεία στον άνθρωπο, για να μπορέσει να πραγματοποιήσει μια αξιοθαύμαστη πρόοδο σε όλους τους τομείς της πληροφορικής.

Η μεγάλη ανάγκη ανθρώπων, οργανισμών και εταιρειών για αναζήτηση, αποθήκευση και επεξεργασία πληροφοριών, έδωσε το έναυσμα για την δημιουργία πολύπλοκων (από άποψη τοπολογίας) και πολυσύνδετων δικτύων υπολογιστών, που είτε εκτείνονται σε μεγάλες περιοχές του κόσμου είτε έχουν τοπικό χαρακτήρα. Τα δίκτυα αυτά εξυπηρετούν την ανάγκη για επικοινωνία και ανταλλαγή πληροφοριών. Παράδειγμα ενός τέτοιου δικτύου δίνεται στο Σχήμα 1-1.



Σχήμα 1-1:Ένα σύγχρονο δίκτυο επικοινωνιών

Η αλματώδης εξάπλωση των δικτύων δίνει τη δυνατότητα σε χρήστες από κάθε σημείο του πλανήτη να έχουν πρόσβαση στις πληροφορίες που διακινούνται μέσω ενός δικτύου. Αυτή η δυνατότητα πρόσβασης , σε πολλές περιπτώσεις, κρίνεται απαραίτητο να περιορισθεί, καθώς η μεταφορά δεδομένων έχει ιδιωτικό ή εμπιστευτικό χαρακτήρα και πρέπει να εξασφαλίζεται η ακεραιότητά της, καθώς επίσης και η απόκρυψη αυτών των δεδομένων από άτομα που δεν είναι εξουσιοδοτημένα να τα επεξεργαστούν με οποιονδήποτε τρόπο. Αυτές ,ακριβώς, οι απαιτήσεις συνέβαλλαν ,ώστε η ασφάλεια των δικτύων να συγκαταλέγεται στις μέρες μας ανάμεσα στα πλέον σημαντικά θέματα .

Επειδή δεν ζούμε σε έναν κόσμο που είναι αγγελικά πλασμένος, πολλοί είναι αυτοί που προσπαθούν (με επιτυχία πολλές φορές) να εισχωρήσουν στις διαδικασίες επεξεργασίας και μεταφοράς πληροφοριών, με αποτέλεσμα να πραγματοποιούν τα κακοπροαίρετα και επιβλαβή σχέδιά τους. Δυστυχώς όμως, παρά τις προσπάθειες που έχουν γίνει ως σήμερα, δεν ήταν

δυνατόν να εξαλειφθούν οι επιθέσεις κατά της ασφάλειας της πληροφορίας. Αυτό με μια πρώτη ματιά φαίνεται να είναι κάπως αντιφατικό, καθώς η ραγδαία ανάπτυξη της τεχνολογίας (θα σκεφτόταν κανείς) έπρεπε να παρέχει τα απαραίτητα εργαλεία για να μην υπάρχει παρανομία ηλεκτρονικής μορφής.

Ωστόσο, δεν πρέπει να ξεχνούμε πως η τεχνολογία που χρησιμοποιείται προκειμένου να « θωρακίσει » ένα δίκτυο από επιθέσεις κατά της ασφάλειας , μπορεί εξίσου να δώσει πολλά «όπλα» σε όσους επιθυμούν να ενεργήσουν παράνομα στον κόσμο της πληροφορίας. Κατά συνέπεια, η ανάπτυξη της τεχνολογίας, παρόλο που μπορεί να δίνει λύσεις όσον αφορά στην ασφάλεια των δικτύων, αποτελεί και πηγή δημιουργίας ολοένα και περισσότερων κινδύνων.

Επιπλέον, έχει παρατηρηθεί πως ,παρόλο που από την στιγμή που πραγματοποιείται μια επίθεση ,μεσολαβεί μικρό σχετικά χρονικό διάστημα έως ότου δημιουργηθεί κάποιος καινούριος μηχανισμός ασφάλειας που αποτρέπει παρόμοιες επιθέσεις ,το ίδιο σύντομα βρίσκεται ένας νέος πιο αποτελεσματικός τρόπος να παρακαμφθεί ο μηχανισμός αυτός. Με άλλα λόγια, θα μπορούσε να πει κανείς, πως είναι αδύνατον να απαλλαχθούμε εντελώς από κινδύνους στην ασφάλεια. Σε καμία ,όμως, περίπτωση δεν πρέπει το γεγονός αυτό να μας αποθαρρύνει από το να προσπαθούμε συνεχώς να ελαχιστοποιούμε τις απειλές εναντίον της πληροφορίας. Ακριβώς αυτή η προσπάθεια οδήγησε στη δημιουργία ειδικών πρωτοκόλλων, πολιτικών και διαδικασιών στην ασφάλεια των δικτύων, που σαν στόχο έχουν να εμποδίσουν αυτού του είδους τις επιθέσεις και να εξασφαλίσουν όσο το δυνατόν περισσότερο την ασφάλεια των πληροφοριών.

Πριν προχωρήσουμε θα δώσουμε μερικούς βασικούς ορισμούς που αφορούν την ασφάλεια :

- **Εισβολέας (Intruder) - Πειρατής(Hacker)** :Μεμονωμένες οντότητες που αποκτούν ή προσπαθούν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση σε ένα υπολογιστικό σύστημα καθώς και μη εξουσιοδοτημένα προνόμια σε αυτό.
- **Ιός (Virus)** : Κώδικας ενσωματωμένος σε ένα πρόγραμμα που δημιουργεί αντίγραφο του εαυτού του , το οποίο εισάγεται σε ένα ή περισσότερα άλλα προγράμματα. Εκτός από τη διάδοσή του ο ιός συνήθως εκτελεί και κάποια ανεπιθύμητη λειτουργία.
- **Λογισμικό Σκουλήκι (Worm)** :Πρόγραμμα (Λογισμικό) το οποίο αναπαράγει τον εαυτό του και στέλνει αντίγραφα από υπολογιστή σε υπολογιστή κατά μήκος μιας σύνδεσης δικτύου.
- **Μικρόβιο** ή **Βακτήριο (Bacteria)** :Πρόγραμμα το οποίο καταναλώνει πόρους του συστήματος αναπαράγοντας διαρκώς τον εαυτό του .
- **Δούρειος Ίππος (Trojan Horse)** : Ένα πρόγραμμα υπολογιστή με μία φαινομενικά ή πραγματικά χρήσιμη λειτουργία που περιλαμβάνει κάποια πρόσθετη (κρυμμένη) λειτουργία ,η οποία λαθραία εκμεταλλεύεται τη νόμιμη εξουσιοδότηση της επικαλούμενης διαδικασίας για ζημιά της ασφάλειας.

Σ' αυτό το σημείο είναι χρήσιμο να κάνουμε ένα μικρό διαχωρισμό, όσον αφορά στην ασφάλεια των πληροφοριών. Το κριτήριο σύμφωνα με το οποίο γίνεται αυτός ο διαχωρισμός, είναι κατά κάποιο τρόπο θα λέγαμε «τοπολογικό» , καθώς χρησιμοποιούμε τον όρο **ασφάλεια των υπολογιστών (computer security)** , όταν αναφερόμαστε στην προστασία πληροφοριών σε μεμονωμένους υπολογιστές, ενώ κάνουμε λόγο για **ασφάλεια δικτύων (network security)**, εννοώντας το σύνολο των διαδικασιών που σαν στόχο έχουν να αποτρέψουν και να παρεμποδίσουν επιθέσεις σε δεδομένα κατά τη διάρκεια της μετάδοσής τους μέσα από ένα δίκτυο.

Ένα σημαντικό πρόβλημα ασφάλειας για τα συστήματα δικτύου είναι η εχθρική , ή τουλάχιστον ανεπιθύμητη , παράνομη δράση των χρηστών ή του λογισμικού. Η παράνομη δράση των χρηστών μπορεί να λάβει τη μορφή ανεπιθύμητης σύνδεσης σε μία μηχανή, ή στην περίπτωση μη εξουσιοδοτημένου χρήστη απόκτησης προνομίων ή τη μορφή εκτέλεσης ενεργειών πέρα όσων είχαν εξουσιοδοτηθεί. Η παράνομη δραστηριότητα του λογισμικού μπορεί να λάβει τη μορφή ενός ιού ή σκουληκιού ή Δούρειου Ίππου.

Όλες αυτές οι επιθέσεις σχετίζονται με την ασφάλεια δικτύου καθώς η είσοδος σε ένα σύστημα μπορεί να γίνει με χρήση των μέσων ενός δικτύου. Ωστόσο ,αυτές οι επιθέσεις δεν περιορίζονται σε επιθέσεις βασιζόμενες στα δίκτυα. Ένας χρήστης με δυνατότητα πρόσβασης σε ένα τοπικό τερματικό μπορεί να αποπειραθεί να παρανομήσει χωρίς να χρειαστεί να χρησιμοποιήσει κάποιο ενδιάμεσο δίκτυο. Ένας ιός ή ένας Δούρειος Ίππος μπορεί να εισαχθεί σε ένα τερματικό μέσω μίας δισκέτας. Μόνο το Σκουλήκι είναι ένα μοναδικό δικτυακό φαινόμενο. Επομένως , η παρανομία στα συστήματα είναι μία ενέργεια για την οποία η Ασφάλεια Δικτύων και η Ασφάλεια Υπολογιστών έχουν ιδιαίτερη βαρύτητα.

Ακριβώς όπως γίνεται και με κάθε είδους παράνομη δραστηριότητα, οι επιθέσεις εναντίον πληροφοριών και δικτύων, προέρχονται από ένα μικρό ποσοστό του πληθυσμού. Ανεξάρτητα από το τι προσπαθούν οι άνθρωποι να προστατέψουν (το δίκτυό τους, το αυτοκίνητό τους, το σπίτι τους) είναι πολύ σημαντικό να έχουν μια γενικότερη ιδέα για τους πιθανούς κινδύνους που μπορεί να παρουσιάζονται κατά καιρούς. Μόνο έχοντας αυτή τη γνώση, θα μπορέσουν να επιλέξουν είτε μια απλή είτε μια πιο πολύπλοκη στρατηγική (ανάλογα κυρίως με την αξία της ιδιοκτησίας τους), καθώς και τα κατάλληλα εργαλεία ή διαδικασίες για να προστατέψουν αυτό που από την αρχή είχαν στο μυαλό τους.

Συγκεκριμένα, όσον αφορά στην ασφάλεια των δικτύων, η διαδικασία που ακολουθείται ,προκειμένου καταλήξει κανείς στην απόφαση σχετικά με την πιο ενδεδειγμένο τρόπο να προστατευτεί ένα δίκτυο και στη συνέχεια να προβεί στην υλοποίηση είναι ιδιαίτερα επίπονη καθώς πρέπει να ληφθούν υπόψη πολλές παράμετροι. Η διαδικασία αυτή καλείται **Διαχείριση Διακινδύνευσης** και αναλύεται στην επόμενη ενότητα.

1.2 Διαχείριση Διακινδύνευσης

Η **Διαχείριση Διακινδύνευσης (Risk Management)** η οποία χωρίζεται σε δύο σκέλη:

- την **αξιολόγηση διακινδύνευσης (risk assessment)** και
- τον έλεγχο **διακινδύνευσης (risk control)** ,

καθένα από τα οποία χωρίζεται με τη σειρά του σε επιμέρους βήματα. Τα βήματα της διαχείρισης διακινδύνευσης , όπως παρατηρούμε και στο Σχήμα 1-2, είναι :

- **Συλλογή στοιχείων**: Εκτελείται απογραφή στοιχείων ποσοτικού και λειτουργικού χαρακτήρα σχετικά με το δίκτυο στο σύνολό του, όπως είναι ο υπάρχον εξοπλισμός , τα πρωτόκολλα που χρησιμοποιούνται , η κίνηση του δικτύου , η τρέχουσα πολιτική ασφάλειας και οι υπηρεσίες ασφάλειας που παρέχει το δίκτυο .

- **Ανάλυση Διακινδύνευσης** : Πρόκειται για μία ιδιαίτερα πολύπλοκη διαδικασία με στόχο, αφού αξιολογηθούν ποιοτικά χαρακτηριστικά σχετικά με το δίκτυο ,όπως είναι η αξιοπιστία του δικτύου και η ακεραιότητά του αλλά και οι απειλές στις οποίες είναι εκτεθειμένο , να καθοριστούν οι πρόσθετες ανάγκες σε υλικό και σε λογισμικό ,που θα συμβαδίζουν με τους διαθέσιμους οικονομικούς πόρους μιας εταιρείας και θα μπορούν να εγγυηθούν την ασφάλεια του δικτύου.

- **Πίνακας Ενεργειών**: Αφορά στην καταγραφή των πρόσθετων αναγκών σε υλικό και λογισμικό προκειμένου να ενισχυθεί το δίκτυο από άποψη ασφάλειας .

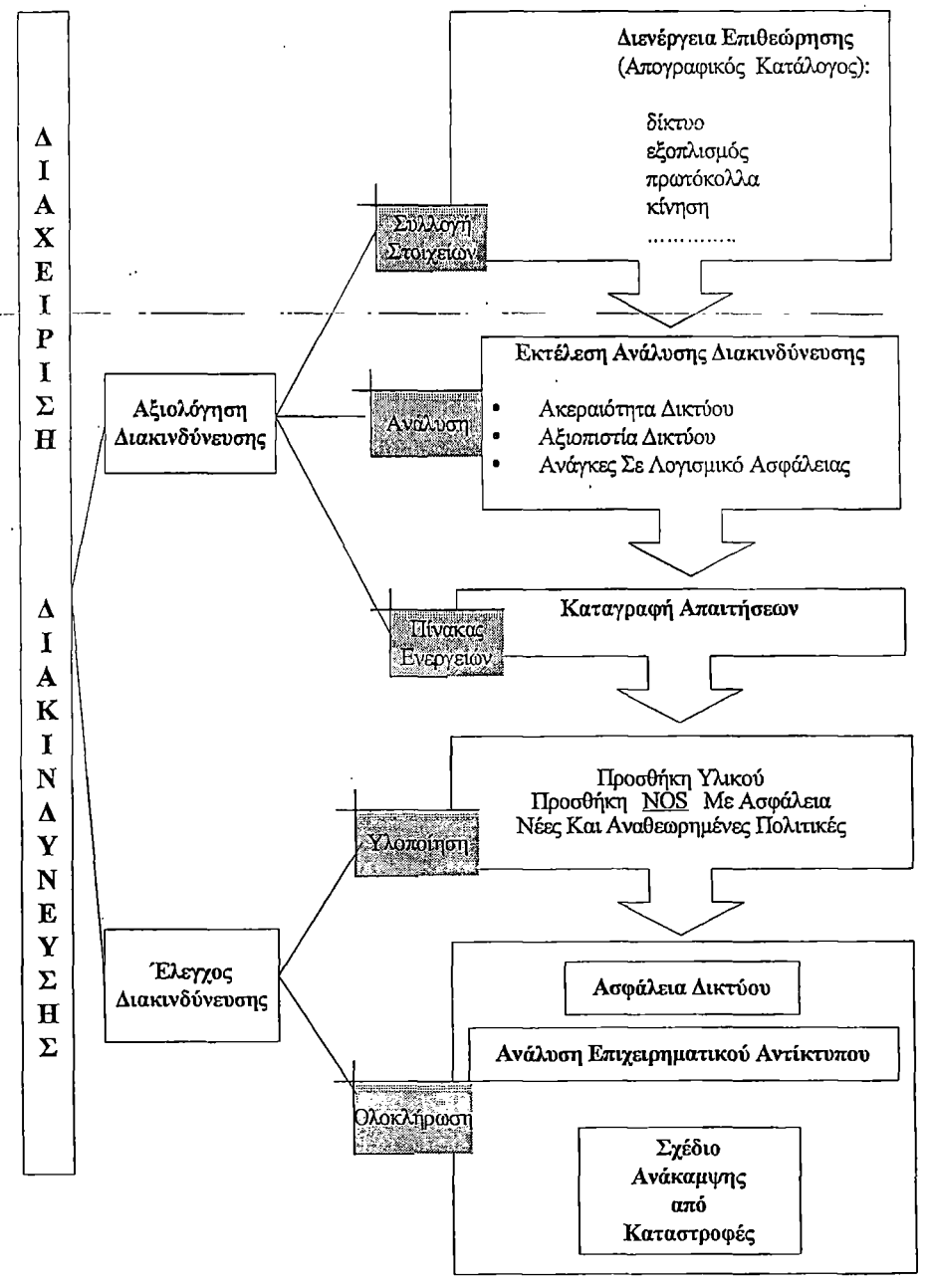
- **Υλοποίηση**:Εφαρμογή όσων έχουν αποφασιστεί στα παραπάνω βήματα.

- **Ολοκλήρωση**: Όλη η παραπάνω μελέτη ολοκληρώνεται (συμπληρώνεται) με την ανάλυση των συνεπειών που θα επιφέρει (αντίκτυπος) σε μία επιχείρηση μία επιτυχημένη επίθεση κατά της ασφάλειας του δικτύου της **(Business Impact Analysis - BIA)**. Επιπλέον προτείνονται τρόποι με τους οποίους μπορεί η επιχείρηση να ανακάμψει από καταστροφές

καθώς και το αντίστοιχο χρονοδιάγραμμα στο οποίο αυτή η ανάκαμψη είναι εφικτή **(Disaster Recovery Plan - DRP).**

Η συλλογή στοιχείων , η ανάλυση διακινδύνευσης και η καταγραφή απαιτήσεων απαρτίζουν την αξιολόγηση διακινδύνευσης , ενώ η υλοποίηση και η ολοκλήρωση απαρτίζουν τον έλεγχο διακινδύνευσης .

Στη συνέχεια γίνεται ανάλυση των επιμέρους βημάτων. Έτσι στην ενότητα 1.3 αναλύεται το θέμα της ακεραιότητας και της αξιοπιστίας του δικτύου ,στην ενότητα 1.4 δίδονται γενικές έννοιες που αφορούν στην ασφάλεια του λογισμικού του δικτύου .



Σχήμα 1-2:Τα στάδια της Διαχείρισης Διακινδύνευσης

Τέλος στην ενότητα 1.5 αναλύεται το θέμα της Σχεδίασης της συνέχισης της λειτουργίας σε μια επιχείρηση (ή σε ένα δίκτυο που ανήκει στην επιχείρηση) μετά από μια καταστροφή.

Η ανάλυση που ακολουθεί αφορά αποκλειστικά την ασφάλεια δικτύων ή γενικότερα των Τηλεπικοινωνιών και όχι την φυσική ασφάλεια (π.χ. φρουρά , κάμερες κλπ). Για παράδειγμα θα μπορούσε να αναφέρεται στην ασφάλεια δικτύου Υπολογιστών που ανήκει σε μία επιχείρηση (π.χ. τράπεζα) και έχει υποκαταστήματα σε διάφορα σημεία της χώρας.

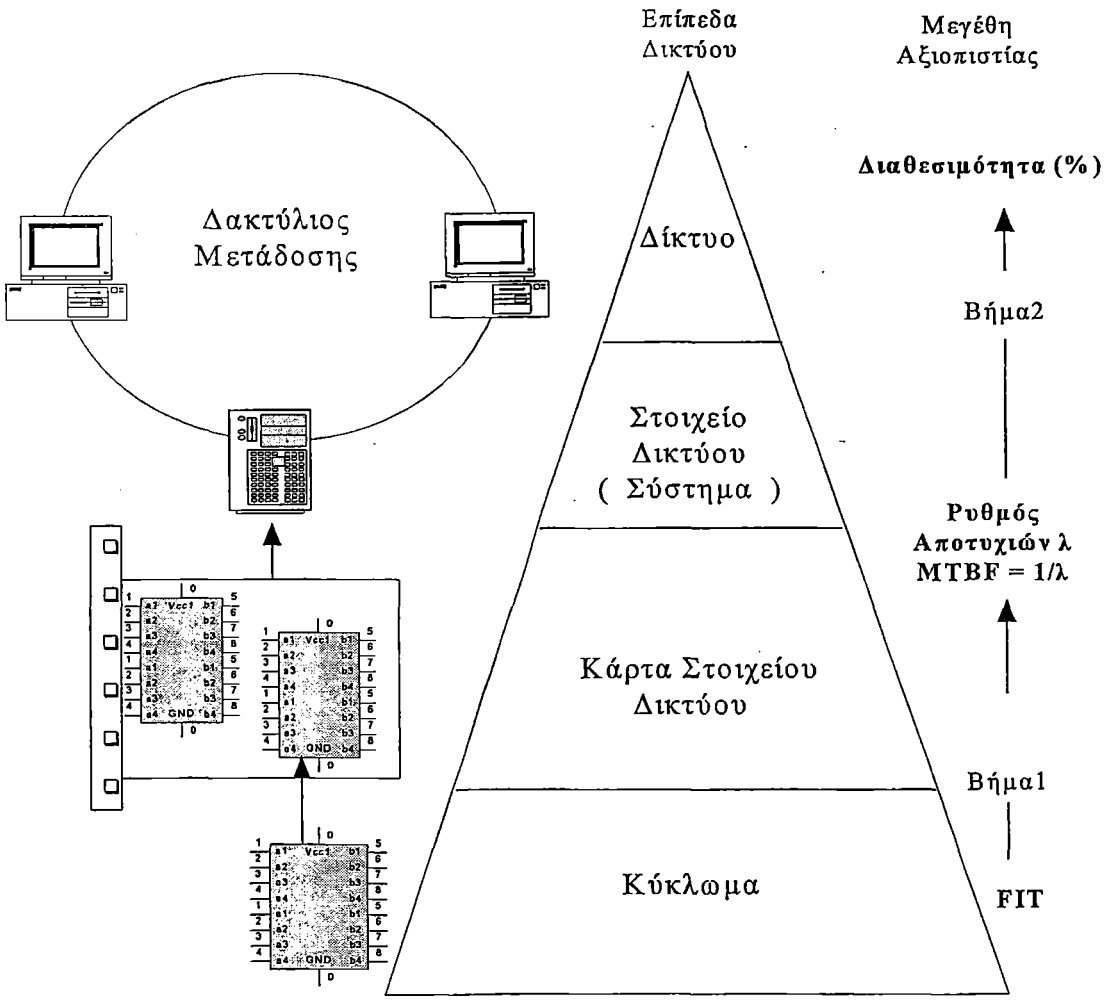
1.3 Ακεραιότητα και Αξιοπιστία Δικτύου

Η ακεραιότητα ενός δικτύου (Integrity) προσδιορίζεται κυρίως από τα μεμονωμένα σημεία αποτυχίας (Single Point of Failure – SPoF) που μπορεί να έχει .Ένα τέτοιο σημείο σε ένα δίκτυο μπορεί να είναι εξαρτήματα ή διαδρομές η αποτυχία των οποίων θα μπορούσε να θέσει το δίκτυο εκτός λειτουργίας. Για παράδειγμα αναφέρουμε μια διαδρομή στην οποία τόσο η κύρια όσο και η εφεδρική οπτική ίνα περνούν από τον ίδιο αγωγό. Σε αυτή την περίπτωση , ένα κόψιμο του αγωγού θα έχει ως αποτέλεσμα την απώλεια της ζεύξης.

Η αξιοπιστία ενός δικτύου (Reliability) χαρακτηρίζεται από την διαθεσιμότητα (Availability) αυτού, δηλαδή από την πιθανότητα που έχει να λειτουργεί και να είναι διαθέσιμο στους χρήστες. Ένα δίκτυο που έχει διαθεσιμότητα 99,999% είναι πολύ αξιόπιστο .Στο Σχήμα 1-3 δίνονται σε μία ιεραρχική δομή τα συστατικά στοιχεία ενός δικτύου (αριστερά) καθώς και τα διάφορα μεγέθη που χαρακτηρίζουν την αξιοπιστία των στοιχείων αυτών (δεξιά).

Ένα κύκλωμα χαρακτηρίζεται από την αριθμό των αποτυχιών (βλάβες) σε κάποιο χρονικό διάστημα συνήθως 10^9 ώρες. (Failure In time-FIT). Μια κάρτα στοιχείου δικτύου χαρακτηρίζεται από τον ρυθμό αποτυχιών λ (failure rate) που στην ουσία είναι τα άθροισμα των FIT των κυκλωμάτων από τα οποία αποτελείται αυτή η κάρτα .Το αντίστροφο αυτού του μεγέθους δίδει το Μέσο Χρόνο Μεταξύ δύο Διαδοχικών Αποτυχιών (Mean Time Between Failure –MTBF). Ισχύει:

$$MTBF = 1 / \lambda$$



Σχήμα 1-3:Ιεραρχική δομή στοιχείων δικτύου και χαρακτηριστικά μεγέθη της Αξιοπιστίας ενός δικτύου

Το στοιχείο δικτύου αποτελείται από διάφορες κάρτες που άλλες βρίσκονται σε σειρά και άλλες είναι παράλληλα για λόγους πλεονασμού (εφεδρείας).Από τα λ αυτών των καρτών υπολογίζεται το λ του στοιχείου του δικτύου. Τέλος ένα ολόκληρο δίκτυο χαρακτηρίζεται από τη Διαθεσιμότητα (Availability-A) που είναι η επί τοις εκατό πιθανότητα τα στοιχεία του δικτύου να λειτουργούν καλά. Ο υπολογισμός των μεγεθών που αναφέρονται παραπάνω ξεφεύγει από τα όρια αυτής της μελέτης καθώς απαιτεί πολύπλοκους μαθηματικούς τύπους και έννοιες από τη θεωρία πιθανοτήτων.

1.4 Βασικές Έννοιες Ασφάλειας Δικτύου

Ο όρος **επιθέσεις** κατά της ασφάλειας **(security attacks)** αναφέρεται σε ενέργειες κάθε είδους, που ως στόχο έχουν να παρακάμψουν την ασφάλεια του δικτύου, για να παρέμβουν με οποιονδήποτε τρόπο στην πληροφορία ενός οργανισμού, καθώς και στην κίνηση της μέσα στο δίκτυο. Οι πιθανές ενέργειες που μπορεί να έχει μια επιτυχημένη επίθεση εναντίον της ασφάλειας ενός δικτύου αποτελούν τις λεγόμενες **διακινδυνεύσεις ασφάλειας** (**security risks**).

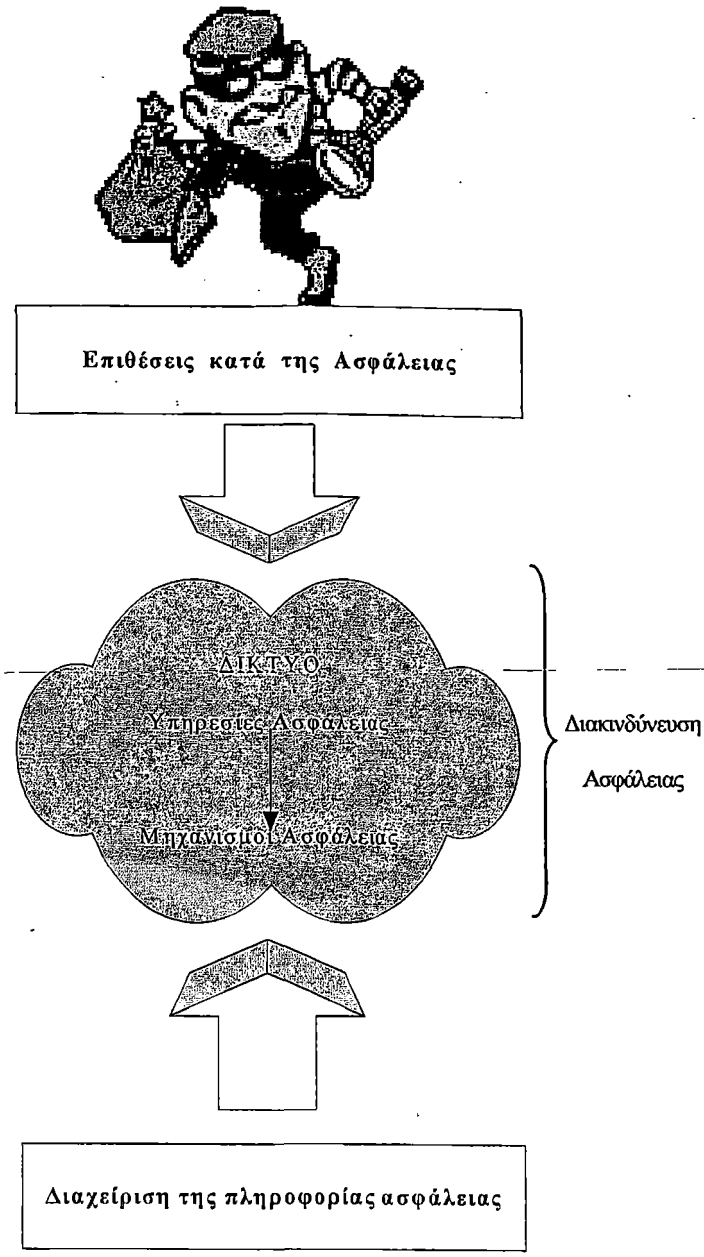
Στη διεθνή βιβλιογραφία ο αναγνώστης πιθανό να συναντήσει και τον όρο απειλή (threat) κατά της ασφάλειας. Με τον όρο αυτό εννοούμε κάθε περιστατικό ή γεγονός που έχει τη δυνατότητα να παραβιάσει την ασφάλεια του δικτύου. Προς αποφυγή σύγχυσης ο όρος αυτός δε θα χρησιμοποιηθεί ξανά στην ανάλυση που ακολουθεί.

Παρόλο που δεν είναι εφικτό να προστατευθεί ένα δίκτυο ή στοιχείο δικτύου απόλυτα από τις επιθέσεις, ωστόσο η λήψη προληπτικών μέτρων μπορεί ως ένα βαθμό να παρέχει ικανοποιητικά επίπεδα ασφάλειας. Για το λόγο αυτό, κάθε οργανισμός οφείλει να καθορίσει τα επίπεδα διακινδύνευσης που είναι ανεκτά για να μπορέσει να λειτουργήσει και να λάβει προληπτικά μέτρα ασφάλειας για εκείνες τις επιθέσεις που θα καθιστούσαν δύσκολη, αν όχι αδύνατη , την συνέχιση των εργασιών του .

Έτσι καθορίζονται **οι υπηρεσίες ασφάλειας (security services)** . Πρόκειται για υπηρεσίες που σαν σκοπό έχουν να παρέχουν την απαραίτητη ασφάλεια στα συστήματα αποθήκευσης και επεξεργασίας δεδομένων ενός οργανισμού αλλά και να προστατεύουν πληροφορίες κατά τη μετάδοση τους στο δίκτυο. Οι υπηρεσίες ασφάλειας στοχεύουν στο να αντικρούουν κάθε πιθανή επίθεση κατά της ασφάλειας του δικτύου και για το σκοπό αυτό χρησιμοποιούν διάφορους **μηχανισμούς ασφάλειας (security mechanisms).** Οι τελευταίοι , είναι μηχανισμοί σχεδιασμένοι να ανιχνεύουν ένα δίκτυο για να αποτρέπουν πιθανές επιθέσεις κατά της ασφάλειάς του, ή και να συμβάλλουν στην ανάκαμψη του δικτύου ύστερα από κάποια επιτυχημένη επίθεση.

Ο αυτόματος έλεγχος της καλής λειτουργίας του λογισμικού ασφάλειας (δηλαδή των **μηχανισμών** και των **υπηρεσιών ασφάλειας** που αναφέραμε λίγο πριν) εξασφαλίζεται μέσω συστημάτων διαχείρισης. Ανάλυση των Συστημάτων Διαχείρισης Ασφάλειας Δικτύων TCP /IP γίνεται στο κεφάλαιο 4 .

Το Σχήμα 1-4 δείχνει με απλό και κατανοητό τρόπο, το πως αλληλεπιδρούν και συνδέονται όλα τα παραπάνω, δίνοντας μια συνολική και γενική εικόνα για το τι συμβαίνει στον τομέα της ασφάλειας.



Σχήμα 1-4:Το περιβάλλον της ασφάλειας δικτύων και η διαχείριση

1.4.1 Μηχανισμοί Ασφάλειας (Security Mechanisms)

Οι **μηχανισμοί ασφάλειας (security mechanisms)** αποτελούνται από διάφορους αλγόριθμους και πρωτόκολλα και υποστηρίζουν την υλοποίηση των υπηρεσιών ασφάλειας. Ωστόσο, δεν μπορεί ένας μεμονωμένος μηχανισμός ασφάλειας να παρέχει όλες τις υπηρεσίες ασφάλειας, ενώ περισσότεροι του ενός μηχανισμοί μπορεί να υποστηρίζουν την ίδια υπηρεσία . Ένα γενικό χαρακτηριστικό των μηχανισμών ασφάλειας είναι ότι χρησιμοποιούν τεχνικές κρυπτογραφίας . Οι βασικοί μηχανισμοί ασφάλειας είναι :

- Έλεγχος Πρόσβασης (Access Control)
- Κατακερματισμός και σύνοψη μηνύματος (Message Hashing and Digest)
- Κρυπτογράφηση (Encryption),που διακρίνεται με τη σειρά της σε συμμετρική (Symmetric Encryption)και σε μη συμμετρική (Asymmetric Encryptions)

- Ψηφιακή Υπογραφή (Digital Signature)
- Ψηφιακά Πιστοποιητικά (Digital Certificates)

1.4.2 Υπηρεσίες ασφάλειας (Security Services)

Έχοντας κάνει μια γενική αναφορά στα είδη των επιθέσεων που μπορεί να δεχθεί ένα δίκτυο, πρέπει να αναφερθούμε και στις κυριότερες υπηρεσίες ασφάλειας που προσφέρονται για την αντιμετώπισή τους. Οι υπηρεσίες αυτές απευθύνονται σε διαφορετικές περιοχές της προστασίας ενός δικτύου και ταξινομούνται στις ακόλουθες κατηγορίες:

- **Έλεγχος Πρόσβασης (Access Control):** Γνωστοποιεί την ταυτότητα του χρήστη και αποφασίζει, με βάση το προφίλ του, όσον αφορά στην πρόσβαση ή στην χρήση πληροφοριών και εφαρμογών. Στοχεύει στον έλεγχο και στον περιορισμό της πρόσβασης σε συστήματα και εφαρμογές διαμέσου επικοινωνιακών συνδέσεων. Στο στρώμα δικτύου εγγυάται ότι μόνο εξουσιοδοτημένες συσκευές μπορούν να αιτηθούν την εγκατάσταση συνόδου με στοιχεία του δικτύου. Στο στρώμα της εφαρμογής εγγυάται ότι μόνο εξουσιοδοτημένες οντότητες μπορούν να εγκαταστήσουν με επιτυχία σύνδεση με στοιχεία του δικτύου.

Σε επίπεδο εφαρμογής χρήστη εξασφαλίζει ότι μόνο εξουσιοδοτημένοι χρήστες, των οποίων η ταυτότητα θα επαληθεύεται προηγούμενα, θα μπορούν να έχουν πρόσβαση σε πόρους (εφαρμογές) του δικτύου. Επιπλέον σε ορισμένες περιπτώσεις , επιτρέπει πολύ περιορισμένη πρόσβαση, ακόμη και σε μη εξουσιοδοτημένους χρήστες, σε συγκεκριμένους πόρους του δικτύου. Ακόμη μπορεί να επιτρέψει ή να αρνηθεί την ικανοποίηση αιτήσεων ανάλογα με τη στιγμή της ημέρας ή τη μέρα της εβδομάδας κατά την οποία υποβάλλεται αυτή η αίτηση ή τη φυσική διεύθυνση προέλευσης του μηνύματος αίτησης.

- **Επαλήθευση Ομότιμης Οντότητας (Peer Entity Authentication):** Επιβεβαιώνει ότι η επικοινωνία μεταξύ οντοτήτων του δικτύου είναι αυθεντική. Κατά τη διάρκεια εγκατάστασης της σύνδεσης μεταξύ των οντοτήτων ,η υπηρεσία επιβεβαιώνει ότι και οι δύο οντότητες είναι αυθεντικές ,δηλαδή ότι πραγματικά είναι αυτές που ισχυρίζονται. Πρόκειται δηλαδή για το ισοδύναμό του κωδικού ασφαλούς εισόδου χρήστη στο επίπεδο της διμερούς επικοινωνίας. Επίσης ,η υπηρεσία επιβεβαιώνει ότι στη σύνδεση των δύο οντοτήτων δε θα σημειωθεί καμία παρεμβολή από κάποια τρίτη μη εξουσιοδοτημένη οντότητα ,η οποία θα μπορούσε να μεταμφιεστεί σε μία από τις δύο αυθεντικές οντότητες προκειμένου να υποκλέψει πληροφορία ή να προβεί σε επαναδρομολόγηση ή και σε διαγραφή της.

- **Επαλήθευση Προέλευσης Δεδομένων (Data Origin Authentication):** Μετά την εγκατάσταση μιας σύνδεσης μεταξύ εξουσιοδοτημένων οντοτήτων είναι πιθανό ένας εισβολέας να «καταλάβει » αυτή τη σύνδεση διοχετεύοντας δικά του μηνύματα προς οποιαδήποτε από τις οντότητες που επικοινωνούν. Η υπηρεσία επαλήθευσης προέλευσης δεδομένων εξασφαλίζει ότι τα μηνύματα που λαμβάνει καθεμιά από τις οντότητες σε αυτή την επικοινωνία προέρχονται από την άλλη και δεν έχουν εισαχθεί από κάποια εξωτερική μη εξουσιοδοτημένη οντότητα. Η υπηρεσία μπορεί να εφαρμόζεται σε όλα τα μηνύματα που ανταλλάσσουν οι δύο οντότητες ή σε ορισμένα από αυτά.

Πριν προχωρήσουμε στις υπόλοιπες υπηρεσίες ασφάλειας πρέπει να διευκρινίσουμε τη βασική διαφορά που υπάρχει μεταξύ Ελέγχου Πρόσβασης και Επαλήθευσης. Επαλήθευση ενός χρήστη σημαίνει μόνο αναγνώριση της ταυτότητάς του και όχι εκχώρηση δικαιωμάτων για πρόσβαση στα στοιχεία του δικτύου. Αυτό γίνεται με τον Έλεγχο Πρόσβασης που εξασφαλίζει και σε ποια ακριβώς ασφάλεια δικτύου ο χρήστης μπορεί να έχει πρόσβαση.

- **Ακεραιότητα Δεδομένων (Data Integrity):** Προστατεύει την πληροφορία που μεταδίδεται στο δίκτυο από επιθέσεις τροποποίησής της. Ανιχνεύει, δηλαδή προσπάθειες εισβολέων να μεταβάλλουν μηνύματα , προς όφελός τους. Η ανίχνευση τέτοιων παράνομων τροποποιήσεων μηνυμάτων ωθεί τους εξουσιοδοτημένους χρήστες σε λήψη μέτρων

ανάκαμψης ,χωρίς ωστόσο η τελευταία να αποτελεί το σκοπό της υπηρεσίας ακεραιότητας δεδομένων. Εφαρμόζεται είτε σε ένα σύνολο μηνυμάτων ,είτε σε μεμονωμένα μηνύματα , είτε σε επιλεγμένα πεδία ενός μηνύματος.

Ακεραιότητα επιλεγμένων πεδίων (Selective Field Integrity):

Εφαρμόζεται σε περίπτωση που για ορισμένα μόνο πεδία ενός μηνύματος απαιτείται προστασία της ακεραιότητας τους ή τα μέσα που διαθέτει το δίκτυο καθιστούν μη εφαρμόσιμη την ακεραιότητα πλήρους μηνύματος.

Ακεραιότητα πλήρους μηνύματος (Whole Message Integrity) :

Επιτρέπει στον παραλήπτη ενός μηνύματος να διακρίνει εάν το πλήρες μήνυμα που έλαβε έχει υποστεί μεταβολές κατά τη διάρκεια της μετάδοσής του. Στη γενική περίπτωση , πάντως ,δεν εξασφαλίζει αυτόματη επαναφορά από το τροποποιημένο μήνυμα στο αυθεντικό.

Ακεραιότητα συνόδου (Session Integrity) :

Ανιχνεύει τις προσπάθειες εισβολέων να χειριστούν γνήσια μηνύματα που κυκλοφορούν στο δίκτυο με τέτοιο τρόπο ώστε να μη τροποποιείται η πληροφορία που φέρει ένα μήνυμα αλλά αυτούσιο το μήνυμα να δέχεται ένα συνδυασμό από επιθέσεις όπως είναι η επανάληψη, η διαγραφή, η επαναδρομολόγηση και η κακή δρομολόγηση του.

- **Εμπιστευτικότητα Δεδομένων (Data Confidentiality):** Προστατεύει την πληροφορία κατά τη διάρκεια της μετάδοσής της έναντι παθητικών επιθέσεων, όπως είναι η ανάγνωση μηνυμάτων που μεταφέρουν πληροφορία η οποία θεωρείται εμπιστευτική. Βεβαιώνει ότι τα μηνύματα δεν μπορούν να υποκλαπούν από μη εξουσιοδοτημένο χρήστη. Μπορούν μόνο να διαβαστούν από τον προκαθορισμένο παραλήπτη τους. Στη γενική περίπτωση η υπηρεσία της εμπιστευτικότητας εξασφαλίζει ότι το περιεχόμενο ενός μηνύματος δε μπορεί να τροποποιηθεί στο σύνολό του από κάποιον εισβολέα. Ωστόσο, δεν εξασφαλίζει ότι εισβολείς δεν θα επιχειρήσουν αυθαίρετες μεταβολές σε κάποια πεδία του μηνύματος , με τέτοιο τρόπο ώστε ο παραλήπτης του μηνύματος να μη μπορεί να διακρίνει ότι το μήνυμα έχει τροποποιηθεί. Όμοια με την ακεραιότητα δεδομένων η εμπιστευτικότητα παρουσιάζεται σε τρεις μορφές.

Εμπιστευτικότητα επιλεγμένων πεδίων (Selective Field Confidentiality)

Όπως φανερώνει και το όνομά της προστατεύει ένα μικρό αριθμό από επιλεγμένα πεδία ενός μηνύματος. Χρησιμοποιείται στις ακόλουθες περιπτώσεις :

- Μόνο ορισμένα πεδία ενός εκτενούς μηνύματος (όπως είναι η διεύθυνση αποστολέα και παραλήπτη) αποτελούν εμπιστευτική πληροφορία που χρειάζεται να προστατευτεί από μη εξουσιοδοτημένους χρήστες. Τα πεδία αυτά κρυπτογραφούνται.
- Το μήνυμα περιέχει αρκετά εμπιστευτικά πεδία και διαφορετικοί εξουσιοδοτημένοι χρήστες επιτρέπεται να διαβάσουν ορισμένα μόνο -και όχι όλοι τα ίδια- από αυτά τα πεδία. Σε αυτή την περίπτωση τα διάφορα πεδία κρυπτογραφούνται με διαφορετικά κλειδιά και ανάλογα με το επίπεδο ασφάλειας που απαιτεί το καθένα πιθανώς να χρησιμοποιούνται διαφορετικοί αλγόριθμοι κρυπτογράφησης.
- Όταν δεν είναι διαθέσιμη η εμπιστευτικότητα πλήρους μηνύματος .

Εμπιστευτικότητα πλήρους μηνύματος (Whole Message Confidentiality)

Προστατεύει από υποκλοπή το περιεχόμενο ενός μηνύματος στο σύνολό του. Χρησιμοποιείται στις ακόλουθες περιπτώσεις :

- Είναι αναγκαίο να παραμείνει εμπιστευτικό όλο το περιεχόμενο του μηνύματος.
- Μόνο ένα τμήμα του μηνύματος περιέχει εμπιστευτική πληροφορία όμως είναι ευκολότερη η κρυπτογράφηση ολόκληρου του μηνύματος, παρά κάποιου τμήματός του.

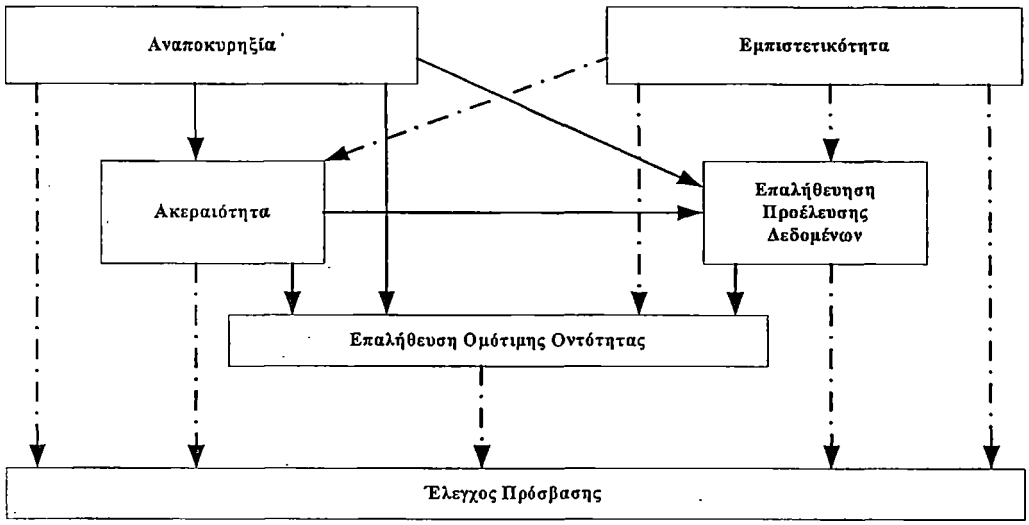
- Μόνο ορισμένα πεδία του μηνύματος είναι εμπιστευτικά ,αλλά δεν είναι διαθέσιμη η εμπιστευτικότητα επιλεγμένων πεδίων.

Εμπιστευτικότητα Ροής Κίνησης (Traffic Flow Confidentiality)

Σε σπάνιες περιπτώσεις είναι απαραίτητο ένας εισβολέας να μη γνωρίζει ότι ένα μήνυμα κατά τη δρομολόγησή του διέρχεται από συγκεκριμένες θέσεις μέσα στο δίκτυο. Πολύ περισσότερο δεν πρέπει να γνωρίζει το μέγεθος και το πλήθος αυτών των μηνυμάτων. Αυτή η δυνατότητα είναι απαραίτητη περισσότερο σε ειδικές εφαρμογές όπως είναι οι στρατιωτικές εφαρμογές .

- **Αναποκυρηξία (Non Repudiation) :**Δεν επιτρέπει ούτε στον αποστολέα ούτε στον παραλήπτη ενός μηνύματος να αρνηθούν τη μετάδοση του μηνύματος αυτού. Με τον τρόπο αυτό ,όταν ο παραλήπτης λάβει κάποιο μήνυμα δεν μπορεί να αμφισβητήσει ούτε τον αποστολέα αυτού του μηνύματος ούτε αν και πότε έλαβε το μήνυμα . Όμοια, ούτε ο αποστολέας μπορεί να αμφισβητήσει τον παραλήπτη ενός μηνύματος καθώς και την ώρα και μέρα παραλαβής του. Έτσι αποτρέπεται η επίθεση ***τροποποίησης πληροφορίας*** , που περιλαμβάνει την εισχώρηση μηνυμάτων από εισβολείς στην επικοινωνία που εγκαθίσταται κάθε φορά μεταξύ ενός παραλήπτη και ενός αποστολέα.

Στο Σχήμα 1-5 δίδεται η σχέση μεταξύ των υπηρεσιών ασφάλειας. Το συμπαγές βέλος φανερώνει ότι μία υπηρεσία ασφάλειας ενδογενώς παρέχει μία άλλη ,ενώ το διακεκομμένο βέλος υποδηλώνει ότι μία υπηρεσία ασφάλειας υποστηρίζει και μπορεί να είναι επαρκής για μία άλλη , ωστόσο όχι πάντα.



Σχήμα 1-5: Σχέση μεταξύ των υπηρεσιών ασφάλειας

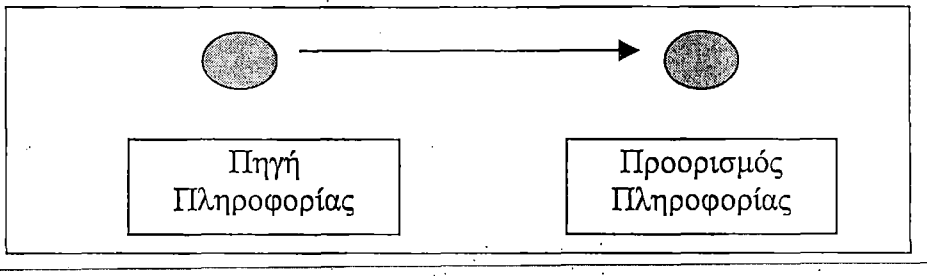
1.4.3 Επιθέσεις κατά της ασφάλειας(Security Attacks)

Για να αναλύσουμε περισσότερο τις επιθέσεις που μπορεί να πραγματοποιηθούν σε ένα δίκτυο, πρέπει πρώτα απ' όλα να έχουμε υπόψη μας ότι τα συστήματα ασφάλειας έχουν ως στόχο να εμποδίζουν επιθέσεις ή αν αυτό δεν είναι δυνατόν να γίνει, να τις ανιχνεύουν.

Ένα από τα μεγαλύτερα προβλήματα, είναι η μεγάλη εφευρετικότητα και ποικιλία που μπορεί να παρουσιάζουν οι τρόποι με τους οποίους επιχειρείται η επίθεση. Ο λόγος, όμως, που κάνει τόσο κρίσιμες τις επιθέσεις κατά της ασφάλειας του δικτύου ενός οργανισμού είναι η διακινδύνευση στην οποία θέτουν το δίκτυο και οι πιθανές συνέπειες στις εργασίες του οργανισμού. Το ελάχιστο που πρέπει να ξέρει λοιπόν κανείς, είναι όλες οι κατηγορίες των επιθέσεων που έχουν εμφανιστεί έως σήμερα, ούτως ώστε να μην βρίσκεται προ εκπλήξεων

όταν κάποια από αυτές λάβει χώρα. Είναι , λοιπόν , αναγκαίο να είναι προετοιμασμένος να αντιμετωπίσει τουλάχιστον τις κατηγορίες ήδη γνωστών επιθέσεων, και να διαθέτει τα κατάλληλα εργαλεία, τα οποία διατίθενται στο εμπόριο.

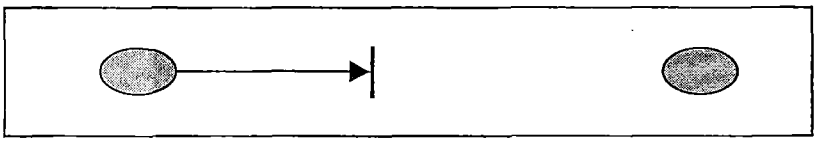
Στο σημείο αυτό θα ήταν χρήσιμο να αναφερθούμε στις επιθέσεις που μπορεί να δεχθεί ένα δίκτυο. Για απλούστευση είναι σκόπιμο να θεωρήσουμε πως ένα σύστημα υπολογιστών ή ένα δίκτυο, μπορεί να προσεγγιστεί ως ένα σύστημα παροχής πληροφοριών. Υπό κανονικές συνθήκες, υπάρχει ομαλή ροή πληροφοριών από μια πηγή ,
που μπορεί να είναι ένα αρχείο ή ένα τμήμα της μνήμης , προς έναν προορισμό, που με τη σειρά του μπορεί να είναι είτε κάποιο άλλο αρχείο, είτε κάποιος χρήστης. Η περίπτωση αυτή φαίνεται στο Σχήμα 1-6.



Σχήμα 1-6:Ομαλή ροή πληροφοριών

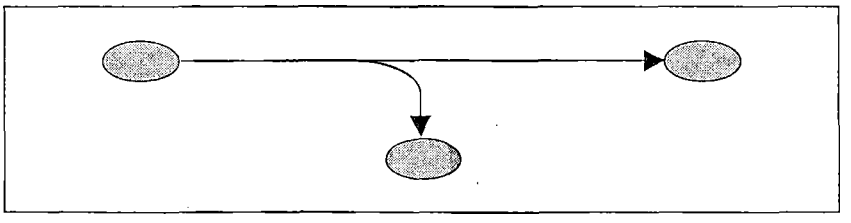
Παρακάτω αναλύονται οι 4 κύριες κατηγορίες επιθέσεων:

➢ **Διακοπή (Interruption):** ένα τμήμα του δικτύου καταστρέφεται ή καθίσταται αδύνατο προς διάθεση ή χρήση. Για παράδειγμα μπορεί να καταστραφεί ένα κομμάτι του υλικού , όπως ο σκληρός δίσκος, να διακοπεί μια τηλεπικοινωνιακή γραμμή ή να αδρανοποιηθεί η λειτουργία του συστήματος διαχείρισης αρχείων. Πρόκειται για μία επίθεση κατά της **διαθεσιμότητας (availability)** του δικτύου. Η περίπτωση αυτή φαίνεται στο Σχήμα 1-7.



Σχήμα 1-7:Διακοπή ροής πληροφοριών

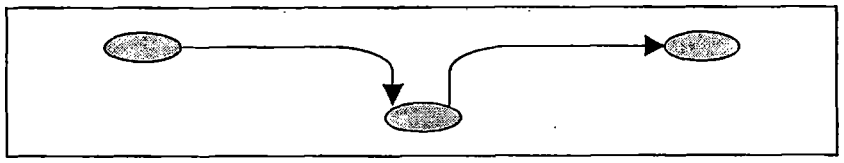
➢ **Αναχαίτιση (Interception):** μια μη εξουσιοδοτημένη οντότητα αποκτά πρόσβαση σε ένα στοιχείο δικτύου. Αυτή η οντότητα μπορεί να είναι ένα άτομο, ένα πρόγραμμα ή ένας υπολογιστής. Παραδείγματα τέτοιου είδους επίθεσης είναι η παράνομη τοποθέτηση καλωδίων για τη σύλληψη δεδομένων από το δίκτυο και η μη εξουσιοδοτημένη αντιγραφή αρχείων ή προγραμμάτων. Πρόκειται για μία επίθεση κατά της **εμπιστευτικότητας (confidentiality)** του δικτύου. Η περίπτωση αυτή φαίνεται στο Σχήμα 1-8.



Σχήμα 1-8:Υποκλοπή πληροφοριών

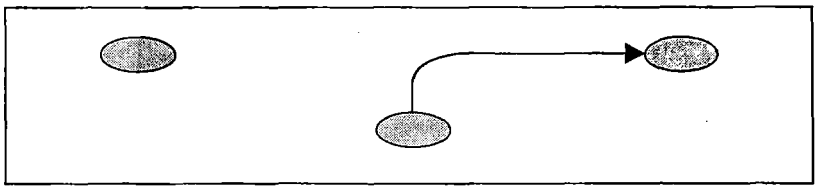
➢ **Τροποποίηση (Modification):** μια μη εξουσιοδοτημένη οντότητα όχι μόνο αποκτά πρόσβαση, αλλά και παραποιεί την πληροφορία που υπάρχει σε κάποιο στοιχείο του δικτύου.

Τέτοιου είδους επιθέσεις περιλαμβάνουν αλλαγή των τιμών στα δεδομένα ενός αρχείου, τροποποίηση ενός προγράμματος ώστε αυτό να εκτελεί διαφορετική λειτουργία από την προκαθορισμένη, καθώς επίσης και τροποποίηση στα περιεχόμενα ενός μηνύματος που μεταφέρεται μέσα στο δίκτυο. Πρόκειται για μία επίθεση κατά της ακεραιότητας (integrity) του δικτύου. Η περίπτωση αυτή φαίνεται στο Σχήμα 1-9.



Σχήμα 1-9:Τροποποίηση πληροφορίας

➢ **Χάλκευση (Fabrication) :** μια μη εξουσιοδοτημένη οντότητα εισαγάγει δικές της οντότητες μέσα στο δίκτυο. Ως παραδείγματα μπορούμε να αναφέρουμε την εισαγωγή ανωφελών – χωρίς ουσιώδη πληροφορία - μηνυμάτων στο δίκτυο, την αναστολή της λειτουργικότητας τμήματος λογισμικού (όπως είναι η παραποίηση πρωτοκόλλων),εισάγοντας συνήθως κάποια αντίστροφη λειτουργία, καθώς και την επικόλληση εγγραφών μέσα σε ένα αρχείο. Είναι μία επίθεση κατά της **αυθεντικότητας (authenticity)** του δικτύου. Η περίπτωση αυτή φαίνεται στο Σχήμα 1-10.



Σχήμα 1-10:Χάλκευση του δικτύου

Μπορούμε ,ακόμη , να κατηγοριοποιήσουμε τις επιθέσεις κατά της ασφάλειας σε δύο μεγάλες ομάδες με κριτήριο αν, κατά τη διάρκεια της επίθεσης, υπάρχει αλλοίωση της πληροφορίας ή όχι. Έτσι διακρίνουμε τις επιθέσεις κατά της ασφάλειας σε **παθητικές** και σε **ενεργές** επιθέσεις .

1.4.3.1 Παθητικές επιθέσεις (Passive attacks)

Το χαρακτηριστικό των παθητικών επιθέσεων είναι η παρακολούθηση μόνο της πληροφορίας που κυκλοφορεί σε ένα δίκτυο. Οι οντότητες που επιτίθενται στο δίκτυο, έχουν ως σκοπό να υποκλέπτουν τις πληροφορίες που μεταδίδονται σε αυτό. Ως παθητικές χαρακτηρίζονται οι ακόλουθες επιθέσεις.

- Λαθρακρόαση (eavesdropping) και
- Ανάλυση της δικτυακής κίνησης (network traffic analysis) .

Η ***λαθροακρόαση*** αναφέρεται στην περίπτωση που ένας εισβολέας έχει τη δυνατότητα να αλληλεπιδρά με τηλεπικοινωνιακά κανάλια , με τέτοιο τρόπο ώστε να μπορεί να εξάγει πληροφορία που κυκλοφορεί στο κανάλι , πιθανότατα χωρίς τη σύμφωνη γνώμη των οντοτήτων που επικοινωνούν. Η λαθροακρόαση μπορεί να θέσει σε μεγάλο κίνδυνο την ασφάλεια του δικτύου καθώς επιτρέπει σε μη εξουσιοδοτημένους χρήστες να γνωρίζουν εμπιστευτική πληροφορία που ανταλλάσσεται στο δίκτυο.

Στην περίπτωση της ***ανάλυσης της δικτυακής κίνησης*** , ακόμα και αν το περιεχόμενο των μηνυμάτων που κυκλοφορούν σε ένα δίκτυο προστατεύεται , με εφαρμογή τεχνικών κρυπτογράφησης , από τα « αδιάκριτα » μάτια εισβολέων, οι οποίοι ίσως κατορθώνουν να τα υποκλέπτουν, είναι πιθανό οι εισβολείς να μπορούν να ξεχωρίσουν τη δομή των μηνυμάτων αυτών. Μπορούν ,δηλαδή , να ξεχωρίσουν την τοποθεσία και την ταυτότητα αποστολέα και

παραλήπτη και να αποκτήσουν στατιστικά στοιχεία για τη συχνότητα, με την οποία οι δύο αυτοί εξουσιοδοτημένοι χρήστες ανταλλάσσουν μηνύματα , και την έκταση των μηνυμάτων αυτών. Τα στοιχεία αυτά μπορεί να βοηθούν στον καθορισμό του είδους της επικοινωνίας που λαμβάνει χώρα μεταξύ των δύο αυτών χρηστών.

Δυστυχώς, οι παθητικές επιθέσεις είναι πάρα πολύ δύσκολο να ανιχνευθούν, καθώς δεν πραγματοποιείται κανενός είδους αλλοίωση ή επεξεργασία των δεδομένων, επομένως δεν υπάρχουν και εμφανή σημάδια που να μαρτυρούν ότι έγινε επίθεση. Παρόλα αυτά, υπάρχουν τρόποι να παρεμποδιστεί η επιτυχία των παθητικών επιθέσεων. Άρα, εύκολα καταλαβαίνει κανείς πως όσον αφορά σε αυτή την κατηγορία επιθέσεων, σκοπός είναι η πρόληψή παρά ο εντοπισμός τους (καθώς, όπως είπαμε παραπάνω ,αυτό είναι αδύνατον).

1.4.3.2 Ενεργές επιθέσεις (Active attacks)

Οι ενεργές επιθέσεις παρουσιάζουν ακριβώς τα αντίθετα χαρακτηριστικά από τις παθητικές, καθώς στην συγκεκριμένη περίπτωση οι επιθέσεις δεν περιορίζονται σε παρακολούθηση της πληροφορίας που μεταδίδεται στο δίκτυο, αλλά περιλαμβάνουν τροποποίηση δεδομένων ή και δημιουργία και διοχέτευση στο δίκτυο εσφαλμένων δεδομένων, προκειμένου να διευκολυνθεί παράνομη δραστηριότητα έναντι στοιχείων του δικτύου. Οι παρακάτω επιθέσεις συγκαταλέγονται στις ενεργές επιθέσεις κατά της ασφάλειας ενός δικτύου.

- Μεταμφίεση (Masquerade)
- Τροποποίηση της Πληροφορίας (Modification of Information)
- Αποκήρυξη (Repudiation)
- Επανάληψη , Επαναδρομολόγηση , Κακή Δρομολόγηση , Διαγραφή Μηνυμάτων (Replay , Reroute , Misroute,Delete Messages)

Η ***μεταμφίεση (Masquerade)*** πραγματοποιείται όταν μία οντότητα υποδύεται μία άλλη οντότητα . Κάτι τέτοιο καθίσταται δυνατό σε περίπτωση που αποκτήσει στοιχεία επαλήθευσης της ταυτότητας μιας οντότητας, όπως είναι η δικτυακή της διεύθυνση, η ψηφιακή υπογραφή ή ο κωδικός εισόδου ενός εξουσιοδοτημένου χρήστη . Αυτό έχει ως αποτέλεσμα μία οντότητα με λίγα δικαιώματα στους πόρους του δικτύου να αποκτήσει τα δικαιώματα της οντότητας που μιμείται ,τα οποία είναι συνήθως περισσότερα.

Έτσι, ένας εισβολέας μπορεί να μιμείται έναν εξουσιοδοτημένο χρήστη, με τέτοιο τρόπο ώστε όλες οι οντότητες του δικτύου να θεωρούν ότι πρόκειται για τον εξουσιοδοτημένο αυτό χρήστη. Η μεταμφίεση, λοιπόν , του δίνει πρόσβαση - που προηγούμενα δεν είχε – σε εμπιστευτική πληροφορία καθώς και τη δυνατότητα να μετατρέψει αυτή την πληροφορία προς όφελός του. Δηλαδή η μεταμφίεση συνδυάζεται και με άλλες μορφές δυναμικών επιθέσεων όπως είναι η ***τροποποίηση πληροφορίας***.

Η ***τροποποίηση πληροφορίας (modification of information)*** , αφορά στην εισαγωγή από, μη εξουσιοδοτημένη οντότητα , πληροφορίας σε πόρους του δικτύου. Πραγματοποιείται είτε ως εισαγωγή αυτούσιας πληροφορίας στο δίκτυο , είτε ως μετατροπή ενός πρωτότυπου μηνύματος τη στιγμή που αυτό μεταδίδεται. Στην πρώτη περίπτωση, μπορεί μία μη εξουσιοδοτημένη οντότητα να προσθέτει κώδικα σε κάποιο στοιχείο του δικτύου ,το οποίο θα εκτελεί αυτό τον κώδικα, με αποτέλεσμα την αλλοίωση της συμπεριφοράς του μέσα στο δίκτυο. Η δεύτερη περίπτωση περιλαμβάνει τροποποίηση τμήματος ενός μηνύματος που κυκλοφορεί στο δίκτυο, αναδιάταξή του ή και καθυστέρηση στη δρομολόγησή του με σκοπό κάποια αθέμιτη ενέργεια. Ένα συνηθισμένο παράδειγμα είναι η παροχή δικαιωμάτων πρόσβασης σε εμπιστευτικά αρχεία ή καταλόγους σε διαφορετικό (μη εξουσιοδοτημένο) χρήστη ,από τον πραγματικό παραλήπτη του μηνύματος . Η τροποποίηση πληροφορίας , λοιπόν, είναι μία επίθεση που μπορεί να προκαλέσει σημαντικό ρήγμα ασφάλειας σε ένα δίκτυο όπως είναι η αλλαγή των μέτρων ασφάλειας σε ένα πόρο του δικτύου η οποία θα επιτρέπει την είσοδο μη εξουσιοδοτημένων χρηστών, στο δίκτυο όποτε αυτοί το επιθυμούν.

Η ***αποκήρυξη (repudiation)*** είναι μία δυναμική επίθεση κατά της ασφάλειας κατά την οποία μία οντότητα αρνείται ότι έχει λάβει υπηρεσίες τις οποίες έχει ζητήσει ή /και έχει λάβει παρεμποδίζοντας τη σωστή λειτουργία συγκεκριμένων υπηρεσιών επικοινωνιακού εξοπλισμού. Έτσι μπορεί να οδηγήσει σε διαφωνία ανάμεσα σε δύο οντότητες σχετικά με την κοστολόγηση υπηρεσιών τις οποίες μία από τις δύο αρνείται ότι έλαβε.

Μια επίθεση ***επανάληψης μηνυμάτων (replay messages)*** ξεκινά με παθητική υποκλοπή ενός γνήσιου μηνύματος και συνεχίζει με την επαναχρησιμοποίηση αυτού του μηνύματος προκειμένου κάποια μη εξουσιοδοτημένη οντότητα να αποκτήσει πρόσβαση σε πόρους του δικτύου έτσι ώστε να απολαμβάνει υπηρεσιών για τις οποίες δεν έχει εξουσιοδότηση. Σε μία επίθεση ***επαναδρομολόγησης μηνυμάτων (reroute messages)*** μια οντότητα μεταβάλλει το μονοπάτι μέσω του οποίου δρομολογείται ένα μήνυμα ,κατά τη διαδρομή του από τον αποστολέα έως τον παραλήπτη. Έτσι η οντότητα που επιτίθεται , μπορεί ευκολότερα να υποκλέψει την πληροφορία που φέρει το μήνυμα , καθώς αυτό ταξιδεύει μεταξύ πηγής και προορισμού διαμέσου του νέου μονοπατιού. Μια επίθεση ***κακής δρομολόγησης μηνυμάτων (misroute messages)*** οδηγεί ένα μήνυμα σε διαφορετικό παραλήπτη σε σχέση με αυτόν που καθορίζει ο αποστολέας ,ενώ σε μία επίθεση ***διαγραφής μηνυμάτων (delete messages)*** το μήνυμα εμποδίζεται να φτάσει σε οποιοδήποτε προορισμό.

Η παρεμπόδιση των δυναμικών επιθέσεων είναι κατά βάση ανέφικτη, καθώς αυτές μπορεί να γίνουν σε οποιαδήποτε οντότητα ή κομμάτι του δικτύου και θα απαιτείτο πλήρης κάλυψη ολόκληρου του συστήματος, κάτι που είναι οικονομικά πολύ ασύμφορο. Για αυτό ο στόχος είναι η δυνατότητα ανίχνευσης δυναμικών επιθέσεων και η ανάκαμψη του δικτύου από τις καταστροφές και τις καθυστερήσεις που προκαλούν αυτές σε αυτό. Καθώς η ανίχνευση τέτοιων επιθέσεων αναχαιτίζει τις συνέπειές τους ,μπορεί να οδηγήσει και στον περιορισμό τους.

Υπάρχουν ακόμη δύο κύρια είδη επιθέσεων κατά της ασφάλειας του δικτύου που δεν μπορούν να καταταγούν ούτε στις παθητικές ούτε στις ενεργές επιθέσεις .Πρόκειται για τη ***μη εξουσιοδοτημένη πρόσβαση (unauthorized access)*** και για την ***πλημμυρίδα δικτύου (network flooding)***.

Σε περίπτωση ***μη εξουσιοδοτημένης πρόσβασης (unauthorized access)*** ένας εισβολέας αποκτά πρόσβαση και συγκεντρώνει πληροφορίες από κάποιο πόρο του δικτύου στον οποίο δεν έχει εξουσιοδότηση. Η πρόσβαση εξασφαλίζεται είτε μέσω φυσικών είτε μέσω ηλεκτρονικών μεθόδων.

Στην περίπτωση των ηλεκτρονικών μεθόδων ένας εισβολέας αποκτά πρόσβαση σε κάποιο πόρο είτε επειδή ο τελευταίος δεν προστατεύεται αρκετά, όπως είναι μια μη προστατευόμενη συσκευή διαποδιαμορφωτή (modem) μιας τηλεφωνικής σύνδεσης, είτε «ξεγελώντας» τον χρησιμοποιώντας γνήσια στοιχεία επαλήθευσης ταυτότητας ενός εξουσιοδοτημένου χρήστη ,τα οποία έχει προηγούμενα αποκτήσει λαθραία. Δηλαδή η μη εξουσιοδοτημένη πρόσβαση περιλαμβάνει και την παθητική επίθεση της λαθροακρόασης που αναλύθηκε παραπάνω.

Πάντως, οποιαδήποτε μέθοδος και αν χρησιμοποιείται προκειμένου να προκληθεί ρήγμα στην ασφάλεια κάποιου πόρου του δικτύου μπορεί να επιφέρει καταστρεπτικά αποτελέσματα για την ασφάλεια του ίδιου ή και του δικτύου στο σύνολό του. Τα κυριότερα από αυτά είναι ότι ένας εισβολέας μπορεί να παρέμβει ώστε να εκμεταλλευτεί προς όφελός του τις δυνατότητες που προσφέρει ο πόρος στον οποίο έχει αποκτήσει πρόσβαση και να διαβάσει , διαγράψει ή τροποποιήσει εμπιστευτική πληροφορία .

Η ***πλημμυρίδα δικτύου (network flooding)*** λαμβάνει χώρα όταν μία οντότητα πλημμυρίζει ένα δίκτυο με πλαστά ή ανώφελα μηνύματα Πλημμυρίζοντας το δίκτυο με κίβδηλες αιτήσεις οδηγεί σε σπατάλη πόρων εκ μέρους του δικτύου, στην προσπάθειά του τελευταίου να επεξεργαστεί τέτοια παράνομα μηνύματα. Αν το δίκτυο κατακλύζεται από μεγάλο αριθμό τέτοιων αιτήσεων δε θα είναι σε θέση να ικανοποιήσει νόμιμες αιτήσεις, με αποτέλεσμα να μειώνεται αισθητά η αποδοτικότητά του .

1.4.4 Διακινδυνεύσεις Ασφάλειας (Security Risks)

Πρόκειται για τις πιθανές συνέπειες που μπορεί να επιφέρουν στο δίκτυο οι επιθέσεις κατά της ασφάλειας που αναλύθηκαν στην προηγούμενη ενότητα. Αυτές οι διακινδυνεύσεις ασφάλειας μπορεί να είναι:

- Υποκλοπή πληροφορίας (Theft of Information)
- Μη εξουσιοδοτημένη χρήση πόρων (Unauthorised Use of Resources)
- Υποκλοπή Υπηρεσιών (Theft of Service)
- Άρνηση Παροχής Υπηρεσιών (Denial of Service)

Η ***υποκλοπή πληροφορίας*** πραγματοποιείται κάθε φορά που μία οντότητα ,μη εξουσιοδοτημένη ,αποκτά πρόσβαση είτε διαμέσου ενός κόμβου του δικτύου είτε διαμέσου ενός καναλιού επικοινωνίας μεταξύ δύο κόμβων, σε εμπιστευτική πληροφορία περιορισμένης προσβασιμότητας .Η υποκλοπή πληροφορίας μπορεί να είναι το αποτέλεσμα των επιθέσεων της ***μη εξουσιοδοτημένης πρόσβασης*** ,της ***μεταμφίεσης*** ή της ***λαθροακρόασης***.

Η ***μη εξουσιοδοτημένη χρήση πόρων*** επιτρέπει σε μία οντότητα τη χρήση πόρων για τους οποίους δεν έχει εξουσιοδότηση. Η μη εξουσιοδοτημένη χρήση πόρων μπορεί να είναι το αποτέλεσμα των επιθέσεων της ***μη εξουσιοδοτημένης πρόσβασης*** ,της ***μεταμφίεσης*** , της ***τροποποίησης πληροφορίας*** , της ***επανάληψης*** , της ***επαναδρομολόγησης*** και της ***κακής δρομολόγησης μηνυμάτων***.

Η ***υποκλοπή υπηρεσιών*** περιλαμβάνει χρήση υπηρεσιών για τις οποίες δεν υπάρχει εξουσιοδότηση ή δεν καταβάλλεται το αντίστοιχοκόστος. Αποτελεί τη συνέπεια μιας συνδυασμένης επίθεσης κατά της ασφάλειας ενός δικτύου που περιλαμβάνει τις εξής επιθέσεις: ***μη εξουσιοδοτημένη πρόσβαση, μεταμφίεση, τροποποίηση πληροφορίας, επανάληψη*** και ***επαναδρομολόγηση, κακή δρομολόγηση*** και ***διαγραφή μηνυμάτων***.

Τέλος ,η ***άρνηση παροχής υπηρεσιών*** έχει ως αποτέλεσμα ένα στοιχείο δικτύου να παρεκκλίνει από την αναμενόμενη λειτουργία του . Είναι συνέπεια ενός συνδυασμού πέντε επιθέσεων, της ***μη εξουσιοδοτημένης πρόσβασης*** , της ***μεταμφίεσης*** , της ***τροποποίησης πληροφορίας*** διαχείρισης πόρων του δικτύου, της ***επαναδρομολόγησης, κακής δρομολόγησης*** και ***διαγραφής μηνυμάτων*** και της ***πλημμυρίδα δικτύου***. Η άρνηση υπηρεσιών μπορεί να επηρεάζει είτε μεμονωμένους χρήστες είτε τους χρήστες του δικτύου στο σύνολό τους.

Στην περίπτωση μεμονωμένων χρηστών ένας εισβολέας μπορεί να παρεμποδίσει την πρόσβαση ενός εξουσιοδοτημένου χρήστη σε πόρους του δικτύου με δύο τρόπους. Ένας από αυτούς είναι η υποκλοπή εμπιστευτικής πληροφορίας που τον αφορά , μέσω της διαγραφής μηνυμάτων που έχουν ως αποστολέα ή παραλήπτη το χρήστη αυτό. Ο δεύτερος αφορά στην τροποποίηση της πληροφορίας ασφάλειας ενός στοιχείου δικτύου, ώστε το τελευταίο να αρνείται την πρόσβαση στον εξουσιοδοτημένο χρήστη.

Στην περίπτωση άρνησης παροχής υπηρεσιών σε όλους τους χρήστες του δικτύου , εισβολείς προσπαθούν να αναχαιτίσουν τη ροή της κίνησης έγκυρων δεδομένων διαμέσου ενός καναλιού επικοινωνίας του δικτύου πλημμυρίζοντας το κανάλι με έναν τεράστιο αριθμό από ανωφελή ή ψευδή μηνύματα. Δεδομένης της πλημμυρίδας του δικτύου με μηνύματα χωρίς χρήσιμη πληροφορία, οι πόροι του δικτύου υπερφορτώνονται με αποτέλεσμα να αδυνατούν να παρακολουθήσουν οποιαδήποτε πληροφορία εισέρχεται από το κανάλι. Σε περίπτωση πλημμυρίδας του δικτύου με ψευδή μηνύματα ,εισβολείς περιλαμβάνουν σε καθένα από αυτά πολυάριθμες αιτήσεις προς τους πόρους του δικτύου με τρόπο ώστε οι τελευταίοι να τις θεωρούν πραγματικές αιτήσεις και να προσπαθούν να τις επεξεργαστούν ,με αποτέλεσμα να αδυνατούν να εξυπηρετήσουν έγκυρες αιτήσεις που προέρχονται από εξουσιοδοτημένες οντότητες .

Σε αυτό το σημείο θα ήταν χρήσιμο να παραθέσουμε μερικούς πίνακες, οι οποίοι παρουσιάζουν τις σχέσεις μεταξύ επιθέσεων κατά της ασφάλειας (security attacks) ,

διακινδυνεύσεων ασφάλειας (security risks), υπηρεσιών ασφάλειας (security services) και μηχανισμών ασφάλειας (security mechanisms).

Έτσι δίδεται η σχέση μεταξύ αφενός των μηχανισμών ασφάλειας και αφετέρου των υπηρεσιών ασφάλειας (πίνακας 1-1) και επιθέσεων κατά της ασφάλειας (πίνακας 1-2).Στη συνέχεια δίδεται η σχέση μεταξύ των επιθέσεων κατά της ασφάλειας και των διακινδυνεύσεων ασφάλειας (πίνακας 1-3).Επίσης δίδεται η σχέση μεταξύ αφενός των υπηρεσιών ασφάλειας και αφετέρου των επιθέσεων ασφάλειας (πίνακας 1-4) και διακινδυνεύσεων ασφάλειας (πίνακας 1-5). Η προσεκτική μελέτη των πινάκων αυτών θα βοηθήσει τον αναγνώστη στην καλύτερη κατανόηση των εννοιών που αναφέρθηκαν σε αυτό το κεφάλαιο. Έτσι στον πίνακα 1-1 δίδονται οι μηχανισμοί ασφάλειας που υποστηρίζουν τις διάφορες υπηρεσίες . Για παράδειγμα η Κρυπτογράφηση υποστηρίζει την υπηρεσία Εμπιστευτικότητας.

Στον πίνακα 1-1 δίδονται οι μηχανισμοί ασφάλειας σε σχέση με τις υπηρεσίες ασφάλειας.

ΥΠΗΡΕΣΙΑ ΑΣΦΑΛΕΙΑΣ / ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ	Έλεγχος Πρόσβασης	Σηματοδοσία Ομοιότητας	Επαλήθευση Προέλευσης Δεδομένων	Ακεραιότητα Δεδομένων	Εμπιστευτικότητα Δεδομένων	Αναποκρυπτία
Μηχανισμοί Ελέγχου Πρόσβασης	√					
Κατακερματισμός και Σύνοψη		√	√	√		
Συμμετρική Κρυπτογράφηση		√			√	
Μη Συμμετρική Κρυπτογράφηση		√			√	
Ψηφιακή Υπογραφή		√	√	√		√
Ψηφιακά Πιστοποιητικά		√				

Πίνακας 1-1: Μηχανισμοί ασφάλειας (security mechanisms) σε σχέση με τις υπηρεσίες ασφάλειας (security services)

Στον πίνακα 1-2 δίδονται οι μηχανισμοί ασφάλειας σε σχέση με τις επιθέσεις κατά της ασφάλειας.

ΕΠΙΘΕΣΕΙΣ ΚΑΤΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ / ΜΗΧΑΝΙΣΜΟΙ ΑΣΦΑΛΕΙΑΣ	Μη Εξουσιοδοτημένη Πρόσβαση	Διαθεσιμότητα	Μεταβίβαση	Τροποποίηση Πληροφορίας	Αποκήρυξη	Επανάληψη, Διαγραφή Επαναδρομολόγηση	Πλημμύρα Δικτύου
Έλεγχος Πρόσβασης	√		√	√			√
Κατακερματισμός και σύνοψη	√		√	√		√	
Συμμετρική Κρυπτογράφηση	√	√	√				
Μη Συμμετρική Κρυπτογράφηση	√	√	√				
Ψηφιακή Υπογραφή	√		√	√	√		
Ψηφιακά Πιστοποιητικά	√		√				

Πίνακας 1-2: Μηχανισμοί ασφάλειας (security mechanisms) σε σχέση με τις επιθέσεις κατά της ασφάλειας (security threats)

Στον πίνακα 1-3 δίδεται η σχέση μεταξύ των επιθέσεων κατά της ασφάλειας και των διακινδυνεύσεων ασφάλειας

ΔΙΑΚΙΝΔΥΝΕΥΣΕΙΣ ΑΣΦΑΛΕΙΑΣ / ΕΠΙΘΕΣΕΙΣ ΚΑΤΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ	Υποκλοπή Πληροφορίας	Μη Εξουσιοδοτημένη Χρήση Πόρων	Υποκλοπή Υπηρεσιών	Άρνηση Παροχής Υπηρεσιών
Μη Εξουσιοδοτημένη Πρόσβαση	√	√	√	√
Λαθρακρόαση	√			
Μεταμφίεση	√	√	√	√
Τροποποίηση Πληροφορίας		√	√	√
Επανάληψη		√	√	
Αποκήρυξη			√	
Επαναδρομολόγηση Κακή Δρομολόγηση Διαγραφή Μηνυμάτων		√	√	√
Πλημμυρίδα Δικτύου				√

Πίνακας 1-3: Επιθέσεις κατά της ασφάλειας (security attacks) σε σχέση με τις διακινδυνεύσεις κατά της ασφάλειας (security risks)

Στον πίνακα 1-4 δίδονται οι υπηρεσίες ασφάλειας σε σχέση με τις επιθέσεις κατά της ασφάλειας.

ΕΠΙΘΕΣΕΙΣ ΚΑΤΑ ΤΗΣ ΑΣΦΑΛΕΙΑΣ / ΥΠΗΡΕΣΙΑ ΑΣΦΑΛΕΙΑΣ	Μη Εξουσιοδοτημένη Πρόσβαση	Λαθροακρόαση	Μεταμφίεση	Τροποποίηση Πληροφορίας	Αποκήρυξη	Επανάληψη, Επαναδρομολόγηση, Διαγραφή	Πλημμύρα Δικτύου
Έλεγχος Πρόσβασης	√			√			√
Επαλήθευση Ομότιμης Οντότητας	√		√				
Επαλήθευση Προέλευσης Δεδομένων	√		√				
Ακεραιότητα Δεδομένων			√	√		√	
Εμπιστευτικότητα Δεδομένων		√	√				
Αναποκυρηξία					√		

Πίνακας 1-4:Σχέση υπηρεσιών ασφάλειας (security services) και επιθέσεων κατά της ασφάλειας (security attacks)

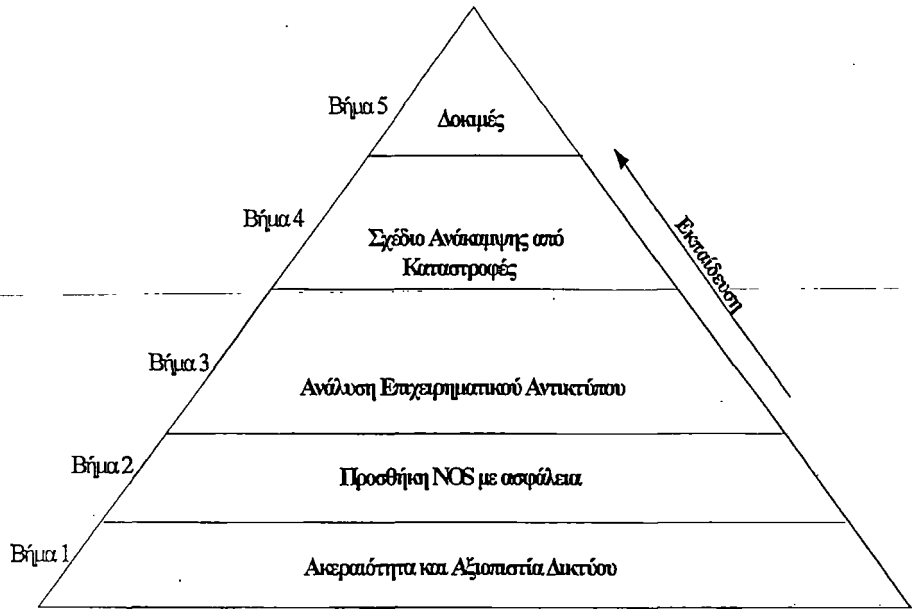
Στον πίνακα 1-5 δίδονται οι υπηρεσίες ασφάλειας σε σχέση με τις διακινδυνεύσεις ασφάλειας.

ΔΙΑΚΙΝΔΥΝΕΥΣΕΙΣ ΑΣΦΑΛΕΙΑΣ / ΥΠΗΡΕΣΙΑ ΑΣΦΑΛΕΙΑΣ	Υποκλοπή Πληροφορίας	Μη Εξουσιοδοτημένη Χρήση Πόρων	Υποκλοπή Υπηρεσιών	Άρνηση Παροχής Υπηρεσιών
Έλεγχος Πρόσβασης	√	√	√	√
Επαλήθευση Ομότιμης Οντότητας		√	√	
Επαλήθευση Προέλευσης Δεδομένων		√	√	
Ακεραιότητα Δεδομένων	√	√	√	√
Εμπιστευτικότητα Δεδομένων	√	√		√
Αναποκυρηξία			√	

Πίνακας 1-5:Σχέση υπηρεσιών ασφάλειας (security services) με τις διακινδυνεύσεις ασφάλειας (security risks)

1.5 Ολοκλήρωση της Μελέτης Ασφάλειας

Όσα εξετάστηκαν προηγούμενα (Ακεραιότητα , Αξιοπιστία , Λογισμικό NOS με Ασφάλεια κλπ) αποτελούν βασικά βήματα που πρέπει να γίνουν σε μια μελέτη Διαχείρισης Διακινδύνευσης. Εδώ θα πρέπει να ληφθεί υπόψη ότι το δίκτυο αυτό ανήκει σε κάποια επιχείρηση που το χρησιμοποιεί για να κάνει τη δουλειά της. Έτσι για την ολοκλήρωση της μελέτης απαιτούνται κάποια ακόμα πρόσθετα βήματα. Τα βήματα αυτά έχουν σχέση με την ίδια την επιχείρηση που διαθέτει το δίκτυο και απεικονίζονται σε μορφή πυραμίδας στο Σχήμα 1-11.



Σχήμα 1-11: Ολοκλήρωση της Μελέτης Ασφάλειας

Για το βήμα 1 μιλήσαμε στην ενότητα 1.3 , για το βήμα 2 είπαμε μερικές εισαγωγικές έννοιες στην ενότητα 1.4. Ειδικά στο βήμα αυτό είναι αφιερωμένο όλη η υπόλοιπη μελέτη. Για καθένα από τα υπόλοιπα βήματα θα μπορούσε να γίνει μια ξεχωριστή μελέτη . Εδώ δίνονται μόνο κάποια εισαγωγικά στοιχεία. Το βήμα 3 αφορά στην **Ανάλυση του Επιχειρηματικού Αντίκτυπου** (**Business Impact Analysis-BIA**). Αυτό σημαίνει ότι θα πρέπει να αναγνωριστούν οι κρίσιμες για μια επιχείρηση διεργασίες ή γεγονότα (π.χ. Ηλεκτρική Τροφοδοσία, καταιγίδα κ.λ.π.) και για κάθε ένα από αυτά να καθοριστεί ο λειτουργικός και οικονομικός αντίκτυπος που θα υπάρχει στην επιχείρηση αν αυτά λάβουν χώρα. Έτσι θα μπορούσαμε να πούμε ότι μια διακοπή της ηλεκτρικής τροφοδοσίας στην επιχείρηση μπορεί να στοιχίσει την πρώτη μέρα 10.000 ευρώ, την τρίτη ημέρα 30.000 ευρώ κ.ο.κ.

Το βήμα 4 αφορά **Σχέδια Ανάκαμψης από Καταστροφές** (**Disaster Recovery Plan – DRP**) . Αφορούν διαδικασίες για την αντιμετώπιση των καταστροφών. Έτσι ,για την περίπτωση διακοπής ηλεκτρικής τροφοδοσίας σε μία επιχείρηση ένα τέτοιο σχέδιο θα μπορούσε να προβλέπει μια αδιάκοπη τροφοδοσία (Uninterruptible Power Supply-UPS) τουλάχιστον για τις βασικές μονάδες της επιχείρησης.

Το βήμα 5 ακολουθεί μετά την ολοκλήρωση της μελέτης ασφάλειας και αφορά διάφορες **Τεχνικές Δοκιμές** (**Technical Rehearsal-TR**) που πρέπει να γίνουν, οι οποίες εξασφαλίζουν ότι η μελέτη διαχείρισης διακινδύνευσης που έγινε είναι σωστή και ανταποκρίνεται στις προσδοκίες της επιχείρησης. Η υλοποίηση τεχνικών δοκιμών με πολλαπλά σενάρια επιθέσεων είναι γνωστή σαν πολεμικά παιχνίδια (War Games) και

εξασφαλίζει ότι μια επιχείρηση μπορεί να αντεπεξέλθει σε πολλαπλές ταυτόχρονες επιθέσεις στο δίκτυο της.

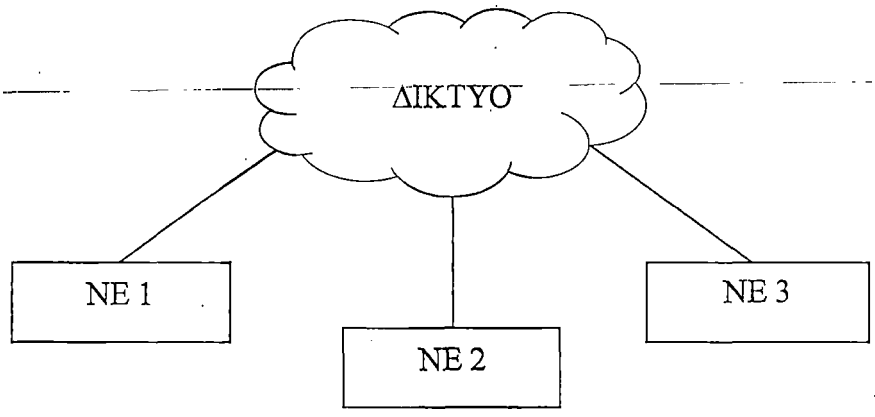
Είναι πιθανό, κατά τη φάση αυτή να καταλήξουμε στο συμπέρασμα ότι απαιτούνται κάποιες αλλαγές / βελτιώσεις ή και ακόμη προσθήκες στη μελέτη μας. Στο βήμα λοιπόν αυτό περιλαμβάνεται και η φάση συντήρησης (Maintain) της όλης μελέτης δηλαδή κάθε πότε πρέπει να κάνουμε μία ανασκόπηση ή αναθεώρηση , ώστε να περιλάβουμε και όλα τα νέα δεδομένα / καταστάσεις και αλλαγές που έγιναν στο μεσοδιάστημα αυτό στην επιχείρηση. Στην ξένη βιβλιογραφία τα βήματα 3 και 4 αναφέρονται ως **Σχεδίαση Συνέχισης της Επιχείρησης** (**Business Continuity Plan-BCP**) διότι μέσω αυτών των βημάτων καθορίζεται πως βασικές λειτουργίες μιας επιχείρησης διατηρούνται (συνεχίζονται) και μετά από κάποια σημαντική καταστροφή.

Φυσικά η σωστή εκπαίδευση του προσωπικού της επιχείρησης σε όλα τα παραπάνω βήματα εξασφαλίζει και την επιτυχία στην υλοποίηση της διαχείρισης διακινδύνευσης.

2. ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ TCP / IP

2.1 Εισαγωγή στις Αρχιτεκτονικές και στα Στρώματα Δικτύων Υπολογιστών

Ο παλαιός τρόπος εργασίας με ένα μοναδικό υπολογιστή που κάλυπτε όλες τις ανάγκες σε μία επιχείρηση, έχει πλέον αντικατασταθεί από ένα **Δίκτυο Υπολογιστών** που αποτελείται από πολλούς, ανεξάρτητους αλλά συνδεδεμένους μεταξύ τους υπολογιστές. Το μέρος του δικτύου υπολογιστών που εξασφαλίζει την σύνδεση των υπολογιστών αυτών είναι το **Δίκτυο Επικοινωνίας Δεδομένων (Data Communication Network-DCN)** ή απλώς Δίκτυο για συντομία. Τις διατάξεις που αυτό συνδέει θα τις ονομάζουμε από εδώ και στο εξής **Στοιχεία Δικτύου (Network Elements-NE)** για να δηλώσουμε μια ευρύτερη κατηγορία διατάξεων που μπορεί να συνδέονται με αυτό όπως είναι υπολογιστές, εκτυπωτές, τηλέφωνα κ.α. Στο Σχήμα 2-1 (α) απεικονίζεται ένα δίκτυο υπολογιστών.

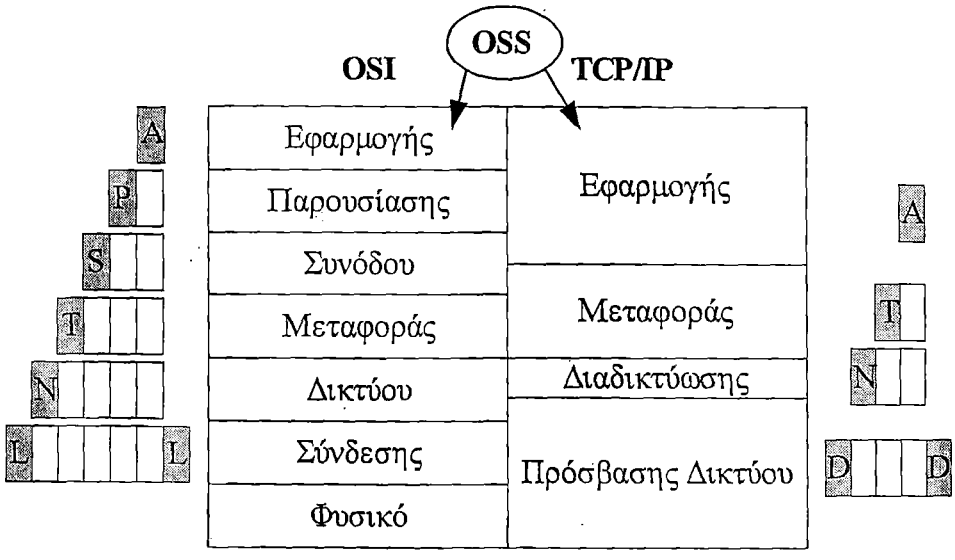


Σχήμα 2-1:Δίκτυο Υπολογιστών και Σύστημα Διαχείρισης Δικτύων Υπολογιστών

Οι αρχιτεκτονικές δικτύων υπολογιστών που έχουν επικρατήσει σήμερα είναι η αρχιτεκτονική Πρωτοκόλλου Ελέγχου Μετάδοσης / Πρωτοκόλλου Διαδικτύωσης (Transmission Control Protocol/Internet Protocol - TCP/IP) και η αρχιτεκτονική Διασύνδεσης Ανοικτών Συστημάτων (Open System Interconnection - OSI).

Ουσιαστικά τα στρώματα στις αρχιτεκτονικές αυτές αφορούν **λογισμικό** που χρησιμοποιείται σε κάθε υπολογιστή που θέλουμε να τον συνδέσουμε σε δίκτυο. Φυσικά κάθε υπολογιστής είναι εφοδιασμένος και με το λογισμικό του λειτουργικού συστήματος OS (Operating System). Ειδικά το λογισμικό του ανώτερου στρώματος κάθε αρχιτεκτονικής υποστηρίζει τις λειτουργίες (εφαρμογές) και ονομάζεται σύστημα υποστήριξης λειτουργιών OSS (Operation Support System) ή απλά **σύστημα λειτουργιών**. Έτσι μπορεί να έχουμε σύστημα λειτουργιών διαχείρισης δικτύων, σύστημα λειτουργιών ηλεκτρονικού ταχυδρομείου κ.λπ.

Στο Σχήμα 2-2 φαίνονται τα διαδοχικά στρώματα των δύο αρχιτεκτονικών, οι αντιστοιχίες των στρωμάτων μεταξύ τους και η ροή των δεδομένων από στρώμα σε στρώμα. Σε κάθε στρώμα διακρίνουμε τις υπηρεσίες (services) που προσφέρει αυτό στα ανώτερά του στρώματα καθώς και το πρωτόκολλο (protocol) που είναι ένα σύνολο από κανόνες επικοινωνίας του στρώματος με το ομότιμό του στρώμα και συμβάλλει στην υλοποίηση των υπηρεσιών.Τα χαμηλά στρώματα παρέχουν υπηρεσίες μεταφοράς των πληροφοριών μεταξύ των υπολογιστών του δικτύου, ενώ τα υψηλά στρώματα έχουν άμεση σχέση με την εφαρμογή που χρησιμοποιεί ο χρήστης του δικτύου υπολογιστών.



Σχήμα 2-2:Στρωμάτωση αρχιτεκτονικών OSI και TCP/IP

Για να ζητήσουμε τις διάφορες υπηρεσίες κάνουμε χρήση των πρωτογενών λειτουργιών (primitive functions) που είναι διαθέσιμες στον χρήστη ή σε κάποιο άλλο στρώμα. Στην γλώσσα των προγραμματισμών οι πρωτογενείς λειτουργίες μπορούμε να πούμε ότι είναι διαδικασίες με παραμέτρους. Γενικά έχουμε τέσσερις πρωτογενείς λειτουργίες:

- Αίτηση (Request)
- Ένδειξη (Indication)
- Απόκριση (Response)
- Επιβεβαίωση (Confirmation)

Έτσι στο προηγούμενο παράδειγμα αν θέλουμε να ζητήσουμε την υπηρεσία get κάνουμε χρήση της πρωτογενούς λειτουργίας getRequest.

Και στις δύο αρχιτεκτονικές, τα δεδομένα προωθούνται στην στοίβα προς τα κάτω όταν στέλνονται προς το δίκτυο και αντίστροφα προωθούνται προς τα πάνω όταν λαμβάνονται από το δίκτυο. Κάθε στρώμα της στοίβας προσθέτει πληροφορίες ελέγχου κατά την εκπομπή των δεδομένων για να εξασφαλίσει την ορθή μετάδοση. Αυτές οι πληροφορίες ελέγχου ονομάζονται **κεφαλίδες (headers)** επειδή τοποθετούνται μπροστά από τα δεδομένα που πρόκειται να εκπεμφθούν. Κάθε στρώμα συμπεριφέρεται σε όλες τις πληροφορίες που λαμβάνει από το ανώτερό του στρώμα, σαν αυτές να ήταν δεδομένα. Τοποθετεί τη δική του κεφαλίδα μπροστά και τα στέλνει στο κατώτερο στρώμα. Αυτή η διαδικασία που εκτελείται σε κάθε στρώμα, ονομάζεται **ενθυλάκωση (encapsulation)**. Όταν λαμβάνονται τα δεδομένα ακολουθείται η αντίστροφη διαδικασία. Κάθε στρώμα αφαιρεί την κεφαλίδα που το αφορά και στέλνει τα δεδομένα στο ανώτερο στρώμα.

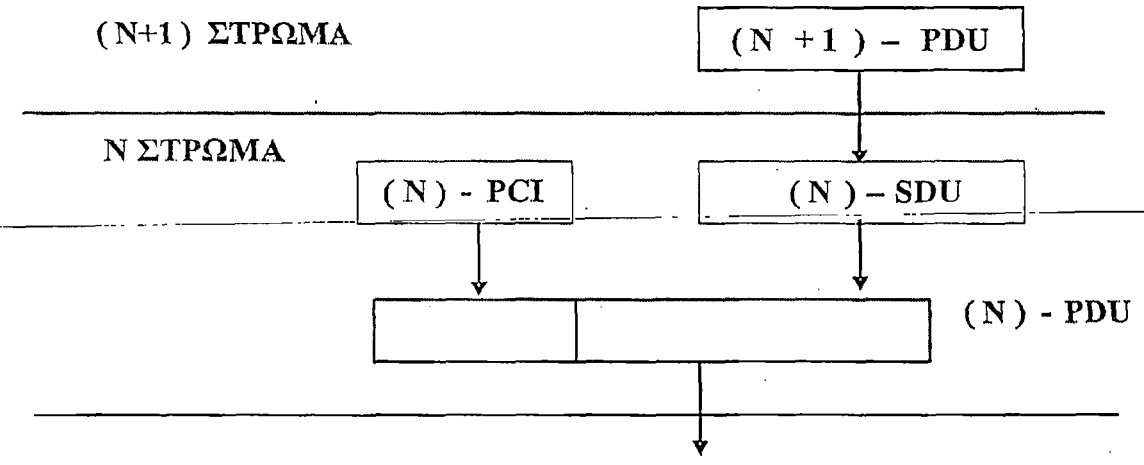
Στην αρχιτεκτονική TCP/IP, τα δεδομένα που εκπέμπονται από το στρώμα εφαρμογής ονομάζονται **ρεύμα δεδομένων (stream of data)**, από το στρώμα μεταφοράς **τμήμα (segment)**, από το στρώμα διαδικτύωσης **δεδομενόγραμμα (datagram)** και από το στρώμα πρόσβασης δικτύου **πλαίσιο (frame)**. Στην αρχιτεκτονική OSI τα δεδομένα που εκπέμπονται από το στρώμα δικτύου ονομάζονται **πακέτο (packet)** και από το στρώμα σύνδεσης **πλαίσιο (frame)**.

Αναλυτικότερα στην επικοινωνία μεταξύ των στρωμάτων διακρίνουμε τις παρακάτω μονάδες:

- Μονάδα Δεδομένων Υπηρεσίας SDU (Service Data Unit). Αποτελείται από τα δεδομένα και τις πληροφορίες ελέγχου που δημιουργούνται στο ανώτερο στρώμα.

- Πληροφορίες Ελέγχου πρωτοκόλλου PCI (Protocol Control Information). Το συναντήσαμε σαν κεφαλίδα και περιέχει πληροφορίες σχετικές με το πρωτόκολλο του εκάστοτε στρώματος.
- Μονάδα Δεδομένων Πρωτοκόλλου PDU (Protocol Data Unit). Είναι ένας συνδυασμός SDU και PCI.

Στο Σχήμα 2-3 βλέπουμε πως ανταλλάσσονται οι μονάδες αυτές κατά την επικοινωνία μεταξύ δύο διαδοχικών στρωμάτων N και N-1. Όταν το PDU περνά από το στρώμα N στο στρώμα N-1 γίνεται ένα SDU. Σε αυτό προστίθεται το PCI του στρώματος N-1 και γίνεται ένα PDU του στρώματος N-1 το οποίο με τη σειρά του περνά στο στρώμα που βρίσκεται από κάτω. Η διαδικασία αυτή επαναλαμβάνεται από στρώμα σε στρώμα μέχρι την μετάδοση των δεδομένων στο φυσικό μέσο.



Σχήμα 2-3 :Η σχέση των PDU, SDU και PCI

2.2 Εισαγωγή στη Διαχείριση Δικτύων

Σήμερα οι επιχειρήσεις επενδύουν σε χρήμα και χρόνο για την υλοποίηση σύνθετων δικτύων υπολογιστών. Αντί η επιχείρηση να τοποθετεί έναν ή περισσότερους μηχανικούς δικτύων για τη λειτουργία και τη συντήρηση αυτών των δικτύων, είναι πιο οικονομικό το σύστημα να φροντίζει από μόνο του για την καλή λειτουργία του. Αυτό θα έχει σαν αποτέλεσμα να ελευθερωθούν οι μηχανικοί και να μπορέσουν να εργασθούν στην μελλοντική ανάπτυξη του δικτύου. Από αυτή την ανάγκη προέκυψε η ιδέα της διαχείρισης. Έτσι, **διαχείριση δικτύων** υπολογιστών είναι η διαδικασία του αυτόματου ελέγχου ενός σύνθετου δικτύου υπολογιστών, με σκοπό την ελαχιστοποίηση του κόστους λειτουργίας και συντήρησής του και την μεγιστοποίηση της απόδοσης και παραγωγικότητας αυτού.

Το γενικό μοντέλο που χρησιμοποιείται σήμερα στη διαχείριση δικτύων υπολογιστών απεικονίζεται στο Σχήμα 2-4. Κρίνεται σκόπιμο ο αναγνώστης να κάνει μία σύγκριση του Σχήματος αυτού με το Σχήμα 2-1 προκειμένου να διαπιστώσει τις επιπλέον μονάδες που προσετέθησαν ώστε το δίκτυο να διαθέτει διαχείριση.

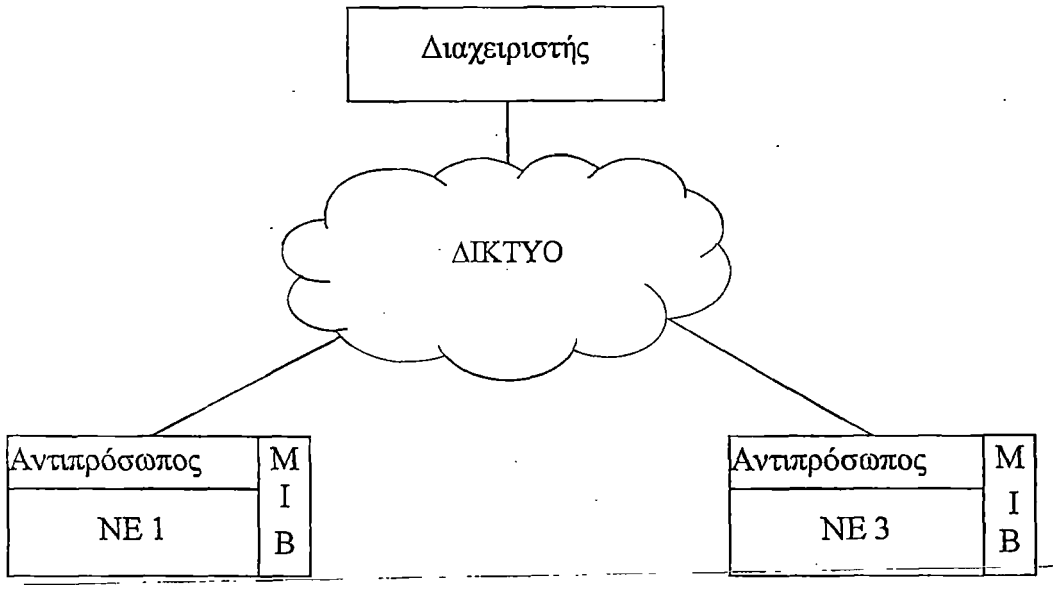
Το μοντέλο διαχείρισης δικτύων υπολογιστών είναι της μορφής πελάτη-εξυπηρετητή (client-server) και αποτελείται από τα στοιχεία δικτύου NE (network elements) που θέλουμε να διαχειριστούμε, τον **Διαχειριστή (Manager),** τους **Αντιπροσώπους (Agents)** και την **Βάση Πληροφοριών Διαχείρισης (Management Information Base - MIB).**

Ο Διαχειριστής αναλαμβάνει την διαδικασία διαχείρισης του δικτύου υπολογιστών, μέσω πρωτοκόλλων επικοινωνίας που μεταφέρουν πληροφορίες διαχείρισης προς και από τα NE.

Οι Αντιπρόσωποι είναι λογισμικό που εγκαθίσταται συνήθως στα NE του δικτύου υπολογιστών. Αναλαμβάνουν την διαδικασία αντιπροσώπευσης των στοιχείων του δικτύου στον διαχειριστή. Αναφέρουν στον Διαχειριστή σχετικά με την κατάσταση των διαχειριζόμενων NE και λαμβάνουν κατευθύνσεις από αυτόν για ενέργειες που πρέπει να εκτελέσουν στα NE που αντιπροσωπεύουν.

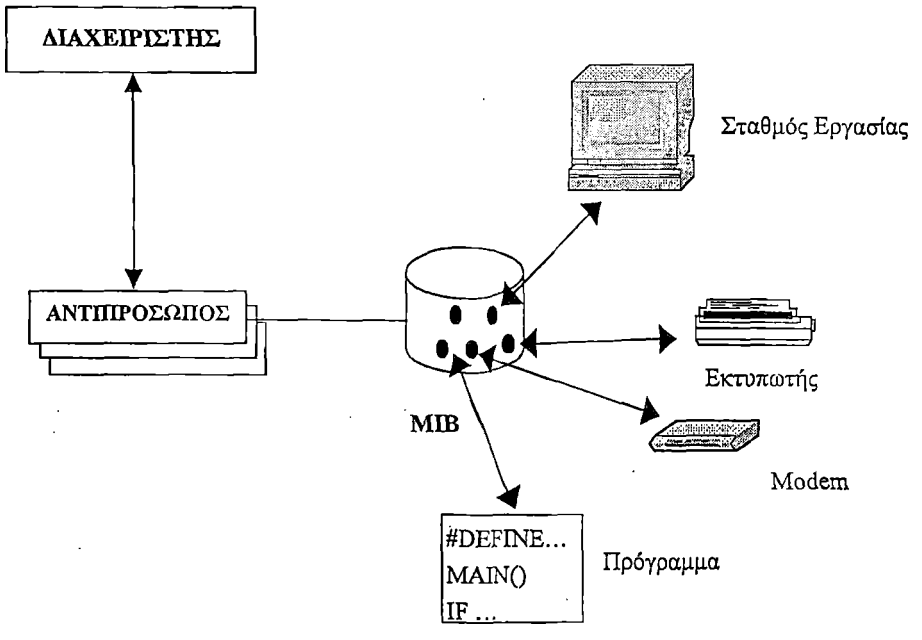
Η Βάση Πληροφοριών Διαχείρισης είναι ουσιαστικά μία βάση δεδομένων που μοιράζεται μεταξύ του Διαχειριστή και των Αντιπροσώπων, για να παρέχει πληροφορίες

σχετικά με τα διαχειριζόμενα NE. Χρησιμοποιείται επίσης στον καθορισμό της δομής και του περιεχομένου της υπό διαχείριση πληροφορίας.



Σχήμα 2-4:Σύστημα Διαχείρισης Δικτύων Υπολογιστών

Η ακριβής σχέση των μονάδων που περιγράψαμε παραπάνω φαίνεται στο Σχήμα 2-5 στο οποίο βλέπουμε επίσης μέσα στην MIB κάποιες μαύρες κουκίδες. Με αυτές παριστάνουμε τα **Υπό Διαχείριση Αντικείμενα (Managed Objects - MO)***. Όλα τα στοιχεία δικτύου εκπροσωπούνται μέσα σε ένα σύστημα διαχείρισης από αυτά. Ο Διαχειριστής δεν αναγνωρίζει τα στοιχεία δικτύου, γι' αυτό το λόγο φτιάχνουμε τα υπό διαχείριση αντικείμενα που εκπροσωπούν τα στοιχεία δικτύου στο διαχειριστή. Ο Διαχειριστής επικοινωνεί μέσω των αντιπροσώπων με τα υπό διαχείριση αντικείμενα (και όχι με τα ίδια τα στοιχεία δικτύου) προκειμένου να πάρει πληροφορίες που αφορούν τα στοιχεία δικτύου. Τα υπό διαχείριση αντικείμενα στην ουσία αποτελούν την λογική εκπροσώπηση των στοιχείων δικτύου και βρίσκονται στην MIB.



Σχήμα 2-5: Σχέση των διαφόρων μονάδων στη διαχείριση δικτύων

Συμπερασματικά, η διαχείριση δικτύων υπολογιστών είναι Εφαρμογή (Στρώμα εφαρμογής στις αρχιτεκτονικές TCP/IP και OSI). Όπως αναφέρθηκε και προηγούμενα, σήμερα

έχουν επικρατήσει δύο αρχιτεκτονικές δικτύων υπολογιστών, η αρχιτεκτονική TCP/IP και η αρχιτεκτονική OSI. Για το λόγο αυτό και τη διαχείριση δικτύων υπολογιστών την διακρίνουμε:

1. Διαχείριση δικτύων υπολογιστών TCP/IP με το **Απλό Πρωτόκολλο Διαχείρισης Δικτύου (Simple Network Management Protocol- SNMP)** που αναλαμβάνει τη μεταφορά των μηνυμάτων Διαχείρισης
2. Διαχείριση δικτύων υπολογιστών OSI με το **Πρωτόκολλο Πληροφοριών Κοινής Διαχείρισης, (Common Management Information Protocol - CMIP).**

Σε αυτά τα δύο είδη διαχείρισης πρέπει να προσθέσουμε και το **Δίκτυο Διαχείρισης Τηλεπικοινωνιών (Telecommunications Management Network - TMN)** που βασίζεται πάνω στη Διαχείριση OSI και αφορά αποκλειστικά τη διαχείριση στοιχείων δικτύου (Κέντρα, SDH, PDH κ.λπ.) που κάνουν χρήση οι Τηλεπικοινωνίες.

Οι βασικές λειτουργίες διαχείρισης είναι **Διαχείριση Βλαβών (Fault), Διάρθρωσης (Configuration), Λογιστικής (Accounting), Επίδοσης (Performance) και Ασφάλειας (Security).**Στη συνέχεια της μελέτης αυτής (Κεφάλαιο 3) θα ασχοληθούμε με την Ασφάλεια στα δίκτυα TCP/IP . Η υλοποίηση των διαφόρων υπηρεσιών ασφάλειας (Έλεγχοι Πρόσβασης, Επαλήθευση κλπ) απαιτεί την τοποθέτηση του αντίστοιχου λογισμικού ασφάλειας μέσα στο NOS. Ο αυτόματος έλεγχος αυτού του λογισμικού είναι η Διαχείριση της Πληροφορίας Ασφάλειας (Κεφάλαιο 4).

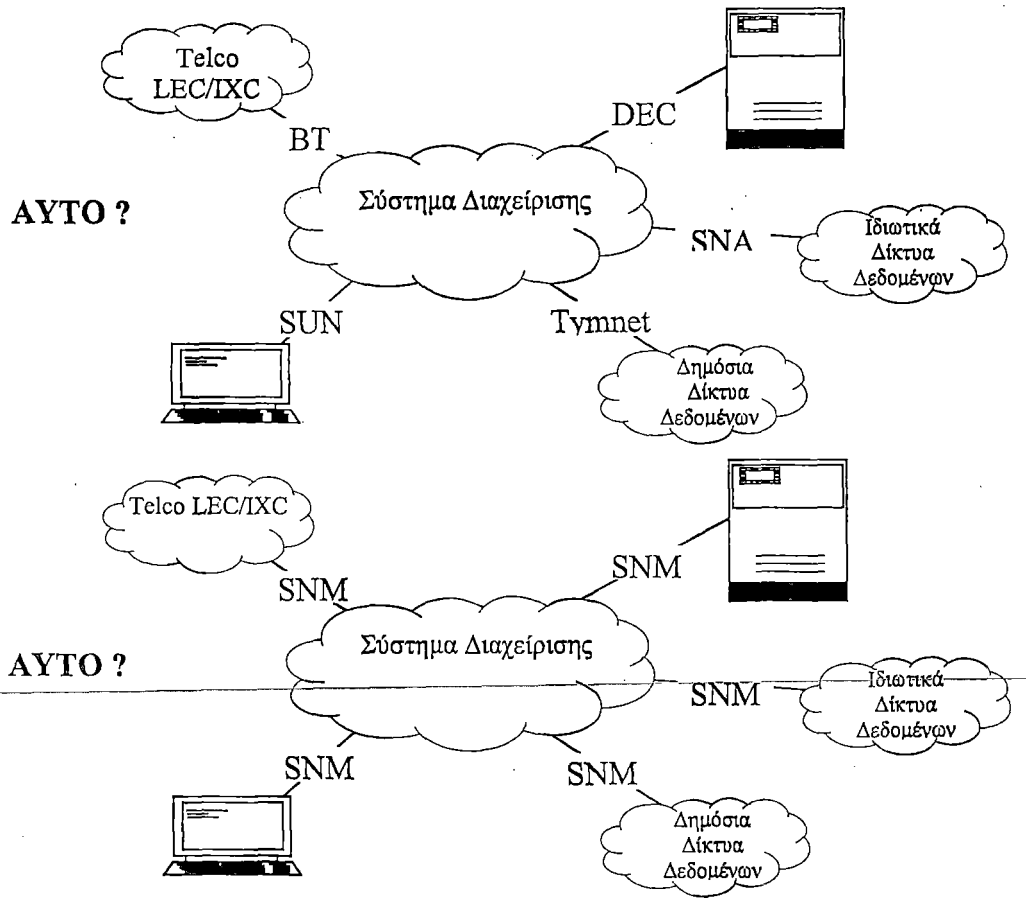
Στις ενότητες που ακολουθούν θα ασχοληθούμε με τη μελέτη της Διαχείρισης Δικτύων TCP / IP και συγκεκριμένα με τα υπό διαχείριση αντικείμενα ,τις ομάδες αντικειμένων της MIB ,τη δομή της πληροφορίας διαχείρισης και το πρωτόκολλο SNMP. Πρώτα όμως θα μελετήσουμε την τυποποίηση στη διαχείριση των δικτύων.

2.3 Η τυποποίηση στη Διαχείριση των Δικτύων

Στο παρελθόν κάθε ένας προμηθευτής δικτύων ανέπτυσσε και διέθετε στην αγορά τα δικά του προϊόντα διαχείρισης δικτύου. Αυτά λειτουργούσαν πολύ καλά εντός του δικτύου του συγκεκριμένου προμηθευτή αλλά, εκτός ελαχίστων εξαιρέσεων, η συνεργασία τους με προϊόντα διαχείρισης δικτύου άλλου προμηθευτή ήταν πολύ δύσκολη.

Στο Σχήμα 2-6 φαίνεται αρχικά ένα δίκτυο χωρίς τυποποιημένη διαχείριση και στην συνέχεια το ίδιο δίκτυο με τυποποιημένη διαχείριση. Το σύννεφο στο κέντρο απεικονίζει ένα δίκτυο με το σύστημα διαχείρισής του. Χωρίς τυποποιημένη διαχείριση το σύστημα διαχείρισης θα έπρεπε να είχε εγκατεστημένο λογισμικό πέντε διαφορετικών προμηθευτών (SUN, DEC κλπ) καθώς και λογισμικό που να λειτουργεί σαν διεπαφή μεταξύ τους. Αυτό συνήθως είχε σαν αποτέλεσμα το αυξημένο κόστος και την χαμηλή επίδοση του δικτύου. Η τυποποιημένη διαχείριση επιτρέπει στο σύστημα διαχείρισης να χρησιμοποιεί μόνο ένα είδος τυποποιημένου λογισμικού **SNM** (Standard Network Management) για την επικοινωνία του με τους διάφορους προμηθευτές δικτυακών παροχών. Το πλεονέκτημα αυτού του είδους διαχείρισης είναι ότι αναγκάζει τους προμηθευτές να εγκαταστήσουν όλοι το ίδιο τυποποιημένο λογισμικό στα προϊόντα τους, με συνέπεια να ωφελείται ο τελικός χρήστης ως προς την μείωση του κόστους και να αυξάνει η επίδοση του δικτύου λόγω της απλούστευσης των απαιτούμενων χειρισμών.

Ο Διεθνής Οργανισμός Τυποποίησης **ISO (International Organisation for Standardisation)** για να καταστήσει δυνατή την εκμετάλλευση και το μοίρασμα των πληροφοριών διαχείρισης, εργάστηκε για πολλά χρόνια πάνω στην ανάπτυξη διαφόρων ανοικτών συστημάτων για τυποποιημένη διαχείριση του δικτύου.Προς αυτή την κατεύθυνση εργάστηκε και η Διεθνής Ένωση Τηλεπικοινωνιών-Τηλεπικοινωνία **(International Telecommunication Union-Telecommunications)**. Επιπλέον το συμβούλιο δραστηριοτήτων διαδικτύου **IAB (Internet Activities Board)**, που έχει αναλάβει την ευθύνη της καθιέρωσης τυποποιήσεων για το διαδίκτυο , έχει υιοθετήσει το αίτημα για σχολιασμό RFC (Request For Comments) ως διαδικασία δημιουργίας προτύπων διαχείρισης. Συστάσεις RFC σχετικές με τη Διαχείριση και την Ασφάλεια δικτύων TCP/IP περιλαμβάνονται στο Παράρτημα Α.



Σχήμα 2-6:Η τυποποίηση στην Διαχείριση Δικτύων

2.4 Διαχείριση Δικτύων TCP / IP

2.4.1 Υπό Διαχείρισή Αντικείμενα

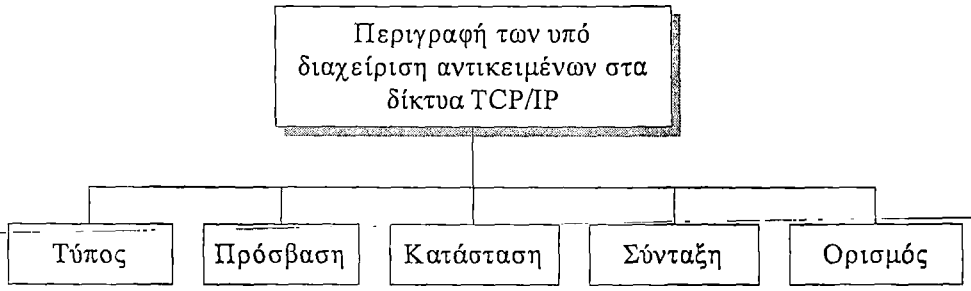
Ο αντιπρόσωπος διατηρεί για κάθε υπό διαχείριση αντικείμενο ένα σύνολο από δομημένες πληροφορίες, στην βάση πληροφοριών διαχείρισης MIB. Ο διαχειριστής, μέσω ενός τυποποιημένου συνόλου μεθόδων πρόσβασης στη MIB, παρακολουθεί και χειρίζεται το υπό διαχείριση αντικείμενο και κατ' επέκταση το στοιχείο του δικτύου.

Όπως φαίνεται και στο Σχήμα 2-7, ένα υπό διαχείριση αντικείμενο στη διαχείριση δικτύων TCP/IP περιγράφεται από :

- Τον **τύπο (type)** που χρησιμοποιείται για τον καθορισμό του αντικειμένου. Για αυτό τον σκοπό σε κάθε τύπο υπάρχουν ένα όνομα (Name) και μια ταυτότητα ID (Identifier).
- Την **πρόσβαση (access)** που επιτρέπεται στο αντικείμενο. Ο προσδιορισμός πρόσβασης, παρέχει πληροφορίες σχετικά με τον επιτρεπτό βαθμό πρόσβασης στο αντικείμενο. Οι παρακάτω προσβάσεις επιτρέπονται σε ένα διαχειριζόμενο αντικείμενο:
  - ◊ **Read-write**, δηλώνοντας ότι τα στιγμιότυπα σε αυτό το αντικείμενο μπορεί και να διαβαστούν και να γραφτούν.
  - ◊ **Read-only**, δηλώνοντας ότι τα στιγμιότυπα σε αυτό το αντικείμενο μπορεί μόνο να διαβαστούν.
  - ◊ **Write-only**, δηλώνοντας ότι τα στιγμιότυπα σε αυτό το αντικείμενο μπορεί να γραφτούν αλλά όχι να διαβαστούν.
  - ◊ **Not-accessible**, δηλώνοντας ότι τα στιγμιότυπα σε αυτό το αντικείμενο δεν μπορεί ούτε να διαβαστούν ούτε να γραφτούν.
- Την **κατάσταση** (status) δηλαδή τις απαιτήσεις για την υλοποίηση του αντικειμένου. Η κατάσταση ενός αντικειμένου μπορεί να είναι:

- ◊ *mandatory*, όταν κάθε διαχειριζόμενος κόμβος απαιτείται να υλοποιεί το διαχειριζόμενο αντικείμενο
- ◊ *optional*, όταν κάθε διαχειριζόμενος κόμβος προαιρετικά υλοποιεί το διαχειριζόμενο αντικείμενο
- ◊ *obsolete*, όταν το διαχειριζόμενο αντικείμενο δεν είναι πλέον χρησιμοποιήσιμο και οι διαχειριζόμενοι κόμβοι δεν χρειάζεται να το υλοποιούν.

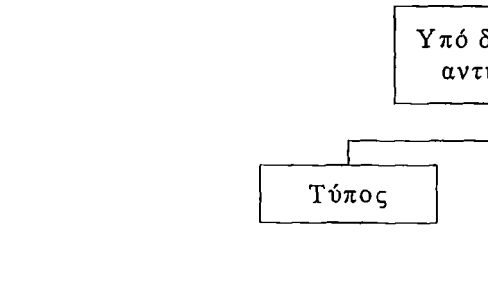
- Τη **σύνταξη (syntax).** Σε αυτήν καθορίζεται η ASN.1 σύνταξη των υπό διαχείριση αντικειμένων.
- Τον **ορισμό (definition).** Αποτελεί περιγραφή του υπό διαχείριση αντικειμένου σε κείμενο.



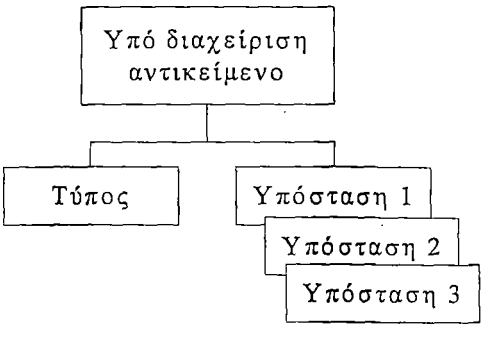
Σχήμα 2-7 :Περιγραφή Διαχειριζόμενων Αντικειμένων

Η υπόσταση (instance) ενός υπό διαχείριση αντικειμένου προκύπτει από αυτό δίδοντας κάποιες τιμές στα γνωρίσματα που το περιγράφουν. Για παράδειγμα ας θεωρήσουμε το υπό διαχείριση αντικείμενο Hub. Σε ένα συγκεκριμένο δίκτυο είναι δυνατό να υπάρχει η υπόσταση Hub 1 με IP διεύθυνση για παράδειγμα 172.16.46.2 και η υπόσταση Hub 2 με IP διεύθυνση για παράδειγμα 172.16.46.3.

Γενικά μπορούμε να πούμε ότι ένα υπό διαχείριση αντικείμενο αποτελείται από τον τύπο και την υπόσταση, όπως βλέπουμε στο Σχήμα 2-8(α). Υπάρχουν υπό διαχείριση αντικείμενα που έχουν πολλές υποστάσεις όπως βλέπουμε στο Σχήμα 2-8(β). Τέλος, σε αυτή την κατηγορία, αν υπάρχουν πολλά αντικείμενα που σχετίζονται μεταξύ τους, τότε μπορούμε να απεικονίσουμε αυτό το σύνολο (Aggregate objects) με ένα πίνακα όπως βλέπουμε στο Σχήμα 2-8(γ). Οι γραμμές του πίνακα αυτού παριστούν τις υποστάσεις που υπάρχουν.



(α)



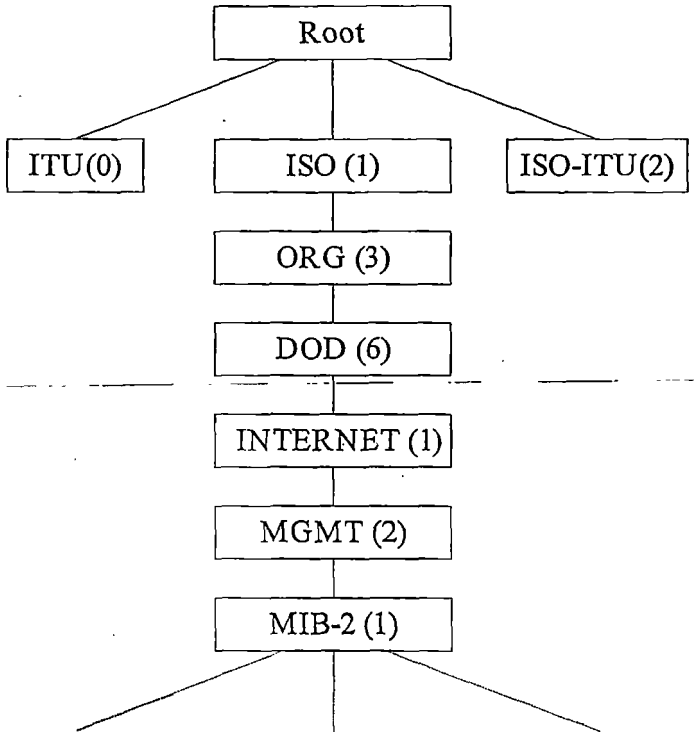
(β)

	MO	.....	MO
Υπόσταση 1	Τιμή		Τιμή
Υπόσταση 2	Τιμή		Τιμή
Υπόσταση 3	Τιμή		Τιμή

(γ)

Σχήμα 2-8:Το υπό διαχείριση αντικείμενο και η υπόσταση

Τα υπό διαχείριση αντικείμενα βρίσκονται μέσα στη Βάση Πληροφοριών Διαχείρισης σε ένα δένδρο που ονομάζεται **Δένδρο Περίεξης (Containment Tree)**. Το δέντρο αυτό ονομάζεται έτσι επειδή τα υπό διαχείριση αντικείμενα βρίσκονται διατεταγμένα στο δένδρο αυτό έτσι ώστε το ένα να περιέχει το άλλο.Επιπλέον, τα υπό διαχείριση αντικείμενα της MIB (υποστάσεις) καταχωρούνται στα κλαδιά του ISO δένδρου καταχώρησης που βλέπουμε στο Σχήμα 2-9.



Σχήμα 2-9:Δένδρο καταχώρησης

Για τον εντοπισμό των υπό διαχείριση αντικειμένων που βρίσκονται στο δένδρο καταχώρησης μιας MIB γίνεται χρήση της ταυτότητας. Ολόκληρη η ταυτότητα στο δένδρο ονομάζεται Απόλυτο Όνομα AN (Absolute Name). Η συνήθης πρακτική είναι να χρησιμοποιείται μόνο το καταληκτικό μέρος δηλαδή το τελευταίο ψηφίο. Αυτό ονομάζεται Σχετικό Όνομα RN (Relative Name). Για πληρέστερη κατανόηση δίδεται η ταυτότητα της mib-2:

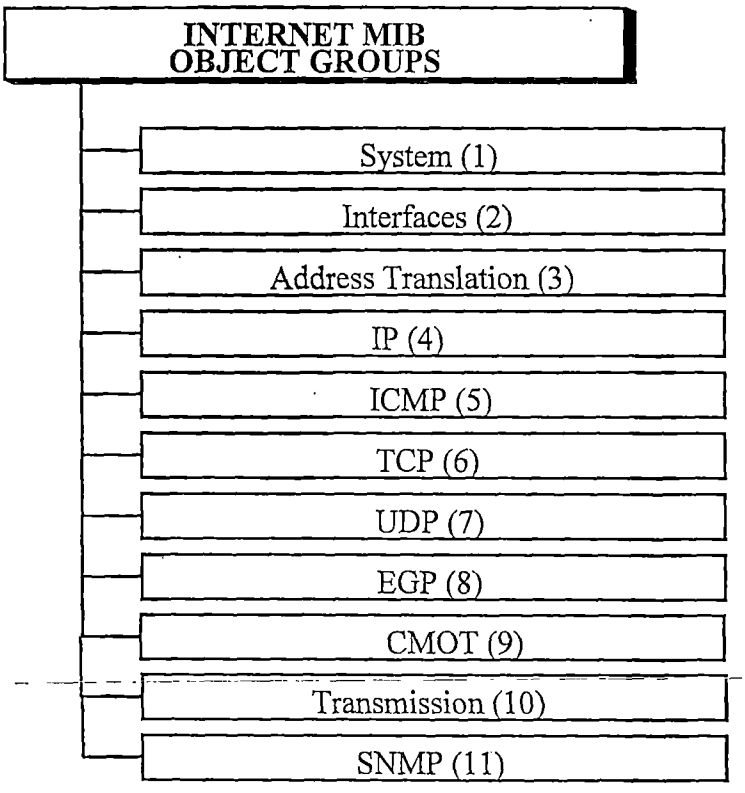
Απόλυτο Όνομα MIB-2 ObjectIdentifier :: = {ISO 36 1 2 1}
Σχετικό Όνομα MIB-2 ObjectIdentifier :: = {MGMT 1}

Έτσι εξασφαλίζουμε πρόσβαση μονοσήμαντα σε κάποιο υπό διαχείριση αντικείμενο που βρίσκεται σε μια MIB, η οποία ανήκει σε κάποιο στοιχείο δικτύου. Φυσικά σε ένα δίκτυο έχουμε πολλά στοιχεία δικτύου τα οποία εντοπίζονται με την IP διεύθυνσή τους. Εύλογο λοιπόν είναι ότι για να έχουμε πρόσβαση σε κάποιο υπό διαχείριση αντικείμενο σε ένα δίκτυο πρέπει να γίνει χρήση της IP διεύθυνσης του στοιχείου δικτύου στο οποίο βρίσκεται η MIB. Η διεύθυνση αυτή τοποθετείται στο τέλος της ταυτότητας. Έτσι για το προηγούμενο παράδειγμα και για MIB-2 που ανήκει στο HUB1 θα έχουμε:

ISO.3.6.1.2.1.172.16.46.2

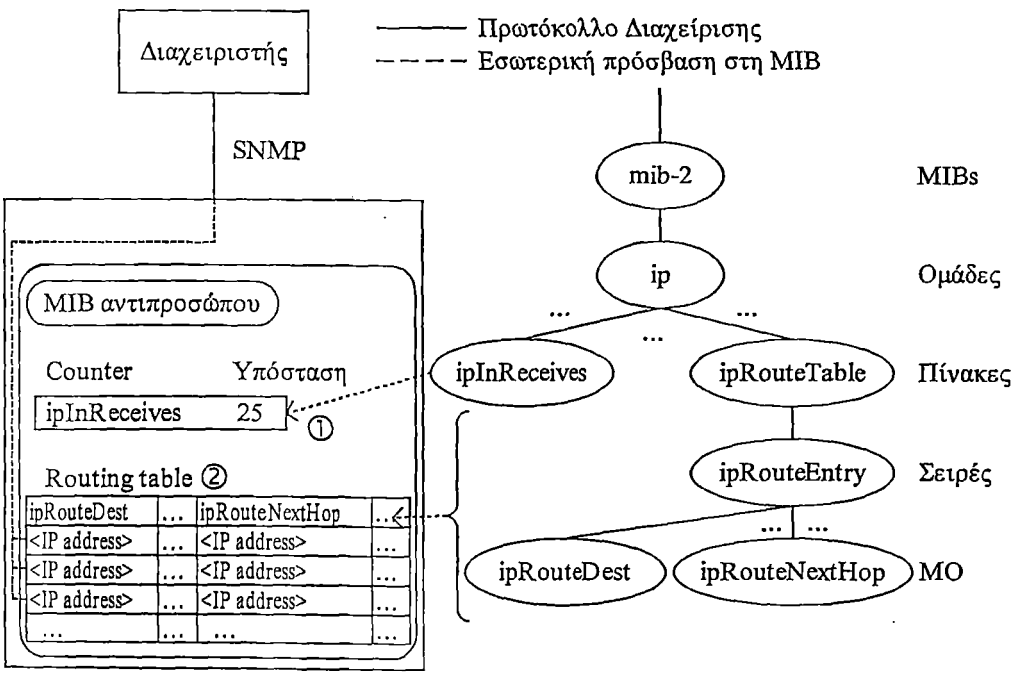
2.4.2 Ομάδες Αντικειμένων της MIB

Η δομή της πληροφορίας διαχείρισης των δικτύων TCP/IP είναι οργανωμένη σε ομάδες αντικειμένων (Object Groups). Προς το παρόν υπάρχουν 11 ομάδες αντικειμένων ορισμένες σαν μέλη της MIB όπως φαίνεται στο Σχήμα 2-10 .



Σχήμα 2-10:Ομάδες αντικειμένων της MIB-2

Στο Σχήμα 2-11 δίδονται κάποιες λεπτομέρειες του δένδρου καταχώρησης που βρίσκεται στη MIB. Τα υπό διαχείριση αντικείμενα βρίσκονται μόνο στα κλαδιά του δένδρου είτε σε απλή μορφή ①, είτε σε μορφή πίνακα ②. Η δομή αυτή είναι στατική. Η μεταβλητή <IP Address> παίρνει τιμές των διαφόρων υποστάσεων που έχουμε στον πίνακα.



Σχήμα 2-11:Παράδειγμα δένδρου καταχώρησης σε μία MIB

2.4.3 Δομή της Πληροφορίας Διαχείρισης

Για τον προσδιορισμό των υπό διαχείριση αντικειμένων το SMI (Structure of Management Information) χρησιμοποιεί τα δομοστοιχεία (modules), που ονομάζονται **Δομοστοιχεία Πληροφορίας (Information Modules)**. Τα δομοστοιχεία πληροφορίας χρησιμοποιούν ένα μηχανισμό της ASN.1 που ονομάζεται **macro** και επιτρέπει την δημιουργία νέων τύπων δεδομένων. Κάθε macro χωρίζεται σε τρία μέρη:

- στο πρώτο μέρος (TYPE NOTATION) ορίζεται ο τρόπος σύνταξης του τύπου των πληροφοριών που περιέχει,
- στο δεύτερο μέρος (VALUE NOTATION) δηλώνεται ο τύπος δεδομένων που θα χρησιμοποιηθεί για την τιμή. Για τον σκοπό αυτό γίνεται χρήση ενός OBJECT-IDENTIFIER
- το τρίτο μέρος περιγράφονται αναλυτικά τα είδη πληροφορίας που είναι δυνατόν να χρησιμοποιηθούν στο πρώτο μέρος καθώς και άλλα βοηθητικά στοιχεία.

Η μορφή του macro που προσδιορίζει τα υπό διαχείριση αντικείμενα δίδεται παρακάτω:

```
OBJECT-TYPE MACRO ::=
BEGIN
  TYPE NOTATION ::=
          "SYNTAX" type(Syntax)
          "MAX-ACCESS" Access
          "STATUS" Status
          "DESCRIPTION" Text

  VALUE NOTATION ::=
          value(VALUE OBJECT IDENTIFIER)
  .....
END
```

Επειδή το OBJECT-TYPE είναι το πιο σημαντικό γιατί χρησιμοποιείται για τον καθορισμό των υπό διαχείριση αντικειμένων, καλό είναι να δώσουμε και ένα απλό παράδειγμα. Ας πούμε ότι θέλουμε να ορίσουμε το υπό διαχείριση αντικείμενο που ονομάζεται snmpInPkts. (Αυτό ανήκει στην ομάδα SNMP).

```
snmpInPkts OBJECT-TYPE
    SYNTAX Counter32
    MAX-ACCESS read-only
    STATUS current
    DESCRIPTION
            "The total number of messages delivered to
             the SNMP entity from the transport service"
::= { snmp 1 }
```

Το παράδειγμα είναι προφανές και το μόνο που πρέπει να επαναλάβουμε είναι ότι το {snmp 1} είναι το Object Identifier που καθορίζει το πεδίο VALUE NOTATION.

Η σύνταξη Abstract Syntax Notation Number One – ASN.1 που απεικονίζει τα Υπο Διαχείριση Αντικείμενα , γνωστή ως Συμβολισμός Αφηρημένης Σύνταξης Έκδοση Πρώτη , περιγράφεται αναλυτικά στο Παράρτημα Β.

2.4.4 Το Απλό Πρωτόκολλο Διαχείρισης Δικτύου SNMP

Στην ενότητα αυτή θα μιλήσουμε για το πρωτόκολλο SNMP (ενότητα 2.4.4.1) το οποίο μεταφέρει πληροφορίες διαχείρισης και την αρχιτεκτονική του SNMPv3 (ενότητα 2.4.4.2).

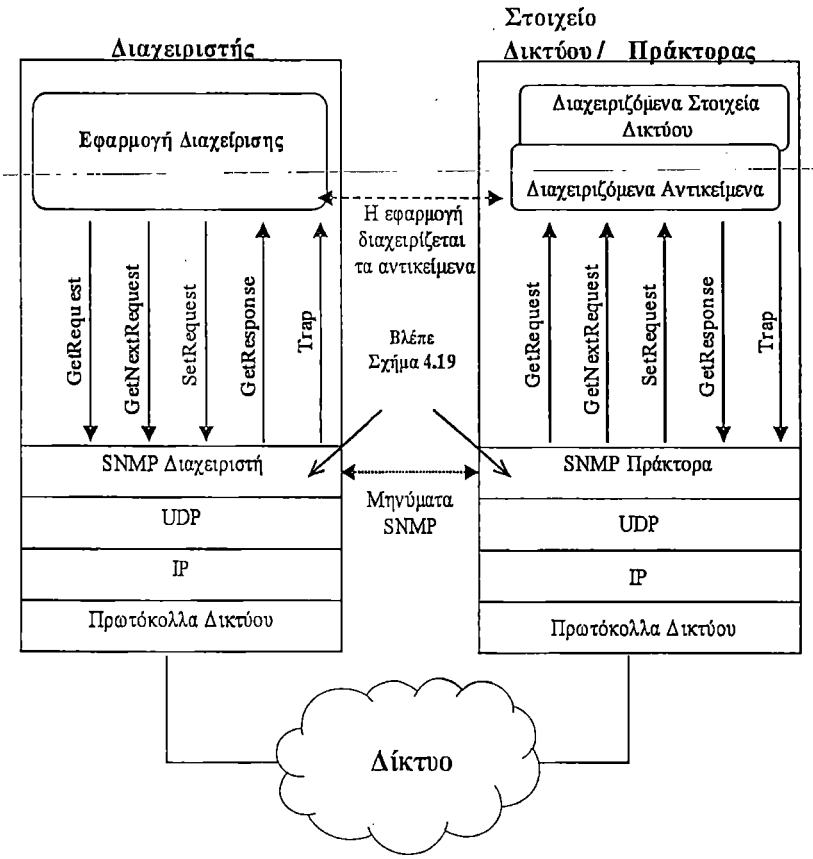
2.4.4.1 Λειτουργίες και Χαρακτηριστικά του SNMP

Το πρωτόκολλο SNMP (Simple Network Management Protocol) είναι ένα απλό πρωτόκολλο του στρώματος εφαρμογής, σχεδιασμένο για να υλοποιεί την ανταλλαγή πληροφοριών διαχείρισης. Οι υπηρεσίες που αυτό παρέχει είναι οι Get, GetNext, Set και Trap. Οι υπηρεσίες αυτές παρέχονται μέσω των πρωτογενών λειτουργιών όπως είναι η GetRequest.

Στο Σχήμα 2-12 επεξηγεί τη λειτουργία του απλού πρωτοκόλλου διαχείρισης δικτύου (SNMP) δίνοντας το γενικό μοντέλο διαχειριστή και αντιπροσώπων καθώς και οι διάφορες πρωτογενείς λειτουργίες που επιτελούνται για τη λειτουργία του πρωτοκόλλου.

Από ένα σταθμό διαχείρισης , εκδίδονται για λογαριασμό των εφαρμογών διαχείρισης τρεις τύποι SNMP μηνυμάτων : GetRequest, GetNextRequest και SetRequest. Τα δύο πρώτα μηνύματα είναι δύο διαφορετικές εκδοχές της λειτουργίας get. Και τα τρία μηνύματα απαντιούνται από τον πράκτορα με το μήνυμα GetResponse, το οποίο περνά στην εφαρμογή διαχείρισης. Επιπλέον , ο πράκτορας μπορεί να εκδώσει ένα μήνυμα παγίδευσης (trap) ως απάντηση σε κάποιο έκτακτο γεγονός που τον επηρεάζει .

Επειδή το πρωτόκολλο SNMP βασίζεται στο πρωτόκολλο UDP, το οποίο είναι ασυνδεσιστρεφές πρωτόκολλο, είναι και αυτό ένα ασυνδεσιστρεφές πρωτόκολλο. Καμία σύνδεση δεν διατηρείται σε εξέλιξη ανάμεσα στον διαχειριστή και στους πράκτορες.



Σχήμα 2-12: Περιβάλλον πρωτοκόλλου SNMP

Στο Σχήμα 2-13 δίδεται σαν παράδειγμα η χρήση της λειτουργίας GetRequest για την άντληση των στοιχείων μιας απλοποιημένης MIB.

Η MIB αυτή περιέχει τα υπό διαχείριση αντικείμενα A, B, T και Z, έκαστο των οποίων αποτελείται από μία υπόσταση. Επίσης περιέχει τον πίνακα E. Η τελεία και το μηδέν που υπάρχει δίπλα σε κάθε υπό διαχείριση αντικείμενο της παρένθεσης δείχνει ότι ζητούμε να πάρουμε την τιμή του αντικειμένου αυτού.

Ας το δούμε αυτό καλύτερα με ένα παράδειγμα, για το υπό διαχείριση αντικείμενο udpInDatagram.

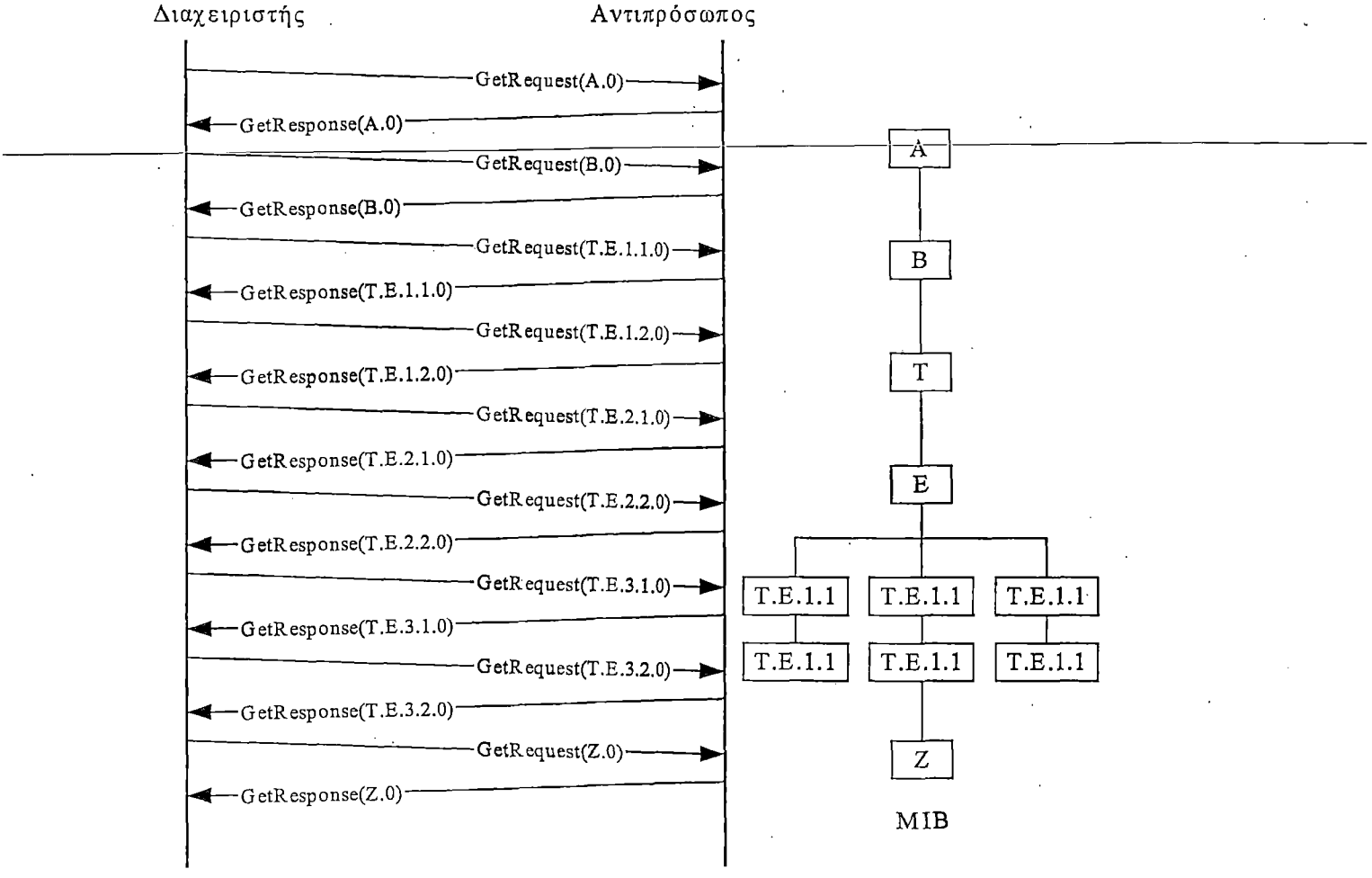
GetRequest(udpInDatagrams.0) δίδει
GetResponse(udpInDatagrams.0=100)

Καθώς το πρωτόκολλο SNMP επιτρέπει την χρήση πολλαπλών παραμέτρων μέσα στην παρένθεση για κάθε λειτουργία, ο σταθμός διαχείρισης μπορεί να στείλει ένα GetRequest με την ακόλουθη μορφή:

GetRequest (udpInDatagrams.0, udpNoPorts.0, udpInErrors.0, udpOutDatagrams.0)

Εάν η MIB που είναι συνδεδεμένη με τον αντιπρόσωπο, υποστηρίζει όλα αυτά τα υπό διαχείριση αντικείμενα, τότε θα επιστραφεί ένα GetResponse, με τις τιμές και των τεσσάρων υπό διαχείριση αντικειμένων.

GetResponse ((udpInDatagrams.0 = 100), (udpNoPorts.0 = 1), (udpInErrors.0 = 2), (udpOutDatagrams.0 = 200))



Σχήμα 2-13:Η GetRequest λειτουργία για τη MIB του σχήματος

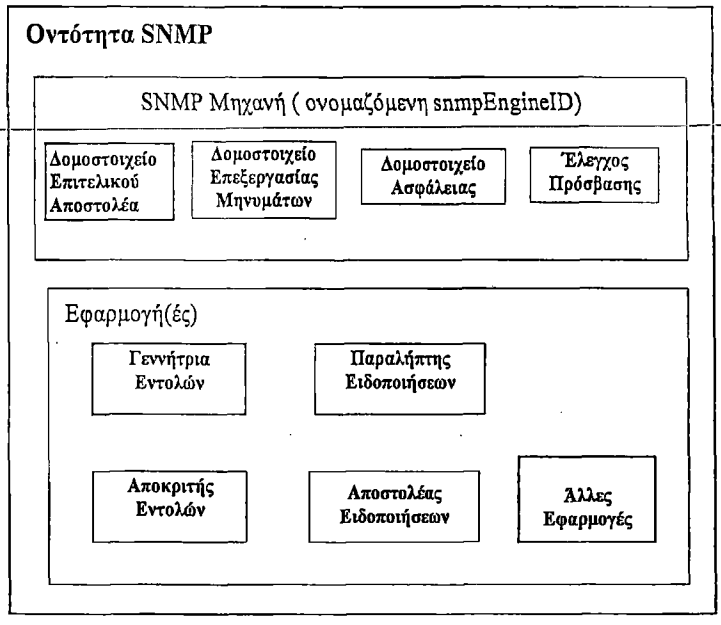
Η ισχύς του SNMP πρωτοκόλλου (έκδοση 1988) είναι η απλότητά του .Το SNMP παρέχει ένα βασικό σύνολο από εργαλεία διαχείρισης δικτύου σε ένα πακέτο το οποίο είναι εύκολο να υλοποιηθεί και ακόμη εύκολο να διαρθρωθεί. Ωστόσο, καθώς οι χρήστες έχουν φτάσει στο σημείο να βασίζονται όλο και περισσότερο στο SNMP ώστε να διαχειριστούν τα ολοένα επεκτεινόμενα δίκτυα με τον συνεχώς αυξανόμενο φόρτο εργασίας ,έχουν γίνει εμφανείς και οι ελλείψεις του. Αυτές οι ελλείψεις εμπίπτουν σε τρεις κατηγορίες:

- Έλλειψη υποστήριξης διαχείρισης κατανεμημένων δικτύων.
- Λειτουργικές ελλείψεις
- Ελλείψεις ασφάλειας

Οι δύο πρώτες κατηγορίες ελλείψεων αντιμετωπίστηκαν στην έκδοση SNMPv2 ,η οποία εκδόθηκε το 1993,με μία επαναληπτική έκδοση το 1996(τρέχουσες συστάσεις RFC. 1901 ,1904 έως 1908 ,2578 και 2579).Το SNMPv2 σύντομα απέκτησε απήχηση και ένας αριθμός από προμηθευτές ανακοίνωσε προϊόντα λίγους μήνες ύστερα από την έκδοση του προτύπου SNMPv2. Οι ελλείψεις σε ασφάλεια καλύφθηκαν στην έκδοση SNMPv3 (έκδοση του 1998, συστάσεις RFC 2570 έως 2575)

2.4.4.2 Αρχιτεκτονική SNMPv3

Τα στοιχεία της αρχιτεκτονικής που σχετίζονται με την SNMP οντότητα, όπως φαίνεται και στο Σχήμα 2-14, αποτελούνται από μία SNMP μηχανή και ένα σύνολο από εφαρμογές. Η SNMP μηχανή , η οποία ονομάζεται snmpEngineID, περιλαμβάνει ένα δομοστοιχείο επιτελικού αποστολέα (dispatcher), ένα δομοστοιχείο επεξεργασίας μηνυμάτων, ένα δομοστοιχείο ασφάλειας και ένα δομοστοιχείο ελέγχου πρόσβασης.



Σχήμα 2-14:Αρχιτεκτονική SNMPv3

Στη συνέχεια θα πούμε λίγα λόγια για καθένα από τα τέσσερα δομοστοιχεία :

Το Δομοστοιχείο Επιτελικού Αποστολέα: Σε μια SNMP μηχανή υπάρχει μόνο ένας επιτελικός αποστολέας, ο οποίος, όμως, μπορεί να χειριστεί πολλαπλές εκδόσεις SNMP μηνυμάτων .Εκτελεί τρία σύνολα από λειτουργίες. Πρώτον, στέλνει μηνύματα στο δίκτυο και λαμβάνει μηνύματα από αυτό. Δεύτερο, καθορίζει σε ποια SNMP έκδοση ανήκει το μήνυμα και αντιδρά ανάλογα με το αντίστοιχο Δομοστοιχείο επεξεργασίας μηνύματος. Τρίτο, ο επιτελικός αποστολέας παρέχει μια διεπαφή σε SNMP εφαρμογές ώστε να μεταφέρουν ένα εισερχόμενο PDU σε μια τοπική εφαρμογή και να στέλνουν ένα PDU από μία τοπική εφαρμογή σε μία απομακρυσμένη οντότητα.

Οι τρεις ξεχωριστές λειτουργίες του Δομσοστοιχείου επιτελικού αποστολέα συντελούνται με χρήση ενός απεικονιστή μεταφοράς ,ενός επιτελικού αποστολέα μηνυμάτων και ενός επιτελικού αποστολέα PDU.

Ο απεικονιστής μεταφοράς μεταφέρει το μήνυμα στο δίκτυο κάνοντας χρήση του κατάλληλου πρωτοκόλλου μεταφοράς. Ο επιτελικός αποστολέας μηνυμάτων δρομολογεί τα εξερχόμενα και τα εισερχόμενα μηνύματα στο κατάλληλο δομοστοιχείο του επεξεργαστή μηνυμάτων .Εάν κάποιο λαμβανόμενο μήνυμα δεν είναι δυνατό να το διαχειριστεί το δομοστοιχείο επεξεργασίας μηνυμάτων μιας συγκεκριμένης SNMP έκδοσης, τότε αυτό μπορεί να απορρίπτεται από τον επιτελικό αποστολέα μηνυμάτων. Ο επιτελικός αποστολέας PDU χειρίζεται την δρομολόγηση της κίνησης των PDU ανάμεσα σε εφαρμογές και στον επεξεργαστή μηνυμάτων.

Το Δομοστοιχείο Επεξεργασίας Μηνυμάτων : Το SNMP Δομοστοιχείο Επεξεργασίας Μηνυμάτων μιας SNMP μηχανής αλληλεπιδρά με τον επιτελικό αποστολέα για το χειρισμό προδιαγεγραμμένων από την έκδοση του SNMP μηνυμάτων. Περιλαμβάνει ένα ή περισσότερα πρότυπα επεξεργασίας μηνυμάτων. Η έκδοση αναγνωρίζεται από το πεδίο έκδοσης της κεφαλίδας.

Το Δομοστοιχείο Ασφάλειας και Ελέγχου Πρόσβασης:Το Δομοστοιχείο Ασφάλειας παρέχει Επαλήθευση και Προστασία του απορρήτου σε επίπεδο μηνύματος. Το Δομοστοιχείο Ελέγχου Πρόσβασης παρέχει ασφάλεια εξουσιοδότησης πρόσβασης.

3. ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ TCP / IP

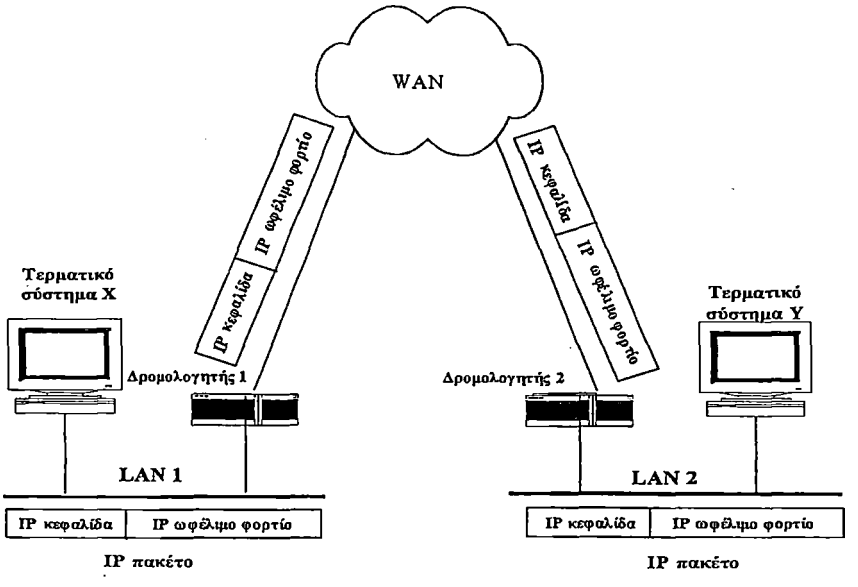
3.1 Ασφάλεια σε Στρώμα IP

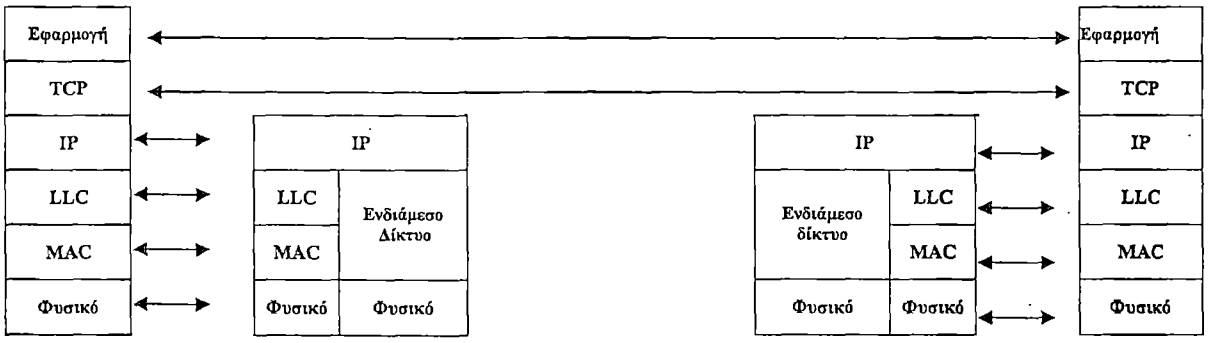
3.1.1 Γενικά για το πρωτόκολλο IP

Ένα διαδικτυακό πρωτόκολλο (Internet Protocol-IP) παρέχει τη λειτουργικότητα για τη διασύνδεση τερματικών συστημάτων δια μέσου πολλαπλών δικτύων. Για το σκοπό αυτό το διαδικτυακό πρωτόκολλο (IP) είναι υλοποιημένο σε κάθε ένα από τα τερματικά συστήματα και στους δρομολογητές οι οποίοι είναι συσκευές που παρέχουν τη σύνδεση ανάμεσα στα δίκτυα. Τα δεδομένα της υψηλότερης στάθμης σε ένα τερματικό σύστημα το οποίο λειτουργεί ως πηγή, ενθυλακώνονται σε μία IP μονάδα δεδομένων πρωτοκόλλου (Protocol Data Unit-PDU) προκειμένου να μεταδοθούν. Αυτή η μονάδα δεδομένων πρωτοκόλλου διασχίζει ένα ή περισσότερα δίκτυα καθώς και τους δρομολογητές που τα συνδέουν για να φτάσει στο τερματικό σύστημα του προορισμού της.

Η λειτουργία ενός δρομολογητή όπως παρουσιάζεται στο Σχήμα 3-1 βασίζεται σε ένα διαδικτυακό πρωτόκολλο. Σε αυτό το παράδειγμα το διαδικτυακό πρωτόκολλο (IP) της στοίβας πρωτοκόλλων TCP/IP εκτελεί αυτήν την λειτουργία. Το πρωτόκολλο IP θα πρέπει να υλοποιείται σε όλα τα τερματικά συστήματα όλων των δικτύων καθώς και σε όλους τους δρομολογητές. Επιπρόσθετα κάθε τερματικό σύστημα θα πρέπει να χρησιμοποιεί συμβατά πρωτόκολλα πάνω από το IP προκειμένου να επικοινωνεί επιτυχώς. Οι ενδιάμεσοι δρομολογητές χρειάζεται μόνο να έχουν πρωτόκολλα μέχρι το IP.

Ας θεωρήσουμε τη μετάδοση δεδομένων από το τερματικό σύστημα X στο τερματικό σύστημα Y όπως φαίνεται στο Σχήμα 3-1. Το στρώμα IP του X παραλαμβάνει τα δεδομένα που πρέπει να αποσταλούν στο Y από το στρώμα TCP του X. Το στρώμα IP επισυνάπτει μία κεφαλίδα που καθορίζει την καθολική διεύθυνση του Y. Αυτή η διεύθυνση διαιρείται σε δύο τμήματα: στο αναγνωριστικό δικτύου και στο αναγνωριστικό τερματικού συστήματος. Στο εξής το σύνολο αυτό των δεδομένων θα το ονομάζουμε IP πακέτο. Κατόπιν το IP αναγνωρίζει ότι ο τελικός προορισμός, δηλαδή το Y βρίσκεται σε ένα άλλο υποδίκτυο. Έτσι το πρώτο βήμα είναι να στείλει το πακέτο αυτό σε ένα δρομολογητή που στην προκειμένη περίπτωση είναι ο δρομολογητής 1.Για να επιτευχθεί αυτό, το IP μεταβιβάζει αυτή τη μονάδα δεδομένων στο υπόστρωμα Λογικού Ελέγχου Σύνδεσης (Logical Link Control-LLC) με τις κατάλληλες πληροφορίες διευθυνσιοδότησης. Το υπόστρωμα Λογικού Ελέγχου Σύνδεσης LLC δημιουργεί μία μονάδα δεδομένων πρωτοκόλλου Λογικού Ελέγχου Σύνδεσης LLC-PDU η οποία μεταβιβάζεται χαμηλότερα στο υπόστρωμα ελέγχου προσπέλασης μέσου (Media Access Control-MAC).Το υπόστρωμα ελέγχου προσπέλασης μέσου κατασκευάζει ένα πακέτο ελέγχου προσπέλασης μέσου του οποίου η κεφαλίδα περιέχει τη διεύθυνση του δρομολογητή 1.





Σχήμα 3-1: Διάρθρωση ενός TCP/IP παραδείγματος.

Κατόπιν , το πακέτο διασχίζει το τοπικό δίκτυο 1 και φτάνει στο δρομολογητή 1. Ο δρομολογητής αφαιρεί το πακέτο και τις LLC κεφαλίδες και ουρές που πρόσθεσε το υπόστρωμα Λογικού Ελέγχου Σύνδεσης μέσου και αναλύει την IP κεφαλίδα προκειμένου να προσδιορίσει τον τελικό προορισμό των δεδομένων που στην προκειμένη περίπτωση είναι το τερματικό Υ. Η γνώση του τελικού προορισμού των δεδομένων Υ είναι απαραίτητη για τον δρομολογητή προκειμένου να λάβει την απόφαση δρομολόγησης.
Υπάρχουν δύο πιθανότητες:

1. Το τερματικό σύστημα που αποτελεί τον τελικό προορισμό, εν προκειμένω το Υ, είναι απευθείας συνδεδεμένο με ένα από τα υποδίκτυα που βρίσκονται σε άμεση επαφή με το δρομολογητή.
2. Χρειάζεται να μεσολαβήσουν ένας ή περισσότεροι επιπλέον δρομολογητές , για να μπορέσουν τα δεδομένα να φτάσουν στον τελικό προορισμό.

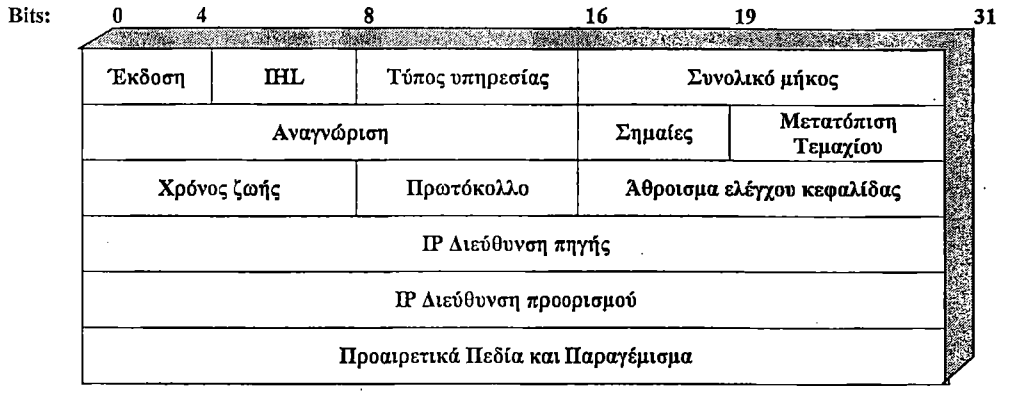
Σε αυτό το παράδειγμα, το πακέτο θα πρέπει να κατευθυνθεί προς το δρομολογητή 2 προκειμένου να φτάσει στον τελικό του προορισμό. Έτσι, ο δρομολογητής 1 δρομολογεί το πακέτο IP, διαμέσω του ενδιάμεσου δικτύου, στον δρομολογητή 2.Για το σκοπό αυτό χρησιμοποιούνται τα πρωτόκολλα του ενδιάμεσου δικτύου. Για παράδειγμα αν το δίκτυο που μεσολαβεί είναι ένα X.25 δίκτυο, η IP μονάδα δεδομένων τυλίγεται σε ένα πακέτο X.25 με τις κατάλληλες πληροφορίες διευθυνσιοδότησης ,ώστε να μπορέσει να φτάσει στο δρομολογητή 2. Όταν το πακέτο φτάσει στο δρομολογητή 2, ο τελευταίος αφαιρεί τις πληροφορίες αυτές. Στη συνέχεια καθορίζει ότι το εν λόγω πακέτο απευθύνεται στο τερματικό σύστημα Υ, το οποίο είναι απευθείας συνδεδεμένο στο υποδίκτυο το οποίο έχει άμεση επαφή με αυτόν. Έτσι δημιουργεί ένα πακέτο με διεύθυνση προορισμού τη δικτυακή διεύθυνση του Υ και το κατευθύνει στο τοπικό δίκτυο 2. Τελικά, τα δεδομένα φτάνουν στο Υ όπου το πακέτο, οι διαδικτυακές κεφαλίδες και ουρές καθώς και αυτές του υποστρώματος λογικού ελέγχου σύνδεσης αφαιρούνται.

Για δεκαετίες η βάση της αρχιτεκτονικής του TCP/IP πρωτοκόλλου ήταν η έκδοση 4 του πρωτοκόλλου IP ,όπως αυτή αναφέρεται στη σύσταση RFC 791. Το Σχήμα 3-2 δείχνει τη διαμόρφωση μίας IP κεφαλίδας η οποία είναι το λιγότερο 20 bytes δηλαδή το λιγότερο 160 bits.

Τα πεδία της κεφαλίδας που φαίνονται και στο Σχήμα 3-2 είναι τα εξής:

- **Τύπος υπηρεσίας (Type of service) 8 bit**: Παρέχει καθοδήγηση στα τερματικά συστήματα και στους δρομολογητές που βρίσκονται κατά μήκος του μονοπατιού που ακολουθεί το πακέτο, όσον αφορά στη σχετική προτεραιότητα του πακέτου.
- **Συνολικό μήκος (Total length) 16 bit**: Δηλώνει το συνολικό μήκος του IP πακέτου σε byte.
- **Αναγνώριση (Identification) 16 bit**: Είναι ένας αριθμός ακολουθίας ο οποίος μαζί με τη διεύθυνση της πηγής, τη διεύθυνση του προορισμού και το πρωτόκολλο χρήστη έχει ως σκοπό την αναγνώριση ενός πακέτου. Για αυτό, το αναγνωριστικό θα πρέπει να είναι μοναδικό για μία συγκεκριμένη διεύθυνση πηγής, προορισμού και πρωτοκόλλου χρήστη για όσο χρόνο το πακέτο θα παραμείνει στο διαδίκτυο.

- **Σημαίες (Flags) 3 bit** : Σε αυτό το πεδίο μόνο δύο bit είναι επί του παρόντος σε χρήση. Το ένα από αυτά ονομάζεται bit Περισσότερα (More) και το άλλο bit του Μη Τεμαχισμού. Όταν ένα πακέτο είναι τεμαχισμένο το bit Περισσότερα υποδεικνύει ποιο είναι το τελευταίο τεμάχιο του αυθεντικού πακέτου. Όταν το bit του Μη Τεμαχισμού έχει την τιμή 1 ο κατατεμαχισμός απαγορεύεται. Αυτό το bit μπορεί να χρησιμεύσει όταν ο παραλήπτης δεν έχει την ικανότητα της επανασυναρμολόγησης των πακέτων. Θα πρέπει πάντως να έχουμε υπόψη μας ότι εάν το bit του μη τεμαχισμού έχει την τιμή 1 και το μήκος του πακέτου υπερβαίνει το επιτρεπόμενο μήκος που μπορεί να δρομολογηθεί μέσα από κάποιο υποδίκτυο, το πακέτο θα απορριφθεί από το υποδίκτυο αυτό. Υπό αυτήν την έννοια εάν το bit του μη τεμαχισμού έχει την τιμή 1 ενδείκνυται να χρησιμοποιούμε δρομολόγηση πηγής (source routing) προκειμένου να αποφύγουμε υποδίκτυα με μικρό μέγιστο μήκος μεταδιδόμενου πακέτου.
- **Μετατόπιση τεμαχίου (Fragment offset) 13 bit**: Υποδεικνύει την ακριβή θέση ενός τεμαχίου μέσα στο πακέτο υποθέτοντας ότι το αυθεντικό πακέτο χωρίζεται σε στοιχειώδη τεμάχια μεγέθους 64 bit. Υπό αυτήν την έννοια το μήκος των δεδομένων όλων των τεμαχίων πλην του τελευταίου θα πρέπει να είναι πολλαπλάσιο των 64 bit.
- **Χρόνος ζωής(Time to live-TTL) 8 bit** : Καθορίζει το μέγιστο χρόνο, μετρημένο σε δευτερόλεπτα, που επιτρέπεται σε ένα πακέτο να παραμείνει στο Διαδίκτυο. Κάθε δρομολογητής οποτεδήποτε προωθεί ένα πακέτο θα πρέπει να μειώνει τον χρόνος ζωής τουλάχιστον κατά 1, δηλαδή ο χρόνος ζωής λειτουργεί σαν μία αντίστροφη μέτρηση.
- **Πρωτόκολλο(Protocol) 8 bit**: Ορίζει το πρωτόκολλο του αμέσως ανώτερου στρώματος το οποίο δέχεται το πεδίο δεδομένων όταν το πακέτο φτάσει στον προορισμό του. Κατά συνέπεια , αυτό το πεδίο καθορίζει τον τύπο της κεφαλίδας στο πακέτο μετά την IP κεφαλίδα.
- **Άθροισμα ελέγχου κεφαλίδας (Header Checksum) 16 bit**: Κώδικας ελέγχου σφαλμάτων που χρησιμοποιείται για την ανίχνευση σφαλμάτων κατά τη μετάδοση δεδομένων. Περιέχει το συμπλήρωμα ως προς 1 όλων των λέξεων μήκους 16 bit της κεφαλίδας IP.Ο έλεγχος σφαλμάτων που παρέχει το IP αφορά μονάχα την κεφαλίδα του πακέτου και όχι τα δεδομένα του πρωτοκόλλου υψηλότερου επιπέδου που περιέχει. Ο έλεγχος των σφαλμάτων αυτών είναι ευθύνη του εκάστοτε πρωτοκόλλου. Επειδή ορισμένα από τα πεδία της κεφαλίδας μπορεί να αλλάξουν κατά τη διάρκεια της μετάδοσης, όπως για παράδειγμα ο χρόνος ζωής , κάθε δρομολογητής υπολογίζει κάθε φορά το άθροισμα ελέγχου που πρέπει να έχει το πακέτο καθώς φεύγει από αυτόν και τοποθετεί τη νέα τιμή στο πεδίο.
- **IP Διεύθυνση πηγής (Source address) 32 bit** : Προσδιορίζει το τερματικό σύστημα που αποτελεί την πηγή καθώς και το δίκτυο στο οποίο αυτό ανήκει. Η κωδικοποίηση επιτρέπει μεταβλητότητα στην κατανομή των bit. Έτσι τα μήκη των συμβολοσειρών που καθορίζουν την πηγή και το αντίστοιχο δίκτυο μπορεί να είναι αντίστοιχα 24 και 7, 16 και 14 ή 8 και 21.
- **IP Διεύθυνση προορισμού (Destination address) 32 bit**: Προσδιορίζει το τερματικό σύστημα που αποτελεί τον προορισμό καθώς και το δίκτυο στο οποίο αυτό ανήκει. Και πάλι η κωδικοποίηση επιτρέπει μεταβλητότητα στην κατανομή των bits με τα μήκη των συμβολοσειρών που καθορίζουν τον προορισμό και το αντίστοιχο δίκτυο να μπορούν και πάλι να πάρουν αντίστοιχα τις τιμές 24 και 7, 16 και 14 ή 8 και 21.
- **Προαιρετικό Πεδίο (Options)**: Κωδικοποιεί τις επιλογές που προτιμά ο αποστολέας. Σε αυτές περιλαμβάνονται η λειτουργία δρομολόγησης από την πηγή (source routing), η χρήση ετικετών ασφάλειας (security label), η καταγραφή της δρομολόγησης (record routing) και η χρονοσήμανση (timestamping). Έχει μεταβλητό μέγεθος.
- **Παραγέμισμα(Padding)**: Χρησιμοποιείται για να διασφαλιστεί ότι η κεφαλίδα του πακέτου θα έχει μήκος πολλαπλάσιο των 32 bit. Έχει μεταβλητό μέγεθος.

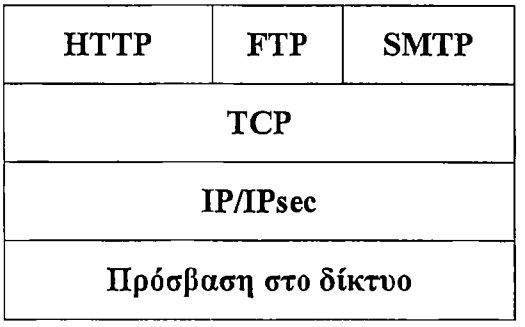


Σχήμα 3-2:IPv4 κεφαλίδα

3.1.2 Ασφάλεια IPsec

3.1.2.1 Αρχιτεκτονική

Στο Σχήμα 3-3 φαίνονται τα στρώματα της αρχιτεκτονικής TCP/IP. Το IPsec βρίσκεται στο δεύτερο στρώμα δηλαδή το στρώμα δικτύου.



Σχήμα 3-3: Τα στρώματα της αρχιτεκτονικής TCP/IP.

Η ασφάλεια του στρώματος IP καλύπτει τρεις λειτουργικές περιοχές : την επαλήθευση, την εμπιστευτικότητα και τη διαχείριση κλειδιών. Ο μηχανισμός της επαλήθευσης εξασφαλίζει ότι το πακέτο που παραλήφθηκε είχε, πραγματικά , μεταδοθεί από την οντότητα η οποία αναγνωρίζεται ως ο αποστολέας του πακέτου και επιπλέον ότι το πακέτο δεν τροποποιήθηκε κατά τη μετάδοση. Η δυνατότητα παροχής εμπιστευτικότητας επιτρέπει στους επικοινωνούντες κόμβους την κρυπτογράφηση των μηνυμάτων ,ώστε να εμποδίζει την λαθρακρόαση από τρίτους. Η δυνατότητα διαχείρισης κλειδιών σχετίζεται με την ασφαλή ανταλλαγή των κλειδιών.

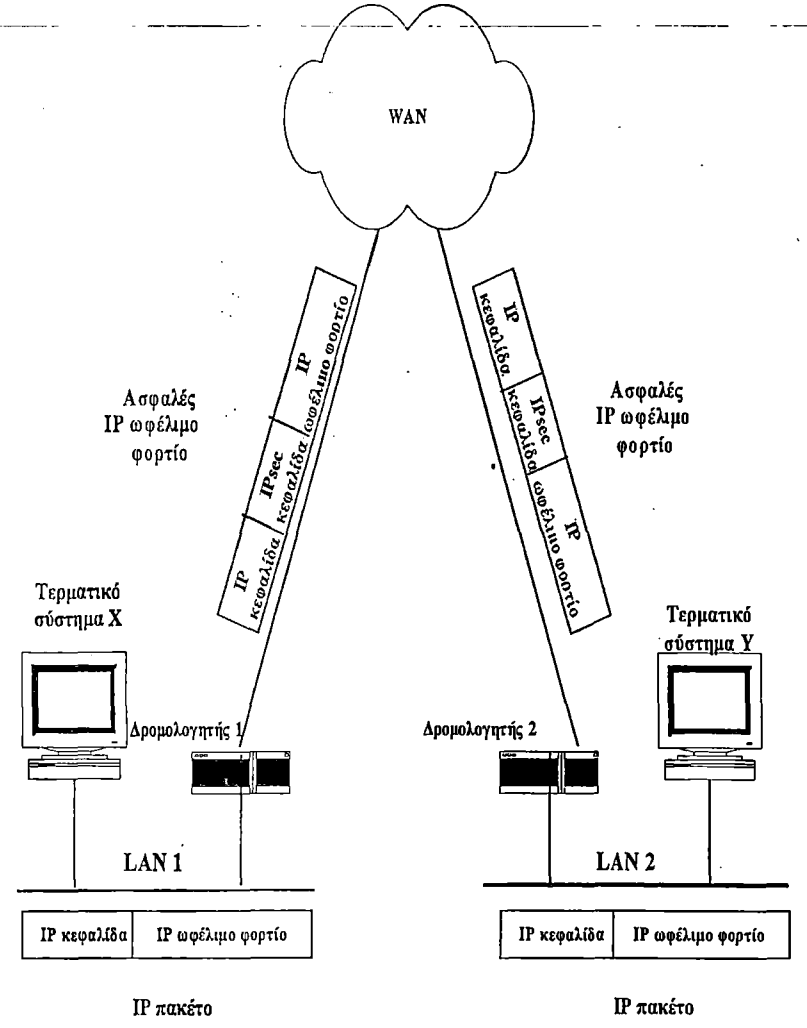
Ξεκινάμε την ενότητα αυτή με μία γενική περιγραφή της ασφάλειας του στρώματος IP (IPsec) και με μία εισαγωγή της αρχιτεκτονικής της ασφάλειας του στρώματος IP. Στη συνέχεια θα εξετάσουμε αναλυτικότερα τις τρεις λειτουργικές περιοχές .

Στο Σχήμα 3-4 έχουμε ένα τυπικό σενάριο της χρήσης του IPsec. Ένας οργανισμός διαθέτει τοπικά δίκτυα που είναι διασκορπισμένα σε διάφορα σημεία. Η δικτυακή κίνηση εσωτερικά σε κάθε ένα από αυτά τα τοπικά δίκτυα γίνεται χωρίς τη χρήση ασφάλειας του στρώματος IP. Πρωτόκολλα ασφάλειας του στρώματος IP χρησιμοποιούνται μόνο στην επικοινωνία αυτών των τοπικών δικτύων μεταξύ τους η οποία γίνεται μέσω ενός δικτύου ευρείας περιοχής (WAN). Τα πρωτόκολλα αυτά εφαρμόζονται σε στοιχεία δικτύου, όπως οι δρομολογητές ή τα τείχη προστασίας (firewall) τα οποία συνδέουν τα τοπικά δίκτυα με τον έξω κόσμο. Κάθε IPSec δικτυακή συσκευή από τη μία κρυπτογραφεί και συμπιέζει όλη τη δικτυακή κίνηση που κατευθύνεται από τα τοπικά δίκτυα προς το δίκτυο ευρείας περιοχής και από την άλλη αποκρυπτογραφεί και αποσυμπιέζει όλη τη δικτυακή κίνηση που κατευθύνεται από το δίκτυο ευρείας περιοχής προς τα τοπικά δίκτυα. Οι λειτουργίες αυτές είναι διαφανείς στους σταθμούς εργασίας (workstation) και στους εξυπηρετητές (servers) των τοπικών δικτύων. Επιπλέον είναι εφικτή η ασφαλής μετάδοση για τους μεμονωμένους χρήστες του

δικτύου ευρείας περιοχής. Για να παρέχεται ασφάλεια στους χρήστες αυτούς οι αντίστοιχοι σταθμοί εργασίας πρέπει να υλοποιούν τα IPsec πρωτόκολλα.

Το IPSec παρέχει υπηρεσίες ασφάλειας στο στρώμα IP ενεργοποιώντας ένα σύστημα το οποίο επιλέγει τα απαιτούμενα πρωτοκόλλα ασφάλειας, καθορίζει τον ή τους αλγόριθμους που πρέπει να χρησιμοποιηθούν και θέτει σε ισχύ τα απαραίτητα κλειδιά κρυπτογράφησης για την παροχή των απαιτούμενων υπηρεσιών.Για πληρέστερη κατανόηση κρίνεται σκόπιμο να γίνει σύγκριση του Σχήματος 3-4 με το Σχήμα 3-1.

Το IPSec αποτελείται από δύο ξεχωριστά πρωτόκολλα: το πρωτόκολλο Κεφαλίδας Επαλήθευσης (Authentication Header-AH) (σύσταση RFC 2402) και το πρωτόκολλο Ασφαλούς Ενθυλάκωσης Ωφέλιμου Φορτίου (Encapsulating Security Payload-ESP) (σύσταση RFC 2406). Η χρήση του ενός δεν περιορίζει τη χρήση του άλλου. Η κεφαλίδα επαλήθευσης AH παρέχει ακεραιότητα δεδομένων και επαλήθευση για το ωφέλιμο φορτίο και τα αμετάβλητα πεδία της IP κεφαλίδας, όπως είναι τα πεδία τα οποία δε μπορούν να τροποποιηθούν από τους ενδιάμεσους δρομολογητές με κανένα απρόβλεπτο τρόπο. Το πρωτόκολλο ασφαλούς ενθυλάκωσης ωφέλιμου φορτίου ESP παρέχει Εμπιστευτικότητα δεδομένων και / ή επαλήθευση για το IP ωφέλιμο φορτίο.



Σχήμα 3-4: Τυπικό IPsec σενάριο ασφάλειας.

Ο Πίνακας 3-1 δείχνει ποιες υπηρεσίες παρέχονται από τα πρωτόκολλα AH και ESP. Για τα πρωτόκολλα ESP υπάρχουν δύο περιπτώσεις: Είτε να παρέχουν και επαλήθευση είτε όχι. Και τα AH και τα ESP πρωτόκολλα είναι φορείς του ελέγχου πρόσβασης, βασισμένα στη διανομή των κλειδιών κρυπτογράφησης και στη διαχείριση ροών κίνησης σχετιζόμενων με αυτά τα πρωτόκολλα ασφάλειας.

Πρωτόκολλο / Υπηρεσία	AH	ESP	
		ESP (Μόνο κρυπτογράφηση)	ESP (Επαλήθευση και κρυπτογράφηση)
Έλεγχος πρόσβασης.	√	√	√
Ασυνδεσμική ακεραιότητα.	√	√	√
Επαλήθευση προέλευσης δεδομένων.	√		√
Απόρριψη επαναλαμβανόμενων πακέτων.	√	√	√
Εμπιστευτικότητα.		√	√
Εμπιστευτικότητα περιορισμένης ροής κίνησης.		√	√

Πίνακας 3-1:Υπηρεσίες που παρέχουν τα πρωτόκολλα AH και ESP

3.1.2.2 Συσχετισμοί ασφάλειας

Η ιδέα κλειδί, η οποία εμφανίζεται στις υπηρεσίες τόσο της επαλήθευσης όσο και της εμπιστευτικότητας, είναι ο συσχετισμός ασφάλειας (Security Association-SA). Με τον όρο συσχετισμός εννοούμε μία μονόδρομη σχέση μεταξύ ενός αποστολέα και ενός παραλήπτη, η οποία παρέχει υπηρεσίες ασφάλειας στην κίνηση που υποστηρίζει. Εάν είναι απαραίτητη σε μία ομότιμη σχέση να επιτύχουμε ασφαλείς αμφίδρομες συναλλαγές , τότε χρειαζόμαστε δύο συσχετισμούς ασφάλειας.

Ένας συσχετισμός ασφάλειας μπορεί να υλοποιείται είτε σε ένα πρωτόκολλο κεφαλίδας επαλήθευσης AH είτε σε ένα πρωτόκολλο ασφαλούς ενθυλάκωσης ωφέλιμου φορτίου ESP , όχι όμως ταυτόχρονα και στα δύο. Ο συσχετισμός ασφάλειας καθορίζει ποιο πρωτόκολλο χρησιμοποιείται: το πρωτόκολλο κεφαλίδας επαλήθευσης AH ή το πρωτόκολλο ασφαλούς ενθυλάκωσης ωφέλιμου φορτίου ESP. Αν χρησιμοποιείται το πρωτόκολλο ασφαλούς ενθυλάκωσης ωφέλιμου φορτίου ESP, ο συσχετισμός ασφάλειας καθορίζει εάν θα χρησιμοποιηθεί για να παρέχει υπηρεσία ακεραιότητας δεδομένων, εμπιστευτικότητας ή και τις δύο (αλλά ποτέ καμία υπηρεσία). Επιπλέον, ο συσχετισμός ασφάλειας καθορίζει ποιος ή ποιοι αλγόριθμοι καθώς και ποιες παράμετροι (όπως είναι τα κλειδιά κρυπτογράφησης) χρησιμοποιούνται από κάθε ένα από τα επιλεγμένα πρωτόκολλα. Εάν ένα IP πακέτο απαιτεί τις υπηρεσίες τόσο του πρωτοκόλλου AH όσο και του πρωτοκόλλου ESP, μπορεί να προστατεύεται από δύο συσχετισμούς ασφάλειας SA, που αποτελούν μία δέσμη συσχετισμών ασφάλειας .

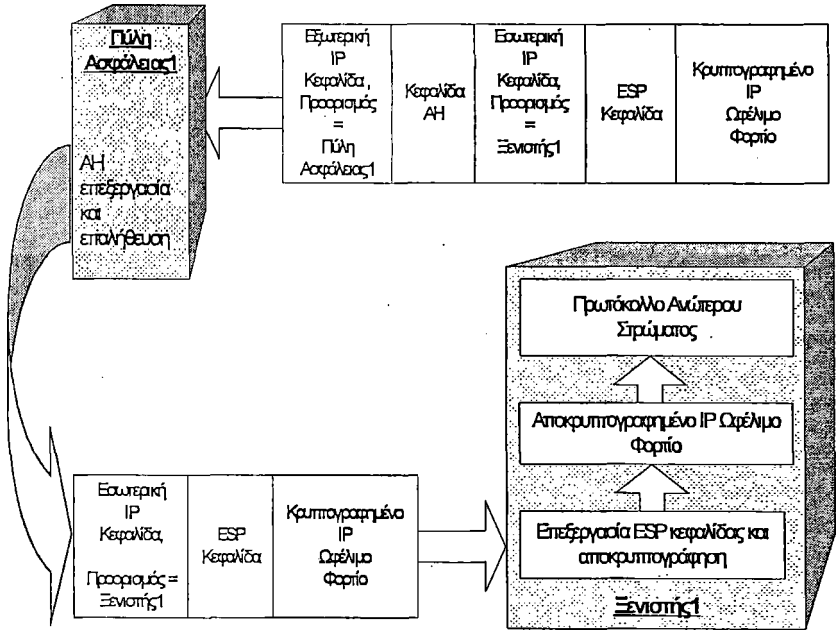
Ένας συσχετισμός ασφάλειας προσδιορίζεται από τρεις παραμέτρους:

- **Δείκτης παραμέτρων ασφάλειας (Security Parameters Index – SPI)** : Είναι μία bit συμβολοσειρά που εκχωρείται σε ένα συσχετισμό ασφάλειας και έχει μονάχα τοπική ισχύ. Ο δείκτης παραμέτρων ασφάλειας εμπεριέχεται στις AH και ESP κεφαλίδες προκειμένου να καθιστά ικανό τον παραλήπτη να επιλέξει το συσχετισμό ασφάλειας με τον οποίο θα πρέπει να γίνει η επεξεργασία του λαμβανόμενου πακέτου.
- **Η IP διεύθυνση προορισμού (IP Destination Address)**: Επί του παρόντος μονάχα διευθύνσεις μονοεκπομπής επιτρέπονται. Η IP διεύθυνση προορισμού είναι η IP διεύθυνση του τελικού προορισμού ο οποίος μαζί με τον αποστολέα αποτελούν τις δύο οντότητες στις οποίες παρέχεται η υπηρεσία συσχέτισης. Μπορεί να είναι η διεύθυνση ενός τελικού χρήστη, ή ενός στοιχείου δικτύου όπως για παράδειγμα ενός τείχους προστασίας ή ενός δρομολογητή.
- **Ο αναγνωριστής πρωτοκόλλου ασφάλειας (Security Protocol Identifier)**: Ο αναγνωριστής πρωτοκόλλου ασφάλειας δηλώνει αν ο συσχετισμός ασφάλειας είναι ένας AH ή ESP συσχετισμός ασφάλειας.

3.1.2.3 Τρόπος Μεταφοράς (Transport Mode)και Σήραγγας (Tunnel Mode)

Τόσο το πρωτόκολλο επαλήθευσης κεφαλίδας (Authentication Header-AH) όσο και το πρωτόκολλο ασφαλούς ενθυλάκωσης ωφέλιμου φορτίου (Encapsulating Security Payload-ESP) υποστηρίζουν 2 τρόπους χρήσης: τον **τρόπο μεταφοράς** και τον **τρόπο σήραγγας**. Η λειτουργία αυτών των δύο τρόπων γίνεται καλύτερα αντιληπτή στα πλαίσια της περιγραφής των AH και ESP, τα οποία αναλύονται στις ενότητες 3.1.3 και 3.1.4 αντίστοιχα. Στη συνέχεια παρέχουμε μια συνοπτική περιγραφή.

Υπάρχουν δύο τύποι συσχετισμών ασφάλειας: ο **τρόπος μεταφοράς** και ο **τρόπος σήραγγας**. Ο τρόπος μεταφοράς μπορεί να χρησιμοποιείται μόνο για επικοινωνίες μεταξύ ξενιστών. Ο τρόπος αυτός παρέχει διατερματική ασφάλεια. Ο τρόπος σήραγγας πρέπει να χρησιμοποιείται εάν η IPSec επεξεργασία σε ένα ή και στα δύο άκρα της επικοινωνίας πραγματοποιείται από μία ενδιάμεση πύλη ασφάλειας (security gateway), όπως είναι ένα τείχος προστασίας. (Τα τείχη προστασίας αναλύονται στο Κεφάλαιο 6). Σε αυτή την περίπτωση, το IP πακέτο θα αποτελείται από μία εξωτερική IP κεφαλίδα, η οποία διευθυνσιοδοτεί την πύλη ασφάλειας ,από μία IPSec κεφαλίδα η οποία θα χρησιμοποιείται από την πύλη ασφάλειας και μία εσωτερική IP κεφαλίδα που διευθυνσιοδοτεί τον τελικό προορισμό του πακέτου. Ο τρόπος σήραγγας παρέχει ασφάλεια ανάμεσα σε δύο πύλες ασφάλειας ή ανάμεσα σε μία πύλη ασφάλειας και σε έναν τερματικό χρήστη. Το Σχήμα 3-5 αναπαριστά τη χρήση και των δύο τρόπων για ένα μοναδικό πακέτο.



Σχήμα 3-5:Παράδειγμα επαλήθευσης του τρόπου σήραγγας και κρυπτογράφησης του τρόπου μεταφοράς.

Εάν ο τελικός προορισμός ενός IP πακέτου είναι μία πύλη ασφάλειας , αν για παράδειγμα το πακέτο μεταφέρει μία εντολή του απλού πρωτοκόλλου διαχείρισης δικτύου (SNMP) στην πύλη ασφάλειας, τότε η πύλη ασφάλειας θεωρείται ξενιστής και ο τύπος συσχετισμού ασφάλειας μπορεί να είναι ο τρόπος μεταφοράς. Ο Πίνακας 3-2 περιγράφει περιληπτικά τη λειτουργικότητα των τρόπων μεταφοράς και σήραγγας.

Τρόπος / Πρωτόκολλο	Τρόπος Μεταφοράς Συσχετισμού Ασφάλειας	Τρόπος Σήραγγας Συσχετισμού Ασφάλειας
AH	Επαληθεύει το ωφέλιμο φορτίο του IP πακέτου και επιλεγμένα τμήματα της IP κεφαλίδας	Επαληθεύει το συνολικό εσωτερικό IP πακέτο (εσωτερική κεφαλίδα και το IP ωφέλιμο φορτίο) συν επιλεγμένα τμήματα της εξωτερικής IP κεφαλίδας
ESP	Κρυπτογραφεί το IP ωφέλιμο φορτίο	Κρυπτογραφεί το συνολικό εσωτερικό IP πακέτο
ESP με επαλήθευση	Κρυπτογραφεί το IP ωφέλιμο φορτίο. Επαληθεύει το IP ωφέλιμο φορτίο αλλά όχι την IP κεφαλίδα.	Κρυπτογραφεί το συνολικό εσωτερικό IP πακέτο . Επαληθεύει το συνολικό εσωτερικό IP πακέτο.

Πίνακας 3-2:Η λειτουργικότητα του τρόπου μεταφοράς και του τρόπου σήραγγας

3.1.3 Η Υπηρεσία Επαλήθευσης

3.1.3.1 Η κεφαλίδα AH

Η Κεφαλίδα Επαλήθευσης υποστηρίζει τις υπηρεσίες ακεραιότητας δεδομένων και επαλήθευσης των IP πακέτων. Η υπηρεσία της ακεραιότητας δεδομένων εξασφαλίζει ότι δεν είναι δυνατό να μην ανιχνευθεί οποιαδήποτε τροποποίηση των περιεχομένων ενός IP πακέτου κατά τη μεταβίβαση του. Το χαρακτηριστικό της επαλήθευσης ταυτότητας επιτρέπει σε ένα τερματικό σύστημα ή σε ένα στοιχείο δικτύου να επαληθεύει ένα χρήστη ή μια εφαρμογή και ανάλογα να επιτρέπει ή όχι την κίνηση στο δίκτυο. Ακόμη εμποδίζει τις επιθέσεις παρακολούθησης διευθύνσεων, οι οποίες παρατηρούνται σήμερα στο Διαδίκτυο. Επιπλέον, η κεφαλίδα επαλήθευσης AH παρέχει προστασία έναντι στις επιθέσεις επανάληψης. Η επαλήθευση βασίζεται στη χρήση του κωδικού επαλήθευσης μηνύματος (Message Authentication Code-MAC). Ωστόσο και τα δύο μέρη που επικοινωνούν πρέπει να μοιράζονται ένα μυστικό κλειδί. Μία κεφαλίδα επαλήθευσης AH αποτελείται από τα ακόλουθα πεδία, τα οποία παριστάνονται στο Σχήμα 3-6.

Επόμενη Κεφαλίδα (8 bit) :Δηλώνει τον τύπο κάθε κεφαλίδας η οποία ακολουθεί αμέσως μετά από αυτή την κεφαλίδα.

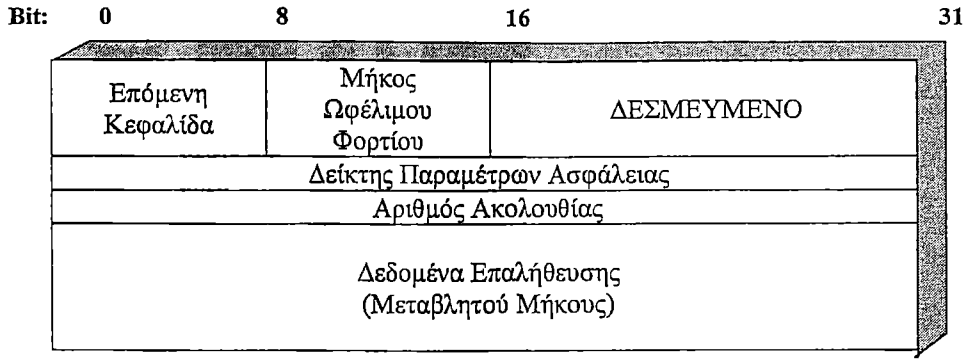
Μήκος Ωφέλιμου Φορτίου (8 bit) :Το μήκος της κεφαλίδας επαλήθευσης σε λέξεις 32 bit, μείον 2. Για παράδειγμα, το προκαθορισμένο μήκος των πεδίων των δεδομένων επαλήθευσης είναι 96 bit, δηλαδή τρεις λέξεις των 32 bit. Με σταθερή κεφαλίδα μήκους τριών λέξεων, υπάρχουν συνολικά έξι λέξεις στη κεφαλίδα και το μήκος του ωφέλιμου φορτίου έχει τιμή ίση με τέσσερα.

Δεσμευμένο (16 bit): Για μελλοντική χρήση .

Δείκτης παραμέτρων ασφάλειας(Security Parameters Index-SPI) (32 bit): Δηλώνει ένα συσχετισμό ασφάλειας.

Αριθμός Ακολουθίας (32 bit) : Η τιμή ενός μονότονα αυξανόμενου μετρητή .

Δεδομένα Επαλήθευσης (μεταβλητό μέγεθος) : Ένα μεταβλητού , αλλά πολλαπλάσιου των 32 bit λέξεων, μήκους πεδίο το οποίο περιέχει την Τιμή Ελέγχου Ακεραιότητας (Integrity Check Value-ICV) ή κάποιο κώδικα επαλήθευσης μηνύματος (MAC), για το πακέτο αυτό.



Σχήμα 3-6:IPSec Κεφαλίδα Επαλήθευσης.

Η τρέχουσα προδιαγραφή του MAC ορίζει ότι μια υλοποίηση του πρέπει να υποστηρίζει τους παρακάτω:

- HMAC-MD5-96
- HMAC-SHA-1-96

Και οι δύο κώδικες χρησιμοποιούν τον HMAC αλγόριθμο, μόνο που ο πρώτος τον χρησιμοποιεί μαζί με τον MD5 κώδικα κατακερματισμού και ο δεύτερος μαζί με τον SHA-1 κώδικα κατακερματισμού. Και στις δύο περιπτώσεις υπολογίζεται η πλήρης HMAC τιμή και κατόπιν αποκόπτονται μόνο τα 96 πρώτα bit, τα οποία αποτελούν το προκαθορισμένο μήκος του πεδίου Δεδομένων Επαλήθευσης.

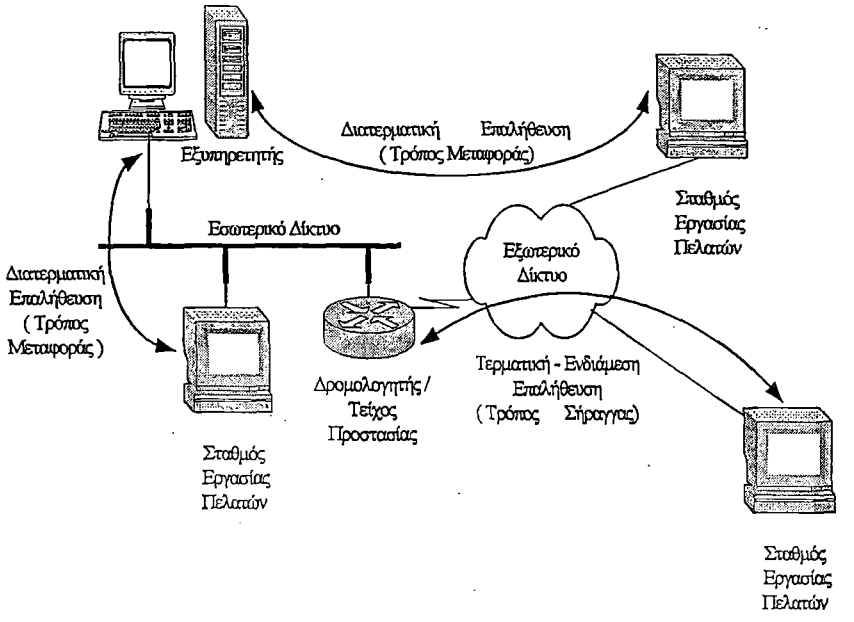
Ο κώδικας επαλήθευσης μηνύματος (MAC) υπολογίζεται στα παρακάτω:

- Στα πεδία IP κεφαλίδας που είτε δεν αλλάζουν κατά τη μεταβίβαση (αμετάβλητα) ή είναι προβλέψιμες οι αλλαγές της τιμής τους κατά την άφιξή τους στο άκρο τερματισμού του συσχετισμού ασφάλειας επαλήθευσης κεφαλίδας (AH). Στα πεδία τα οποία μπορεί να μεταβάλλονται κατά τη μεταβίβασή τους και των οποίων η τιμή κατά την άφιξή τους δεν είναι προβλέψιμη, δίνεται για λόγους υπολογισμού τιμή μηδέν τόσο στον προορισμό όσο και στην πηγή.
- Στην κεφαλίδα επαλήθευσης εκτός από το πεδίο Δεδομένων Επαλήθευσης. Στο τελευταίο δίνεται τιμή μηδέν για περιπτώσεις υπολογισμού τόσο στην πηγή όσο και στον προορισμό.
- Στο σύνολο των δεδομένων του πρωτοκόλλου ανώτερου στρώματος, το οποίο θεωρείται ότι δεν αλλάζει τιμή κατά τη μεταβίβαση, όπως είναι το τμήμα TCP ή ένα εσωτερικό IP πακέτο στον τρόπο σήραγγας.

3.1.3.2 Τρόπος Μεταφοράς και Σήραγγας για AH

Στο Σχήμα 3-7 παριστάνονται δύο τρόποι εφαρμογής της υπηρεσίας επαλήθευσης του πρωτοκόλλου IPSec. Στην πρώτη περίπτωση, η επαλήθευση παρέχεται απευθείας ανάμεσα σε έναν εξυπηρετητή και σε ένα σταθμό εργασίας. Ο σταθμός εργασίας μπορεί να βρίσκονται είτε στο ίδιο δίκτυο όπως ο εξυπηρετητής είτε σε κάποιο άλλο δίκτυο. Για όσο διάστημα ο σταθμός εργασίας και ο εξυπηρετητής διαμοιράζονται το ίδιο προστατευμένο μυστικό κλειδί η διαδικασία επαλήθευσης θεωρείται ασφαλής. Αυτή η περίπτωση χρησιμοποιεί ένα συσχετισμό ασφάλειας που βασίζεται στον τρόπο μεταφοράς.

Στη δεύτερη περίπτωση ένας απομακρυσμένος σταθμός εργασίας επαληθεύει τη δική του ταυτότητα στο εταιρικό τείχος προστασίας είτε για να εξασφαλίσει πρόσβαση σε κάθε σημείο του εσωτερικού δικτύου είτε γιατί ο εξυπηρετητής που ζήτησε δεν υποστηρίζει το χαρακτηριστικό της επαλήθευσης. Σε αυτή την περίπτωση χρησιμοποιείται ένας συσχετισμός ασφάλειας που βασίζεται στον τρόπο σήραγγας.

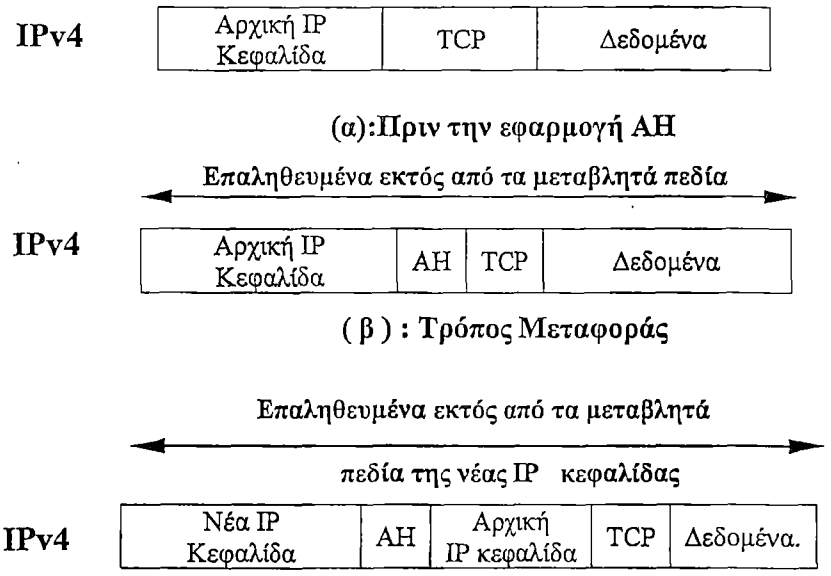


Σχήμα 3-7: Διατερματική έναντι Τερματική=προς=Ενδιάμεση Επαλήθευση

Στον τρόπο μεταφοράς Κεφαλίδας Επαλήθευσης AH, που χρησιμοποιεί το πρωτόκολλο IPv4, η Κεφαλίδα Επαλήθευσης εισάγεται ανάμεσα στην κεφαλίδα του αρχικού IP μηνύματος και στο ωφέλιμο φορτίο του IP μηνύματος, το οποίο μπορεί να είναι ένα τμήμα TCP.Αυτό παριστάνει και το Σχήμα 3-8β .Η επαλήθευση καλύπτει το συνολικό πακέτο με εξαίρεση μεταβλητά πεδία στην IPv4 κεφαλίδα, τα οποία τίθενται ίσα με μηδέν για τον υπολογισμό του κώδικα επαλήθευσης μηνύματος MAC.

Στον τρόπο σήραγγας Κεφαλίδας Επαλήθευσης AH, επαληθεύεται το συνολικό πρωτότυπο IP πακέτο και η κεφαλίδα επαλήθευσης εισάγεται ανάμεσα στην αρχική IP κεφαλίδα και στη νέα εξωτερική IP κεφαλίδα, όπως φαίνεται στο Σχήμα 3-8γ.Η εσωτερική IP κεφαλίδα μεταφέρει τις τελικές διευθύνσεις πηγής και προορισμού, ενώ η εξωτερική IP κεφαλίδα μπορεί να περιλαμβάνει διαφορετικές IP διευθύνσεις, όπως είναι η διεύθυνση ενός τείχους προστασίας ή διευθύνσεις άλλων πυλών ασφάλειας.

Με τον τρόπο σήραγγας το σύνολο του εσωτερικού IP πακέτου συμπεριλαμβανομένης και της εσωτερικής IP κεφαλίδας προστατεύεται από την κεφαλίδα επαλήθευσης (AH). Η εξωτερική IP κεφαλίδα προστατεύεται εκτός από τα μεταβλητά και μη προβλέψιμα πεδία.



Σχήμα 3-8:Εμβέλεια του AH επαληθευτή.

3.1.4 Η Υπηρεσία Εμπιστευτικότητας

3.1.4.1 Το πακέτο ESP

Η ασφαλής ενθυλάκωση ωφέλιμου φορτίου ESP υποστηρίζει υπηρεσίες εμπιστευτικότητας, συμπεριλαμβανομένης της εμπιστευτικότητας των περιεχομένων του μηνύματος καθώς και της εμπιστευτικότητας περιορισμένης ροής κίνησης στο δίκτυο. Επιλεκτικά το πρωτόκολλο ασφαλούς ενθυλάκωσης ωφέλιμου φορτίου μπορεί επιπλέον να παρέχει τις ίδιες υπηρεσίες επαλήθευσης με αυτές που παρέχει η κεφαλίδα επαλήθευσης.

Το πακέτο ESP

Το Σχήμα 3-9 δείχνει το μορφότυπο του ESP πακέτου, το οποίο περιλαμβάνει τα ακόλουθα πεδία:

- **Δείκτης Παραμέτρων Ασφάλειας** (32 bit):Αναγνωρίζει ένα συσχετισμό ασφάλειας

- **Αριθμός Ακολουθίας** (32 bit):Η τιμή ενός μονότονα αυξανόμενου μετρητή. Παρέχει λειτουργία ενάντια στις επιθέσεις επανάληψης ,όπως ακριβώς και στην περίπτωση της Κεφαλίδας Επαλήθευσης AH.

- **Δεδομένα Ωφέλιμου Φορτίου** (μεταβλητού μήκους):Στην περίπτωση του τρόπου μεταφοράς πρόκειται για το τμήμα του στρώματος μεταφοράς ,ενώ στην περίπτωση του τρόπου σήραγγας πρόκειται για ένα IP πακέτο. Και στις δύο περιπτώσεις προστατεύεται το πεδίο αυτό από κρυπτογράφηση.

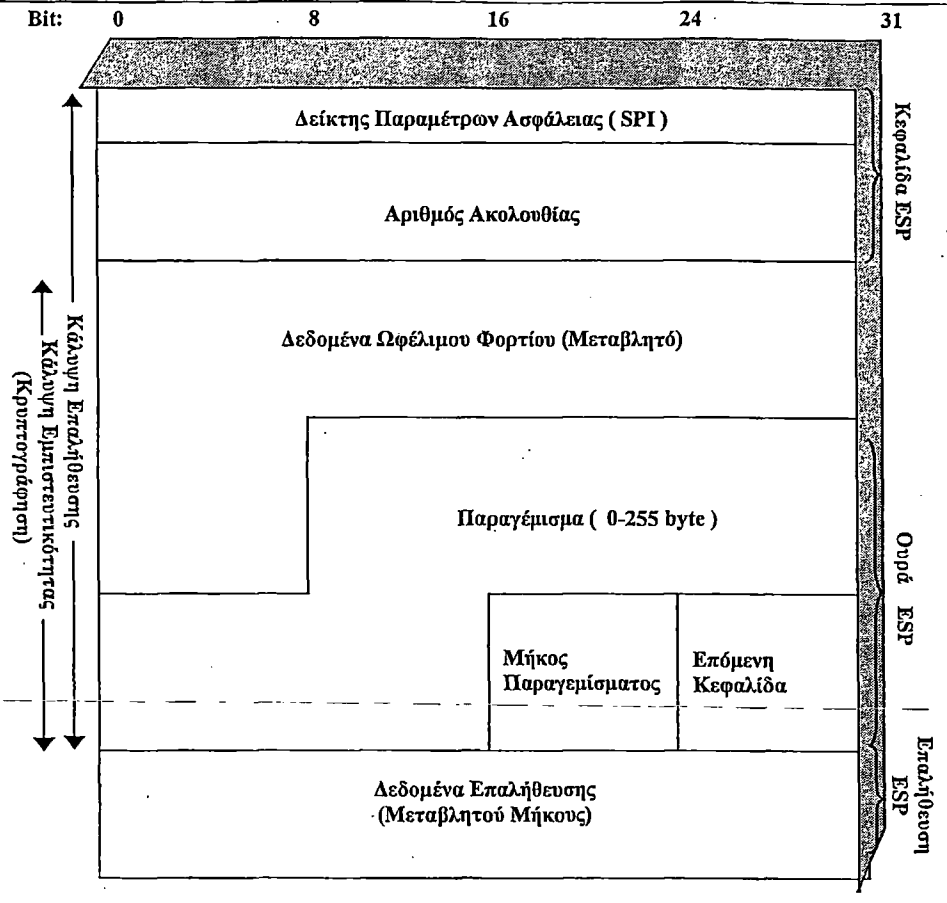
- **Παραγέμισμα** (μεταβλητού μήκους): Το μήκος του κυμαίνεται από 0 έως 255 byte.

- **Μήκος Παραγεμίσματος** (8 bit): Δείχνει τον αριθμό των byte παραγεμίσματος που ακολουθούν αυτό το πεδίο.

- **Επόμενη Κεφαλίδα** (8 bit): Αναγνωρίζει τον τύπο δεδομένων που περιέχονται στο πεδίο δεδομένων του ωφέλιμου φορτίου αναγνωρίζοντας την πρώτη κεφαλίδα στο ωφέλιμο αυτό φορτίο. Για παράδειγμα ένα ανώτερου στρώματος πρωτόκολλο όπως το TCP.

- **Δεδομένα Επαλήθευσης** (μεταβλητού μήκους):Ένα μεταβλητού μήκους πεδίο, πολλαπλάσιου του μήκους λέξης των 32 bit, το οποίο περιέχει την Τιμή Ελέγχου Ακεραιότητας υπολογισμένη στο ESP πακέτο εξαιρουμένου του πεδίου Δεδομένων Επαλήθευσης.

Τα πεδία **Δεδομένα Ωφέλιμου Φορτίου, Παραγέμισμα , Μήκος Παραγεμίσματος** και **Επόμενη Κεφαλίδα** κρυπτογραφούνται από την υπηρεσία ESP . Σε περίπτωση που ο αλγόριθμος που χρησιμοποιείται για την κρυπτογράφηση του ωφέλιμου φορτίου απαιτεί δεδομένα συγχρονισμού Κρυπτογράφησης, όπως ένα διάνυσμα αρχικοποίησης (Initialisation Vector-IV), τότε αυτά τα δεδομένα τοποθετούνται ξεχωριστά στην αρχή του πεδίου Δεδομένα Ωφέλιμου Φορτίου.



Σχήμα 3-9:IPSec Μορφότυπο ESP.

Αν περιλαμβάνεται ένα διάνυσμα αρχικοποίησης συνήθως δεν κρυπτογραφείται, παρότι συχνά αναφέρεται σαν να είναι τμήμα ενός κρυπτογραφημένου κειμένου.

Οι προδιαγραφές δηλώνουν ότι κάθε υλοποίηση πρέπει να υποστηρίζει το Πρότυπο Κρυπτογράφησης Δεδομένων (Data Encryption Standard-DES) στη μορφή αλύσωσης κρυπτογραφημένων ενοτήτων (Cipher Block Chaining-CBC). Ένας αριθμός και από άλλους αλγόριθμους μπορούν αυτό να χρησιμοποιούνται για κρυπτογράφηση. Σε αυτούς τους αλγόριθμους περιλαμβάνονται και οι παρακάτω:

- Τριπλό DES τριών κλειδιών
- RC5
- IDEA
- Τριπλό IDEA τριών κλειδιών
- CAST
- Blowfish.

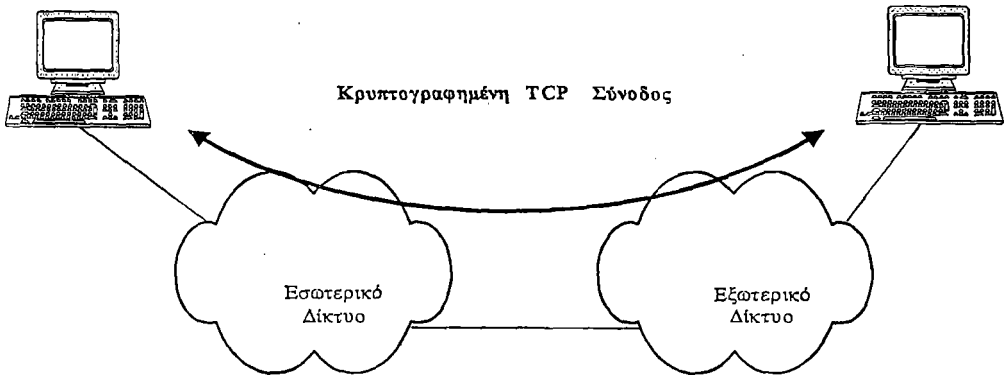
Όπως η Κεφαλίδα Επαλήθευσης (AH), έτσι και το πρωτόκολλο Ασφαλούς Ενθυλάκωσης Ωφέλιμου Φορτίου(ESP) υποστηρίζει τη χρήση ενός κώδικα επαλήθευσης μηνύματος (MAC), με προκαθορισμένο μήκος 96 bit.

3.1.4.2 Τρόπος Μεταφοράς και Σήραγγας για ESP

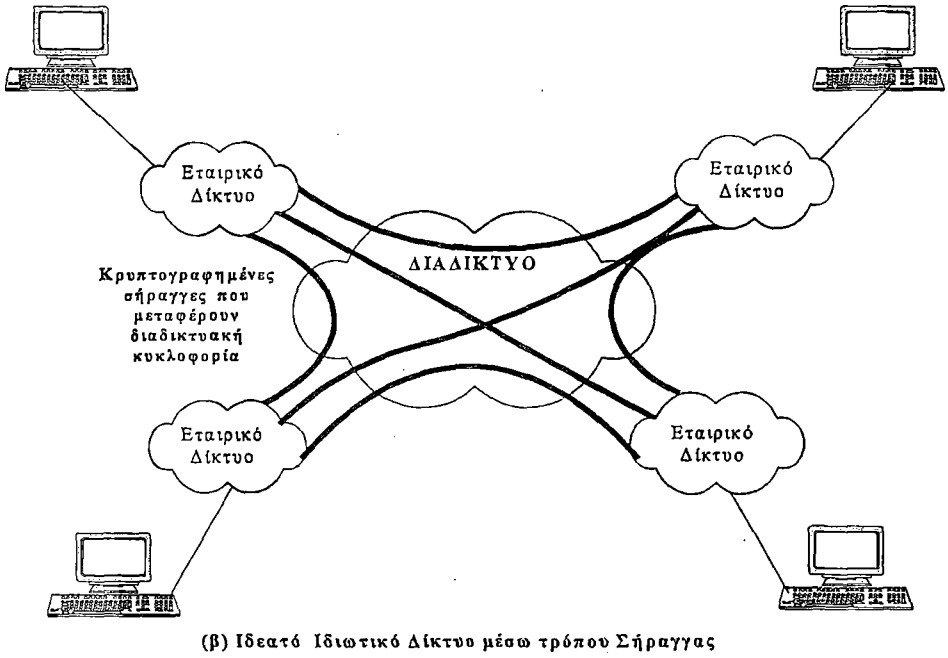
Οι τρόποι με τους οποίους μπορεί να χρησιμοποιηθεί η υπηρεσία ESP του IPSec είναι δύο, όπως φαίνεται στο Σχήμα 3-10. Συγκεκριμένα στο Σχήμα 3-10α παρατηρούμε ότι, η κρυπτογράφηση (και επιλεκτικά η επαλήθευση) παρέχεται απευθείας από τους ξενιστές, ενώ στο Σχήμα 3-10β, παρατηρούμε πως η λειτουργία του τρόπου σήραγγας μπορεί να χρησιμοποιείται για να εγκαθιδρύει ένα ιδεατό ιδιωτικό δίκτυο. Στο παράδειγμα του Σχήματος ένας οργανισμός έχει τέσσερα ιδιωτικά δίκτυα διασυνδεδεμένα στο Διαδίκτυο. Οι ξενιστές των

εσωτερικών δικτύων χρησιμοποιούν το Διαδίκτυο για τη μεταφορά δεδομένων χωρίς να αλληλεπιδρούν με άλλους ξενιστές του Διαδικτύου. Τερματίζοντας τις σήραγγες στην πύλη ασφάλειας κάθε εσωτερικού δικτύου, η διάρθρωση επιτρέπει σε κάθε ξενιστή να παραλείπει να υλοποιεί τη δυνατότητα ασφάλειας. Η πρώτη τεχνική στηρίζεται σε συσχετισμό ασφάλειας τρόπου μεταφοράς, ενώ η τελευταία σε συσχετισμό ασφάλειας τρόπου σήραγγας.

Ο τρόπος μεταφοράς στο ESP χρησιμοποιείται για να κρυπτογραφεί και



(α) Ασφάλεια Τρόπου Μεταφοράς



(β) Ιδεατό Ιδιωτικό Δίκτυο μέσω τρόπου Σήραγγας

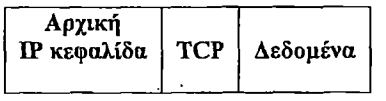
Σχήμα 3-10:Κρυπτογράφηση Τρόπου Μεταφοράς (α) σε σχέση με Κρυπτογράφηση Τρόπου Σήραγγας (β)

επιλεκτικά να επαληθεύει τα δεδομένα , τα οποία μεταφέρονται μέσω του IP πρωτοκόλλου, όπως ένα τμήμα TCP.

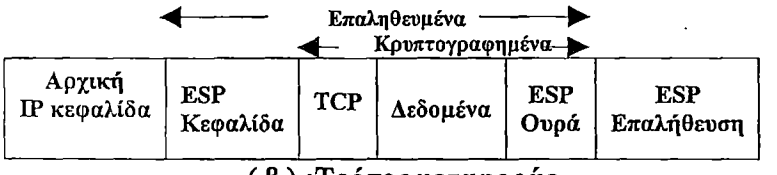
Στο Σχήμα 3-11β παριστάνεται η εμβέλεια της ESP Κρυπτογράφησης και Επαλήθευσης. Για τον τρόπο μεταφοράς που χρησιμοποιεί το πρωτόκολλο IPv4, η ESP κεφαλίδα εισάγεται στο IP πακέτο ακριβώς πριν από την κεφαλίδα στρώματος μεταφοράς, όπως τα TCP,UDP και ICMP, και μία ESP ουρά (πεδία **Παραγέμισμα** , **Μήκος Παραγεμίσματος** και **Επόμενη κεφαλίδα**) τοποθετείται μετά το IP πακέτο. Σε περίπτωση που έχει επιλεγεί επαλήθευση ,το ESP πεδίο Δεδομένων Επαλήθευσης προστίθεται μετά την ESP ουρά. Το συνολικό τμήμα στρώματος μεταφοράς μαζί με την ESP ουρά

κρυπτογραφούνται. Η Επαλήθευση καλύπτει το σύνολο του κρυπτογραφημένου κειμένου καθώς και την ESP κεφαλίδα.

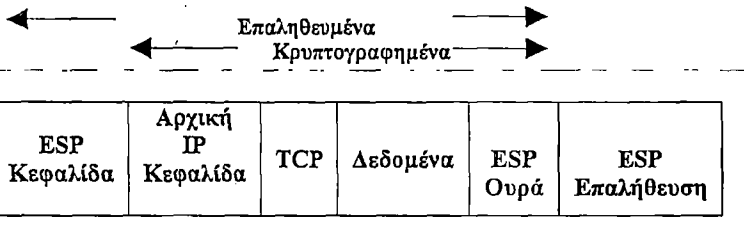
Ο τρόπος σήραγγας στο ESP χρησιμοποιείται για την κρυπτογράφηση ολόκληρου του IP πακέτου, όπως φαίνεται στο Σχήμα 3-11γ. Στον τρόπο αυτό, η ESP κεφαλίδα τοποθετείται ως πρόθεμα στο πακέτο και στη συνέχεια το νέο μεγαλύτερο πακέτο μαζί με την ESP ουρά κρυπτογραφούνται.



(α) :Πριν την εφαρμογή του ESP



(β) :Τρόπος μεταφοράς



(γ): Τρόπος Σήραγγας

Σχήμα 3-11:Εμβέλεια της ESP Κρυπτογράφησης και Επαλήθευσης

3.1.5 Συνδυάζοντας Συσχετισμούς Ασφάλειας

Κάθε μεμονωμένος συσχετισμός ασφάλειας μπορεί να υλοποιεί είτε το πρωτόκολλο AH είτε το πρωτόκολλο ESP ,αλλά ποτέ και τα δύο μαζί. Ωστόσο, σε κάποιες περιπτώσεις μια συγκεκριμένη ροή κίνησης στο δίκτυο μπορεί να χρειάζεται υπηρεσίες που παρέχονται και από τα δύο πρωτόκολλα, AH και ESP. Επιπλέον, μια συγκεκριμένη ροή κίνησης μπορεί να απαιτεί υπηρεσίες του IPSec ανάμεσα σε ξενιστές , και για την ίδια ροή να απαιτούνται διαφορετικές υπηρεσίες ανάμεσα σε πύλες ασφάλειας, όπως είναι τα τείχη προστασίας. Σε όλες τις παραπάνω περιπτώσεις, πολλαπλοί συσχετισμοί ασφάλειας τίθενται σε εφαρμογή προκειμένου να εξασφαλιστούν οι επιθυμητές υπηρεσίες του IPSec. Ο όρος Δέσμη Συσχετισμού Ασφάλειας (Security Association Bundle) αναφέρεται σε μία αλληλουχία από συσχετισμούς ασφάλειας οι οποίοι επεξεργάζονται την κίνηση στο δίκτυο προκειμένου να εξασφαλίσουν το επιθυμητό σύνολο των υπηρεσιών του IPSec. Οι συσχετισμοί ασφάλειας της δέσμης μπορεί να τερματίζουν σε διαφορετικά ή στο ίδιο σημείο τερματισμού.

Οι συσχετισμοί ασφάλειας μπορεί να συνδυάζονται σε δέσμες με δύο τρόπους:

- **Παρακείμενη Μεταφορά**: Αναφέρεται στην εφαρμογή περισσότερων του ενός πρωτοκόλλου ασφάλειας στο ίδιο IP πακέτο, χωρίς να παρεμβάλλεται σηράγγωση. Αυτή η προσέγγιση του συνδυασμού των AH και ESP επιτρέπει το συνδυασμό μόνο σε ένα επίπεδο. Περαιτέρω εμφωλιασμός δεν παρέχει πρόσθετα πλεονεκτήματα αφού η επεξεργασία πραγματοποιείται σε ένα και μόνο στιγμιότυπο του IPSec: τον τελικό προορισμό.

- **Επαναλαμβανόμενη Σηράγγωση** : Αναφέρεται στην εφαρμογή πολλαπλών στρωμάτων πρωτοκόλλων ασφάλειας τα οποία εφαρμόζονται διαμέσου IP σήραγγας. Αυτή η θεώρηση μπορεί να επιτρέπει πολλαπλά επίπεδα εμφωλιασμού ,αφού κάθε

σήραγγα μπορεί να ξεκινά ή να καταλήγει σε διαφορετικά IPSec σημεία κατά μήκος του μονοπατιού.

Οι δύο προσεγγίσεις μπορούν να συνδυαστούν. Είναι δυνατό για παράδειγμα, σε ένα συσχετισμό ασφάλειας του τρόπου μεταφοράς ανάμεσα σε ξενιστές να έχουμε τμήμα του δρόμου με συσχετισμό ασφάλειας τρόπου σήραγγας ανάμεσα σε πύλες ασφάλειας.

Ένα ενδιαφέρον θέμα το οποίο προκύπτει κάθε φορά που εξετάζουμε τις δέσμες συσχετίσεων ασφάλειας είναι η σειρά με την οποία η Επαλήθευση και η Κρυπτογράφηση μπορούν να εφαρμόζονται ανάμεσα σε ένα δεδομένο ζευγάρι τερματικών σημείων καθώς και οι τρόποι με τους οποίους εφαρμόζονται. Εξετάζουμε αυτό το θέμα παρακάτω και θεωρούμε συνδυασμούς από συσχετισμούς ασφάλειας οι οποίοι περιλαμβάνουν τουλάχιστον μία σήραγγα.

Το έγγραφο Αρχιτεκτονικής του IPSec παραθέτει τέσσερα παραδείγματα συνδυασμών από συσχετισμούς ασφάλειας που μπορούν να υποστηριχθούν από ξενιστές συμμορφούμενους με το IPSec, όπως είναι οι εξυπηρετητές και οι σταθμοί εργασίας, ή από πύλες ασφάλειας, όπως είναι τείχη προστασίας και δρομολογητές. Στο Σχήμα 3-12 παρατίθενται οι τέσσερις διαφορετικές περιπτώσεις. Το κατώτερο τμήμα κάθε περίπτωσης στο σχήμα αυτό παριστάνει την φυσική διασύνδεση αυτών των στοιχείων. Το ανώτερο τμήμα παριστάνει τη λογική διασύνδεση διαμέσου ενός ή περισσότερων φωλιασμένων συσχετισμών ασφάλειας. Κάθε φωλιασμένος συσχετισμός ασφάλειας μπορεί να ανήκει είτε στο AH είτε στο ESP. Για συσχετισμούς ασφάλειας από ξενιστή σε ξενιστή, ο τρόπος που χρησιμοποιείται μπορεί να είναι είτε τρόπος μεταφοράς είτε τρόπος σήραγγας. Στις άλλες περιπτώσεις συσχετισμών ασφάλειας ,ο τρόπος που χρησιμοποιείται είναι ο τρόπος σήραγγας.

Στην **περίπτωση 1** (Σχήμα 3-12α) κάθε μορφής ασφάλεια παρέχεται μεταξύ τερματικών συστημάτων τα οποία υλοποιούν το IPSec. Για να επικοινωνούν δύο οποιαδήποτε τερματικά συστήματα διαμέσου ενός συσχετισμού ασφάλειας , πρέπει να μοιράζονται και τα δύο τα κατάλληλα μυστικά κλειδιά. Ανάμεσα στους πιθανούς συνδυασμούς συγκαταλέγονται :

- AH στον τρόπο μεταφοράς
- ESP στον τρόπο μεταφοράς
- AH ακολουθούμενο από ESP στον τρόπο μεταφοράς (ένας AH συσχετισμός ασφάλειας που εμπεριέχεται σε ένα ESP συσχετισμό ασφάλειας)
- Κάθε συνδυασμός των προηγουμένων εντός του τρόπου σήραγγας για AH ή ESP.

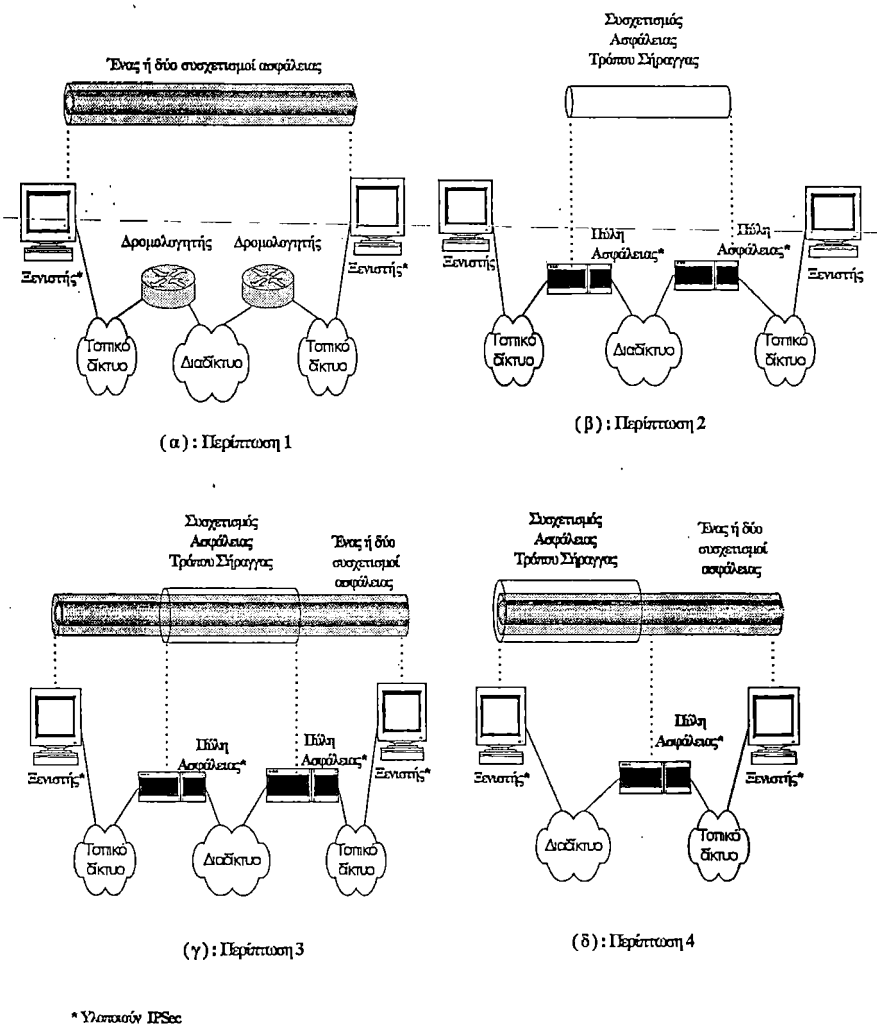
Έχουμε ήδη αναφέρει πώς οι διάφοροι συνδυασμοί μπορούν να υποστηρίξουν υπηρεσίες Επαλήθευσης και Κρυπτογράφησης, καθώς και Επαλήθευση πριν την Κρυπτογράφηση αλλά και μετά την Κρυπτογράφηση.

Στην **περίπτωση 2** (Σχήμα 3-12β) η ασφάλεια παρέχεται αποκλειστικά μεταξύ πυλών ασφάλειας ,όπως δρομολογητές και τείχη προστασίας ,ενώ κανένας ξενιστής δεν υλοποιεί το IPSec. Αυτή η περίπτωση παριστάνει υποστήριξη ενός απλού ιδεατού ιδιωτικού δικτύου. Το έγγραφο αρχιτεκτονικής ασφάλειας προδιαγράφει ότι μόνο ένας ξεχωριστός συσχετισμός ασφάλειας του τρόπου σήραγγας χρειάζεται σε αυτή την περίπτωση. Η σήραγγα μπορεί να υποστηρίξει τα AH , ESP και το ESP με επιλογή επαλήθευσης. Επιπλέον δεν απαιτούνται φωλιασμένες σήραγγες καθώς οι υπηρεσίες του IPSec εφαρμόζονται σε ολόκληρο το εσωτερικό πακέτο.

Η **περίπτωση 3** (Σχήμα 3-12γ) χτίζεται πάνω στην **περίπτωση 2** προσθέτοντας διατερματική ασφάλεια. Οι ίδιοι συνδυασμοί που αφορούσαν στην περίπτωση 1 και 2 επιτρέπεται να εφαρμοστούν και εδώ. Η διαπυλική σήραγγα παρέχει είτε υπηρεσίες επαλήθευσης είτε υπηρεσίες εμπιστευτικότητας δεδομένων είτε και τα δύο για το σύνολο της δικτυακής κίνησης ανάμεσα σε τερματικά συστήματα του δικτύου. Στην περίπτωση διαπύλικης σήραγγας με ESP , παρέχεται σε περιορισμένη μορφή και υπηρεσία

εμπιστευτικότητας της δικτυακής κίνησης. Μεμονωμένοι ξενιστές μπορούν μέσω διατερματικών συσχετισμών ασφάλειας να υλοποιούν κάθε πρόσθετη υπηρεσία του IPSec, η οποία απαιτείται από εξειδικευμένες εφαρμογές ή συγκεκριμένους χρήστες .

Στην **περίπτωση 4** (Σχήμα 3-12δ) παρέχεται σε κάθε απομακρυσμένο ξενιστή που χρησιμοποιεί το διαδίκτυο για να φτάσει το τείχος προστασίας ενός οργανισμού και στη συνέχεια να αποκτήσει πρόσβαση σε κάποιο σταθμό εργασίας ή εξυπηρετητή που βρίσκεται πίσω από αυτό το τείχος. Ανάμεσα στον απομακρυσμένου ξενιστή και στο τείχος προστασίας απαιτείται μόνο ο τρόπος σήραγγας. Όπως και στην περίπτωση 1, μεταξύ ενός απομακρυσμένου και ενός τοπικού ξενιστή μπορεί να χρησιμοποιούνται ένας ή δύο συσχετισμοί ασφάλειας.



Σχήμα 3-12:Βασικοί συνδυασμοί Συσχετισμών Ασφάλειας

3.1.6 Διαχείριση Κλειδιών

Η λειτουργία διαχείρισης κλειδιών στο IPSec περιλαμβάνει τον καθορισμό και την διανομή των μυστικών κλειδιών. Τυπικά απαιτούνται τέσσερα κλειδιά για την επικοινωνία ανάμεσα σε δύο εφαρμογές, τα οποία απαρτίζουν δύο ζεύγη : το ζεύγος εκπομπής και το ζεύγος λήψης τόσο για το πρωτόκολλο κεφαλίδας επαλήθευσης (AH) όσο και για το πρωτόκολλο ασφαλούς ενθυλάκωσης ωφέλιμου φορτίου (ESP). Το έγγραφο της αρχιτεκτονικής του IPSec υπαγορεύει την υποστήριξη δύο τύπων διαχείρισης κλειδιών :

- **Χειροκίνητος**: Ο διαχειριστής συστήματος χειρονακτικά διαρθρώνει κάθε σύστημα παρέχοντάς του τα δικά του κλειδιά καθώς και τα κλειδιά των άλλων συστημάτων

επικοινωνίας. Αυτός ο τύπος διαχείρισης κλειδιών είναι πρακτικός για μικρά και σχετικά στατικά περιβάλλοντα.

- **Αυτοματοποιημένος:** Ένα αυτοματοποιημένο σύστημα επιτρέπει τη δημιουργία ,κατόπιν αιτήσεως ,των απαραίτητων κλειδιών για τους συσχετισμούς ασφάλειας και διευκολύνει τη χρήση των κλειδιών σε κάθε μεγάλης κλίμακας κατανεμημένο σύστημα με εξελισσόμενη διάρθρωση.

Το προκαθορισμένο αυτοματοποιημένο πρωτόκολλο διαχείρισης κλειδιών για το IPSec αναφέρεται ως ISAKMP/Oakley και αποτελείται από τα παρακάτω στοιχεία:

- **Oakley Πρωτόκολλο Προσδιορισμού Κλειδιού:** Το Oakley είναι ένα πρωτόκολλο ανταλλαγής κλειδιού βασισμένο στον αλγόριθμο Diffie-Hellman παρέχοντας όμως πρόσθετη ασφάλεια. Το Oakley αποτελεί γένιο πρωτόκολλο καθώς δεν υπαγορεύει τη χρήση συγκεκριμένων μορφοτύπων.

- **Διαδυκτιακός Συσχετισμός Ασφάλειας και Πρωτόκολλο Διαχείρισης Κλειδιών (Internet Security Association and Key Management Protocol-ISAKMP):**Το ISAKMP παρέχει ένα πλαίσιο εργασίας για τη διαχείριση κλειδιών στο διαδίκτυο καθώς και συγκεκριμένη υποστήριξη πρωτοκόλλου η οποία περιλαμβάνει μορφότυπα για διαπραγματεύσεις σχετικές με τα ίδια χαρακτηριστικά ασφάλειας.

Το πρωτόκολλο ISAKMP από μόνο του δεν υπαγορεύει την εφαρμογή συγκεκριμένου αλγόριθμου για την ανταλλαγή κλειδιών. Αποτελείται από ένα σύνολο από τύπους μηνυμάτων που επιτρέπουν τη χρήση μιας ποικιλίας αλγορίθμων ανταλλαγής κλειδιών. Το Oakley είναι ένα συγκεκριμένος αλγόριθμος ανταλλαγής κλειδιών που υπαγορεύεται για χρήση από την αρχική έκδοση του ISAMKP.Μια πιο λεπτομερής περιγραφή των δύο παραπάνω πρωτοκόλλων ξεφεύγει από τα πλαίσια της παρούσας μελέτης.

3.2 Ασφάλεια πάνω από το Στρώμα Μεταφοράς

3.2.1 Το στρώμα SSL

Σχετικά με το θέμα της παροχής ασφάλειας στον παγκόσμιο ιστό, υπάρχουν πολυάριθμες προσεγγίσεις, οι οποίες αν και είναι παρόμοιες στο επίπεδο των υπηρεσιών που παρέχουν και έως ένα σημείο και στους μηχανισμούς ασφάλειας που χρησιμοποιούν, διαφέρουν ως προς την εμβέλεια της δυνατότητας εφαρμογής τους και ως προς τη σχετική τους θέση στη στοίβα του πρωτοκόλλου TCP / IP.

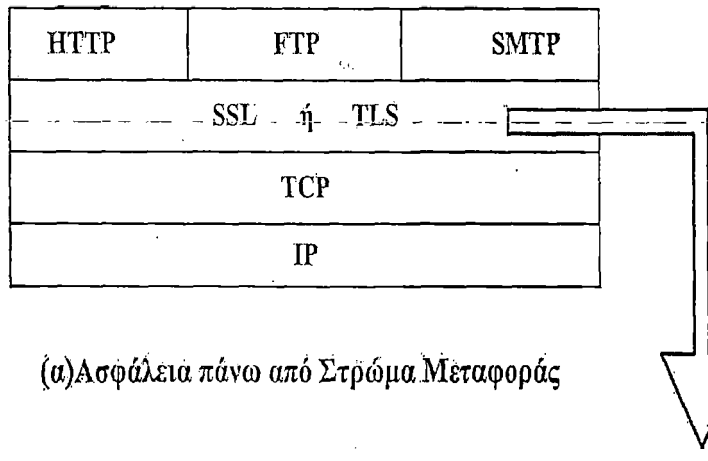
Ένας τρόπος παροχής ασφάλειας στον παγκόσμιο ιστό είναι μέσω της χρήσης IP ασφάλειας. Το πλεονέκτημα της χρήσης του πρωτοκόλλου IPSec είναι η διαφάνειά του στους τελικούς χρήστες και στις τελικές εφαρμογές και παρέχει μία λύση γενικού σκοπού. Περαιτέρω, το πρωτόκολλο IPSec εμπεριέχει τη δυνατότητα φιλτραρίσματος έτσι ώστε μόνο η επιλεγμένη κίνηση στο δίκτυο να χρειάζεται να υφίσταται τον επιπλέον επίφορτο της IPSec επεξεργασίας.

Μια άλλη σχετικά γενικού σκοπού λύση , είναι η υλοποίηση της ασφάλειας ακριβώς πάνω από το στρώμα TCP (Σχήμα 3-13α).Το πλέον γνωστό παράδειγμα αυτής της προσέγγισης αποτελεί το Στρώμα Ασφαλούς Υποδοχής (Secure Socket Layer-SSL) και η Ασφάλεια Στρώματος Μεταφοράς (Transport Layer Security-TLS). Στο στρώμα αυτό υπάρχουν δύο δυνατότητες υλοποίησης. Στη γενικότερη περίπτωση το SSL (ή το TLS) μπορεί να παρέχεται ως τμήμα της υποκείμενης στοίβας πρωτοκόλλων και εξαιτίας αυτού είναι διαφανές στις εφαρμογές. Εναλλακτικά ,το SSL μπορεί να είναι ενσωματωμένο σε συγκεκριμένα λογισμικά εφαρμογών. Για παράδειγμα οι διαφυλλιστές Netscape και Microsoft Explorer παρέχονται μαζί με το στρώμα SSL και οι περισσότεροι εξυπηρετητές διαδικτύου υλοποιούν αυτό το πρωτόκολλο.

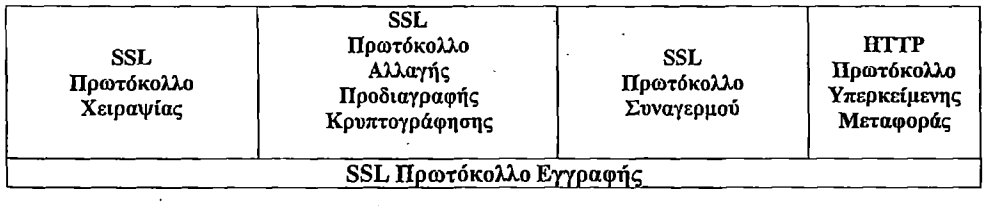
Το SSL είναι σχεδιασμένο να κάνει χρήση του TCP ώστε να παρέχει μια αξιόπιστη διατερματική υπηρεσία ασφάλειας. Το SSL δεν είναι ένα απλό στρώμα αλλά δύο στρώματα, όπως παρατηρούμε και στο Σχήμα 3-13β.

Το SSL πρωτόκολλο Εγγραφής (SSL Record Protocol) παρέχει βασικές υπηρεσίες ασφάλειας σε ένα πλήθος από πρωτόκολλα ανώτερου στρώματος:Συγκεκριμένα, το πρωτόκολλο Υπερκείμενης Μεταφοράς (Hyper Text Transfer Protocol-HTTP), το οποίο καθορίζεται στη σύσταση RFC 2068 και παρέχει την υπηρεσία μεταφοράς για την αλληλεπίδραση μεταξύ πελάτη και εξυπηρετητή στα πλαίσια του Παγκόσμιου Ιστού, μπορεί να λειτουργεί στην κορυφή του SSL. Τρία ανώτερου στρώματος πρωτόκολλα καθορίζονται ως τμήματα του SSL πρωτοκόλλου: το πρωτόκολλο Αλλαγής Προδιαγραφής Κρυπτογράφησης (Change Cipher Spec Protocol) το πρωτόκολλο Χειραψίας (Handshake Protocol) και το πρωτόκολλο Συναγερμού (Alert Protocol).

Τα τρία αυτά SSL πρωτόκολλα χρησιμοποιούνται στη διαχείριση των SSL ανταλλαγών και εξετάζονται παρακάτω σε αυτή την ενότητα



(α)Ασφάλεια πάνω από Στρώμα Μεταφοράς



(β): Στοίβα Στρώματος Ασφαλούς Υποδοχής (SSL)

Σχήμα 3-13:Το στρώμα SSL/TLS

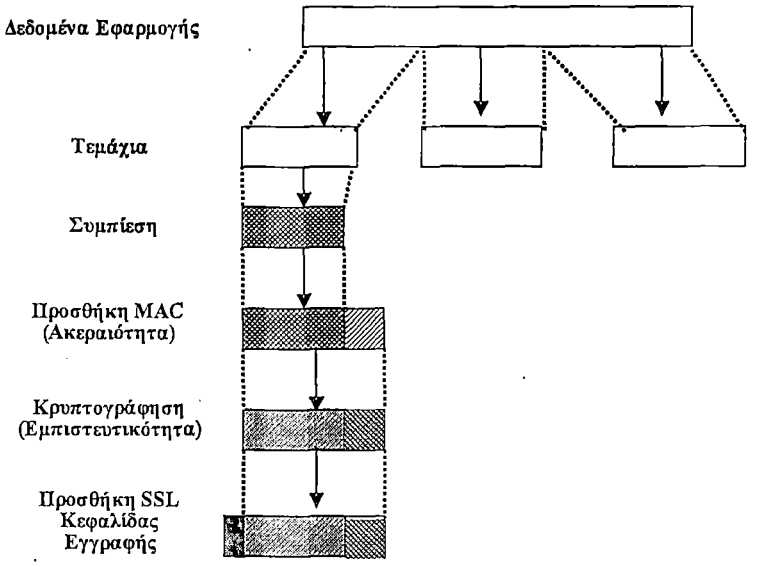
3.2.1.1 Το πρωτόκολλο Εγγραφής

Το SSL πρωτόκολλο εγγραφής παρέχει δύο υπηρεσίες για SSL συνδέσεις :

- **Εμπιστευτικότητα** : Το πρωτόκολλο χειραψίας ορίζει ένα διαμοιραζόμενο μυστικό κλειδί το οποίο χρησιμοποιείται για τη συμβατική κρυπτογράφηση των SSL ωφέλιμων φορτίων.

- **Ακεραιότητα Μηνύματος** : Το πρωτόκολλο χειραψίας επίσης ορίζει ένα διαμοιραζόμενο μυστικό κλειδί το οποίο χρησιμοποιείται για το σχηματισμό του κώδικα επαλήθευσης μηνύματος (MAC).

Στο Σχήμα 3-14 παριστάνεται η συνολική λειτουργία του SSL πρωτοκόλλου εγγραφής.



Σχήμα 3-14:Λειτουργία Πρωτοκόλλου Εγγραφής

Το πρώτο βήμα περιλαμβάνει τον τεμαχισμό των δεδομένων εφαρμογής. Στο επόμενο βήμα εφαρμόζεται επιλεκτικά συμπίεση των δεδομένων. Στο τρίτο βήμα υπολογίζεται ο κώδικας επαλήθευσης μηνύματος (MAC) για τα συμπιεσμένα δεδομένα. Στη συνέχεια τα συμπιεσμένα δεδομένα μαζί με το MAC κρυπτογραφούνται με χρήση συμμετρικής κρυπτογράφησης. Στο τελικό βήμα προστίθεται η κεφαλίδα εγγραφής SSL , η οποία αποτελείται από τα ακόλουθα πεδία:

Τύπος Περιεχομένου(8 bit):Το πρωτόκολλο ανώτερου στρώματος που χρησιμοποιείται για να επεξεργαστεί το περιεχόμενου τεμαχίου.

Μείζονα Έκδοση (8 bit): Υποδηλώνει την μείζονα έκδοση του SSL που χρησιμοποιείται. Για το SSLv3 , η τιμή του πεδίου αυτού είναι ίση με 3.

Ελάσσονα Έκδοση (8 bit) : Υποδηλώνει την ελάσσονα έκδοση που χρησιμοποιείται. Για το SSLv3, η τιμή του πεδίου αυτού είναι ίση με 0.

Συμπιεσμένο Μήκος (16 bit): Το μήκος σε bytes του τμήματος άκρυπτου κειμένου (ή το συμπιεσμένο τμήμα ,εάν χρησιμοποιείται συμπίεση). Η μέγιστη τιμή αυτού του πεδίου είναι ίση με $(2^{14} + 2048)$

Στο Σχήμα 3-15 φαίνεται το μορφότυπο SSL εγγραφής. Τα δεδομένα που παραλαμβάνονται αποκρυπτογραφούνται, επαληθεύονται, αποσυμπιέζονται, και επανασυναρμολογούνται αντίστοιχα, και στη συνέχεια μεταφέρονται στους χρήστες ανώτερων στρωμάτων.

Τύπος Περιεχομένου	Μείζονα Έκδοση	Ελάσσονα Έκδοση	Συμπιεσμένο Μήκος
Άκρυπτο Κείμενο (υποστηρίζεται επιλεκτικά η συμπίεση)			
Κώδικας MAC (0 ,16 ή 20 byte)			

Σχήμα 3-15:Μορφότυπο της SSL Εγγραφής

3.2.1.2 Το πρωτόκολλο Αλλαγής Προδιαγραφής Κρυπτογράφησης

Το πρωτόκολλο Αλλαγής Προδιαγραφής Κρυπτογράφησης (Change Spec Cipher) είναι ένα από τα τρία προδιαγεγραμμένα με βάση το SSL πρωτόκολλα που χρησιμοποιούν το SSL πρωτόκολλο εγγραφής και είναι το πιο εύκολο. Αυτό το πρωτόκολλο αποτελείται από ένα και μόνο μήνυμα του ενός byte ,το οποίο φέρει την τιμή 1.Ο αποκλειστικός σκοπός αυτού του

μηνύματος είναι να προκαλέσει μια κατάσταση που αναμένει , να αντιγραφεί στην τρέχουσα κατάσταση , η οποία ενημερώνει για την ακολουθία κρυπτογράφησης που θα χρησιμοποιηθεί σε αυτή τη σύνδεση.

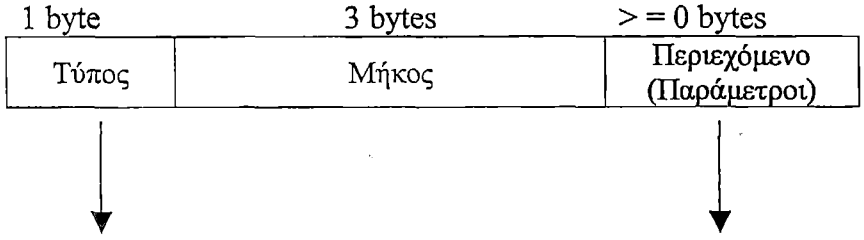
3.2.1.3 Το πρωτόκολλο χειραψίας

Το πιο πολύπλοκο τμήμα του στρώματος ασφαλούς υποδοχής SSL είναι το πρωτόκολλο χειραψίας (Handshake Protocol). Αυτό επιτρέπει σε κάθε πελάτη και σε κάθε εξυπηρετητή να επαληθεύει ο ένας την ταυτότητα του άλλου και να διαπραγματεύονται την κρυπτογράφηση, τον αλγόριθμο MAC και τα κλειδιά κρυπτογράφησης που θα χρησιμοποιηθούν για να προστατέψουν τα δεδομένα που αποστέλλονται σε μία SSL εγγραφή. Το πρωτόκολλο χειραψίας χρησιμοποιείται πριν από κάθε μετάδοση δεδομένων μιας εφαρμογής .

Το πρωτόκολλο χειραψίας αποτελείται από μηνύματα τα οποία ανταλλάσσονται μεταξύ πελάτη και εξυπηρετητή . Καθένα από τα μηνύματα έχει τη μορφή που φαίνεται στο Σχήμα 3-16,και αποτελείται από τα τρία πεδία :

- **Τύπος (type) 1byte**:Ορίζει ποιο από τα δέκα μηνύματα χρησιμοποιείται.
- **Μήκος (length) 3 byte** : Το μήκος του μηνύματος χειραψίας σε byte
- **Περιεχόμενο (content) >=1byte**: Οι παράμετροι που σχετίζονται με το μήνυμα αυτό.

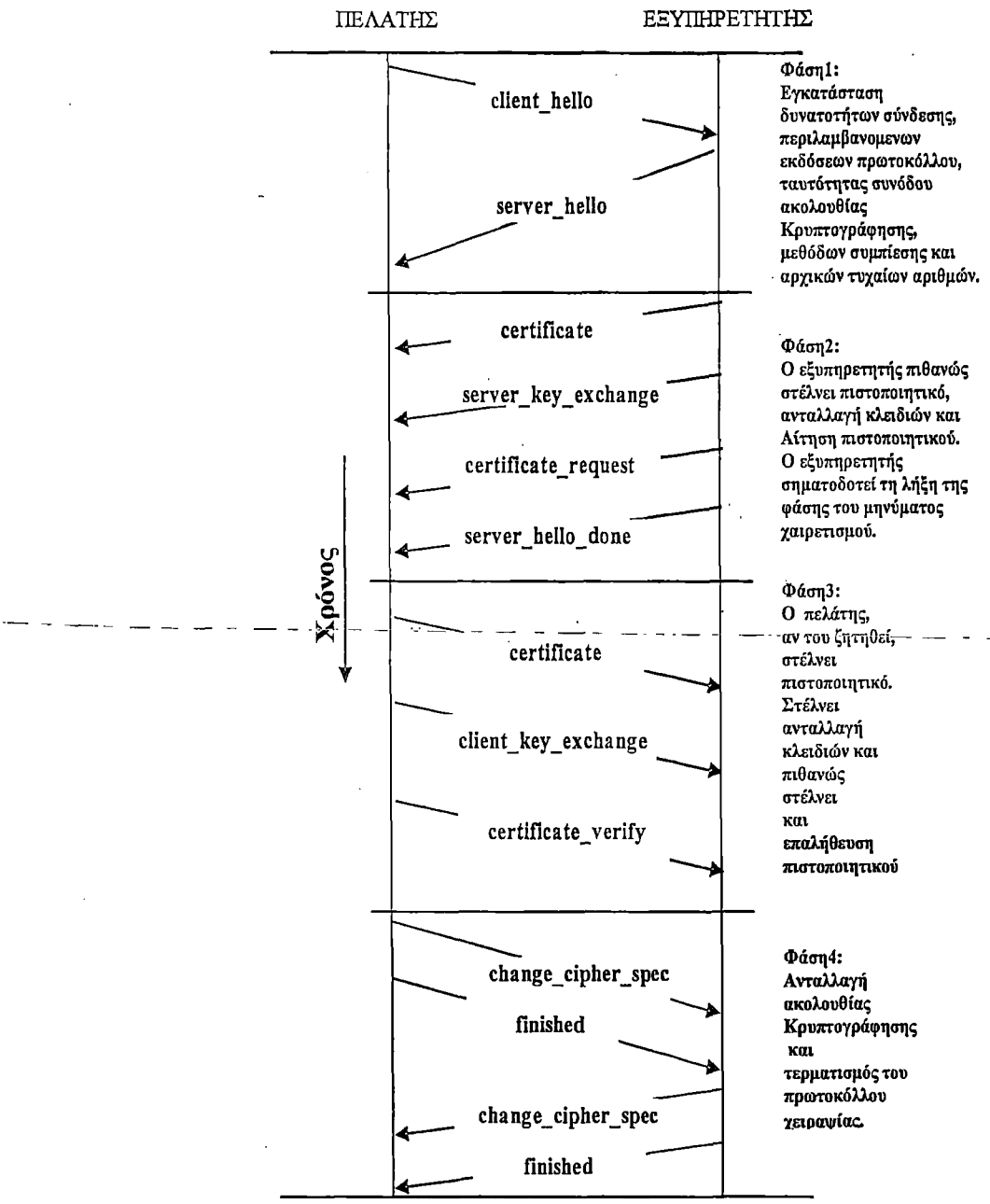
Στο Σχήμα 3-16 φαίνονται επίσης οι τιμές των πεδίων τύπος (type) και περιεχόμενο (content).



Τύπος	Παράμετροι
hello_request	Καμία
client_hello	Έκδοση,τυχαίο,ταυτότητα συνόδου, ακολουθία Κρυπτογράφησης , μέθοδος συμπίεσης
server_hello	Έκδοση,τυχαίο,ταυτότητα συνόδου, ακολουθία Κρυπτογράφησης, μέθοδος συμπίεσης
certificate	Αλυσίδα από X.509v3 πιστοποιητικά
server_key_exchange	Παράμετροι ,υπογραφή
certificate_request	Τύπος ,αρχές
server_done	Καμία
certificate_verify	Υπογραφή
client_key_exchange	Παράμετροι, υπογραφή
finished	Τιμή Κατακερματισμού

Σχήμα 3-16:Μορφή του μηνυμάτων του πρωτοκόλλου χειραψίας.

Το Σχήμα 3-17 δείχνει την αρχική ανταλλαγή μηνυμάτων που χρειάζεται προκειμένου να εγκατασταθεί μία λογική σύνδεση ανάμεσα σε έναν πελάτη και σε ένα εξυπηρετητή. Η ανταλλαγή αυτή μπορεί να θεωρηθεί ότι αποτελείται από τέσσερις φάσεις.



Σχήμα 3-17:Λειτουργία του πρωτοκόλλου χειραψίας

3.2.1.4 Το πρωτόκολλο Συναγερμού

Το πρωτόκολλο Συναγερμού χρησιμοποιείται για να μεταφέρει συναγερμούς σχετικούς με το SSL σε ομότιμες οντότητες. Όπως άλλες εφαρμογές που χρησιμοποιούν το SSL έτσι και τα μηνύματα συναγερμού συμπιέζονται και κρυπτογραφούνται, με τρόπο που προδιαγράφεται από την τρέχουσα κατάσταση.

Κάθε μήνυμα στο πρωτόκολλο αυτό αποτελείται από 2 byte .Το πρώτο byte παίρνει την τιμή warning (προειδοποίηση) (1) ή την τιμή fatal (κρίσιμο) (2) για να μεταφέρει τη σοβαρότητα του μηνύματος. Εάν το επίπεδο σοβαρότητας είναι fatal, τότε το SSL άμεσα τερματίζει τη σύνδεση. Άλλες συνδέσεις στην ίδια σύνοδο μπορεί να συνεχίζουν, αλλά καμία νέα σύνδεση δεν μπορεί να εγκατασταθεί σε αυτή τη σύνοδο. Το δεύτερο byte περιλαμβάνει ένα κώδικα που υποδηλώνει το είδος του συγκεκριμένου συναγερμού. Στη συνέχεια παραθέτουμε ορισμένους συναγερμούς που είναι πάντα κρίσιμοι (ορισμοί από την SSL προδιαγραφή):

- **Unexpected_message (μη αναμενόμενο μήνυμα)** : Λαμβάνεται ένα ακατάλληλο μήνυμα.

- **Bad_record_mac (κακή MAC εγγραφή)** : Λαμβάνεται κάποιος λανθασμένος κώδικας επαλήθευσης μηνύματος (message authentication code-MAC).

- **Decompression_failure (αποτυχία συμπίεσης)** : Η συνάρτηση απόσυμπίεσης έχει λάβει λανθασμένη είσοδο (για παράδειγμα αδυναμία αποσυμπίεσης ή αποσυμπίεση σε μήκος μεγαλύτερο από το μέγιστο επιτρεπόμενο.

- **Handshake_failure (αποτυχία χειραψίας)**: Δεδομένων των διαθέσιμων επιλογών από παραμέτρους ασφάλειας , ο αποστολέας δεν καταφέρνει να διαπραγματώνει ένα αποδεκτό σύνολο από παραμέτρους ασφάλειας .

- **Illegal_parameter (Παράνομη παράμετρος)** : Ένα πεδίο του μηνύματος χειραψίας είναι εκτός περιοχής ή σε ανακολουθία με τα υπόλοιπα πεδία.

3.2.2 Το στρώμα TLS

Το TLS αποτελεί μια πρωτοβουλία τυποποίησης από την IETF η οποία έχει ως στόχο την παραγωγή μιάς τυποποιημένης διαδικτυακής έκδοσης του SSL. Το τρέχον προτεινόμενο πρότυπο του TLS , όπως καθορίζεται στη σύσταση RFC 2246, ομοιάζει πάρα πολύ στο SSLv3.

3.3 Ασφάλεια Εφαρμογής

3.3.1 Ασφάλεια Στρώματος Εφαρμογής

Αρχικά αναλύουμε την ασφάλεια μιας ειδικής εφαρμογής όπως είναι η διαχείριση δικτύων. Πιο συγκεκριμένα στην ενότητα 3.3.1.1 θα μιλήσουμε για τις εφαρμογές του πρωτοκόλλου SNMP (ενότητα 3.3.1.1.1) το οποίο , όπως αναλύθηκε και στο Κεφάλαιο 2, μεταφέρει πληροφορίες διαχείρισης και τον τρόπο με τον οποίο εξασφαλίζεται η ασφάλεια στο πρωτόκολλο αυτό (USM)(ενότητα 3.3.1.1.2). Στη συνέχεια , θα αναλύσουμε πως γίνεται ο έλεγχος πρόσβασης σε μια SNMP MIB (VACM) στην ενότητα 3.3.1.2 .Τέλος εξετάζουμε μια πιο γενική εφαρμογή όπως είναι η επικοινωνία μεταξύ πελάτη και εξυπηρετητή και θα δούμε πως εξασφαλίζεται η υπηρεσία Επαλήθευσης σε αυτή την εφαρμογή(Σύστημα Kerberos). Αυτό γίνεται στην ενότητα 3.3.1.3.

3.3.1.1 Εφαρμογές του SNMP και η Ασφάλειά του (USM)

3.3.1.1.1 SNMPv3 Εφαρμογές

Η έκδοση SNMPv3 τυπικά καθορίζει πέντε τύπους εφαρμογών, οι οποίες, όμως, δεν είναι οι ίδιες με αυτές του λειτουργικού δομοστοιχείου το οποίο παρουσιάζει το Δομοστοιχείο OSI. Αυτοί οι τύποι εφαρμογών μπορεί να μη θεωρούνται στοιχεία εφαρμογών υπηρεσίας που χρησιμοποιούνται για τη δημιουργία εφαρμογών. Αυτές είναι : η γεννήτρια εντολών, ο αποκριτής σε εντολές, ο αποστολέας ειδοποιήσεων και ο παραλήπτης ειδοποιήσεων και περιγράφονται στη σύσταση RFC 2273.

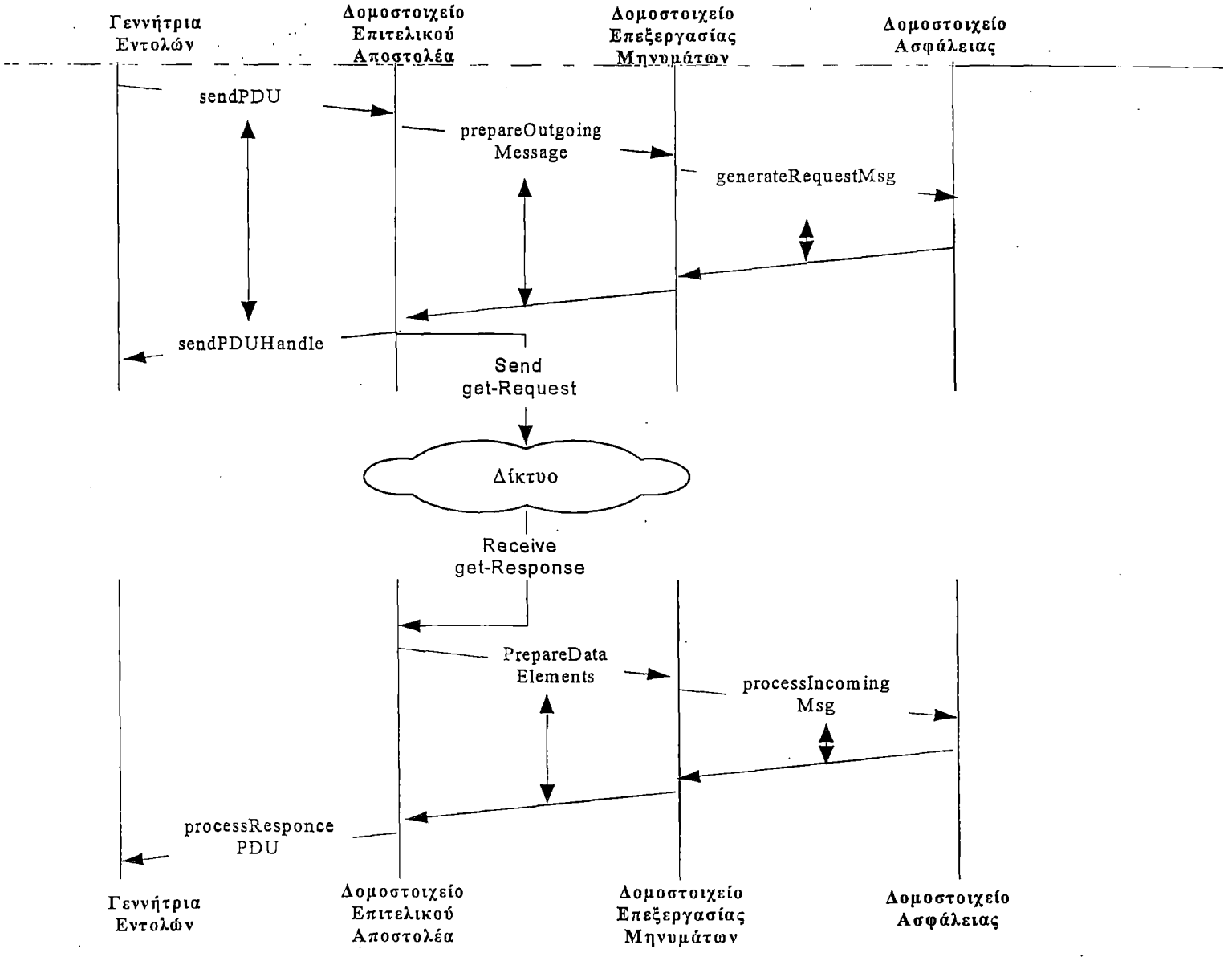
Η Γεννήτρια Εντολών:Η Γεννήτρια Εντολών χρησιμοποιείται για να παράγει get-request, get-next-request και set-request μηνύματα. Επιπλέον , επεξεργάζεται την απάντηση σε κάθε εντολή που έχει αποσταλεί. Τυπικά , η εφαρμογή γεννήτριας εντολών συνδέεται με τη διαδικασία διαχειριστή δικτύου. Στο Σχήμα 3-18 φαίνεται ο τρόπος με τον οποίο η Γεννήτρια Εντολών χρησιμοποιείται με τα get-request και get-response μηνύματα.

Αποκριτής Εντολών:Ο Αποκριτής Εντολών επεξεργάζεται τις αιτήσεις get και set που απευθύνονται σε αυτόν από κάποια απομακρυσμένη οντότητα. Εκτελεί την κατάλληλη get ή set ενέργεια στα στοιχεία δικτύου , προετοιμάζει ένα get-response μήνυμα και το αποστέλλει

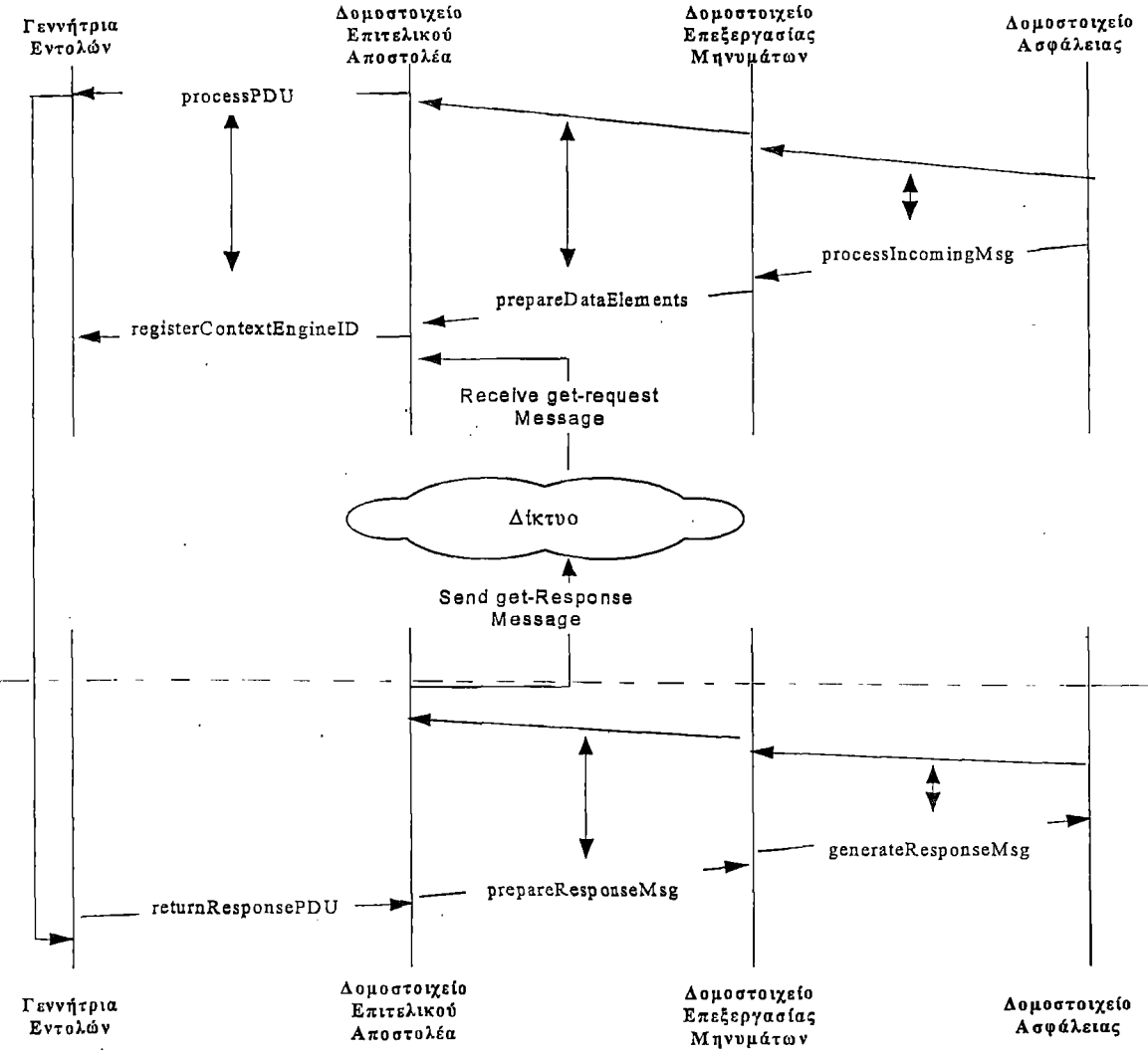
στην απομακρυσμένη οντότητα η οποία απέστειλε την αίτηση ,όπως φαίνεται και στο Σχήμα 3-19. Συνήθως ,ο αποκριτής εντολών βρίσκεται στον πράκτορα διαχείρισης που συνδέεται με το υπό διαχείριση αντικείμενο .

Αποστολέας Ειδοποιήσεων:Η εφαρμογή Αποστολέα Ειδοποιήσεων παράγει ένα μήνυμα είτε παγίδευσης (trap) είτε πληροφόρησης. Η λειτουργία της είναι παρόμοια με αυτή του αποκριτή εντολών, με τη διαφορά ότι ο αποστολέας ειδοποιήσεων χρειάζεται να βρει που πρέπει να στείλει το μήνυμα και ποια SNMP έκδοση και ποιες παραμέτρους ασφάλειας να χρησιμοποιήσει.

Παραλήπτης Ειδοποιήσεων:Η εφαρμογή παραλαβής ειδοποιήσεων λαμβάνει SNMP μηνύματα ειδοποιήσεων. Συνεργάζεται με την SNMP μηχανή για να παραλάβει αυτά τα μηνύματα , όπως ακριβώς ενεργεί η εφαρμογή αποκριτή εντολών ώστε να παραλάβει τα get και set μηνύματα.



Σχήμα 3-18: Γεννήτρια Εντολών



Σχήμα 3-19:Εφαρμογή του Αποκριτή Εντολών

3.3.1.1.2 Υπηρεσίες Ασφάλειας SNMP

Ένας από τους κύριους στόχους ,αν όχι ο κυριότερος στόχος , της ανάπτυξης του SNMPv3 ήταν η προσθήκη χαρακτηριστικών ασφάλειας για τη διαχείριση στο SNMP όπως είναι η Επαλήθευση και το Απόρρητο της πληροφορίας.

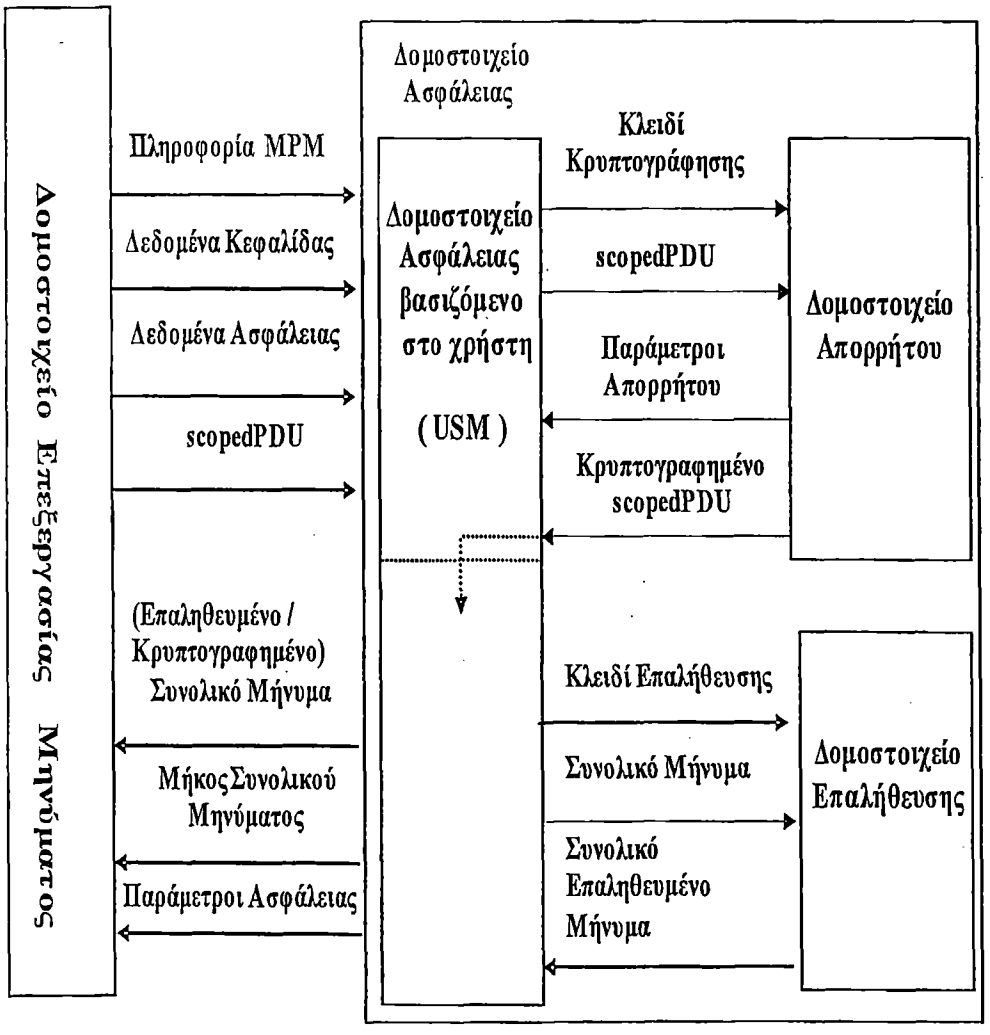
Το Δομοστοιχείο Ασφάλειας του SNMPv3 είναι ένα δομοστοιχείο ασφάλειας βασιζόμενο στο χρήστη (User-based Security Module-USM) που βρίσκεται στο Δομοστοιχείο Ασφάλειας της SNMP μηχανής. Όπως ακριβώς ορίσαμε τις διεπαφές αφηρημένων υπηρεσιών ανάμεσα στα διάφορα υποσυστήματα μιας SNMP μηχανής ,μπορούμε να ορίσουμε και τις διεπαφές αφηρημένων υπηρεσιών στο USM. Αυτοί οι ορισμοί καλύπτουν εννοιολογικές διεπαφές ανάμεσα σε γένιες USM υπηρεσίες και σε αυτοτελείς υπηρεσίες επαλήθευσης και απορρήτου. Δύο πρωτογενείς λειτουργίες σχετίζονται με μια υπηρεσία επαλήθευσης, μία για να παράγει ένα επαληθευμένο εξερχόμενο μήνυμα (**authenticateOutgoingMsg**) και μία για να επαληθεύσει το εισερχόμενο επαληθευμένο μήνυμα (**authenticateIncomingMsg**). Παρόμοια, δύο άλλες πρωτογενείς λειτουργίες σχετίζονται με υπηρεσίες απορρήτου: η υπηρεσία **encryptData** για την κρυπτογράφηση των εξερχόμενων μηνυμάτων και η **decryptData** για την αποκρυπτογράφηση των εισερχόμενων μηνυμάτων.

Οι υπηρεσίες παρέχονται , όπως φαίνεται και στα Σχήματα 3-18 και 3-19 , από τα δομοστοιχεία επαλήθευσης και απορρήτου του δομοστοιχείου ασφάλειας για τα εισερχόμενα και τα εξερχόμενα μηνύματα αντίστοιχα. Το Δομοστοιχείο Επεξεργασίας Μηνυμάτων (Message Processing Module-MSM) επικαλείται το δομοστοιχείο ασφάλειας (USM) βασισμένο στο χρήστη που βρίσκεται στο Δομοστοιχείο Ασφάλειας. Με βάση το επίπεδο ασφάλειας του μηνύματος, το USM με τη σειρά επικαλείται τα δομοστοιχεία απορρήτου και

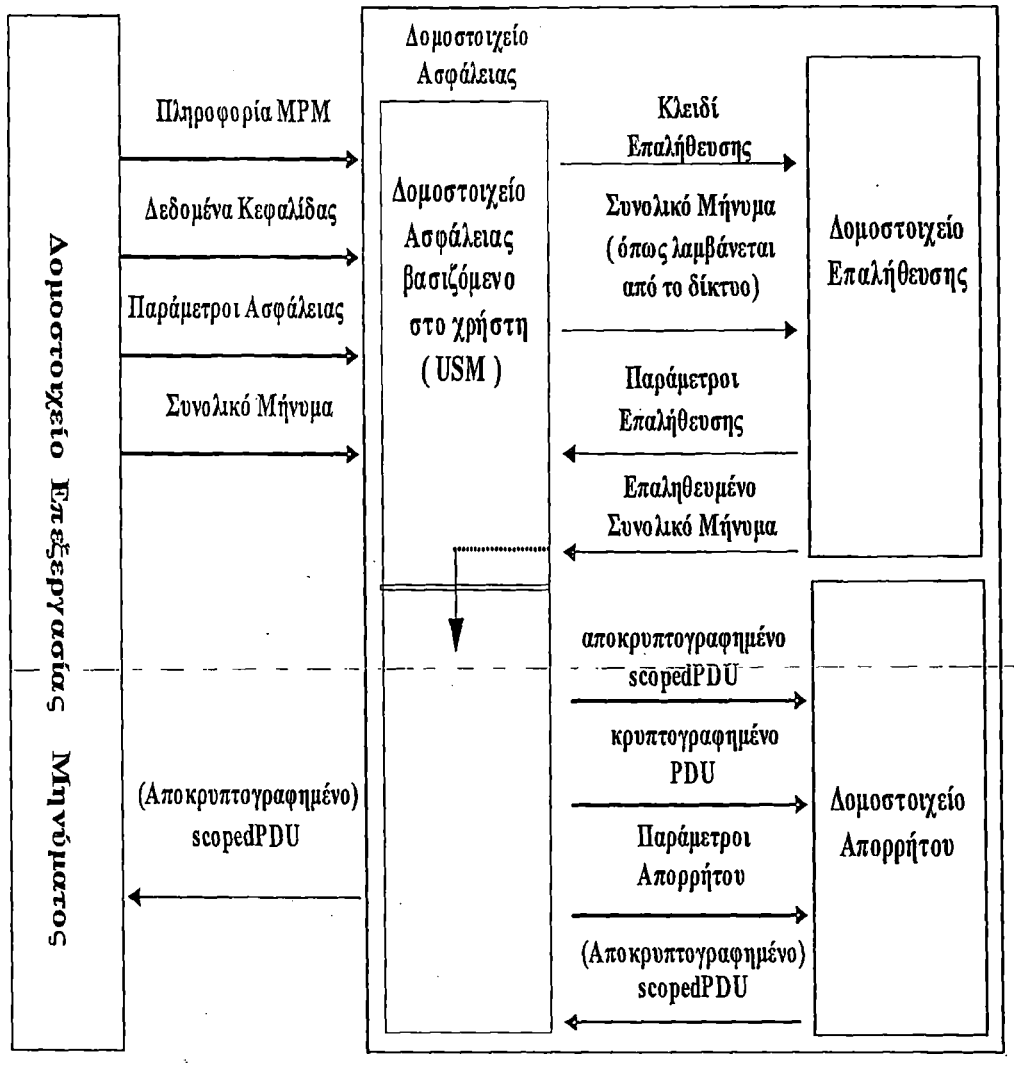
επαλήθευσης. Τα αποτελέσματα επιστρέφονται από το USM στο δομοστοιχείο επεξεργασίας του μηνύματος.

Το Σχήμα 3-20 δείχνει τη διαδικασία που ακολουθείται για ένα εξερχόμενο μήνυμα. Υποθέτουμε ότι οι σημαίες απορρήτου και επαλήθευσης έχουν τοποθετηθεί στην σημαία του μηνύματος στα δεδομένα της κεφαλίδας. Το Δομοστοιχείο Επεξεργασίας Μηνυμάτων MPM εισάγει στο δομοστοιχείο ασφάλειας την πληροφορία του δομοστοιχείου επεξεργασίας μηνύματος, δεδομένα κεφαλίδας, δεδομένα ασφάλειας και scopedPDU. Το USM επικαλείται αρχικά το δομοστοιχείο απορρήτου, παρέχοντας ως είσοδο το κλειδί κρυπτογράφησης και το scopedPDU.

Το δομοστοιχείο απορρήτου εξάγει παραμέτρους απορρήτου (όπως είναι η τιμή salt στην CBC-DES κρυπτογράφηση) οι οποίες αποστέλλονται ως τμήμα του μηνύματος και του κρυπτογραφημένου scopedPDU. Το USM περνά στο δομοστοιχείο επαλήθευσης, το συνολικό μη επαληθευμένο μήνυμα με κρυπτογραφημένο scopePDU και με το κλειδί επαλήθευσης. Το δομοστοιχείο επαλήθευσης επιστρέφει το επαληθευμένο μήνυμα συνολικά , στο USM. Το USM επιστρέφει στο δομοστοιχείο επεξεργασίας μηνύματος το συνολικό επαληθευμένο και κρυπτογραφημένο μήνυμα μαζί με το μήκος μηνύματος και τις παραμέτρους ασφάλειας. Το Σχήμα 3-21 δείχνει την αντίστροφη διαδικασία για ένα εισερχόμενο μήνυμα, το οποίο περνά πρώτα διαμέσου της εξακρίβωσης επαλήθευσης και έπειτα της αποκρυπτογράφησης του μηνύματος από το δομοστοιχείο απορρήτου.



Σχήμα 3-20: Υπηρεσίες Απορρήτου και Επαλήθευσης για Εξερχόμενα μηνύματα



Σχήμα 3-21: Υπηρεσίες Απορρήτου και Επαλήθευσης για Εισερχόμενα μηνύματα

3.3.1.2 Ασφάλεια Πρόσβασης SNMP MIB

Στην προηγούμενη ενότητα καλύψαμε θέματα ασφάλειας του SNMP που αφορούν στην ακεραιότητα δεδομένων, στην επαλήθευση μηνυμάτων,στην εμπιστευτικότητα δεδομένων και στην επικαιρότητα των μηνυμάτων. Εισάγουμε τώρα τον έλεγχο πρόσβασης, ο οποίος ασχολείται με το ποιος έχει πρόσβαση στη διαχείριση δικτύου και σε τι έχει πρόσβαση. Το πρωτόκολλο SNMP εκπροσωπείται στη Βάση Πληροφοριών Διαχείρισης MIB από πολλά Υπό Διαχείριση Αντικείμενα Μ.Ο .Ωστόσο, ένας πράκτορας μπορεί να περιορίζεται να βλέπει ένα μόνο υποσύνολο από αυτά τα υπό διαχείριση αντικείμενα. Αυτό ονομάζεται θέαση της SNMP Βάσης Πληροφοριών Διαχείρισης. Η σύσταση RFC 2575 καθορίζει το βασισμένο στη θέαση μοντέλο ελέγχου πρόσβασης (View-based Access Control Model-VACM). Η RFC 2575 περιγράφει τα πέντε στοιχεία που απαρτίζουν το Δομοστοιχείο VACM: ομάδες, επίπεδα ασφάλειας, πλαίσια εφαρμογής, θεάσεις της MIB και πολιτική πρόσβασης.

- Μία ομάδα ορίζεται ως ένα σύνολο από μηδέν ή περισσότερα <SecurityModel,SecurityName> εκ μέρους των οποίων επιτρέπεται να προσπελαστούν τα SNMP υπό διαχείριση αντικείμενα. Ένα όνομα ασφάλειας αναφέρεται σε κάποια αρχή, ενώ τα δικαιώματα πρόσβασης κάθε αρχής σε μία δεδομένη ομάδα είναι πανομοιότυπα. Ένα ξεχωριστό όνομα ομάδας (groupName) σχετίζεται με κάθε ομάδα. Η ιδέα της ομάδας αποτελεί ένα χρήσιμο εργαλείο για την κατηγοριοποίηση των διαχειριστών ανάλογα με τα δικαιώματα πρόσβασης. Για παράδειγμα , όλοι οι ανώτερου επιπέδου διαχειριστές μπορεί να έχουν ένα σύνολο από δικαιώματα

πρόσβασης ,ενώ οι ενδιάμεσου επιπέδου διαχειριστές μπορεί να έχουν ένα διαφορετικό σύνολο από δικαιώματα.

Κάθε δοσμένος συνδυασμός μοντέλου-ασφάλειας (securityModel) και ονόματος-ασφάλειας (securityName) μπορεί να ανήκει το πολύ σε μία ομάδα. Αυτό σημαίνει ότι, για αυτό τον πράκτορα, μια δεδομένη αρχή της οποίας οι επικοινωνίες προστατεύονται από ένα δεδομένο μοντέλο- ασφάλειας μπορεί να συμπεριληφθεί σε μία μόνο ομάδα.

- Τα δικαιώματα πρόσβασης μιας ομάδας μπορεί να διαφέρουν ανάλογα με το επίπεδο ασφάλειας του μηνύματος που περιέχει την αίτηση. Για παράδειγμα ,ένας πράκτορας μπορεί να επιτρέψει μόνο πρόσβαση για διάβασμα προς ένα μη επαληθευμένο αίτημα, αλλά μπορεί να απαιτεί επαλήθευση για πρόσβαση εγγραφής. Επιπλέον ,για συγκεκριμένα , ευαίσθητα , υπό διαχείριση αντικείμενα ο πράκτορας μπορεί να απαιτεί ότι τόσο η αίτηση όσο και η απάντηση σε αυτό πρέπει να γίνεται χρησιμοποιώντας την υπηρεσία απορρήτου.

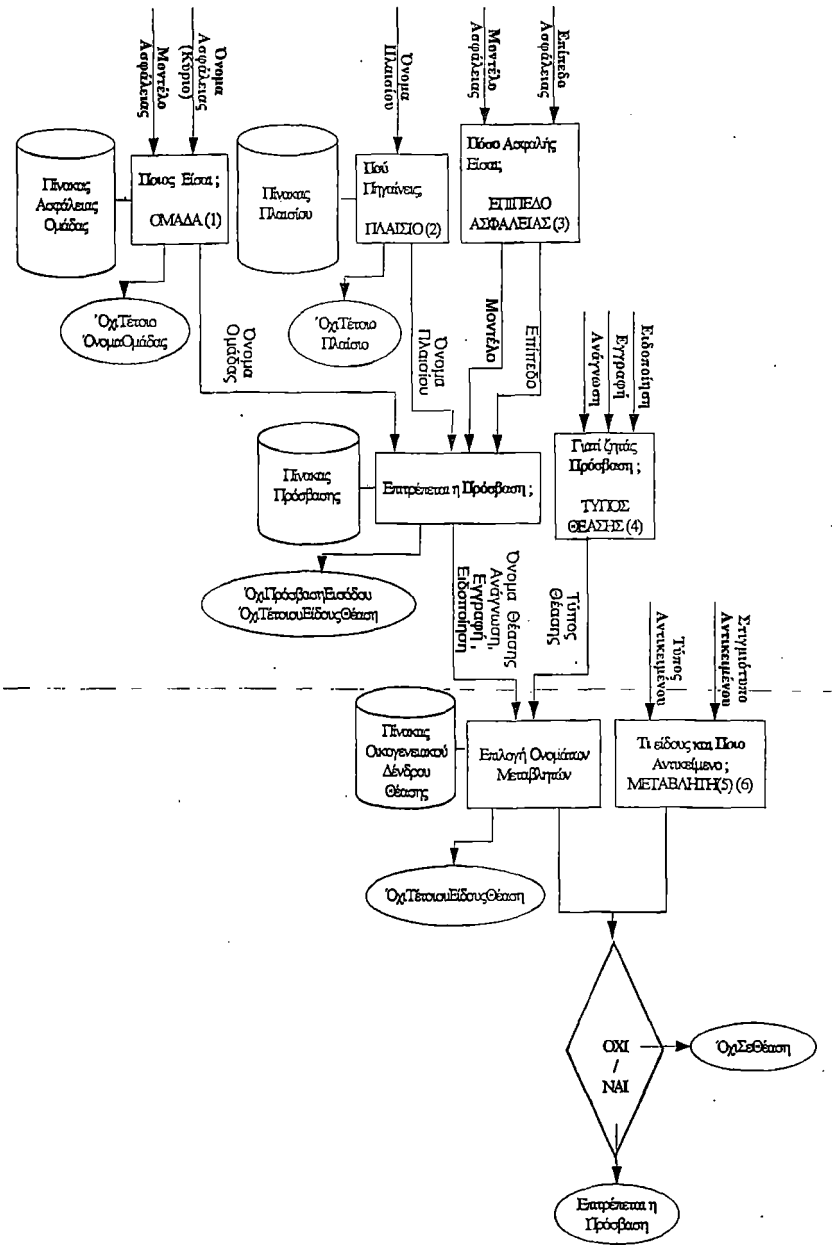
- Το πλαίσιο εφαρμογής μιας MIB είναι ένα ονοματισμένο υποσύνολο των υποστάσεων των υπό διαχείριση αντικειμένων της MIB. Τα πλαίσια εφαρμογής παρέχουν ένα χρήσιμο τρόπο για τη συνάθροιση αντικειμένων σε συλλογές με διαφορετικές πολιτικές πρόσβασης.

- Συχνά συναντάται η περίπτωση να επιθυμούμε να περιορίσουμε την πρόσβαση μιας συγκεκριμένης ομάδας σε ένα υποσύνολο από τα υπό διαχείριση αντικείμενα που υπάρχουν σε έναν πράκτορα. Για να επιτύχουμε αυτό τον σκοπό, η πρόσβαση σε ένα πλαίσιο εφαρμογής γίνεται με τη θέαση της MIB (MIB VIEW).Αυτή καθορίζει ένα προδιαγεγραμμένο σύνολο από υπό διαχείριση αντικείμενα ή επιλεκτικά από υποστάσεις αντικειμένων.

- Η πολιτική πρόσβασης καθορίζει τα δικαιώματα πρόσβασης σε αντικείμενα, όπως είναι **θέαση ανάγνωσης**, **θέαση εγγραφής** και **θέαση ειδοποίησης**. Για μια δεδομένη *ομάδα* , *πλαίσιο εφαρμογής* , *μοντέλο ασφάλειας* και *επίπεδο ασφάλειας* τα δικαιώματα πρόσβασης της ομάδας καθορίζονται από το συνδυασμό των τριών θεάσεων ή από την αδυναμία πρόσβασης.

Η διαδικασία VACM παρουσιάζεται στο διάγραμμα ροής του Σχήματος 3-22.Θα αναλύσουμε τη διαδικασία αυτή για ένα SNMP πράκτορα που έχει μια SNMP MIB , που είναι υπεύθυνη για πολλές εφαρμογές πλαισίου. Η VACM διαδικασία απαντά στις έξι ερωτήσεις οι οποίες σχετίζονται με την πρόσβαση σε πληροφορία διαχείρισης και είναι:

1. Ποιος είσαι (ομάδα , που περιλαμβάνει μοντέλο ασφάλειας και όνομα ασφάλειας) ;
2. Που ζητάς να πας (πλαίσιο εφαρμογής για το οποίο ζητείται πρόσβαση) ;
3. Πόσο ασφαλής είσαι ώστε να αποκτήσεις πρόσβαση σε πληροφορία (μοντέλο ασφάλειας και επίπεδο ασφάλειας) ;
4. Για ποιο λόγο ζητάς πρόσβαση σε πληροφορία (για ανάγνωση, εγγραφή ή για αποστολή ειδοποίησης);
5. Σε τί τύπο αντικειμένου ζητάς να έχεις πρόσβαση;
6. Σε ποιο αντικείμενο (Υπόσταση) ζητάς πρόσβαση;



Σχήμα 3-22:Η διαδικασία VACM

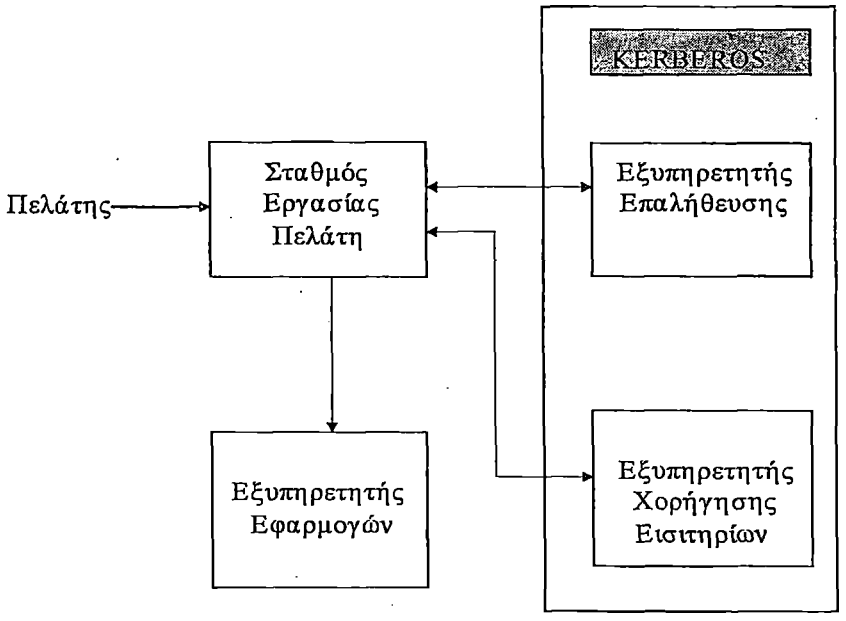
3.3.1.3 Ασφάλεια Επαλήθευσης

Η Επαλήθευση (Authentication) είναι η εξακρίβωση της ταυτότητας ενός χρήστη ενώ εξουσιοδότηση (Authorisation) είναι η παραχώρηση δικαιωμάτων πρόσβασης στην Πληροφορία. Δύο βασικές κατηγορίες συστημάτων παρουσιάζουν ενδιαφέρον για μας στην υλοποίηση της επαλήθευσης. Η πρώτη κατηγορία αφορά στο περιβάλλον πελάτη-εξυπηρετητή στο οποίο αναπτύσσεται επικοινωνία ερωτοαποκρίσεων μεταξύ πελάτη και εξυπηρετητή. Ο πελάτης ξεκινά με μια αίτηση για υπηρεσία προς τον εξυπηρετητή και ο εξυπηρετητής απαντά με το αποτέλεσμα της υπηρεσίας που εκτελέστηκε- δηλαδή έχουμε απαραίτητα αμφίδρομη επικοινωνία. Στο περιβάλλον αυτό εκτός από την επαλήθευση (και, φυσικά τον έλεγχο ακεραιότητας) είναι απαραίτητη και η εξουσιοδότηση.

Στη δεύτερη κατηγορία ανήκει η μονόδρομη επικοινωνία , όπως είναι το ηλεκτρονικό ταχυδρομείο ή οι ηλεκτρονικές συναλλαγές. Το μήνυμα μεταδίδεται από μία πηγή και παραλαμβάνεται από τον προορισμό με σημαντική καθυστέρηση -ορισμένες φορές η καθυστέρηση αυτή μπορεί και να διαρκεί ακόμη και μέρες εάν υπάρχουν ενδιάμεσοι εξυπηρετητές. Σε αυτή την περίπτωση η επαλήθευση και ο έλεγχος ακεραιότητας είναι απαραίτητο να εκτελούνται στο άκρο παραλαβής.

Σε αυτή την ενότητα θα αναλύσουμε τα συστήματα επαλήθευσης πελάτη-εξυπηρετητή ενώ τη μονόδρομη επαλήθευση μηνύματος και τα συστήματα προστασίας της ακεραιότητας θα αναλυθούν σε ξεχωριστή ενότητα (ενότητα 3.3.2). Εκεί θα εξεταστεί η ασφάλεια εφαρμογών του χρήστη. Ας μην ξεχνάμε ότι σε αυτή εδώ την ενότητα εξετάζεται μόνο η ασφάλεια εφαρμογών NOS, στην περίπτωση του TCP / IP .

Σύστημα Χορήγησης Εισιτηρίων (Ticket-Granting System) : Θα εξηγήσουμε το σύστημα χορήγησης Εισιτηρίων περιγράφοντας την πιο δημοφιλή μέθοδο ,το Kerberos, ένα σύστημα το οποίο αναπτύχθηκε από το MIT ως τμήμα του προγράμματος «Athena».Όπως φαίνεται και στο Σχήμα 3-23 το Kerberos αποτελείται από έναν εξυπηρετητή επαλήθευσης και από έναν εξυπηρετητή χορήγησης εισιτηρίων. Ένας χρήστης κάνει έναρξη συνόδου σε ένα σταθμό εργασίας πελατών και στέλνει μία αίτηση συνόδου στον εξυπηρετητή επαλήθευσης. Αφού εξακριβωθεί ότι ο χρήστης εμπεριέχεται στη λίστα ελέγχου πρόσβασης, ο εξυπηρετητής επαλήθευσης χορηγεί στον πελάτη ένα κρυπτογραφημένο εισιτήριο. Ο σταθμός εργασίας ζητά από τον χρήστη λήξη πρόσβασης (password), την οποία χρησιμοποιεί στη συνέχεια για να αποκρυπτογραφήσει το μήνυμα που λαμβάνει από τον εξυπηρετητή επαλήθευσης. Ο πελάτης στη συνέχεια αλληλεπιδρά με τον εξυπηρετητή χορήγησης εισιτηρίων και αποκτά μία υπηρεσία χορήγησης εισιτηρίων και ένα κλειδί συνόδου για χρήση από τον εξυπηρετητή εφαρμογών. Έπειτα σταθμός εργασίας του πελάτη ζητά μια υπηρεσία από τον εξυπηρετητή εφαρμογών ,δίνοντας το κλειδί χορήγησης υπηρεσίας και το κλειδί συνόδου. Ο εξυπηρετητής εφαρμογών, αφού επικυρώσει το εισιτήριο και το κλειδί συνόδου, παρέχει την υπηρεσία στο χρήστη. Αυτή η διαδικασία ,η οποία συμβαίνει στο παρασκήνιο , είναι διάφανη στο χρήστη , του οποίου η μόνη αλληλεπίδραση είναι η αίτηση υπηρεσίας εφαρμογών από το σταθμό εργασίας πελατών.



Σχήμα 3-23:Σύστημα Χορήγησης Εισιτηρίων

3.3.2 Ασφάλεια Εφαρμογών Χρήστη

Σε αυτή την ενότητα εξετάζεται αποκλειστικά η ασφάλεια των εφαρμογών του χρήστη δικτύου. Συγκεκριμένα , στην υποενότητα 3.3.2.1 εξετάζονται τρεις εφαρμογές που αφορούν στη μεταφορά μηνυμάτων δηλαδή το ηλεκτρονικό ταχυδρομείο ,ενώ στην υποενότητα 3.3.2.2 εξετάζεται η εφαρμογή που αφορά στο ηλεκτρονικό εμπόριο δηλαδή οι ηλεκτρονικές συναλλαγές.

3.3.2.1 Ασφάλεια Ηλεκτρονικού Ταχυδρομείου(S/MIME , PGP, PEM)

Το μονόδρομο σύστημα μεταφοράς μηνυμάτων δεν είναι αλληλεπιδραστικό. Για παράδειγμα , εάν μία χρήστης με το όνομα Μαρία λάβει ένα ηλεκτρονικό μήνυμα από άλλο χρήστη που ισχυρίζεται ότι είναι ο χρήστης με το όνομα Γιάννης, χρειάζεται να επαληθεύσει την ταυτότητα του Γιάννη ως αποστολέα του μηνύματος και να εξασφαλίσει ότι κανείς δεν έχει παραποιήσει το μήνυμα αυτό. Ακόμη ο Δημήτρης θα μπορούσε να στείλει από το κινητό του τηλέφωνο μέσα στο αυτοκίνητο μία εντολή πώλησης για προϊόντα. Ο Κώστας θα μπορούσε να υποκλέψει το μήνυμα αυτό και να μεταβάλει τον αριθμό των διαθέσιμων προϊόντων ή το αντίτιμο. Θα αντιμετωπίσουμε τέτοιες περιπτώσεις εξασφαλίζοντας την ασφάλεια των συστημάτων ταχυδρομείου.

Υπάρχουν τρία ασφαλή συστήματα ταχυδρομείου : το Ασφαλές-MIME (Secure/Multipurpose Internet Mail Extensions-S/MIME), το ταχυδρομείο βελτιωμένου απορρήτου (Privacy Enhanced Mail-PEM) και το σύστημα αρκετά καλού απορρήτου (Pretty Good Privacy-PGP).

3.3.2.1.1 Ασφαλής Πολύσκοπη Επέκταση Ταχυδρομείου Διαδικτύου.

Η Ασφαλής Πολύσκοπη Επέκταση Ταχυδρομείου Διαδικτύου (Secure / Multipurpose Internet Mail Extension-S/MIME) αποτελεί μια βελτίωση ασφάλειας του MIME προτύπου ηλεκτρονικού ταχυδρομείου Διαδικτύου, βασισμένου στην τεχνολογία RSA Ασφάλεια Δεδομένων και καθορισμένου στις συστάσεις RFC. Παρότι, τόσο το PGP όσο και το S/MIME ακολουθούν τα πρότυπα της ομάδας έργου μηχανίκευσης Διαδικτύου (Internet Engineering Task Force-IETF), ωστόσο φαίνεται ότι το S/MIME θα αναδειχθεί σε ένα βιομηχανικό προϊόν για εμπορική και επιχειρησιακή χρήση, ενώ το PGP θα παραμείνει η επιλογή πολλών χρηστών όσον αφορά στην ασφάλεια του προσωπικού ηλεκτρονικού ταχυδρομείου.

Για να γίνει αντιληπτό το S/MIME, χρειάζεται αρχικά να έχουμε μια γενική κατανόηση του υποκείμενου ηλεκτρονικού ταχυδρομείου που χρησιμοποιεί, δηλαδή του MIME. Για να κατανοήσουμε ,όμως, τη σπουδαιότητα του MIME , χρειάζεται να ανατρέξουμε στο παραδοσιακό μορφότυπο για το ηλεκτρονικό ταχυδρομείο SMTP, που περιγράφεται στη σύσταση RFC 822 και το οποίο ακόμη χρησιμοποιείται ευρέως . Συνεπώς ,αυτή η ενότητα παρέχει αρχικά μια εισαγωγή σε αυτά τα δύο προηγούμενα πρότυπα δηλαδή του MIME και SMTP και έπειτα προχωρεί σε μία ανάλυση του S/MIME.

Η γενική δομή ενός μηνύματος ,το οποίο είναι συμβατό με τη σύσταση RFC 822 είναι πολύ απλή .Παραθέτουμε ένα παράδειγμα τέτοιου μηνύματος :

Date :Tue,16 Jan 2004,10:37:17 (EST)
From : 'Lefteris Economou'<le@ote.gr>
Subject: The Syntax in RFC 822
To : Smith@Other-host.com
Cc : Jones@Yet-Another-Host.com

} Κεφαλίδα Μηνύματος

Καλησπέρα. Αυτή η ενότητα ξεκινά το ουσιαστικό σώμα μηνύματος, το οποίο χωρίζεται από την κεφαλίδα μηνύματος μέσω μιας κενής γραμμής.

} Σώμα Κειμένου

Το MIME είναι μια επέκταση της σύστασης RFC 822 το οποίο έχει ως στόχο να αντιμετωπίσει κάποια από τα προβλήματα και τους περιορισμούς που εισάγει η χρήση του Πρωτοκόλλου Μεταφοράς Απλού Ταχυδρομείου (Simple Mail Transfer Protocol-SMTP) ή άλλων πρωτοκόλλων μεταφοράς ταχυδρομείου. Η προδιαγραφή του MIME παρέχεται στις συστάσεις RFC 2045 έως 2049.Στις συστάσεις αυτές καθορίζονται :

1. Πέντε νέα πεδία κεφαλίδας μηνύματος ,τα οποία μπορούν να περιλαμβάνονται σε μία RFC 822 κεφαλίδα. Τα πεδία αυτά παρέχουν πληροφορία σχετικά με το σώμα ενός μηνύματος.
2. Ένας αριθμός από μορφότυπα σώματος μηνύματος , με τέτοιο τρόπο ώστε να τυποποιούνται οι αναπαραστάσεις που υποστηρίζουν ηλεκτρονικό ταχυδρομείο πολυμέσων.
3. Κωδικοποιήσεις μεταφοράς, οι οποίες επιτρέπουν τη μετατροπή μορφοτύπων σώματος μηνύματος κάθε περιεχομένου, σε μορφότυπο το οποίο προστατεύεται από αλλοίωση μέσω συστήματος ταχυδρομείου.

Με όρους γενικής λειτουργικότητας ,το S/MIME μοιάζει πολύ στο PGP . Και τα δύο παρέχουν τη δυνατότητα να υπογράφουν και/ή να κρυπτογραφούν μηνύματα. Στη συνέχεια, περιγράφουμε περιληπτικά λειτουργίες του S/MIME.

Λειτουργίες

Το S/MIME παρέχει τις παρακάτω λειτουργίες :

- **Εμφακελωμένα Δεδομένα** : Περιλαμβάνουν το κρυπτογραφημένο περιεχόμενο κάθε μορφής καθώς και το κρυπτογραφημένο περιεχόμενο κλειδιών κρυπτογράφησης για έναν ή περισσότερους παραλήπτες.
- **Υπογεγραμμένα Δεδομένα** : Μία ψηφιακή υπογραφή δημιουργείται παίρνοντας τη σύνοψη μηνύματος του περιεχομένου που πρόκειται να υπογραφεί και μετά κρυπτογραφώντας τη με το ιδιωτικό κλειδί του υπογράφοντος. Έπειτα το περιεχόμενο μαζί με την υπογραφή κωδικοποιούνται με χρήση κωδικοποίησης βάσης 64. Μόνο ένας παραλήπτης με ικανότητα S/MIME μπορεί να δει ένα μήνυμα υπογεγραμμένων δεδομένων.
- **Καθαρά Υπογεγραμμένα Δεδομένα** :Όπως και στην περίπτωση των υπογεγραμμένων δεδομένων, δημιουργείται η ψηφιακή υπογραφή του περιεχομένου του μηνύματος. Ωστόσο, στην περίπτωση αυτή, μόνο η ψηφιακή υπογραφή κωδικοποιείται κάνοντας χρήση της κωδικοποίησης βάσης 64. Αυτό έχει ως αποτέλεσμα, παραλήπτες χωρίς S / MIME ικανότητα να μπορούν να δουν το περιεχόμενο ενός μηνύματος, χωρίς ωστόσο να μπορούν να επαληθεύσουν την ψηφιακή υπογραφή.
- **Υπογεγραμμένα και Εμφακελωμένα Δεδομένα** :Μόνο υπογεγραμμένες και κρυπτογραφημένες οντότητες μπορούν να εμφωλιάζονται, έτσι ώστε κρυπτογραφημένα δεδομένα μπορούν να υπογράφονται και υπογεγραμμένα δεδομένα ή καθαρά υπογεγραμμένα δεδομένα μπορεί να κρυπτογραφούνται.

3.3.2.1.2 Ταχυδρομείο Βελτιωμένου Απορρήτου

Το Ταχυδρομείο Βελτιωμένου Απορρήτου (Privacy Enhanced Mail-PEM) αναπτύχθηκε από την ομάδα IETF και οι προδιαγραφές για αυτό είναι καθορισμένες στις συστάσεις RFC 1421 έως 1424. Σκοπός του είναι να παρέχει ταχυδρομείο βελτιωμένου απορρήτου, χρησιμοποιώντας από άκρο-σε-άκρο κρυπτογραφία ανάμεσα στον αποστολέα και στον παραλήπτη. Οι υπηρεσίες που παρέχει το βελτιωμένο απόρρητο είναι: **εμπιστευτικότητα, επαλήθευση, διασφάλιση ακεραιότητας μηνύματος** και **αναποκυρηξία προέλευσης**. Το κλειδί κρυπτογράφησης ,που καλείται Κλειδί Κρυπτογράφησης Δεδομένων (Data Encryption Key-DEK) είναι ευέλικτο, καθώς μπορεί να είναι είτε κάποιο μυστικό κλειδί είτε κάποιο δημόσιο κλειδί, βασισμένο σε συγκεκριμένη υλοποίηση . Ωστόσο, είναι προφανές ότι τα άκρα προέλευσης και τερματισμού πρέπει να έχουν κοινή συμφωνία ως προς το είδος του κλειδιού που θα χρησιμοποιηθεί.

Το Σχήμα 3-24 δείχνει τρεις PEM διαδικασίες βασισμένες στην ακεραιότητα μηνύματος και στην κρυπτογράφηση ,όπως αυτές καθορίζονται από την IETF : MIC-CLEAR , MIC-ONLY και ENCRYPTED. Στο σχήμα φαίνεται μόνο το άκρο προέλευσης. Και στις τρεις περιπτώσεις ,οι διαδικασίες περιλαμβάνουν την εξαγωγή του μηνύματος και την επικύρωση της ταυτότητας του αποστολέα και της ακεραιότητας του μηνύματος. Οι διαφορές

ανάμεσα στις τρεις διαδικασίες εξαρτώνται από την έκταση της κρυπτογράφησης και της κωδικοποίησης μηνύματος που χρησιμοποιούνται. Ο Κώδικας Ακεραιότητας Μηνύματος (Message Integrity Code-MIC) παράγεται , για την ψηφιακή υπογραφή, και περιλαμβάνεται ως τμήμα του ηλεκτρονικού μηνύματος και στις τρεις διαδικασίες.

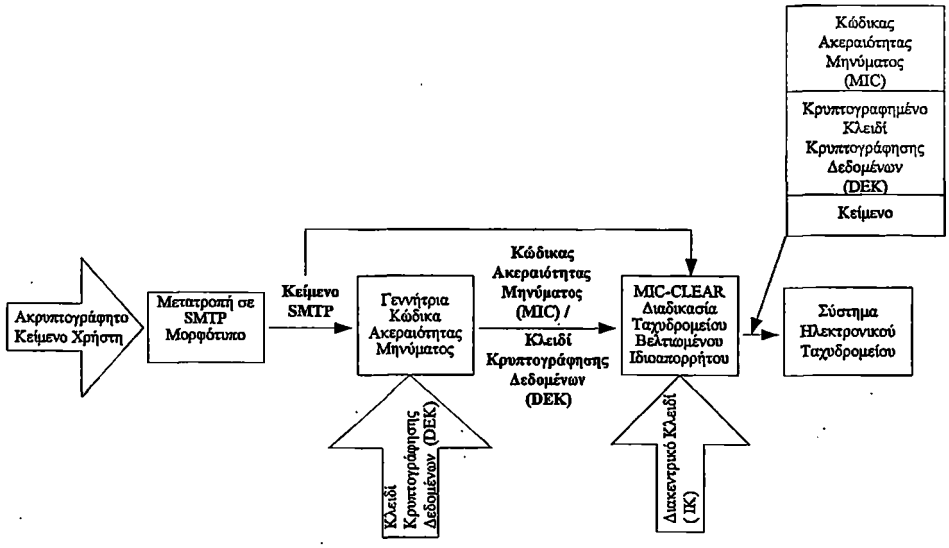
Η προδιαγραφή παρέχει δύο τύπους κλειδιών : ένα **Κλειδί Κρυπτογράφησης Δεδομένων** (Data Encrypting Key-DEK) και ένα **Διακεντρικό Κλειδί** (Interexchange Key-IK). Το Κλειδί Κρυπτογράφησης Δεδομένων DEK είναι ένας τυχαίος αριθμός που παράγεται σε μία ανά μήνυμα βάση, και χρησιμοποιείται για να κρυπτογραφήσει το κείμενο ενός μηνύματος και να παράγει ένα κώδικα ακεραιότητας μηνύματος MIC, εάν αυτός χρειάζεται. Το διακεντρικό κλειδί IK, το οποίο είναι ένα ευρείας κλίμακας κλειδί συμφωνημένο ανάμεσα στον αποστολέα και τον παραλήπτη, χρησιμοποιείται για να κρυπτογραφήσει το κλειδί κρυπτογράφησης δεδομένων DEK για μετάδοση διαμέσω του μηνύματος. Το διακεντρικό κλειδί IK είναι είτε ένα δημόσιο είτε ένα μυστικό κλειδί, ανάλογα με τον τύπο κρυπτογραφικής ανταλλαγής που χρησιμοποιείται.

Εάν για τη κρυπτογράφηση του μηνύματος ,χρησιμοποιείται μη συμμετρική κρυπτογράφηση, ο αποστολέας δε μπορεί να αποκηρύξει τον ιδιοκτήτη του μηνύματος. Νόμιμη απόδειξη των συναλλαγών μηνυμάτων αποθηκεύεται στα δεδομένα , τα οποία χρησιμοποιούνται σε εφαρμογές όπως το ηλεκτρονικό εμπόριο. Ένα άλλο κοινό χαρακτηριστικό τέτοιων διαδικασιών είναι το πρώτο βήμα κατά τη μετατροπή του, παρεχόμενου από τον χρήστη, ακρυπτογράφητου κειμένου σε μία κανονική αναπαράσταση του κειμένου του μηνύματος, η οποία ορίζεται ως ισοδύναμη της δια-SMTP αναπαράστασης του κειμένου του μηνύματος. Η τελική έξοδος σε κάθε διαδικασία χρησιμοποιείται ως το τμήμα κειμένου ενός ηλεκτρονικού μηνύματος σε ένα σύστημα ηλεκτρονικού ταχυδρομείου.

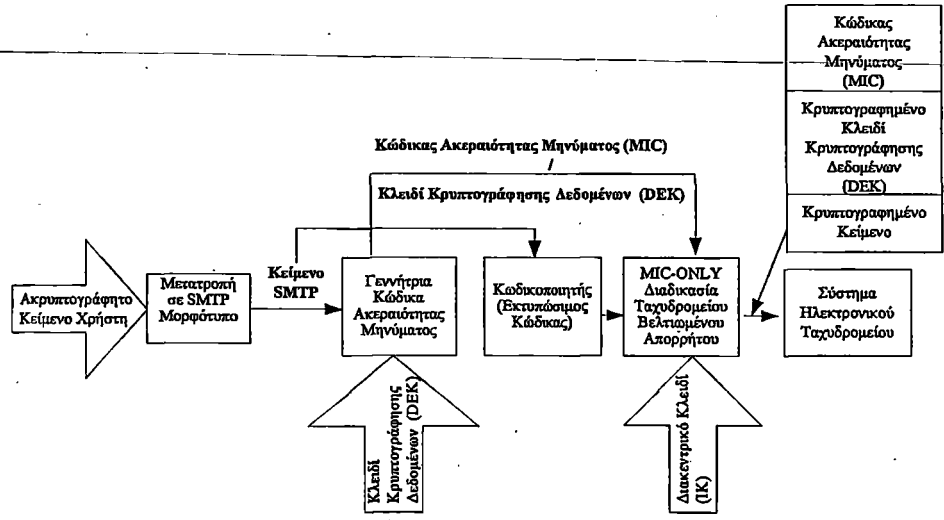
Το Σχήμα 3-24(α) δείχνει την διαδικασία MIC-CLEAR ,η οποία είναι η απλούστερη των τριών διαδικασιών. Ο κώδικας ακεραιότητας μηνύματος MIC που παράγεται συναλυσώνεται με (διαδέχεται αλυσιδωτά) το κρυπτογραφημένο κλειδί κρυπτογράφησης δεδομένων DEK και το SMTP κείμενο και εισάγεται ως το τμήμα κειμένου στο ηλεκτρονικό μήνυμα.

Στη διαδικασία MIC-ONLY ,που φαίνεται στο Σχήμα 3-24(β) , το SMTP κείμενο κωδικοποιείται ως ένα σύνολο εκτυπώσιμων χαρακτήρων . Αποτελείται από ένα περιορισμένο σύνολο χαρακτήρων , οι οποίοι διασφαλίζεται ότι είναι παρόντες σε όλες τις ιστοσελίδες, με τρόπο ώστε να κάνει όλες οι ενδιάμεσες ιστοσελίδες διαφανείς στο μήνυμα. Ο κώδικας ακεραιότητας μηνύματος (MIC) διαδέχεται αλυσιδωτά το κρυπτογραφημένο κλειδί κρυπτογράφησης δεδομένων DEK και το κωδικοποιημένο μήνυμα και τροφοδοτείται στο σύστημα ηλεκτρονικού ταχυδρομείου.

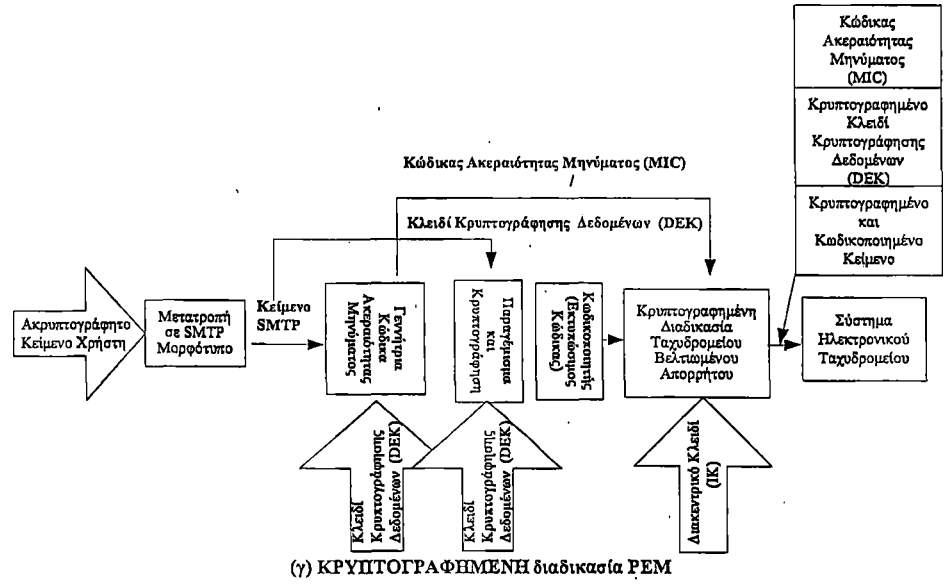
Στο Σχήμα 3-24(γ) αναλύεται η πιο περίπλοκη από τις τρεις διαδικασίες .Το SMTP κείμενο παραγεμίζεται (συμπληρώνεται) , εάν είναι απαραίτητο, και κρυπτογραφείται .Ένα δημόσιο κλειδί αποτελεί την καλύτερη επιλογή σε αυτή την περίπτωση, γιατί εγγυάται την ταυτότητα του αποστολέα. Το κρυπτογραφημένο μήνυμα, ο κρυπτογραφημένος κώδικας ακεραιότητας μηνύματος MIC και το κρυπτογραφημένο κλειδί κρυπτογράφησης δεδομένων DEK κωδικοποιούνται όλα με χρήση εκτυπώσιμου κώδικα έτσι ώστε να περάσουν από το σύστημα ηλεκτρονικού ταχυδρομείου ως σύνηθες κείμενο. Στη συνέχεια συναλυσιδώνονται και τροφοδοτούνται στο σύστημα ηλεκτρονικού ταχυδρομείου.



(α) MIC - CLEAR διαδικασία PEM



(β) MIC - ONLY διαδικασία PEM



(γ) ΚΡΥΠΤΟΓΡΑΦΗΜΕΝΗ διαδικασία PEM

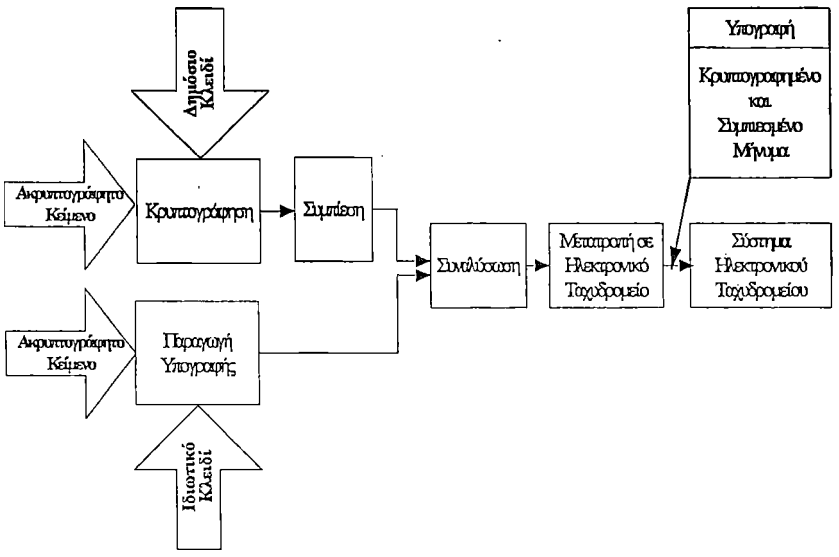
Σχήμα 3-24:Διαδικασίες PEM

3.3.2.1.3 Αρκετά Καλό Απόρρητο

Το Αρκετά Καλά Απόρρητο (Pretty Good Privacy-PGP) είναι ένα ασφαλές ταχυδρομείο, που αναπτύχθηκε από τον Phil Zimmerman, και είναι διαθέσιμο στο δημόσιο τομέα. Στο Σχήμα 3-25 φαίνονται τα διάφορα δομοστοιχεία της PGP διαδικασίας στον αποστολέα προέλευσης. Στο άκρο παραλαβής λαμβάνει χώρα η αντίστροφη διαδικασία, η οποία δε φαίνεται στο σχήμα αυτό. Πρόκειται για μία έξυπνη διαδικασία, η οποία χρησιμοποιεί διάφορα διαθέσιμα δομοστοιχεία ώστε να εκτελέσει τις λειτουργίες που χρειάζονται για τη μετάδοση ενός ασφαλούς μηνύματος , όπως είναι το ηλεκτρονικό ταχυδρομείο.

Το δομοστοιχείο παραγωγής υπογραφής χρησιμοποιεί τον αλγόριθμο MD5 για να παράγει ένα κώδικα κατακερματισμού του μηνύματος και το κρυπτογραφεί με βάση το ιδιωτικό κλειδί κρυπτογράφησης του αποστολέα, χρησιμοποιώντας τον αλγόριθμο RSA. Για την παραγωγή του κρυπτογραφημένου μηνύματος χρησιμοποιείται είτε ο αλγόριθμος RSA είτε ο IDEA. Μάλιστα, ο IDEA είναι πιο αποδοτικός από τον RSA, αλλά απαιτεί συντήρηση του κρυφού κλειδιού, σε αντίθεση με τη χρήση ενός δημόσιου κλειδιού στον RSA. Το κρυπτογραφημένο μήνυμα συμπιέζεται με εφαρμογή του αλγόριθμου ZIP. Η υπογραφή διαδέχεται αλυσιδωτά το κρυπτογραφημένο μήνυμα και στη συνέχεια μετατρέπεται σε μορφότυπο ASCII, χρησιμοποιώντας το δομοστοιχείο της Radix-64 μετατροπής, ώστε να γίνει συμβατό με το σύστημα ηλεκτρονικού ταχυδρομείου.

Το PGP είναι παρόμοιο με το κρυπτογραφημένο PEM ,αλλά διαθέτει την πρόσθετη ικανότητα συμπίεσης. Η βασική διαφορά ανάμεσα στο PGP και στο PEM είναι ο τρόπος διαχείρισης του δημόσιου κλειδιού. Στο PGP, ο τρόπος αυτός επαφίεται στον ιδιοκτήτη. Στο PEM, τυπικά η διαχείριση γίνεται από μία Αρχή Πιστοποίησης που είναι η Αρχή Πιστοποίησης Πολιτικής Διαδικτύου , (Internet Policy Certification Authority – IPCA). Πρακτικά, το PGP χρησιμοποιείται περισσότερο από το PEM. Τόσο το PGP όσο και το PEM παρέχουν περισσότερα από μία υπηρεσία ασφαλούς ταχυδρομείου, μπορούν να χρησιμοποιηθούν για την αποστολή κάθε μηνύματος ή αρχείου.



Σχήμα 3-25:Η διαδικασία PGP

3.3.2.2 Ασφάλεια Ηλεκτρονικών Συναλλαγών (SET)

3.3.2.2.1 Γενικά

Η ασφάλεια Ηλεκτρονικών Συναλλαγών (Security Electronic Transaction-SET) είναι μία κρυπτογράφηση και μια προδιαγραφή ασφάλειας σχεδιασμένη να προφυλάσσει τις συναλλαγές με πιστωτικές κάρτες στο Διαδίκτυο. Η τρέχουσα έκδοση, SETv1, προέκυψε από μία ανάγκη για πρότυπα ασφάλειας από τις MasterCard και Visa το Φεβρουάριο του 1996. Πολλές εταιρείες συμπεριελήφθησαν στην ανάπτυξη του αρχικού προτύπου,

συμπεριλαμβανομένων των IBM, Microsoft, Netscape, RSA,Terisa και Verising. Ξεκινώντας το 1996 πραγματοποιήθηκαν πολυάριθμες δοκιμασίες της ιδέας αυτής και το 1998 το πρώτο κύμα προϊόντων SET ήταν διαθέσιμο.

Η SET δεν αποτελεί από μόνη της ένα σύστημα πληρωμής. Περισσότερο πρόκειται για ένα σύνολο από πρωτόκολλα ασφάλειας και από μορφότυπα, το οποίο επιτρέπει στους χρήστες να χειρίζονται τις υπάρχουσες υποδομές πληρωμής πιστωτικών καρτών σε ένα ανοικτό δίκτυο, όπως είναι το Διαδίκτυο με ασφαλή τρόπο.Στην ουσία, η SET παρέχει τρεις υπηρεσίες:

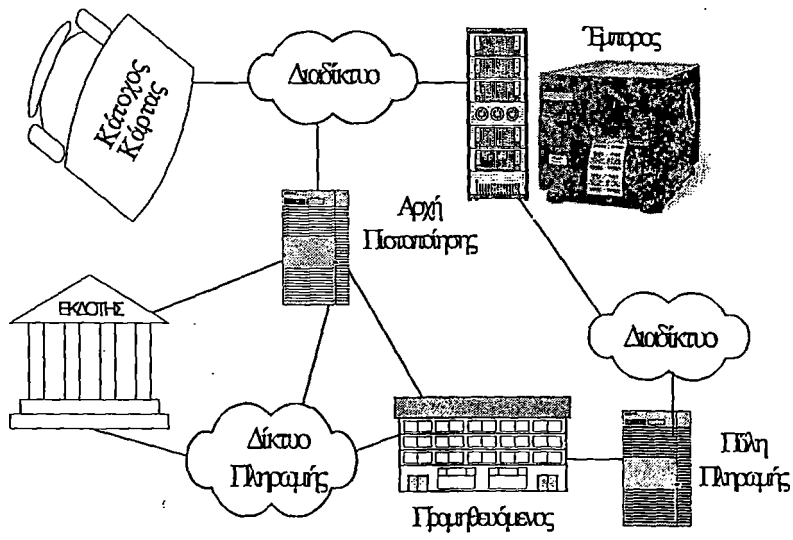
- Παρέχει ένα κανάλι ασφαλών επικοινωνιών μεταξύ όλων των μερών που εμπλέκονται σε μία συναλλαγή.
- Παρέχει εμπίστευση κάνοντας χρήση των X.509v3 ψηφιακών πιστοποιητικών.
- Εξασφαλίζει το απόρρητο, γιατί η πληροφορία παρέχεται μόνο στα μέρη που συνδιαλέγονται μόνο όταν και όπου είναι αυτό απαραίτητο.

Το Σχήμα 3-26 δείχνει τους συμμετέχοντες σε ένα σύστημα SET, που είναι:

- **Κάτοχος Κάρτας**: Σε ένα ηλεκτρονικό περιβάλλον ,οι καταναλωτές και οι εταιρικοί αγοραστές αλληλεπιδρούν με τους εμπόρους από προσωπικούς υπολογιστές μέσω του Διαδικτύου. Ένας κάτοχος κάρτας είναι ένας εξουσιοδοτημένος κάτοχος μιας κάρτας πληρωμών (για παράδειγμα οι κάρτες MasterCard και Visa) , η οποία έχει εκδοθεί από κάποιον εκδότη.
- **Έμπορος**: Ο έμπορος είναι είτε ένα πρόσωπο ή ένας οργανισμός που έχει προϊόντα και υπηρεσίες προς πώληση σε έναν κάτοχο κάρτας. Τυπικά , αυτά τα προϊόντα και οι υπηρεσίες προσφέρονται μέσω μιας ιστοσελίδας του παγκόσμιου ιστού ή μέσω ηλεκτρονικού ταχυδρομείου. Τελικά, ένας έμπορος που αποδέχεται κάρτες πληρωμών πρέπει να έχει κάποια σχέση με έναν προμηθευόμενο.
- **Εκδότης** : Είναι ένα οικονομικό ίδρυμα, όπως μία τράπεζα, που προμηθεύει τον κάτοχο κάρτας με μια κάρτα πληρωμών. Τυπικά οι λογαριασμοί ανοίγονται προσωπικά ή μέσω ηλεκτρονικού μηνύματος. Τελικά, ο εκδότης είναι ο υπεύθυνος για την πληρωμή των χρεών του κατόχου της κάρτας.
- **Προμηθευόμενος** : Πρόκειται για ένα οικονομικό ίδρυμα που εγκαθιδρύει ένα λογαριασμό με κάποιο έμπορο και επεξεργάζεται εξουσιοδοτήσεις καρτών πληρωμών καθώς και τις πληρωμές. Οι έμποροι συνήθως αποδέχονται περισσότερες από μία εμπορικές επωνυμίες πιστωτικών καρτών αλλά δε θέλουν να πραγματεύονται πολλαπλούς συσχετισμούς τραπεζικών καρτών ή με πολλαπλούς μεμονωμένους εκδότες. Ο προμηθευόμενος παρέχει στον εμπόρου την εξουσιοδότηση ότι ένας δεδομένος λογαριασμός κάρτας είναι ενεργός και ότι η προτεινόμενη αγορά δεν υπερβαίνει το πιστωτικό όριο. Επιπλέον, ο προμηθευόμενος παρέχει την ηλεκτρονική μεταφορά των πληρωμών στο λογαριασμό του εμπόρου. Στη συνέχεια, ο προμηθευόμενος αποζημιώνεται από τον εκδότη για κάποιου είδους πληρωμές δικτύου με ηλεκτρονική μεταφορά κεφαλαίων.
- **Πύλη Πληρωμής**: Είναι μία λειτουργία, η οποία εκτελείται από τον προμηθευόμενο ή από μία τρίτη προσδιορισμένη οντότητα, που επεξεργάζεται μηνύματα πληρωμής εμπόρου. Η πύλη πληρωμής αποτελεί μια διεπαφή ανάμεσα στην ασφάλεια ηλεκτρονικών συναλλαγών SET και στα υπάρχοντα δίκτυα πληρωμής τραπεζικών καρτών για εξουσιοδότηση και λειτουργίες πληρωμής. Ο έμπορος ανταλλάσσει στο Διαδίκτυο SET μηνύματα με την πύλη πληρωμής , ενώ η πύλη πληρωμής έχει κάποια άμεση σύνδεση ή σύνδεση δικτύου με το σύστημα επεξεργασίας οικονομικών του προμηθευόμενου.
- **Αρχή Πιστοποίησης**: Πρόκειται για μία οντότητα διαπιστευμένη να εκδίδει X509v3 πιστοποιητικά δημόσιων κλειδιών για κατόχους καρτών, εμπόρους και πύλες πληρωμής. Η επιτυχία του SET θα εξαρτηθεί από την ύπαρξη υποδομής αρχής πιστοποίησης διαθέσιμης για αυτό το σκοπό. Η ιεραρχία των αρχών πιστοποίησης χρησιμοποιείται ώστε οι συμμετέχοντες να μη χρειάζεται να πιστοποιούνται απευθείας από μία θεμελιώδη αρχή.

Θα περιγράψουμε, τώρα, συνοπτικά την ακολουθία των γεγονότων, τα οποία απαιτούνται για μία ηλεκτρονική συναλλαγή. Στη συνέχεια θα αναλύσουμε μερικές λεπτομέρειες κρυπτογράφησης.

1. **Ο πελάτης ανοίγει έναν λογαριασμό** .Ο πελάτης αποκτά ένα λογαριασμό πιστωτικής κάρτας ,όπως είναι η MasterCard και η Visa, σε μία τράπεζα η οποία υποστηρίζει ηλεκτρονική πληρωμή και ασφαλείς ηλεκτρονικές συναλλαγές SET.
2. **Ο πελάτης αποκτά ένα πιστοποιητικό.** Ύστερα από κατάλληλη εξακρίβωση της ταυτότητας του , ο πελάτης λαμβάνει ένα X509v3 ψηφιακό πιστοποιητικό ,το οποίο υπογράφεται από την τράπεζα. Το πιστοποιητικό επαληθεύει το RSA δημόσιο κλειδί του πελάτη καθώς και την ημερομηνία λήξης αυτού. Επιπλέον, εγκαθιστά μία σχέση ,εγγυημένη από την τράπεζα , ανάμεσα στο ζευγάρι κλειδιών του πελάτη και στην πιστωτική του/της κάρτας .
3. **Οι έμποροι έχουν τα δικά τους πιστοποιητικά.** Ένας έμπορος που αποδέχεται συγκεκριμένη «εμπορική επωνυμία» τράπεζας, πρέπει να έχει στην κατοχή του δύο πιστοποιητικά για τα δύο δημόσια κλειδιά που έχει στην ιδιοκτησία του: ένα για την υπογραφή μηνυμάτων και ένα δεύτερο για την ανταλλαγή κλειδιών. Ο έμπορος χρειάζεται ακόμη ένα αντίγραφο του πιστοποιητικού δημόσιου κλειδιού της πύλης πληρωμής.
4. **Ο πελάτης τοποθετεί μία εντολή αγοράς.** Αυτή η διαδικασία μπορεί να περιλαμβάνει την περιήγηση του πελάτη στην ιστοσελίδα του εμπόρου, στον παγκόσμιο ιστό, προκειμένου να επιλέξει προϊόντα και να καθορίσει το αντίτιμο. Έπειτα , ο πελάτης στέλνει μια λίστα από αντικείμενα τα οποία επιθυμεί να αγοράσει από τον έμπορο, κάνοντας χρήση της πιστωτικής του κάρτας. Ο έμπορος με τη σειρά του επιστρέφει στον πελάτη μία φόρμα παραγγελίας, η οποία περιέχει τη λίστα των αντικειμένων, τις τιμές τους, το συνολικό κόστος και έναν αριθμό παραγγελίας.
5. **Γίνεται επαλήθευση του εμπόρου.** Μαζί με τη φόρμα παραγγελίας, ο έμπορος αποστέλλει ένα αντίγραφο του δικού του πιστοποιητικού ώστε ο πελάτης να μπορεί να εξακριβώσει ότι διαπραγματεύεται με ένα έγκυρο κατάστημα.
6. **Η παραγγελία και η πληρωμή αποστέλλονται.** Ο πελάτης στέλνει την εντολή αγοράς και την πληροφορία πληρωμής στον έμπορο, μαζί με το πιστοποιητικό πελάτη. Η εντολή αγοράς επιβεβαιώνει την αγορά των αντικειμένων που περιλαμβάνονται στη φόρμα εντολής. Η πληρωμή περιλαμβάνει λεπτομέρειες σχετικά με την πιστωτική κάρτα . Η πληροφορία πληρωμής κρυπτογραφείται με τέτοιο τρόπο ώστε να μην είναι δυνατό να αναγνωστεί από τον έμπορο. Το πιστοποιητικό πελάτη δίνει τη δυνατότητα στον έμπορο να επαληθεύσει ποιος είναι ο πελάτης.
7. **Ο έμπορος ζητά εξουσιοδότηση πληρωμής.** Ο έμπορος στέλνει την πληροφορία πληρωμής στην πύλη πληρωμής, αιτούμενος εξουσιοδότηση σχετικά με την επάρκεια του διαθέσιμου πιστωτικού ορίου του πελάτη για τη συγκεκριμένη αγορά.
8. **Ο έμπορος επιβεβαιώνει την παραγγελία.** Ο έμπορος στέλνει επιβεβαίωση της εντολής αγοράς του πελάτη.
9. **Ο έμπορος παρέχει τα αγαθά ή τις υπηρεσίες.** Ο έμπορος στέλνει στον πελάτη τα αγαθά ή του παρέχει τις υπηρεσίες που αυτός έχει ζητήσει.
10. **Ο έμπορος ζητά την πληρωμή.** Αυτή η αίτηση αποστέλλεται στην πύλη πληρωμής ,η οποία ασχολείται με τη συνολική διαδικασία πληρωμής.



Σχήμα 3-26:Στοιχεία Ασφαλούς Ηλεκτρονικού Εμπορίου

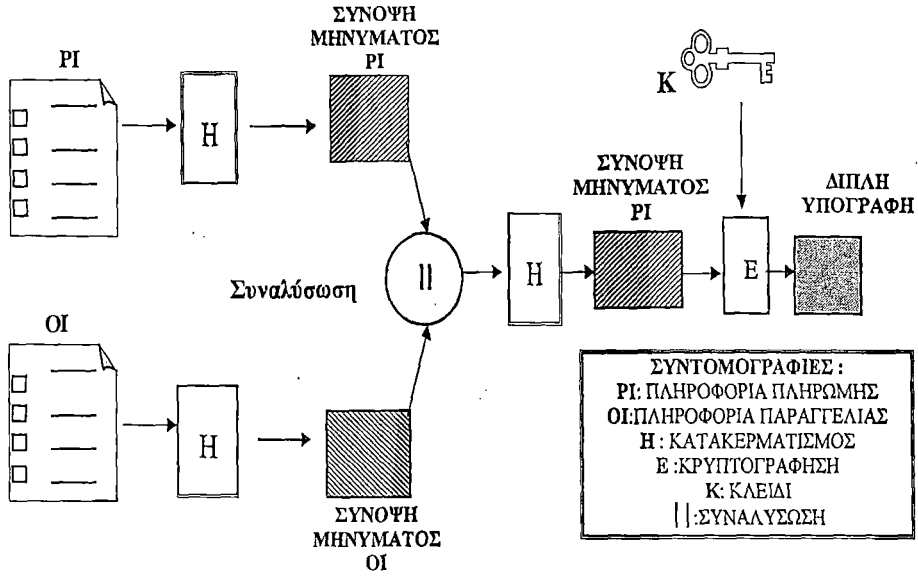
3.3.2.2.2 Διπλή Υπογραφή

Πριν αναλύσουμε τις συναλλαγές SET αναφέρουμε μια καινοτομία που εισήχθηκε σε αυτή της διπλής υπογραφής (Dual signature).

Ο σκοπός της Διπλής Υπογραφής είναι η σύνδεση δύο μηνυμάτων τα οποία απευθύνονται σε δύο διαφορετικούς παραλήπτες. Σε αυτή την κατηγορία μηνυμάτων συγκαταλέγεται και η περίπτωση του πελάτη ο οποίος θέλει να στείλει την πληροφορία παραγγελίας (Order Information-OI) στον έμπορο και την πληροφορία πληρωμής (Payment Information-PI) στην τράπεζα. Ο έμπορος δε χρειάζεται να γνωρίζει τον αριθμό της πιστωτικής κάρτας του πελάτη, ενώ η τράπεζα δε χρειάζεται να γνωρίζει τις λεπτομέρειες της παραγγελίας του πελάτη. Διατηρώντας τα αντικείμενα αυτά, δηλαδή την πληροφορία παραγγελίας και τη πληροφορία πληρωμής, χωριστά ο πελάτης αποκτά πρόσθετη προστασία όσον αφορά στη διαφύλαξη του απορρήτου του. Ωστόσο πρέπει τα αντικείμενα αυτά να μπορούν να συνδέονται με κάποιο τρόπο , ο οποίος θα μπορεί να χρησιμοποιηθεί για την επίλυση διαφορών, σε περίπτωση που αυτές παρουσιαστούν. Η σύνδεση αυτή χρειάζεται έτσι ώστε ο πελάτης να μπορεί να αποδείξει ότι κάποια πληροφορία πληρωμής αφορούσε συγκεκριμένη παραγγελία και όχι κάποια άλλα αγαθά ή υπηρεσίες που πιθανώς του απεστάλησαν.

Για να γίνει κατανοητή η αναγκαιότητα της αυτής της σύνδεσης, ας υποθέσουμε ότι ένας πελάτης στέλνει στον έμπορο δύο μηνύματα: μία υπογεγραμμένη πληροφορία παραγγελίας OI και μία υπογεγραμμένη πληροφορία πληρωμής PI και ότι ο έμπορος προωθεί την υπογεγραμμένη πληροφορία πληρωμής PI στην τράπεζα. Εάν ο έμπορος μπορεί να πάρει μία δεύτερη πληροφορία παραγγελίας OI από τον ίδιο πελάτη, θα μπορεί να ισχυριστεί ότι αυτή, η δεύτερη πληροφορία παραγγελίας, και όχι η πρώτη, συνδέεται με την πληροφορία πληρωμής. Η σύνδεση των δύο μηνυμάτων, που περιγράψαμε παραπάνω, εμποδίζει τέτοια δράση εκ μέρους του εμπόρου.

Στο Σχήμα 3-27 φαίνεται η χρήση της διπλής υπογραφής ώστε να πληρείται η απαίτηση της προηγούμενης παραγράφου. Ο πελάτης λαμβάνει τον κατακερματισμό, που χρησιμοποιεί τον αλγόριθμο SHA–1, της πληροφορίας πληρωμής PI και τον κατακερματισμό της πληροφορίας παραγγελίας OI. Οι κατακερματισμοί των δύο αυτών μηνυμάτων διαδέχονται αλυσυδωτά ο ένας τον άλλο και τελικά αυτό που λαμβάνεται είναι ο κατακερματισμός του αποτελέσματος, το οποίο προκύπτει από τη συναλύσωση αυτή. Τελικά ο πελάτης κρυπτογραφεί τον τελικό κατακερματισμό με το δικό του /της ιδιωτικό κλειδί υπογραφής δημιουργώντας τη διπλή υπογραφή.



Σχήμα 3-27:Κατασκευή Διπλής Υπογραφής

3.3.2.2.3 Αίτηση Αγοράς

Στο SET υπάρχουν τρεις τύποι συναλλαγών.

- Αίτηση Αγοράς (Purchase Request)
- Εξουσιοδότηση Αγοράς (Payment Authorisation)
- Λήψη Πληρωμής (Payment capture)

Εμείς εδώ θα περιοριστούμε σε ένα μόνο από αυτούς που είναι βασικός στην Αίτηση Αγοράς (Purchase Request). Πριν ξεκινήσει η ανταλλαγή της Αίτησης Αγοράς, ο κάτοχος κάρτας έχει συμπληρώσει το διαφύλλισμα (την περιήγηση στον ιστό), την επιλογή και την παραγγελία. Το τέλος της προκαταρκτικής αυτής φάσης λαμβάνει χώρα τη στιγμή που ο έμπορος στέλνει μία ολοκληρωμένη φόρμα παραγγελίας στον πελάτη. Όλα αυτά συμβαίνουν χωρίς τη χρήση του SET .

Η ανταλλαγή της Αίτησης Αγοράς αποτελείται από τέσσερα μηνύματα: **Αίτηση Έναρξης , Απόκριση Έναρξης , Αίτηση Αγοράς** και **Απόκριση Αγοράς**.

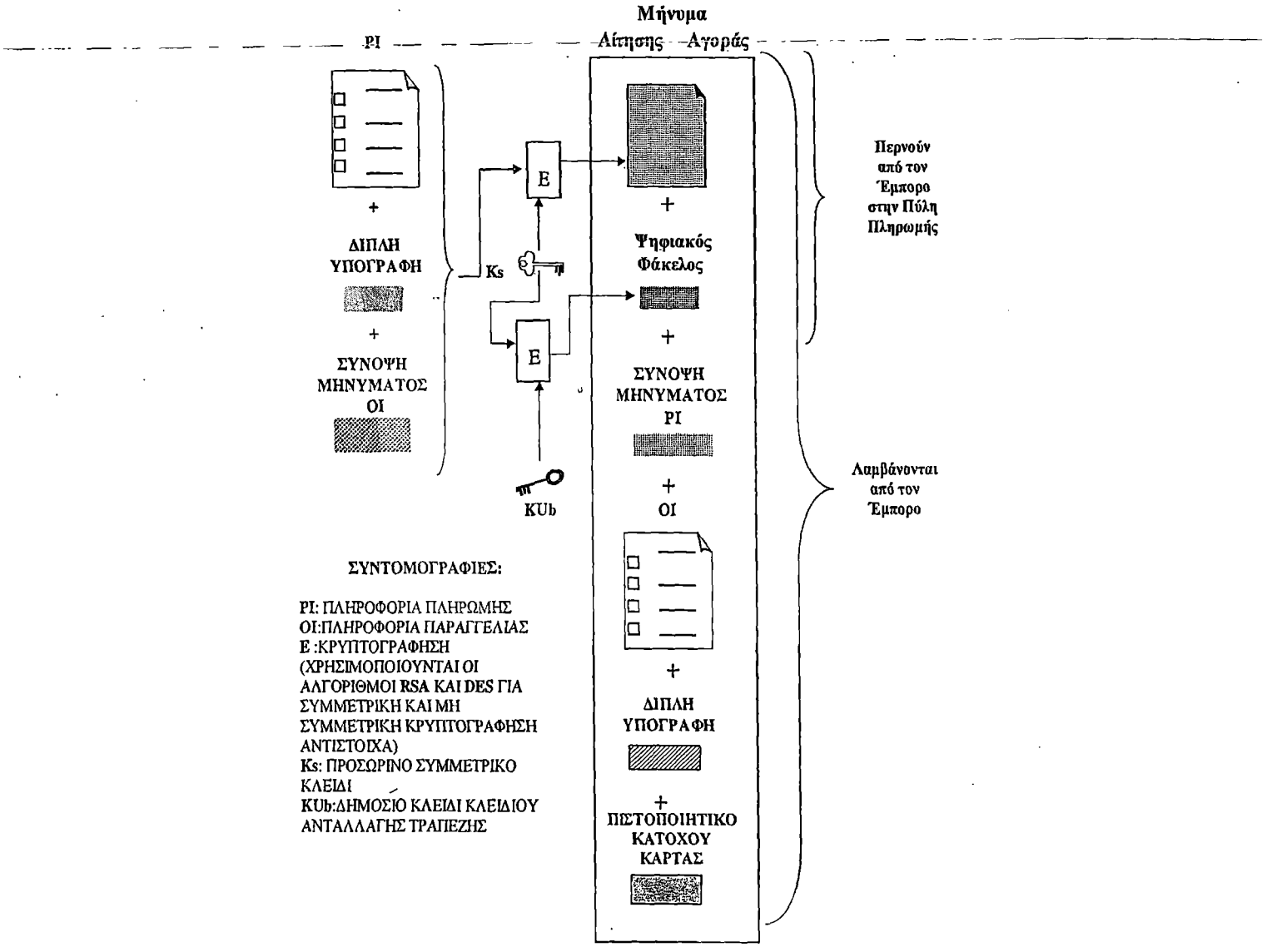
Για να μπορέσει ο κάτοχος κάρτας να στείλει μηνύματα SET στον έμπορο, πρέπει να αντιγράψει τα πιστοποιητικά του εμπόρου και της πύλης πληρωμής. Ο πελάτης ζητά τα πιστοποιητικά ,που έχουν αποσταλεί στον έμπορο, στο μήνυμα Αίτησης Έναρξης . Στο μήνυμα αυτό περιλαμβάνεται η εμπορική επωνυμία της πιστωτικής κάρτας που χρησιμοποιεί ο πελάτης καθώς και η ταυτότητα (ID) η οποία έχει εκχωρηθεί σε αυτό το ζευγάρι αίτησης / απόκρισης από τον πελάτη και μία φράση που χρησιμοποιείται για να επιβεβαιώσει την επικαιρότητα.

Ο έμπορος παράγει μία απόκριση και την υπογράφει με το δικό της ιδιωτικό κλειδί υπογραφής. Η απόκριση περιλαμβάνει κάποια φράση για την περίσταση από τον πελάτη, άλλη φράση για την περίσταση για τον πελάτη, η οποία θα επιστραφεί στο επόμενο μήνυμα και μία ταυτότητα συναλλαγής για τη συναλλαγή αγοράς. Επιπρόσθετα στην υπογεγραμμένη απόκριση, το μήνυμα της **Απόκρισης Έναρξης** περιλαμβάνει το πιστοποιητικό της υπογραφής του εμπόρου και το πιστοποιητικό του κλειδιού ανταλλαγής της πύλης πληρωμής.

Ο έμπορος δημιουργεί μία απόκριση Έναρξης και την υπογράφει με το κλειδί ιδιωτικής υπογραφής.

Ο κάτοχος κάρτας επαληθεύει τα πιστοποιητικά του εμπόρου και της πύλης πληρωμής, μέσω των δικών τους CA υπογραφών, και έπειτα δημιουργεί τα μηνύματα OI και PI .Η ταυτότητα συναλλαγής ID που εκχωρείται από τον έμπορο τοποθετείται τόσο στο μήνυμα OI όσο και στο μήνυμα PI. Το μήνυμα OI δεν περιλαμβάνει εμφανή δεδομένα παραγγελίας όπως είναι ο αριθμός ή η τιμή των αντικειμένων. Αντίθετα , περιλαμβάνει μία αναφορά παραγγελίας, η οποία παράγεται κατά την ανταλλαγή ανάμεσα στον έμπορο και στον πελάτη κατά τη διάρκεια της φάσης αγοράς, πριν από το πρώτο SET μήνυμα.

Στη συνέχεια, όπως φαίνεται στο Σχήμα 3-28, ο κάτοχος της κάρτας ετοιμάζει το μήνυμα **Αίτησης Αγοράς**. Για το σκοπό αυτό, ο κάτοχος κάρτας παράγει ένα μίας χρήσης συμμετρικό κλειδί κρυπτογράφησης,**Ks**.



Σχήμα 3-28:Ο Κάτοχος Κάρτας στέλνει μια Αίτηση Αγοράς

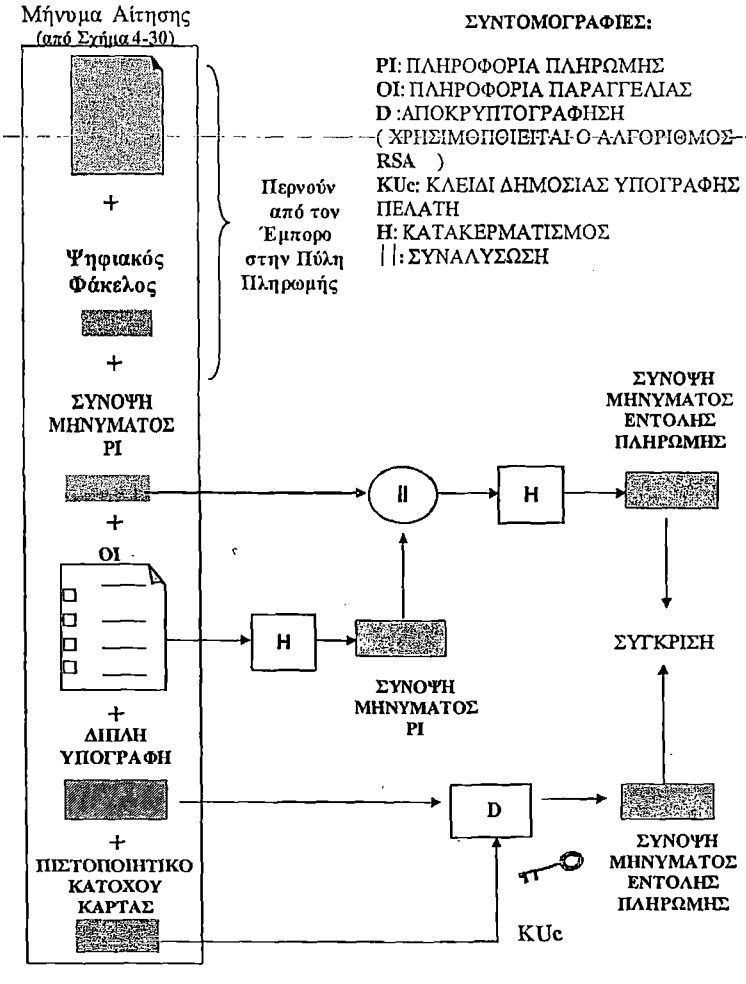
Ο έμπορος , μόλις λάβει το μήνυμα Αίτησης Αγοράς από τον πελάτη, προβαίνει στις ακόλουθες ενέργειες (Σχήμα 3-29):

1. Επαληθεύει τα πιστοποιητικά του κατόχου κάρτας μέσω των δικών του CA υπογραφών.

2. Επαληθεύει τη διπλή υπογραφή χρησιμοποιώντας το δημόσιο κλειδί υπογραφής του πελάτη. Με αυτό τον τρόπο , επιβεβαιώνεται ότι η εντολή του πελάτη δεν έχει παραποιηθεί κατά τη μεταβίβαση και ότι υπογράφηκε χρησιμοποιώντας το ιδιωτικό κλειδί υπογραφής του κατόχου κάρτας.

3. Επεξεργάζεται την εντολή και προωθεί την πληροφορία πληρωμής στην πύλη πληρωμής για εξουσιοδότηση.

4. Αποστέλλει ένα μήνυμα **Απόκρισης Αγοράς** στον κάτοχο της κάρτας.



Σχήμα 3-29:Ο έμπορος επαληθεύει την αίτηση αγοράς του Πελάτη.

4. ΔΙΑΧΕΙΡΙΣΗ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΩΝ TCP / IP

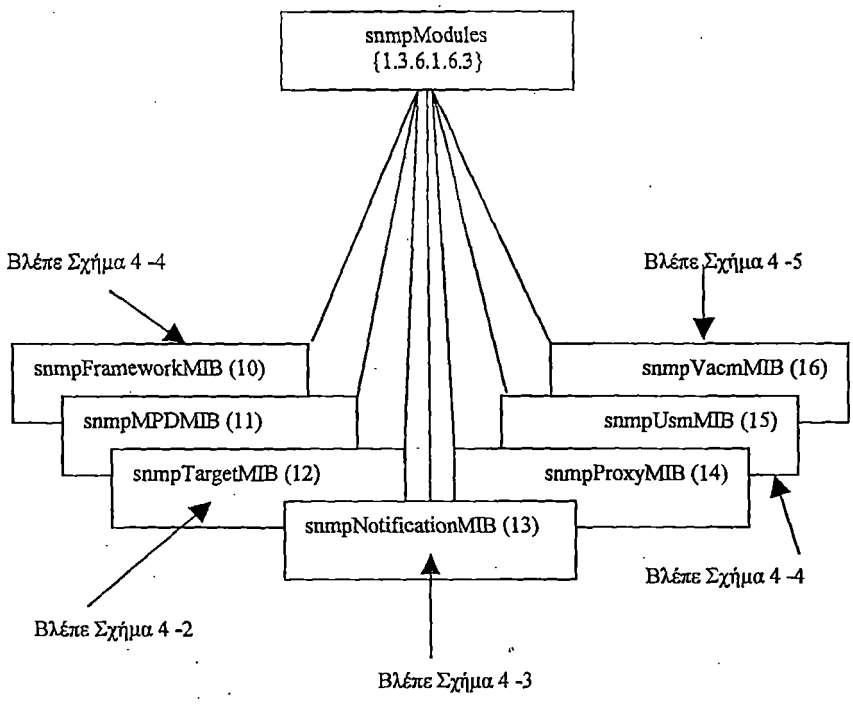
4.1 Διαχείριση Ασφάλειας σε Δίκτυα TCP/IP

Σε αυτό το κεφάλαιο θα εξετάσουμε τη Διαχείριση Ασφάλειας του πρωτοκόλλου SNMP (ενότητα 4.1.1) καθώς και τη Διαχείριση Ελέγχου Πρόσβασης στην MIB (ενότητα 4.2.2). Εκείνο , λοιπόν , που πρέπει να προσδιορίσουμε σε αμφότερες τις περιπτώσεις είναι τα δένδρα της MIB (βλέπε Σχήμα 4-1 και Σχήμα 4-5)

4.1.1 Διαχείριση Ασφάλειας του Πρωτοκόλλου SNMP

4.1.1.1 Η Βάση Πληροφοριών Διαχείρισης του SNMPv3

Στο Σχήμα 4-1 και κάτω από τον κόμβο snmpModules{1.3.6.1.6.3} υπάρχουν τα υπό διαχείριση αντικείμενα για το πρωτόκολλο διαχείρισης snmpv2. Στο Σχήμα 4-2 δίδονται πρόσθετα υπό διαχείριση αντικείμενα που υπάρχουν σε μία επόμενη έκδοση του πρωτοκόλλου, την snmpv3.

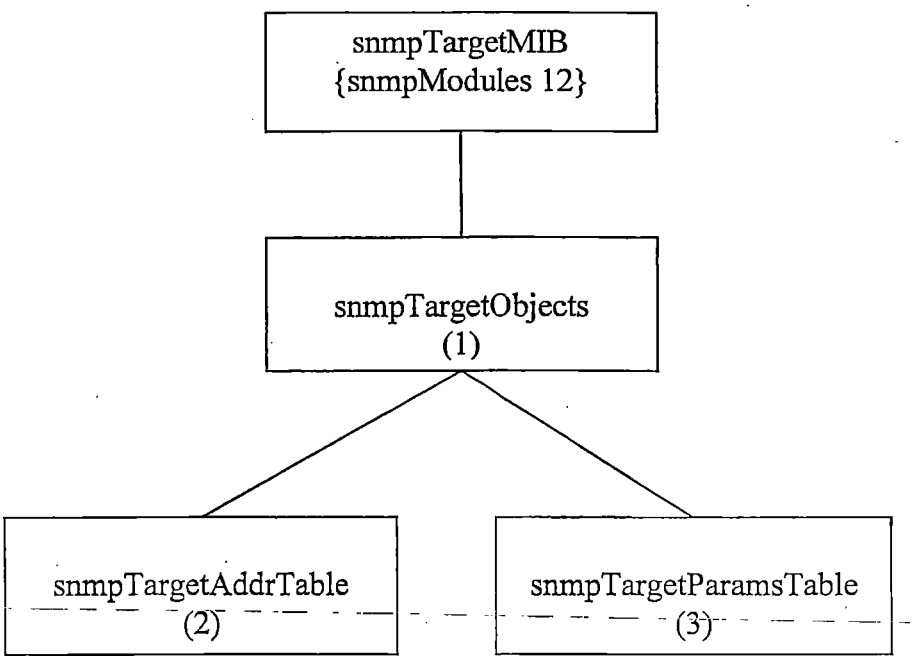


Σχήμα 4-1: SNMPv3 MIB

Υπάρχουν επτά νέες ομάδες στην MIB: η snmpFrameworkMIB (κόμβος 10 κάτω από τον snmpModules) περιγράφει την αρχιτεκτονική διαχείρισης του SNMP. Η ομάδα snmpMPDMIB της MIB (κόμβος 11) προσδιορίζει αντικείμενα στα υποσυστήματα επεξεργασίας και αποστολής μηνύματος.

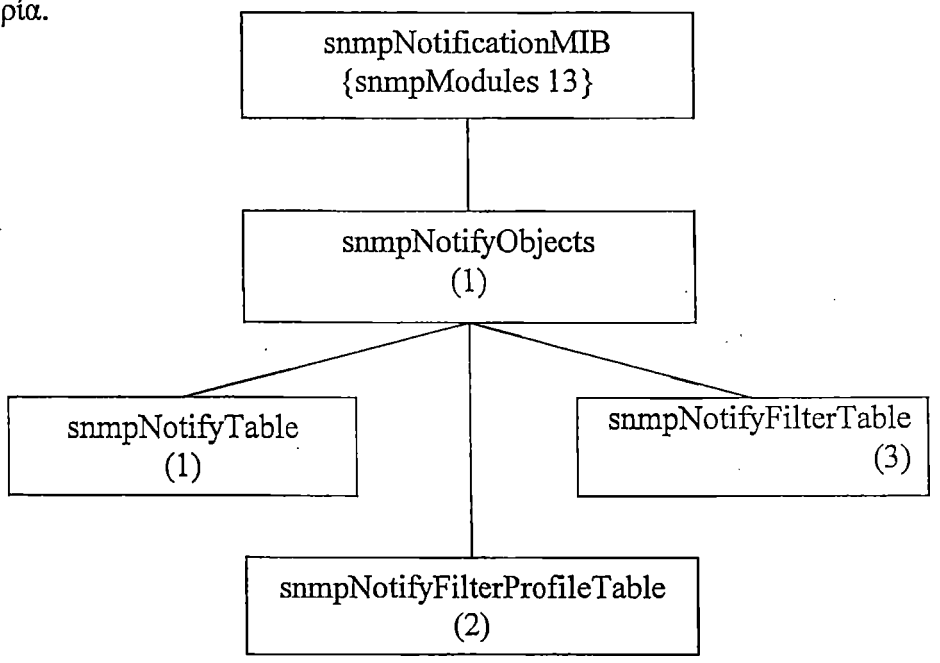
Τρεις ομάδες είναι ορισμένες κάτω από την snmpModules για εφαρμογές: η snmpTargetMIB (κόμβος 12), η snmpNotificationMIB (κόμβος 13) και η snmpProxyMIB (κόμβος 14). Οι πρώτες δύο χρησιμοποιούνται για τη γεννήτρια ειδοποιήσεων. Η snmpTargetMIB περιέχει δύο πίνακες που αφορούν συγκεκριμένα τη δημιουργία των ειδοποιήσεων και φαίνονται στο Σχήμα 4-2. Ο πρώτος πίνακας, ο snmpTargetAddrTable στην ομάδα snmpTargetObjects περιέχει τις διευθύνσεις που χρησιμοποιούνται στη δημιουργία μηνυμάτων του SNMP. Αυτά είναι ομαδοποιημένα στον Πίνακα Ειδοποιήσεων του SNMP και αναγνωρίζονται από ετικέτες κάτω από το SNMP ειδοποιήσεων της MIB. Ο δεύτερος πίνακας στην ομάδα snmpTargetObjects είναι ο πίνακας snmpTargetParamsTable. Η διαδρομή σ' αυτόν τον πίνακα είναι μέσω του αντικειμένου στήλης snmpTargetAddrParams στο

snmpTargetAddrTable. Περιέχει τις παραμέτρους ασφάλειας για την επαλήθευση και το απόρρητο.



Σχήμα 4-2:Πίνακες Διευθύνσεων και Παραμέτρων των Προορισμών

Η snmpNotificationMIB που απεικονίζεται στο Σχήμα 4-3 πραγματεύεται αντικείμενα της MIB που αφορούν τη δημιουργία ειδοποιήσεων. Οι τρεις πίνακες σ' αυτήν την ομάδα είναι ο πίνακας ειδοποίησεων, ο πίνακας που αφορά το προφίλ του φίλτρου των ειδοποιήσεων και ο πίνακας του φίλτρου των ειδοποιήσεων. Βρίσκονται κάτω από τον κόμβο snmpNotifyObjects. Ο πίνακας ειδοποιήσεων του SNMP, snmpNotifyTable, περιλαμβάνει ομάδες αποδεκτών διαχείρισης που πρέπει να λαμβάνουν ειδοποιήσεις καθώς και το είδος της ειδοποίησης που πρέπει να σταλεί. Οι διευθύνσεις στο «Παράμετροι Διεύθυνσης Στόχου» του SNMP που πρόκειται να επιλεγούν βρίσκονται σ' αυτόν τον πίνακα. Η ομάδα του Πίνακα του Προφίλ του φίλτρου των Ειδοποιήσεων snmpNotifyFilterProfileTable χρησιμοποιείται για να συσχετίσει το προφίλ του φίλτρου της ειδοποίησης με ένα συγκεκριμένο σύνολο από παραμέτρους που αφορούν τον αποδέκτη. Η ομάδα του Πίνακα των Φίλτρων των Ειδοποιήσεων, snmpNotifyFilterTable, περιέχει πίνακες με τα προφίλ των αποδεκτών. Το προφίλ του αποδέκτη καθορίζει αν κάποιος συγκεκριμένος αποδέκτης πρέπει να λάβει συγκεκριμένη πληροφορία.



Σχήμα 4-3:Πίνακες ειδοποιήσεων της SNMP

Η snmpProxyMIB (κόμβος 14 στο Σχήμα 4-1) αφορά αντικείμενα σε εφαρμογές που προωθούνται μέσω του πληρεξούσιου, όπως ο πληρεξούσιος εξυπηρετητής του SNMPv2. Περιέχει έναν πίνακα μεταφραστικών παραμέτρων που χρησιμοποιούνται από την εφαρμογή του πληρεξούσιου προωθητή για την προώθηση μηνυμάτων του SNMP.

Τα αντικείμενα του SNMP που αφορούν τον τύπο ασφάλειας που βασίζεται στο χρήστη, καθορίζονται στην κλάση snmpUsmMIB (κόμβος 15 του Σχήματος 4-1). Τέλος, τα αντικείμενα για τον έλεγχο πρόσβασης στην SNMP MIB βάσει της θέασης, καθορίζονται στην κλάση snmpVacmMIB (κόμβος 16 στο Σχήμα 4-1).

4.1.1.2 Διαχείριση Ασφάλειας του Πρωτοκόλλου SNMPv3

Οι παράμετροι ασφάλειας που χρησιμοποιούνται στο μοντέλο ασφάλειας απεικονίζονταν στο Σχήμα. Ο πίνακας 4-1 απαριθμεί τις παραμέτρους και τα αντίστοιχα αντικείμενα του SNMPv3 της MIB.

Παράμετροι Ασφάλειας	**USM ομάδες αντικειμένων χρήστη**
msgAuthoritativeEngineID	snmpEngineID (κάτω από την ομάδα snmpEngine)
msgAuthoritativeEngineBoots	snmpEngineBoots (κάτω από την snmpEngine)
msgAuthoritativeEngineTime	snmpEngineTime (κάτω από την snmpEngine)
msgUserName	usmUserName (στον usmUserTable)
msgAuthenticationParameters	usmUserAuthProtocol (στον usmUserTable)
msgPrivacyParameters	usmUserPrivProtocol (στον usmUserTable)

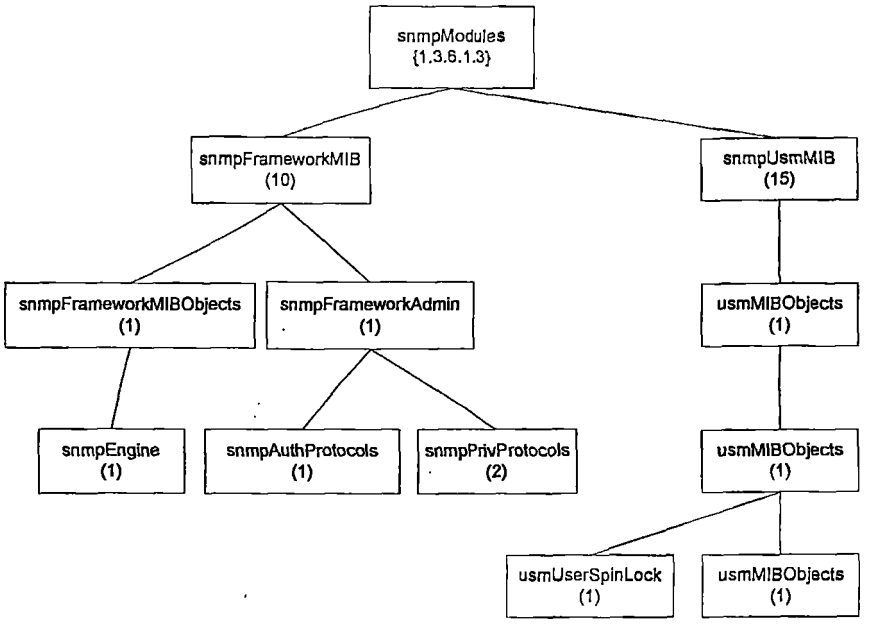
Πίνακας 4-1:Παράμετροι ασφάλειας και τα αντίστοιχα αντικείμενα της MIB

Η θέση των σχετικών αντικειμένων της MIB που σχετίζονται με τις παραμέτρους ασφάλειας ανήκει στις δύο κλάσεις snmpFrameworkMIB και snmpUsmMIB, κάτω από την snmpModules (βλέπε Σχήμα 4-1). Οι λεπτομέρειες των θέσεων των αντικειμένων στη MIB παρουσιάζονται στο Σχήμα 4-4.

Έχουμε ήδη αναφερθεί στις τρεις πρώτες παραμέτρους του Πίνακα 4-1, οι οποίες σχετίζονται με την ταυτότητα της μηχανής, τον αριθμό των εκκινήσεων (boots) και το χρόνο από την τελευταία εκκίνηση. Βρίσκονται στην ομάδα snmpEngine όπως φαίνεται στο Σχήμα 4-4.Οι τελευταίες τρεις παράμετροι στον πίνακα(msgUserName, msgAuthenticationParamaters και msgPrivacyParamaters) εντάσσονται στο usmUserTable στην ομάδα usmUser όπως απεικονίζεται στο Σχήμα 4-4.

Η τέταρτη παράμετρος είναι ο χρήστης (εντολέας) εκ μέρους του οποίου ανταλλάσσεται το μήνυμα. Οι παράμετροι επαλήθευσης προσδιορίζονται από το αντικείμενο του πρωτοκόλλου επαλήθευσης στην usmUserTable. Η usmUserTable περιγράφει τους χρήστες που έχουν διαμορφωθεί στη μηχανή του SNMP και τις παραμέτρους επαλήθευσης σύμφωνα με τον τύπο του πρωτοκόλλου επαλήθευσης που χρησιμοποιείται. Ομοίως, οι παράμετροι απορρήτου περιγράφουν τον τύπο του πρωτοκόλλου απορρήτου που χρησιμοποιείται.

Η usmUserSpinLock είναι μία συμβουλευτική κλειδαριά που χρησιμοποιείται από τις εφαρμογές της SNMP γεννήτριας εντολών για να συντονίζει τη χρήση της λειτουργίας set για τη δημιουργία ή την τροποποίηση μυστικών στη usmUserTable.

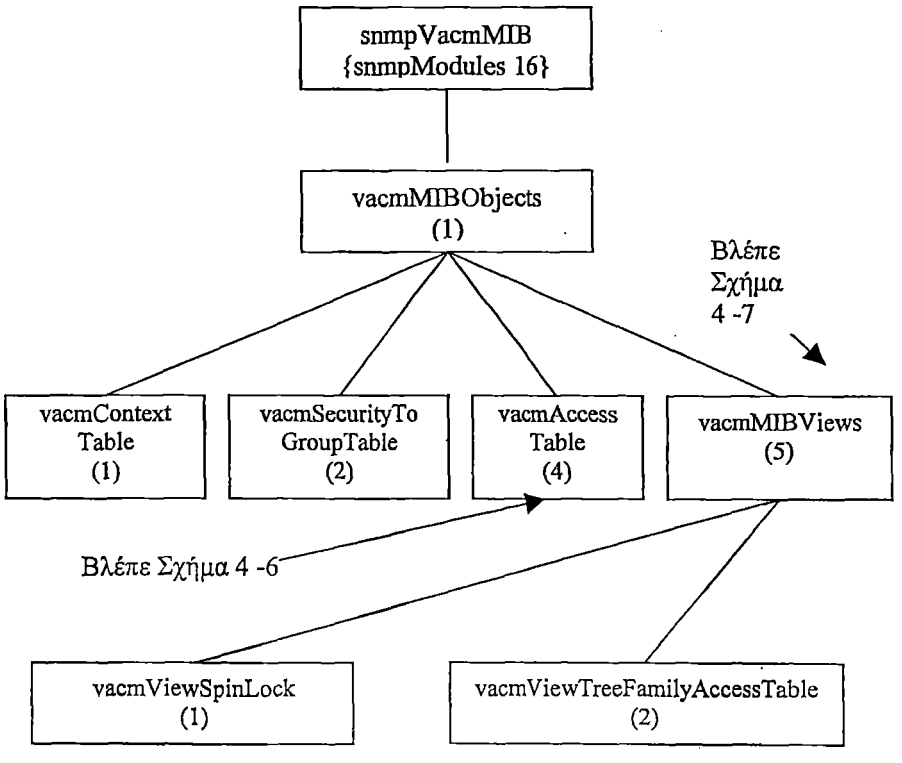


Σχήμα 4-4:Αντικείμενα της SNMPv3 MIB για παραμέτρους ασφάλειας

4.1.2 Διαχείριση Ελέγχου Πρόσβασης VACM

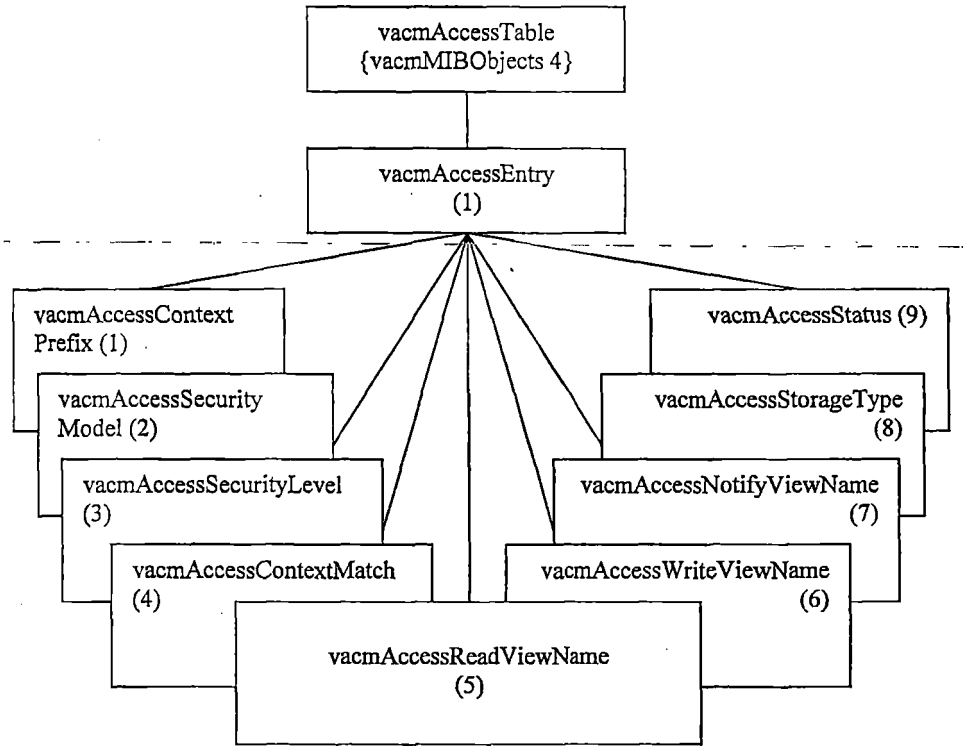
Οι διεργασίες στη VACM χρησιμοποιούν τους πίνακες για να εκτελέσουν τις λειτουργίες που αναφέρθηκαν. Μία VACM MIB έχει καθοριστεί προσδιορίζοντας τα προσφάτως δημιουργηθέντα αντικείμενα, όπως απεικονίζεται στο Σχήμα 4-5. Η snmpVacmMIB βρίσκεται έναν κόμβο κάτω από την snmpModules (βλέπε Σχήμα 4-5). Οι τρεις πίνακες που καθορίζουν την ομάδα (vacmSecurityToGroup Table), το πλαίσιο (vacmContext Table) και την πρόσβαση (vacmAccess Table), στο Σχήμα 4-6 είναι κόμβοι κάτω από τον vacmMIBObjects, ο οποίος είναι ένας κόμβος που βρίσκεται κάτω από τον κόμβο snmpVacmMIB.

Η vacmContextTable είναι μια λίστα από vacmContextNames. Το vacmSecurityToGroupTable περιέχει τα αντικείμενα vacmSecurityModel και vacmSecurityName καθώς επίσης και δείκτες που χρησιμοποιούνται για την ανάκτηση του vacmGroupName.



Σχήμα 4-5:Η VACM MIB

Ο Πίνακας Πρόσβασης του VACM, που φαίνεται στο Σχήμα 4-6, χρησιμοποιείται για να καθορίσει την επιτρεπόμενη πρόσβαση και το viewName. Περιλαμβάνει το vacmGroupName από το vacmSecurityToGroupTable σαν Έναν από τους δείκτες. Οι άλλοι τρεις δείκτες από αυτόν τον πίνακα είναι οι vacmAccessContextPrefix, vacmAccessSecurityModel και η vacmAccessSecurityLevel. Οι ViewName που εκπροσωπούν τις τρεις θεάσεις vacmAccessReadViewName, vacmAccessWriteViewName και vacmAccessNotifyViewName ανακτώνται από τον πίνακα. Οι vacmAccessStorageType και vacmAccessStatus αποτελούν τα αντικείμενα των διαχειριστικών πληροφοριών που σχετίζονται με την πτητικότητα της αποθήκευσης και την κατάσταση της σειράς.



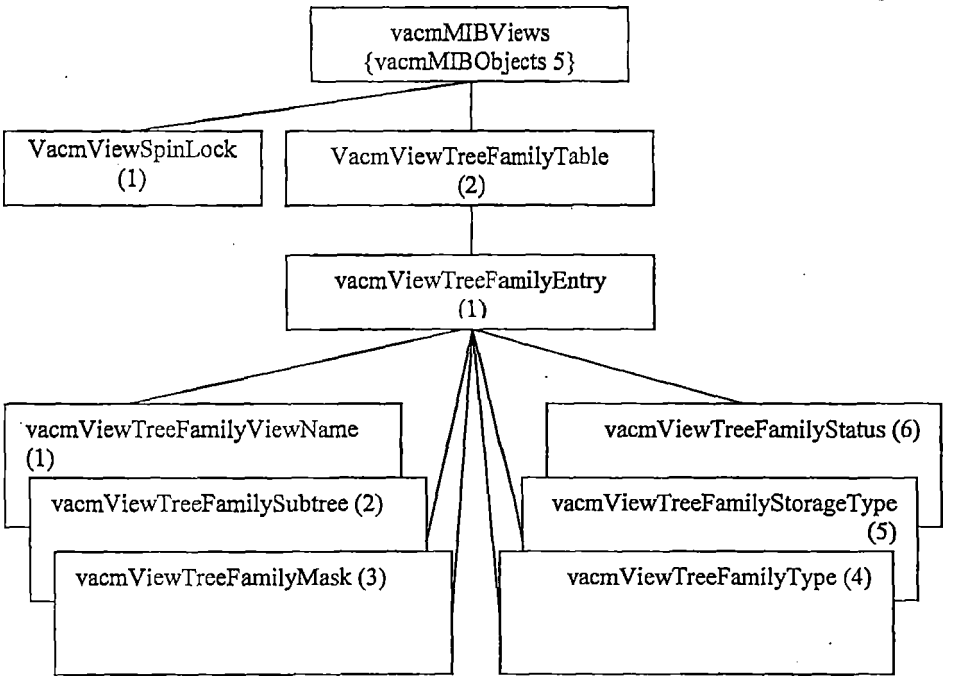
Σχήμα 4-6:Ο πίνακας πρόσβασης της VACM.

Η vacmMIBViews – ο τέταρτος κόμβος κάτω από τον vacmMIBObjects, όπως φαίνεται στο Σχήμα 4-7 - περιλαμβάνει τους δευτερεύοντες κόμβους vacmViewSpinLock και viewTreeFamilyAccessTable. Η vacmViewSpinLock είναι μια συμβουλευτική κλειδαριά που χρησιμοποιείται από τις εφαρμογές παραγωγής εντολών του SNMP για να συντονίζει τη χρήση από αυτές της καθορισμένης λειτουργίας για τη δημιουργία ή την τροποποίηση θεάσεων στους πράκτορες. Είναι ένα προαιρετικό αντικείμενο εφαρμογών.

Ο vacmViewTreeFamilyTable περιγράφει οικογένειες υποδένδρων που είναι διαθέσιμες εντός των θεάσεων της MIB στον τοπικό πράκτορα του SNMP για κάθε πλαίσιο. Κάθε γραμμή σ' αυτόν τον πίνακα περιγράφει ένα υποδένδρο για ένα viewName και ένα αναγνωριστικό αντικείμενο (OBJECT IDENTIFIER) . Για παράδειγμα, αν η διαδικασία «πρόσβαση επιτρεπτή», στο Σχήμα 3-22 του κεφαλαίου 3, αποδίδει τρεις τιμές για το viewName, αυτό θα έχει σαν αποτέλεσμα τρεις γραμμές σ' αυτόν τον πίνακα. Το vacmViewTreeFamilyViewName που αντιπροσωπεύει το viewName είναι ένα από τα αντικείμενα και ένας δείκτης στον πίνακα. Δύο δείκτες καθορίζουν μία γραμμή σ' αυτόν τον πίνακα. Το δεύτερο είναι το vacmViewTreeFamilySubtree, το οποίο είναι ένας κόμβος που αντιπροσωπεύει την κορυφή του δένδρου. Για παράδειγμα, αν το αναγνωριστικό αντικείμενο ήταν 1.3.6.1.2.1.1, θα αντιπροσώπευε το υποδένδρο του *συστήματος*. Το αναγνωριστικό αντικειμένου για τον τοπικό πράκτορα καθορίζεται από το υψηλότερο αναγνωριστικό

αντικειμένου που θα διευθυνσιοδοτούσε όλες τις υποστάσεις αντικειμένων στην τοπική θέαση της MIB.

Σε μερικές περιπτώσεις, μπορεί να θέλουμε να δούμε διαφορετικά υποσύνολα ενός υποδένδρου. Σε τέτοιες περιπτώσεις, μπορούμε να σχηματίσουμε μία οικογένεια από υποδένδρα θεάσεων χρησιμοποιώντας ένα συνδυασμό δύο παραμέτρων. Η πρώτη είναι επιλογή της θέασης, η οποία γίνεται από μία οικογενειακή μάσκα που καθορίζεται από το vacmViewTreeFamilyMask και η δεύτερη είναι ένας οικογενειακός τύπος που ορίζεται από το vacmViewTreeFamilyType. Η οικογενειακή μάσκα είναι μια συμβολοσειρά από bit που χρησιμοποιείται μαζί με το vacmViewTreeFamilySubtree. Όταν αυτό το χαρακτηριστικό χρησιμοποιείται, συγκεκριμένα αντικείμενα μέσα σε ένα υποδένδρο επιλέγονται εάν το αντίστοιχο αναγνωριστικό αντικείμενο ταιριάζει. Αν η τιμή του αντίστοιχου bit είναι 0 στην οικογενειακή μάσκα, εκλαμβάνεται σαν ένας χαρακτήρας αναπλήρωσης και οποιαδήποτε τιμή του αναγνωριστικού αντικειμένου επιλέγεται. Αφού έχει γίνει η επιλογή, αν η τιμή του οικογενειακού τύπου περιλαμβάνεται(1), η θέαση συμπεριλαμβάνεται. Αν δεν περιλαμβάνεται(2), η θέαση αποκλείεται. Ελαστικότητα στις θεάσεις μπορεί να επιτευχθεί εισάγοντας ένα αντικείμενο vacmViewTreeFamilyType που δείχνει αν ένα συγκεκριμένο υποδένδρο στην οικογένεια των υποδένδρων που παράγονται από τα vacmViewTreeFamilySubtree και vacmViewTreeFamilyMask θα συμπεριληφθεί ή θα αποκλειστεί από μία θέαση της MIB.



Σχήμα 4-7: Θεάσεις της VACM MIB

Σαν παράδειγμα της ομάδας του συστήματος που θα συμπεριληφθεί, οι τιμές των διαφόρων παραμέτρων της εγγραφής «οικογένεια»στο Σχήμα 4-7 είναι:

Όνομα της θέασης της οικογένειας = "σύστημα"

Οικογενειακό υποδένδρο = 1.3.6.1.2.1.1

Οικογενειακή μάσκα = ""

Οικογενειακός τύπος = 1

Η συμβολοσειρά μηδενικού μήκους, "", για την τιμή της μάσκας ορίζεται όλο 1 από σύμβαση.

Θα μπορούσαμε να επεκτείνουμε τη θέαση προσθέτοντας μία δεύτερη γραμμή στον πίνακα. Για παράδειγμα, θα μπορούσαμε να προσθέσουμε μία SNMP ομάδα προσθέτοντας άλλη μία γραμμή στον πίνακα που περιέχει το οικογενειακό υποδένδρο 1.3.6.1.2.1.11.

Θα μπορούσαμε επίσης να επεκτείνουμε τη θέαση της MIB προσθέτοντας ένα αντικείμενο στήλης στον πίνακα. Θα μπορούσαμε να επεκτείνουμε τη θέαση σε όλα τα αντικείμενα στήλης μιας γραμμής αντίληψης σε έναν πίνακα. Μια χρήσιμη σύμβαση για την πραγματοποίηση αυτής της προσθήκης είναι να χρησιμοποιήσουμε τον ορισμό του αντικειμένου στήλης 0, ο οποίος καθορίζει όλα τα αντικείμενα στήλης σε έναν πίνακα. Για παράδειγμα, το {1.3.6.1.2.1.2.2.1.0.5} προσδιορίζει όλα τα αντικείμενα στήλης που σχετίζονται με την 5η διεπαφή (interface - που αντιστοιχεί σε μια ifIndex τιμή του 5) στο ifTable.

Αν περισσότερα του ενός ονόματα οικογενειών είναι παρόντα με τον ίδιο αριθμό υποταυτοποιητών, η λεξικογραφική σύμβαση ακολουθείται για υπεροχή. Αυτή η τεχνική βοηθάει με τον ακόλουθο τρόπο: Υποθέστε ότι θέλαμε να επιλέξουμε όλα τα αντικείμενα στήλης στο παράδειγμα του ifTable, εκτός από το ifMtu, το οποίο είναι το 4° αντικείμενο στήλης. Τότε θα επιλέγαμε {1.3.6.1.2.1.2.2.1.4.5} και τον τύπο = 2 για να το αποκλείσουμε. Αυτό το σύνολο είναι λεξικογραφικά υψηλότερο από το {1.3.6.1.2.1.2.2.1.0.5}, οπότε το τελευταίο επικρατεί. Έτσι ο συνδυασμός των δύο θα επιλέξει όλα τα αντικείμενα της 5ης γραμμής εκτός από το ifMtu.

ΠΑΡΑΡΤΗΜΑ Α :ΠΡΟΤΥΠΑ RFC

Α.1 Γενικά για τα Πρότυπα Αίτησης για Σχόλιο

Τα πρότυπα αίτησης για σχόλιο, RFC (Request For Comment) είναι κείμενα τα οποία αποτελούν το αρχικό στάδιο στην διαδικασία δημιουργίας προτύπων του Internet. Πρωτοεμφανίστηκαν το 1969 με σκοπό να ενημερώνουν τους χρήστες του Internet σχετικά με διάφορες απόψεις πάνω στους υπολογιστές και την επικοινωνία μεταξύ τους, εστιάζοντας κυρίως στα πρωτόκολλα, στις διαδικασίες, στα προγράμματα και στις αρχές της δικτύωσης. Επίσης περιέχουν σημειώσεις συναντήσεων, γνώμες και μερικές φορές χιούμορ. Τα RFCs είναι ευρύτατα διαδεδομένα και στο Internet αλλά και σε ομάδες ανθρώπων με ανάλογο ενδιαφέρον, σαν έγγραφα προς εκτύπωση. Σημαντικά RFCs αναφέρονται στη συνέχεια.

Τα διάφορα πρότυπα του Internet, όπως καθορίζονται από την **IETF (Internet Engineering Task Force)** που είναι καθοδηγούμενη από την **IESG (Internet Engineering Steering Group),** δημοσιεύονται σαν RFCs.

Ο **RFC Editor** είναι ο εκδότης των RFCs και είναι υπεύθυνος για την τελική επιθεώρηση των εγγράφων πριν την έκδοσή τους. Ο RFC Editor βρίσκεται και διευθύνεται από το **ISI** (Information Sciences Institute) του **USC** (University of Southern California). Προτάσεις σχετικά με την έκδοση των RFCs ή την υποβολή υλικού για να ληφθεί υπόψη για έκδοση σαν RFC, πρέπει να στέλνονται μέσω ηλεκτρονικού ταχυδρομείου στη διεύθυνση του RFC Editor.

Α.2 Η διαδικασία δημιουργίας RFC

Οποιοσδήποτε μπορεί να γράψει ένα RFC. Υπάρχουν δύο δρόμοι που μπορεί να ακολουθήσει ένα έγγραφο ώστε να μετατραπεί σε RFC.

Ο πρώτος δρόμος είναι μέσω της IETF. Σε αυτήν, διευθυντές τομέων, ADs (Area Directors) είναι υπεύθυνοι για έναν αριθμό από σχετικές ομάδες εργασίας. Αυτές οι ομάδες εργασίας αναπτύσσουν έγγραφα τα οποία μπορεί να εγκριθούν για έκδοση σαν RFCs από τους ADs.

Ο άλλος δρόμος για να δημιουργηθεί ένα RFC είναι να υποβληθεί από κάποιον ανεξάρτητα, στον RFC Editor. Μερικές φορές, έγγραφα που έχουν υποβληθεί ανεξάρτητα, με αντικείμενο που τυγχάνει να έχει αρχίσει ήδη να επεξεργάζεται, παραπέμπονται στην αντίστοιχη ομάδα εργασίας της IETF. Σε αυτές τις περιπτώσεις συνήθως ζητείται από τον συγγραφέα της ανεξάρτητης υποβολής να συνεργαστεί με την IETF για την ανάπτυξη του εγγράφου.

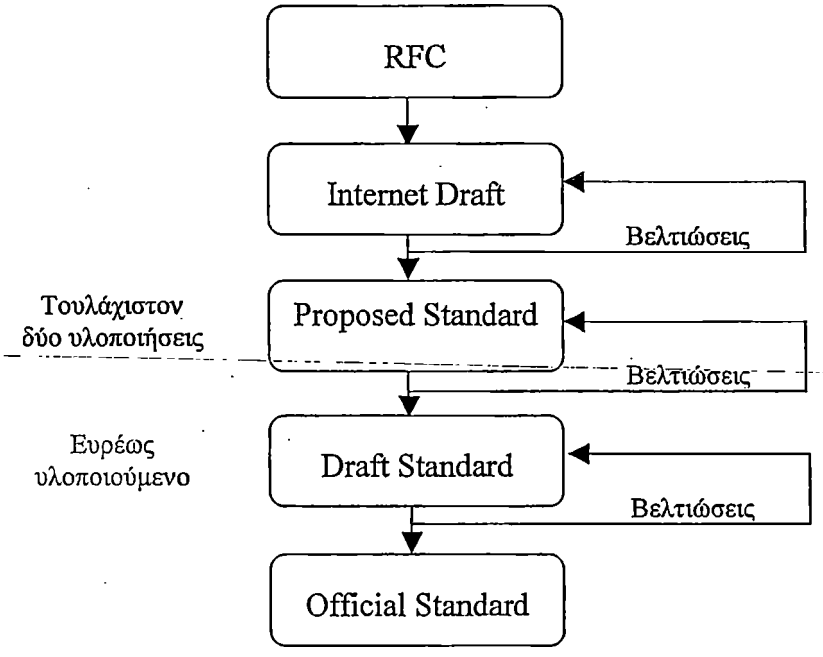
Όσοι θέλουν να ασχοληθούν με την συγγραφή RFCs πρέπει να διαβάσουν το RFC 2223 "Instructions to Authors" πριν ξεκινήσουν να γράφουν ένα έγγραφο.

Η δημιουργία ενός νέου προτύπου του Internet ακολουθεί μια καλά σχεδιασμένη διαδικασία, όπως εμφανίζεται στο Σχήμα Α-1.

Ξεκινάει με μία αίτηση για σχόλιο RFC (Request For Comment). Αυτό είναι συνήθως ένα κείμενο που περιέχει μια συγκεκριμένη πρόταση, μερικές φορές νέα και μερικές φορές τροποποιητική επί ενός ήδη υπάρχοντος προτύπου.

Το RFC συνήθως συζητείται για λίγο μέσα στο ίδιο το δίκτυο, όπου κάθε ένας μπορεί να εκφράσει την γνώμη του, καθώς και σε επίσημες συνεδριάσεις των ομάδων εργασίας της IETF. Μετά από ένα ικανό αριθμό από αναθεωρήσεις και συνεχείς συζητήσεις δημιουργείται και διανέμεται ένα **σχέδιο (Internet draft)**. Αυτό το σχέδιο είναι κοντά στην τελική μορφή του προτύπου, παρέχοντας επίσης συγκεντρωμένα και όλα τα σχόλια που προκάλεσε το RFC.

Το επόμενο βήμα είναι συνήθως να μετατραπεί σε προτεινόμενο πρότυπο (**Proposed Standard**), μορφή στην οποία παραμένει για τουλάχιστον έξι μήνες. Στην διάρκεια αυτής της περιόδου, η **Κοινωνία του Internet (Internet Society)** απαιτεί τουλάχιστον δύο ανεξάρτητες και χρησιμοποιήσιμες (interoperable) υλοποιήσεις, να γραφτούν και να δοκιμασθούν. Όποια προβλήματα προκύψουν από τις πραγματοποιούμενες δοκιμές πρέπει να αναφερθούν. (Στην πράξη συνήθως γράφονται πολλές υλοποιήσεις που έχουν σαν αποτέλεσμα τον αναλυτικό έλεγχο του προτεινόμενου προτύπου)

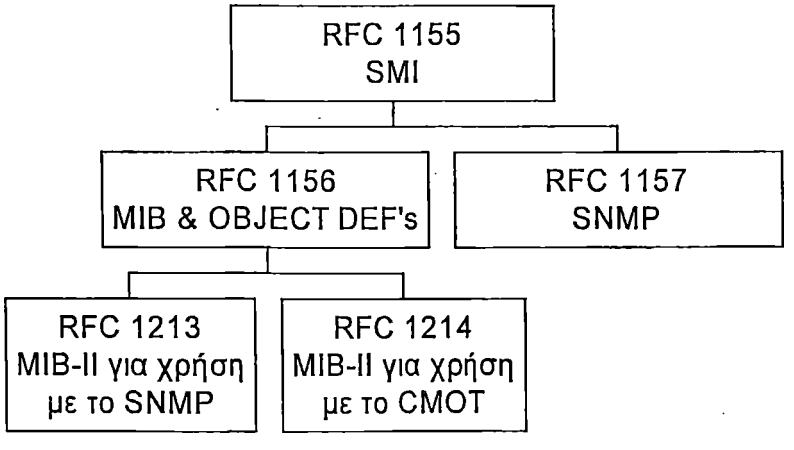


Σχήμα Α-1:Διαδικασία Δημιουργίας Προτύπου

Μετά από την ολοκλήρωση της διαδικασίας ελέγχου και τελειοποίησης, γράφεται ένα σχέδιο προτύπου (**Draft Standard**). Στη μορφή αυτή παραμένει για τουλάχιστον τέσσερις μήνες, χρονικό διάστημα στο οποίο αναπτύσσονται και δοκιμάζονται πολύ περισσότερες υλοποιήσεις. Το τελευταίο βήμα —μετά από πολλούς μήνες—είναι η υιοθέτησή του σαν επίσημο πρότυπο (**Official Standard**), σημείο στο οποίο υλοποιείται από όλους όσους ενδιαφέρονται να το χρησιμοποιήσουν.

Α.3 Σημαντικά RFCs που αφορούν στη Διαχείριση Δικτύων TCP / IP .

Στο Σχήμα Α-2 παρουσιάζονται μερικά από τα σημαντικότερα RFCs που αφορούν στη Διαχείριση των Δικτύων TCP / IP.



Σχήμα Α-2:Σημαντικά RFCs

Το **RFC 1155** περιέχει κοινούς ορισμούς και στοιχεία αναγνώρισης των χρησιμοποιούμενων πληροφοριών στα δίκτυα που βασίζονται στα πρωτόκολλα TCP/IP.

Το **RFC 1156** περιγράφει την μορφή της Βάσης Πληροφοριών Διαχείρισης (MIB) και των αντικειμένων που την αποτελούν. Επίσης παρέχει μία απλή και εφαρμοσμένη αρχιτεκτονική για την διαχείριση διαδικτύων TCP/IP και ειδικότερα του Internet.

Το **RFC 1157** περιγράφει το απλό πρωτόκολλο διαχείρισης δικτύου (SNMP).

Το **RFC 1213** περιέχει πληροφορίες που σχετίζονται με την δεύτερη έκδοση της Βάσης Πληροφοριών Διαχείρισης (MIB - II) σε σχέση με το πρωτόκολλο διαχείρισης SNMP (TCP/IP).

Το **RFC 1214** περιέχει πληροφορίες που σχετίζονται με την δεύτερη έκδοση της Βάσης Πληροφοριών Διαχείρισης (MIB - II) σε σχέση με το πρωτόκολλο διαχείρισης CMOT (OSI).

Α.4 Σημαντικά RFCs που αφορούν στην Ασφάλεια Δικτύων TCP / IP .

Μερικά από τα σημαντικότερα RFCs που αφορούν στην Ασφάλεια των Δικτύων TCP / IP δίνονται παρακάτω:

Το **RFC 2246** περιέχει πληροφορίες υλοποίησης του TLS το οποίο εξασφαλίζει το απόρρητο και την ακεραιότητα των δεδομένων ανάμεσα σε δύο εφαρμογές που επικοινωνούν.

Το **RFC 2402** ορίζει το πρωτόκολλο Κεφαλίδας Επαλήθευσης (AH) του IPsec, το οποίο παρέχει ακεραιότητα δεδομένων και επαλήθευση για το ωφέλιμο φορτίο και τα αμετάβλητα πεδία της IP κεφαλίδας.

Το **RFC 2406** ορίζει το πρωτόκολλο Ασφαλούς Ενθυλάκωσης Ωφέλιμου Φορτίου (ESP) του IPsec, το οποίο παρέχει εμπιστευτικότητα δεδομένων ή/και επαλήθευση για το IP ωφέλιμο φορτίο.

Το **RFC 2575** περιγράφει τα πέντε στοιχεία που απαρτίζουν το μοντέλο ελέγχου πρόσβασης της Βάσης Πληροφοριών Διαχείρισης του SNMP (μοντέλο VACM).

Τα **RFC 2045** έως και **RFC 2049** περιέχουν τις προδιαγραφές για το MIME. Καθορίζουν πέντε νέα πεδία κεφαλίδας μηνύματος ,τα οποία φέρουν πληροφορία σχετική με το σώμα του μηνύματος , καθώς και τις κωδικοποιήσεις μεταφοράς , που παρέχουν προστασία του μηνύματος από αλλοιώσεις μέσω του συστήματος ταχυδρομείου .

Το **RFC 2634** περιγράφει βελτιωμένες υπηρεσίες ασφάλειας για το S/MIME. Ορίζει τη διαδικασία και τα δικαιώματα που απαιτούνται για την εφαρμογή τεσσέρων επεκτάσεων των υπηρεσιών ασφάλειας του S/MIME : υπογεγραμμένες αποδείξεις , μάρκες ασφάλειας , ασφαλείς λίστες ταχυδρομείου και λειτουργία υπογραφής πιστοποιητικών . Οι τρεις πρώτες αφορούν κυρίως σε περιβάλλοντα επιχειρήσεων και οικονομικών δοσοληψιών. Η τελειταία αφορά σε οποιαδήποτε περίσταση μεταδίδονται πιστοποιητικά μαζί με υπογεγγραμμένα μηνύματα.

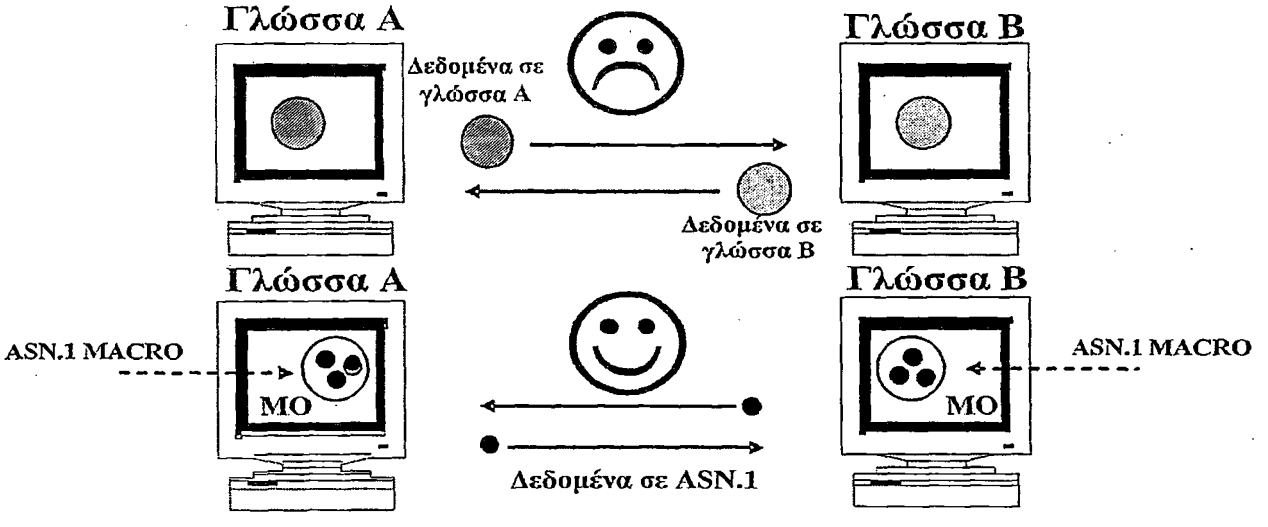
Τα **RFC 1421** έως και **RFC 1424** ορίζουν τις προδιαγραφές του Ταχυδρομείου Βελτιωμένου Απορρήτου (PEM) που διασφαλίζει εμπιστευτικότητα , επαλήθευση και διασφάλιση ακεραιότητας μηνυμάτων και αναποκυρηξία προέλευσης.

ΠΑΡΑΡΤΗΜΑ Β: ΕΙΣΑΓΩΓΗ ΣΤΗΝ ASN.1 / BER

Β.1 Ανάγκη Χρήσης Κοινής Σύνταξης για τη Μεταφορά Δεδομένων μέσω Δικτύου

Όσα θα αναπτύξουμε στη συνέχεια αφορούν αποκλειστικά τους τύπους των δεδομένων που μεταφέρονται από τον ένα υπολογιστή στον άλλο μέσω του δικτύου. Στα κατώτερα στρώματα οι τύποι δεδομένων (διευθύνσεις, πεδία ελέγχου, δεδομένα κ.α.) που μεταφέρονται είναι απλοί και το μόνο που έχουμε να κάνουμε είναι να διατάξουμε την πληροφορία αυτή με κάποια γνωστή σειρά και να τη μεταφέρουμε. Αντίθετα στο στρώμα εφαρμογής οι τύποι δεδομένων που μεταφέρονται είναι πολύ πιο σύνθετοι και η αναπαράστασή τους διαφέρει ανάλογα με τις γλώσσες προγραμματισμού που χρησιμοποιούνται μεταξύ των επικοινωνούντων υπολογιστών.

Σε κάθε κατανεμημένη εφαρμογή (στρώμα εφαρμογής) πρέπει να εξασφαλίσουμε ότι οι τύποι δεδομένων που μεταφέρονται μεταξύ των διεργασιών εφαρμογής μεταφράζονται κατά τον ίδιο τρόπο. Για το σκοπό αυτό ο ISO (σε συνεργασία με την ITU-T) έχουν ορίσει μια αφηρημένη σύνταξη κατάλληλη για την απεικόνιση των τύπων δεδομένων που πρόκειται να μεταφερθούν σε μία κατανεμημένη εφαρμογή. Η σύνταξη αυτή είναι γνωστή σαν Συμβολισμός Αφηρημένης Σύνταξης έκδοση Πρώτη ASN.1 (Abstract Syntax Notation Number One). Βασικό πλεονέκτημα του συμβολισμού είναι ότι όταν αυτός χρησιμοποιείται στα χαρτιά είναι κατανοητός στους ανθρώπους (Βλέπε Σχήμα Β-1)



Σχήμα Β-1:Μεταφορά δεδομένων μέσω δικτύου

Πολλές εταιρείες σήμερα πωλούν ASN.1 μεταγλωττιστές (compilers) για ένα μεγάλο πλήθος γλωσσών προγραμματισμού. Έτσι έχουμε μεταγλωττιστές για τη γλώσσα Pascal, C κ.α. Ο τρόπος χρήσης αυτών των μεταγλωττιστών φαίνεται στο Σχήμα Β-2α. Πρώτα οι τύποι δεδομένων της εφαρμογής γράφονται στην ASN.1. Αν οι δύο διεργασίες εφαρμογής είναι γραμμένες η μία σε PASCAL και η άλλη σε C τότε οι μεταγλωττιστές δίνουν τους τύπους δεδομένων στις γλώσσες αυτές μαζί με ένα σύνολο διαδικασιών κωδικοποίησης και αποκωδικοποίησης για κάθε τύπο δεδομένων. Οι τύποι δεδομένων στη συνέχεια ενσωματώνονται στις αντίστοιχες γλώσσες προγραμματισμού ενώ οι διαδικασίες κωδικοποίησης και αποκωδικοποίησης χρησιμοποιούνται από το στρώμα παρουσίασης του κάθε συστήματος για την κωδικοποίηση/αποκωδικοποίηση του κάθε τύπου δεδομένων. Πιο συγκεκριμένα κάθε τύπος δεδομένων που συσχετίζεται σε μία εφαρμογή έχει μια ετικέτα (tag) που χρησιμεύει για την αναγνώριση του. Αυτή η ετικέτα περνά μαζί με τον τύπο δεδομένων από το στρώμα εφαρμογής στο στρώμα παρουσίασης το οποίο πριν τη μεταφορά του μηνύματος χρησιμοποιεί την ετικέτα αυτή για να καλέσει την κατάλληλη διαδικασία κωδικοποίησης. Το αποτέλεσμα της διαδικασίας αυτής είναι μια σειρά από οκτάδες, η πρώτη

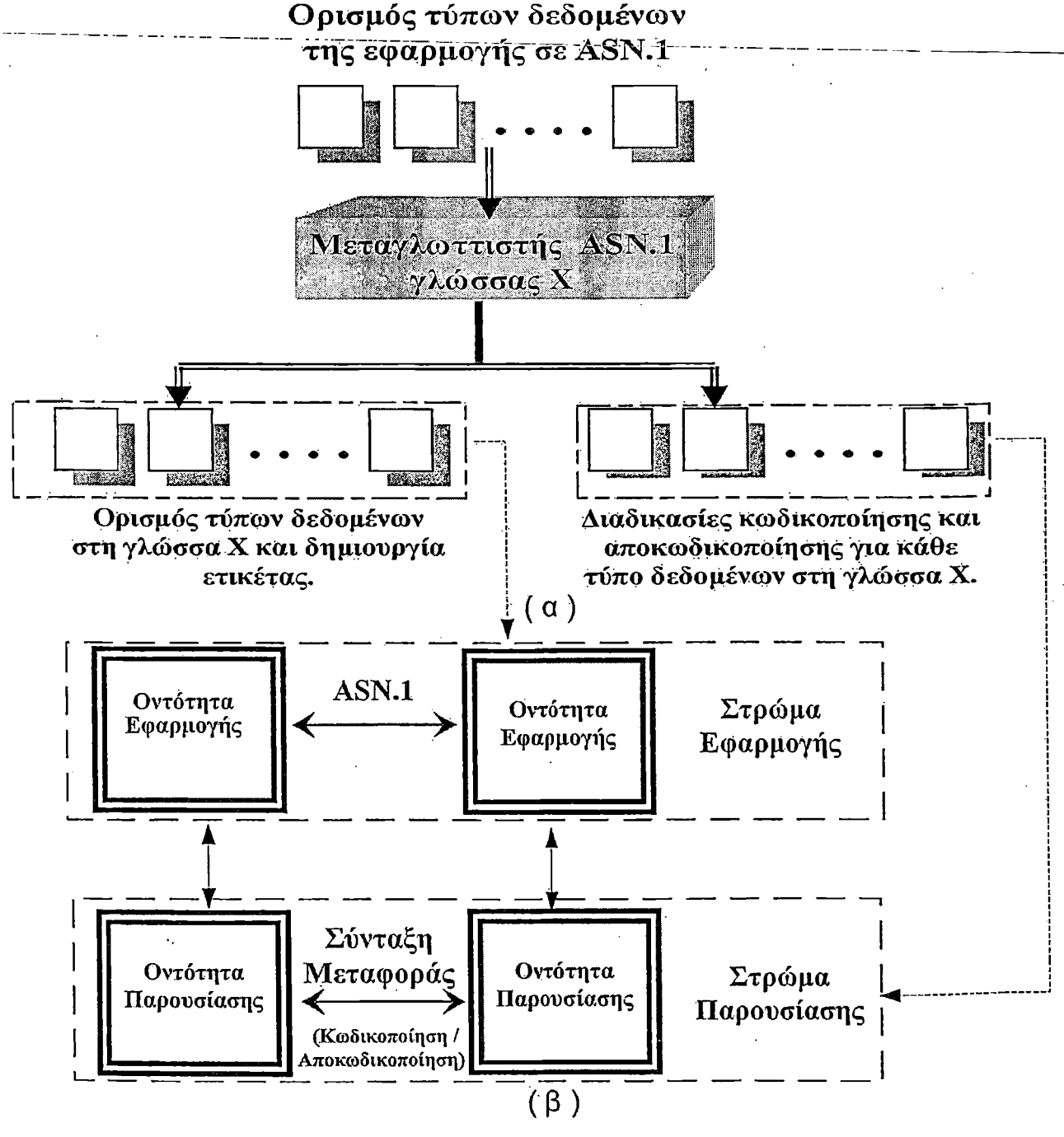
οκτάδα της οποίας προσδιορίζει τον τύπο δεδομένων. Αυτή η σειρά χρησιμοποιείται και από το στρώμα παρουσίασης του παραλήπτη για την επίκληση της αντίστοιχης διαδικασίας αποκωδικοποίησης.

Στο Σχήμα Β-2β απεικονίζεται η ASN.1, η τοπική σύνταξη και η σύνταξη μεταφοράς σε σχέση με τα στρώματα εφαρμογής και παρουσίασης των δύο επικοινωνούντων μέσω του δικτύου υπολογιστών.

Στον πίνακα που ακολουθεί βλέπουμε τα πρότυπα του ISO και τις αντίστοιχες συστάσεις της ITU-T που περιγράφουν τη σύνταξη ASN.1 καθώς και τους Βασικούς Κανόνες Κωδικοποίησης, BER (Basic Encoding Rules)

ITU-T	OSI	Τίτλος
X.208 (1988)	ISO/IEC 8824 (1988)	Προδιαγραφή της ASN.1
X.209 (1988)	ISO/IEC 8825 (1988)	Προδιαγραφή των Βασικών Κανόνων Κωδικοποίησης για την ASN.1

Πίνακας Β-1:Πρότυπα ISO και Συστάσεις της ITU-T για τη σύνταξη ASN.1



Σχήμα Β-2:Η ASN.1 και η σύνταξη μεταφοράς

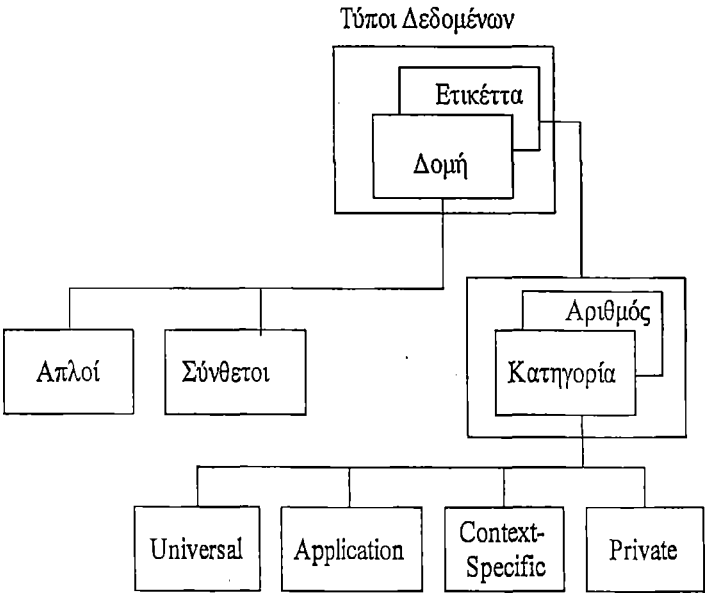
Β.2 Ορισμος και Κατηγορίες Τύπων Δεδομένων

Γενικά ένα τύπο δεδομένων τον ορίζουμε με το παρακάτω μορφότυπο
<type reference>::=<type>
όπου το αριστερό μέλος της σχέσης δίνει το όνομα του τύπου, το σύμβολο σημαίνει "ορίζεται σαν" και το δεξιό μέλος της σχέσης δίδει τον τύπο. Έτσι για παράδειγμα έχουμε
counter::=INTEGER
και στη συνέχεια μετά από τον ορισμό γράφουμε counterINTEGER.

Σε κάθε τύπο δεδομένων μπορούμε να θέσουμε μια τιμή με βάση το μορφότυπο
<value Reference> <type>::=<value>
όπου στο αριστερό μέλος της σχέσης το πεδίο value reference δίδει το όνομα της τιμής, και το πεδίο type δίδει τον τύπο και τέλος το δεξιό μέλος δίδει την τιμή που θέτουμε στον τύπο αυτό. Έτσι για παράδειγμα έχουμε
IfInOctets Counter::=103386

Όπως είπαμε και στην αρχή για να μπορούμε να αναγνωρίζουμε τους διάφορους τύπους κάνουμε χρήση μιας ετικέτας. Κάθε ετικέτα αποτελείται, όπως φαίνεται και στο Σχήμα Β-3, από δύο μέρη την κατηγορία (class) και ένα φυσικό αριθμό (number). Έχουμε τέσσερις κατηγορίες τύπων δεδομένων:

- **Universal** Αφορά τύπους που είναι ενσωματωμένοι (built-in) στην ASN.1.Αναγνωρίζονται με την ετικέτα [UNIVERSAL X] όπου X ένας ακέραιος αριθμός.
- **Application** Αφορά τύπους που τους βρίσκουμε μόνο σε διάφορες εφαρμογές (MHS/X400, FTAM κ.λ.π.). Αναγνωρίζονται με την ετικέτα [APPLICATION X] όπου X ένας φυσικός αριθμός.
- **Context-specific** Αφορά τύπους που αποτελούν ένα τμήμα των εφαρμογών. Αναγνωρίζονται με αριθμούς μέσα σε αγκύλες [1], [2], [3],... που ακολουθούν το όνομά τους.
- **Private-use** Αφορά τύπους για ιδιωτική χρήση και δεν προσδιορίζονται από τα πρότυπα της ASN.1. Αναγνωρίζονται με την ετικέτα [PRIVATE X] όπου X ένας φυσικός αριθμός.



Σχήμα Β-3:Γενική δομή της ASN.1

Όλους τους παραπάνω τύπους, όπως φαίνεται στο Σχήμα Β-3 τους χωρίζουμε σε **Απλούς** (Simple) και **Σύνθετους** (Complex).

Β.2.1 Δομή:Απλοί Τύποι Δεδομένων

Οι απλοί τύποι μπορεί να είναι οι βασικοί τύποι που δεν μπορούν να αναλυθούν περαιτέρω για παράδειγμα οι BOOLEAN, INTEGER ή σε ορισμένες περιπτώσεις μια σειρά από ένα ή περισσότερα bits, οκτάδες ή IAS/γραφικοί χαρακτήρες. Οι λέξεις κλειδιά που χρησιμοποιούνται για αυτούς στην ASN.1 είναι πάντα με κεφαλαία γράμματα. Οι απλοί τύποι είναι οι εξής:

- **BOOLEAN** Παίρνει δύο τιμές True ή False
- **INTEGER** Παριστά **ακέραιους** αριθμούς
- **BITSTRING** Παριστά **πληροφορία** που αποτελείται από μια σειρά από bits
- **OCTETSTRING** Παριστά **πληροφορία** που αποτελείται από μια σειρά από octets
- **REAL** Παριστά τους **πραγματικούς** αριθμούς
- **ENUMERATED** Παίρνει μια **τιμή** από ένα προκαθορισμένο σύνολο τιμών
- **IA5 String** Όλοι οι **χαρακτήρες** του IA5 (ASCII)
- **Graph String** Όλοι οι **κατοχυρωμένοι** γραφικοί χαρακτήρες και το space
- **NULL** Απουσία **οποιουδήποτε** τύπου
- **ANY** Η τιμή ενός τέτοιου τύπου είναι η τιμή ενός από τους οποιουσδήποτε υπάρχοντες τύπους (ακόμα και από αυτούς που έχουμε εμείς ορίσει)

Μερικά παραδείγματα ορισμού απλών τύπων δίδονται στη συνέχεια

```
married::= BOOLEAN--true or false
yrsWithCompany::= INTEGER
accessRights::= BITSTRING {read (0), write (1)}
PDUContents::= OCTETSTRING
name::= IA5String
pi::= REAL--mantissa; base, exponent
workDay::=ENUMERATED{Monday(0),Tuesday(1)
        ....Friday(5) }
```

Το σύμβολο -- εφαρμόζεται πριν από σχόλια. Οι εκχωρήσεις στα επί μέρους bits που συσχετίζονται με τον τύπο BITSTRING δίδονται μέσα σε άγκιστρα. Παρόμοια μέθοδος εφαρμόζεται και στον τύπο ENUMERATED για τον προσδιορισμό πιθανών τιμών της μεταβλητής.

Εδώ θα πρέπει να αναφέρουμε και τύπους που προκύπτουν από τους απλούς με αλλαγή της ετικέτας που αυτοί έχουν. Υπάρχουν δύο τρόποι για να γίνει αλλαγή της ετικέτας ενός τύπου και κατά συνέπεια να δημιουργηθεί ένας διαφορετικός τύπος:

EXPLICIT όπου μια νέα ετικέτα προστίθεται ενώ η παλιά παραμένει. Κατά την κωδικοποίηση και μεταφορά μέσα από το δίκτυο ενός τέτοιου τύπου μεταφέρονται και οι δύο ετικέτες.

Ας δούμε ένα παράδειγμα αυτού του τύπου

EmpNumber [APPLICATION 1] INTEGER

Εδώ προστίθεται μια νέα ετικέτα η [APPLICATION 1] ενώ η αρχική που αντιστοιχεί στον τύπο INTEGER παραμένει.

IMPLICIT όπου μια νέα ετικέτα αντικαθιστά την παλιά. Είναι φυσικό ότι ο τύπος αυτός είναι καλύτερος αφού δίνει λιγότερο επίφορτο (overhead) στο δίκτυο.

Ας δούμε ένα παράδειγμα αυτού του τύπου

EmpNumber [APPLICATION 1] IMPLICIT INTEGER

Για να δηλώσουμε αυτόν τον τύπο τοποθετούμε τη λέξη IMPLICIT μετά τη νέα ετικέτα δηλαδή για την περίπτωσή μας μετά τη λέξη [APPLICATION 1]. Έτσι δημιουργούμε ένα νέο τύπο ο οποίος δεν παύει να είναι INTEGER αλλά κατά τη μεταφορά του μέσα στο δίκτυο αναγνωρίζεται μόνο με τη καινούρια ετικέτα του.

Τέλος πρέπει να γίνει αναφορά στον τύπο OBJECT IDENTIFIER. Πολλά αντικείμενα στο περιβάλλον TCP/IP ή OSI χρειάζονται ένα μοναδικό όνομα. Για να επιτρέψει η ASN.1 τον προσδιορισμό μοναδικών ονομάτων δημιούργησε τον τύπο OBJECT IDENTIFIER. Οι τιμές του τύπου αυτού είναι μια σειρά από φυσικούς αριθμούς κάθε ένας από τους οποίους αναφέρεται στον κόμβο ενός δένδρου στον οποίο βρίσκεται το αντικείμενο αυτό. Έτσι για να βρούμε το όνομα ενός αντικειμένου δεν έχουμε παρά να ξεκινήσουμε από τη ρίζα του δέντρου (Root) στο οποίο βρίσκεται το αντικείμενο και να προχωρήσουμε προς τους αριθμούς των διαφόρων κόμβων μέχρι να φτάσουμε στο αντικείμενο αυτό. Έτσι για παράδειγμα έχουμε SysDescr OBJECT IDENTIFIER.::={13612111}

Β.2.2 Δομή: Σύνθετοι Τύποι

Οι σύνθετοι τύποι ορίζονται από ένα ή περισσότερους άλλους τύπους που μπορεί να είναι απλοί ή ακόμα και σύνθετοι. Οι σύνθετοι τύποι είναι οι εξής:

- **SEQUENCE** Είναι μια διατεταγμένη λίστα διαφορετικών τύπων
- **SEQUENCE OF** Είναι μια διατεταγμένη λίστα ιδίων τύπων
- **SET Είναι** μια μη διατεταγμένη λίστα (η διάταξη εδώ δεν μας ενδιαφέρει) διαφορετικών τύπων
- **SET OF** Είναι μια μη διατεταγμένη λίστα ιδίων τύπων
- **CHOICE** Είναι μια **μη** διατεταγμένη λίστα που σχηματίζεται από ένα σύνολο των παραπάνω τύπων

Στο παράδειγμα που ακολουθεί δίνονται τύποι της μορφής SEQUENCE

```
PersonnelRecord::= SEQUENCE{
                     EmpNumber INTEGER,
                     Name IA5String,
                     YrsWithCompany INTEGER,
                     Married BOOLEAN }

PersonnelRecord::= SEQUENCE{
                    EmpNumber [APPLICATION 1]INTEGER,
                    Name[1] IA5String,
                    YrsWithCompany [2] INTEGER,
                    Married [3] BOOLEAN }

PersonnelRecord::= SEQUENCE{
                   EmpNumber [APPLICATION1]INTEGER ,
                   Name [1] IMPLICIT IA5String,
                   YrsWithCompany [2] IMPLICIT INTEGER,
                   Married [3] IMPLICIT BOOLEAN }
```

Οι αριθμοί [1], [2] και [3] αφορούν μόνο τα συμφραζόμενα σε αυτό τον τύπο, πρόκειται δηλαδή για την περίπτωση τύπου context-specific. Στα παραπάνω παραδείγματα βλέπουμε επίσης διαφόρους τύπους που προκύπτουν από τους μηχανισμούς EXPLICIT και IMPLICIT.

Τώρα που ορίσαμε όλους τους απλούς και σύνθετους τύπους θα δούμε και τις ετικέτες τους για την κατηγορία UNIVERSAL. Επειδή υπάρχουν πολλοί UNIVERSAL τύποι υπάρχει

κάποιος φυσικός αριθμός που χαρακτηρίζει τον καθένα. Με την ετικέτα αυτή μπορούμε να αναφερόμαστε στους παραπάνω τύπους.

Στον πίνακα που ακολουθεί δίδεται η εκχώρηση ετικετών για την κατηγορία UNIVERSAL .

UNIVERSAL 1	BOOLEAN
UNIVERSAL 2	INTEGER
UNIVERSAL 3	BITSTRING
UNIVERSAL 4	OCTETSTRING
UNIVERSAL 5	NULL
UNIVERSAL 6	OBJECT IDENTIFIER
UNIVERSAL 7	Object Description
UNIVERSAL 8	EXTERNAL
UNIVERSAL 9	REAL
UNIVERSAL 10	ENUMERATED
UNIVERSAL 11	ENCRYPTED
UNIVERSAL12-15	Reserved for future use
UNIVERSAL 16	SEQUENCE and SEQUENCE OF
UNIVERSAL 17	SET and SET OF
UNIVERSAL 18	NumericString
UNIVERSAL 19	PrintableString
UNIVERSAL 20	TeletextString
UNIVERSAL 21	VideoString
UNIVERSAL 22	IA5String
UNIVERSAL 23	UTCTime
UNIVERSAL 24	GeneralisedTime
UNIVERSAL 25	GraphicString
UNIVERSAL 26	VisibleString
UNIVERSAL 27	GeneralString
UNIVERSAL 28	CharacterString
UNIVERSAL 29	Reserved for Additions

Πίνακας Β-2:Ετικέττες της κατηγορίας UNIVERSAL

Από τον πίνακα βλέπουμε ότι ο απλός τύπος INTEGER έχει ετικέτα UNIVERSAL 2, οι σύνθετοι τύποι SEQUENCE και SEQUENCE OF έχουν ετικέτα UNIVERSAL 16 κ.λ.π.

3.3 Η ASN.1 MACRO

Η χρήση ενός MACRO γίνεται σε ορισμένες εφαρμογές όπου είναι επιθυμητό να προστεθούν προεκτάσεις στο συντακτικό ASN.1 από τον χρήστη. Έτσι και δίδεται η δυνατότητα να ορίσουμε νέους τύπους. Την ASN.1 MACRO χρησιμοποιούμε για τον προσδιορισμό των υπό διαχείριση αντικειμένων (Structure of Management Information-SMI)

Ο ορισμός του MACRO είναι ο παρακάτω

```
<macroname> MACRO::=
BEGIN
   TYPE NOTATION ::= < new-type-syntax >
   VALUE NOTATION ::= < new-value-syntax >
    < supporting-production >
END
```

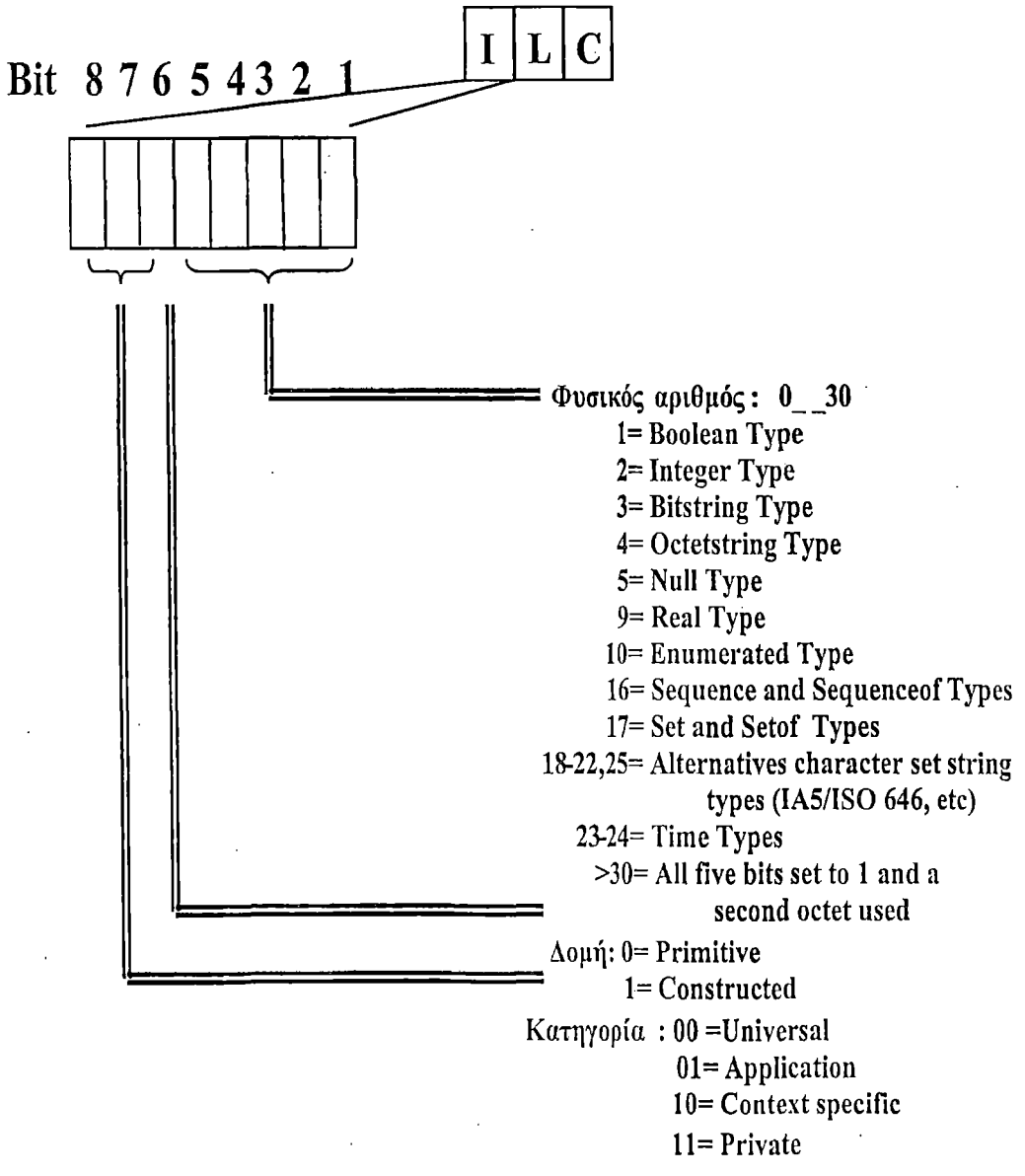
Εκτός από τον ορισμό MACRO έχουμε και την MACRO περίπτωση (instance) που προκύπτει από τον ορισμό μετά από την τοποθέτηση τιμών στις μεταβλητές.

3.4 Βασικοί Κανόνες Κωδικοποίησης BER

Η ITU-T έχει ορίσει μαζί με την ASN.1 και ένα σύνολο από διαδικασίες κωδικοποίησης οι οποίοι για κάθε αφηρημένη σύνταξη (abstract syntax) που ορίζεται με τη βοήθεια της ASN.1 δημιουργούν την αντίστοιχη σύνταξη μεταφοράς (transfer syntax). Οι διαδικασίες αυτές ονομάστηκαν Βασικοί Κανόνες Κωδικοποίησης BER και συνδέθηκαν στενά με την ASN.1 ώστε σήμερα θεωρούνται μέρος της.

Όπως είπαμε στην αρχή η σύνταξη μεταφοράς ασχολείται με την κωδικοποίηση των δεδομένων σε μια σειρά από bits κατάλληλη για τη μεταφορά τους κατά μήκος της γραμμής μετάδοσης. Η κωδικοποιημένη μορφή κάθε τύπου, είτε αυτός είναι απλός είτε σύνθετος, αποτελείται από τρία τμήματα: Το Αναγνωριστικό I (Identifier), το Μήκος L (Length) και το Περιεχόμενο C (Contents).

Το αναγνωριστικό αντιστοιχεί στον τύπο και όπως φαίνεται και στο Σχήμα Β-4 αποτελείται από τρία τμήματα.



Σχήμα Β- 4:Η ASN.1 και η σύνταξη μεταφοράς

Το μήκος L είναι το δεύτερο μέρος κάθε κωδικοποίησης και αποτελείται από τον ακέραιο αριθμό bytes που καταλαμβάνει το περιεχόμενο.

Τα περιεχόμενα C περιέχουν την τιμή του τύπου που δηλώνεται στο τμήμα του αναγνωριστικού.Παραδείγματα κωδικοποίησης διαφόρων τύπων δεδομένων δίδονται στη συνέχεια.

```
Employed ::= BOOLEAN - - assume true
        Identifier = 01 (Hex)          - - Universal 1
        Length     = 01
        Contents   = FF
        Κώδικας: 01  01  FF

RetxCount ::= INTEGER - - assume =29 (decimal)
        Identifier = 02                - - Universal 2
        Length     = 01
        Contents   = 1D                - - 29 decimal
        Κώδικας: 02  01  1D
```

```
FunctionalUnits ::= BITSTRING {read (0), write (1), fileAccess (2) }
    - - assume read only is required
        Identifier = 03                - - Universal 3
        Length     = 01
        Contents   = 80                - - read only = 1 0000 0000
        Κώδικας: 03  01  80

File :: SEQUENCE { userName IAS String, contents OCTETSTRING }
    - - assume userName = ' FRED' and contents = 0F  27  E4  Hex
   Identifier = 30 (Hex)               - - constructed, Universal 16
        Length     = 0B                - - Decimal 11
        Contents   = Identifier = 16   - - Universal 22
                     Length     = 04
                     Contents   = 46  52  45  44
                     Identifier = 04   - - Universal 4
                     Length     = 03
                     Contents   = 0F  27  E4
        Κώδικας: 30  0B 16  04  46  52  45  44  04  03  0F  27  E4
```

ΒΙΒΛΙΟΓΡΑΦΙΑ

Α) ΒΙΒΛΙΟΓΡΑΦΙΑ ΓΙΑ ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ TCP/IP

1. **"Δίκτυα Τηλεπικοινωνιών και η σύγκλιση"** Ε. Οικονόμου, Έκδοση ΟΤΕ 2004
2. **"Network Security Essentials** "w. Stallings, Prentice Hall 2000
3. **"Network Security: The Complete Reference"**
4. **"The Fundamentals of Network Security"** J. Canavan, Artech House 2001
5. **"SSL and TLS : Designing and Building Secure Systems"**
6. **"SSL and TLS Essentials: Security the Web"** S. Thomas, Wiley 2000
7. **"Information Security Architecture"** J. Killmeyer Tubor, CRC Press 2000
8. **" The Internet Security Guidebook"** J. Ellis/ T. Speed/ W. Crowell, Academic Press 2000
9. **"Maximum Security** " G. Shipley, Sams 2001
10. **"Designing Network Security"** M. Kaeo, Cisco Press 1999
11. **"Security Architecture: Design, Deployment and Operations"** Ch. King/ E. Osmanoglou/ C. Dalton, McGraw-Hill 2001
12. **"Network Security: A Beginner's Guide"** E. Maiwald, McGraw-Hill 2001

Β) ΒΙΒΛΙΟΓΡΑΦΙΑ ΓΙΑ ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ TCP/IP

1. **"Ασφάλεια Δικτύων και η διαχείριση της"** Ε. Οικονόμου, Έκδοση ΟΤΕ 2004
2. **"Συστήματα διαχείρισης Τηλεπικοινωνιακού δικτύου ΟΤΕ"**, Έκδοση ΟΤΕ 2001
3. **"Διαχείριση Δικτύων SNMP, CMIP, TMN"** Ε. Οικονόμου, Έκδοση ΟΤΕ 1999
4. **"Network and Systems Management"** I .G. Ghetic, Kluwer Academic Publishers 1997
5. **"Integrated Management of Network Systems"** H. Hegering, S. Abecu, B. Neumair, Morgan Kaufmann Publishers 1999
6. **"SNMP, SNMPv2, SNMPv3 and RMON1 and 2"** William Stallings,
7. Addison-Wesley 1999