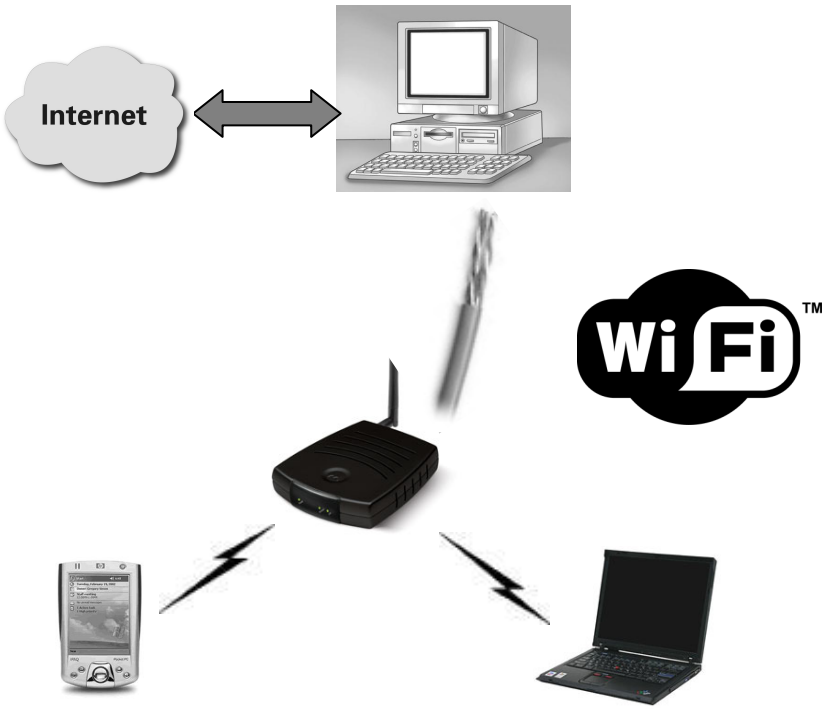
ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΚΡΗΤΗΣ
ΠΑΡΑΡΤΗΜΑ ΧΑΝΙΩΝ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΝΙΚΗΣ



"Ασύρματη δικτύωση με τεχνολογία IEEE 802.11g Ανάλυση-Υλοποίηση-Ασφάλεια-Διαχείριση"

Νικόλαος Α. Βάσσης
Παρασκευάς Ι. Μπουρδούβαλης

Επιβλέπων Καθηγητής : Γεώργιος Σ. Λιοδάκης
Καθηγητής εφαρμογών

Χανιά
Νοέμβριος 2006

Ευχαριστίες

Για το σύνολο της προσπάθειας αυτής αισθανόμαστε ιδιαιτέρα την ανάγκη να ευχαριστήσουμε όσους με οποιοδήποτε τρόπο συνέβαλαν στη πραγματοποίηση της εργασίας αυτής.

Ειδικότερα ευχαριστούμε θερμά τον καθηγητή του ΤΕΙ Ηλεκτρονικής Χανίων κύριο Γεώργιο Λιοδάκη για την ανάθεση της μελέτης καθώς και την ουσιαστική επιστημονική καθοδήγηση του κατά την εκπόνηση και συγγραφή της εργασίας και επίσης τον κύριο Νίκο Λυμπεράκη για την βοήθεια που μας προσέφερε σε τεχνικά θέματα και στην ενσωμάτωση του ασύρματου δικτύου στο δίκτυο του ΤΕΙ.

Τέλος ευχαριστώ θερμά την οικογένεια μου και τη φίλη μου Ελένη για την ηθική υποστήριξη τους κατά τη διεξαγωγή της εργασίας καθώς και τον συμφοιτητή μου Πάρη για τη συνεργασία μας.

Νίκος

Τέλος ευχαριστώ θερμά την οικογένεια μου για την ηθική υποστήριξη κατά τη διεξαγωγή της εργασίας, τους φίλους μου για την υπέροχη παρέα που κάναμε όλα αυτά τα χρόνια στα Χανιά καθώς και τον συμφοιτητή μου Νίκο για τη συνεργασία μας.

Πάρης

ABSTRACT

IEEE 802.11 wireless local area networks (WLANs) are widely deployed in corporate and campus networks as well as public hotspots. However, their introduction is accompanied by a number of issues, such as security and radio coverage. The purpose of the thesis is to present an overview of the IEEE 802.11 technology with possible application services, with emphasis given on location-based services. Furthermore, by the installation of WLAN access point at the Technological Educational Institute of Crete / Branch of Chania , we were concerned about network access and security. In particular, we exploited an open source software for administration of our WLAN in order to provide authentication of users and other related issues. Finally we present the site survey results we got before planning and installation of the WLAN by the use of the Netstumbler software.

ΠΕΡΙΕΧΟΜΕΝΑ

ΚΕΦΑΛΑΙΟ 1
Πρωτόκολλο IEEE 802.11

1.1 Σημασία της ασύρματης διασύνδεσης……... 1
1.2 Ραδιοφάσμα……..... 3
1.3 Τι είναι το πρωτόκολλο 802.11……. 3
1.4 Προδιαγραφές 802.11……..... 4
1.5 Αρχιτεκτονική……..... 5
1.6 Τεχνικά χαρακτηριστικά……..… 6
1.7 Παραλλαγές του 802.11……..... 7
1.8 Τα κυριότερα εμπορικά πρωτόκολλα σήμερα..... 15

ΚΕΦΑΛΑΙΟ 2
Πρωτόκολλα κρυπτογράφησης για δίκτυα IEEE 802.11x

2.1 Γενικά περί ασφάλειας ασυρμάτων δικτύων…….. 17
2.2 Περιγραφή λειτουργίας του πρωτοκόλλου WEP ……. 19
2.2.1 Κρυπτογραφικό υπόβαθρο του WEP…… 19
2.2.2 Ιδιότητες του αλγορίθμου WEP……. 21
2.2.3 Θεωρία λειτουργίας WEP ……..…….……..…. 22
2.2.4 Προβλήματα του WEP…… 26
2.2.5 Το τελικό σπάσιμο του κλειδιού ……. 28
2.2.6 Συμεράσματα και συστάσεις……..... 29
2.3 WPA - Ασύρματη Προστατευμένη Πρόσβαση..……..... 31
2.3.1 Πρωτόκολλο χρονικής ακεραιότητας κλειδιου……..… 31
2.3.2 Επιλογή και χρησιμοποίηση IV…….. 33
2.3.3 Λεπτομέρειες υλοποίησης του TKIP ……. 37
2.3.4 Το 802.1X…….……..... 40
2.4 Πρωτόκολλο Επεκτάσιμης επαλήθευσης Ταυτότητας….. 42
2.5 Ελαφρύ EAP (LEAP)…….. ..……... 43
2.6 Ασφάλεια Επιπέδου μεταφοράς και EAP ……...……. 45

2.7 EAP-TLS... ……..... 47
2.8 Προστατευμένο EAP (PEAP)……..… 50

ΚΕΦΑΛΑΙΟ 3
Υλοποίηση δικτύου WLAN

3.1 Υλοποίηση δικτύου WLAN…….. 52
3.2 Περιγραφή Kerio Winroute Firewall…….. 53
3.2.1 Ανάθεση IP διευθύνσεων μέσω Dhcp Server…… 54
3.2.2 Δημιουργία και πιστοποίηση λογαριασμών χρηστών……. 55
3.2.3 Http Policy…… 62
3.2.4 Απομακρυσμένη διαχείριση…… 63
3.2.5 Λήψη στατιστικών στοιχείων μέσω του Kerio…….. 64
3.3 Περιήγηση – Εργαλεία χρήστη και λογισμικό Kerio…. 66

ΚΕΦΑΛΑΙΟ 4
Μελέτη παροχής LBS σε WLANs

4.1 Γενικά περί εντοπισμού θέσης……. 71
4.2 Σχετική εργασία……. 72
4.3.1 Προσέγγιση βασισμένη σε RSS……. 73
4.3.2 Προσεγγίσεις βασισμένες στο δίκτυο…… 73
4.3.3 Χαρτογράφηση διευθύνσεων…….. 74
4.4 Μια νέα προσέγγιση SNMP……. 75
4.5 Χαρτογράφηση διευθύνσεων IP σε MAC…….. 77
4.6 Χρήση ιδιωτικών διευθύνσεων IP…….. 78
4.7 Χαρτογράφηση διευθύνσεων IP από δημόσια σε ιδιωτική…. 79
4.8 Αναγνωρίζοντας APs με ιδιωτικές IP διευθύνσεις…….. 80
4.9 Ένα πλαίσιο υπηρεσιών ιστού για WLAN LBSs……. 81
4.10 Συμπεράσματα 83

ΚΕΦΑΛΑΙΟ 5

Αποτελέσματα ραδιοκάλυψης του WLAN

5.1 Πληροφορίες WLAN - Μετρήσεις, βελτιστοποίηση απόδοσης…….. 85
5.2.1 Διαδικασία Wardriving…….. 89
5.2.2 Έλεγχος διαμόρφωσης του τοπικού ασύρματου LAN …….. 89
5.2.3 Επαλήθευση κάλυψης του ασύρματου LAN …… 89
5.2.4 Έρευνα περιοχών……. 90
5.2.5 Προσδιορισμός θέσης κεραιών…….. 90
5.3.1 Μετρήσεις σε πραγματικό περιβάλλον ……. 90
5.3.2 Ανάλυση μετρήσεων……. 92
5.3.3 Συμπεράσματα…….. 95

Κεφάλαιο 1

Πρωτόκολλο IEEE 802.11

1.1 Σημασία της ασύρματης διασύνδεσης

Οι παραδοσιακοί τρόποι δικτύωσης έχουν αποδειχθεί ανεπαρκείς να αντιμετωπίσουν τις προκλήσεις που τίθενται από το νέο συλλογικό τρόπο ζωής μας. Εάν οι χρήστες πρέπει να συνδεθούν με ένα δίκτυο με φυσικό μέσο το καλώδιο, η μετακίνησή τους μειώνεται εντυπωσιακά. Η ασύρματη συνδετικότητα όμως, δεν θέτει τέτοιους περιορισμούς και επιτρέπει πολύ περισσότερη ελεύθερη μετακίνηση εκ μέρους του χρήστη. Αυτό το έχουμε βιώσει αρκετά με την ασύρματη τηλεφωνία. Είμαστε στην αρχή μιας εξίσου βαθιάς αλλαγής στη δικτύωση υπολογιστών. Η ασύρματη τηλεφωνία είναι επιτυχής επειδή επιτρέπει στους ανθρώπους να επικοινωνήσουν ο ένας με τον άλλον ανεξάρτητα από τη θέση. Οι νέες τεχνολογίες που στοχεύουν στα δίκτυα υπολογιστών υπόσχονται να κάνουν το ίδιο πράγμα για τη σύνδεση μέσω Διαδικτύου.

Τα ασύρματα δίκτυα προσφέρουν διάφορα πλεονεκτήματα πέρα από τα ενσύρματα δίκτυα:

Κινητικότητα

Οι χρήστες κινούνται, αλλά τα δεδομένα αποθηκεύονται συνήθως κεντρικά. Διευκόλυνση των χρηστών να έχουν πρόσβαση στα δεδομένα ενώ είναι σε κίνηση μπορούν να οδηγήσουν σε μεγάλα κέρδη παραγωγικότητας.

Ευκολία και ταχύτητα της επέκτασης

Πολλές περιοχές είναι δύσκολο να διασυνδεθούν με καλώδιο μέσω ενός παραδοσιακού συνδεμένου με καλώδιο LAN. Τα παλαιότερα κτίρια είναι
συχνά ένα πρόβλημα. Το πέρασμα του καλωδίου μέσω των τοίχων ενός παλαιότερου κτιρίου από πέτρα του οποίου το σχέδιο έχει χαθεί μπορεί να είναι μια πρόκληση. Σε πολλούς ιστορικούς χώρους οι νόμοι συντήρησης καθιστούν δύσκολο το να πραγματοποιηθούν οι νέες εγκαταστάσεις του τοπικού LAN στα παλαιότερα κτήρια. Ακόμη και στις σύγχρονες εγκαταστάσεις, η ενσύρματη εγκατάσταση μπορεί να είναι ακριβή και χρονοβόρα.

Ευελιξία

Η έλλειψη καλωδίων σημαίνει ότι δεν υπάρχει η ανάγκη επανακαλωδίωσης όταν υπάρξει κάποια αλλαγή στο δίκτυο. Τα ασύρματα δίκτυα επιτρέπουν στους χρήστες να διαμορφώσουν γρήγορα άμορφα, μικρά δίκτυα ομάδας για μια συνεδρίαση, και η ασύρματη δικτύωση κάνει την κίνηση μεταξύ θαλάμων και γραφείων κάτι πολύ εύκολο. Η επέκταση με τα ασύρματα δίκτυα είναι εύκολη επειδή το μέσο είναι ήδη παντού. Η ευελιξία είναι το μεγάλο συγκριτικό πλεονέκτημα για την κυρίως αγορά που αποτελείται από τα ξενοδοχεία, τους αερολιμένες, τους σταθμούς τραίνων, τις βιβλιοθήκες και άλλους χώρους όπου βρίσκονται πολλοί κινούμενοι χρήστες.

Κόστος

Σε μερικές περιπτώσεις, οι δαπάνες μπορούν να μειωθούν με τη χρησιμοποίηση της ασύρματης τεχνολογίας. Για παράδειγμα, ο εξοπλισμός ενός 802.11 ασύρματου δικτύου μπορεί να χρησιμοποιηθεί για να δημιουργήσει μια ασύρματη γέφυρα μεταξύ δύο κτηρίων. Η σύσταση μιας ασύρματης γέφυρας απαιτεί κάποιο κόστος αρχικού κεφαλαίου που περιλαμβάνει εξωτερικό εξοπλισμό, σημεία πρόσβασης και ασύρματες διεπαφές. Μετά από τις δαπάνες αρχικού κεφαλαίου, ωστόσο το

βασισμένο στο 802.11 ασύρματο δίκτυο οπτικής επαφής θα έχει αμελητέα επαναλαμβανόμενη μηνιαία δαπάνη. Με το πέρασμα του χρόνου, οι από σημείο σε σημείο ασύρματες συνδέσεις είναι πολύ φτηνότερες από την μίσθωση της τηλεφωνικής γραμμής από την τηλεφωνική επιχείρηση.

Μέχρι την ολοκλήρωση των 802.11 προτύπων το 1997, εντούτοις, χρήστες που ήθελαν να έχουν τα πλεονεκτήματα αυτών των ιδιοτήτων αναγκάστηκαν να υιοθετήσουν λύσεις ενός προμηθευτή με την όλη διακινδύνευση που αυτό συνεπάγεται. Μόλις εισηχθεί το 802.11 οι ταχύτητες αυξήθηκαν γρήγορα από 2 Mbps σε 11 Mbps και έπειτα σε 54 Mbps. Οι τυποποιημένες ασύρματες διεπαφές και οι κεραίες έχουν κάνει δυνατή την δημιουργία ασύρματων δικτύων. Διάφοροι φορείς παροχής υπηρεσιών άρχισαν να συμμετέχουν στην ιδέα, και ενθουσιώδεις εθελοντές στις περισσότερες μεγάλες πόλεις άρχισαν να χτίζουν κοινά ασύρματα δίκτυα βασισμένα στο πρωτόκολλο 802.11.

Το προφανέστερο πλεονέκτημα της ασύρματης δικτύωσης είναι η *κινητικότητα*. Ασύρματοι χρήστες μπορούν να συνδέονται με τα υπάρχοντα δίκτυα και επιτρέπεται έπειτα να περιπλανηθούν ελεύθερα. Με ένα κινητό τηλέφωνο ο χρήστης μπορεί να οδηγήσει χιλιόμετρα κατά τη διάρκεια μιας ενιαίας συνομιλίας επειδή το τηλέφωνο συνδέει χρήστες μέσω των πύργων κυψελών. Αρχικά, η κινητή τηλεφωνία ήταν ακριβή και το κόστος περιόρισε την χρήση της. Χρησιμοποιούνταν από επαγγελματίες που κινούνταν πολύ όπως οι διευθυντές πωλήσεων και από ανώτερους υπαλλήλους υπεύθυνους για τη λήψη αποφάσεων. Η κινητή τηλεφωνία έχει αποδειχθεί ιδιαίτερα χρήσιμη υπηρεσία. Το ίδιο μπορεί να αποδειχθεί και για την ασύρματη σύνδεση δικτύων. Ένα ασύρματο δίκτυο αφήνει ελεύθερο ένα χρήστη από τα δεσμά ενός Ethernet. Οι χρήστες του δικτύου μπορούν να λειτουργήσουν στη βιβλιοθήκη, σε ένα δωμάτιο διασκέψεων, στο χώρο στάθμευσης ή ακόμα και στο σπίτι. Εφ' όσον παραμένουν οι ασύρματοι χρήστες μέσα στην κάλυψη του σταθμού βάσης, μπορούν να εκμεταλλευθούν το δίκτυο.

Τα ασύρματα δίκτυα, όπως και τα αντίστοιχα ενσύρματα, εκμεταλλεύονται την ηλεκτρική τάση, ώστε να είναι δυνατή η επικοινωνία μεταξύ των συσκευών. Μεταβολές στην ισχύ του σήματος από μηδέν μέχρι μια μέγιστη τιμή (πλάτος) και, ο ρυθμός των μεταβολών αυτών (συχνότητα), χρησιμοποιούνται κατάλληλα για την κωδικοποίηση και την αποκωδικοποίηση της πληροφορίας. Όταν δύο συσκευές κατανοούν τις μεθόδους που χρησιμοποιούνται για την κωδικοποίηση και αποωδικοποίηση της πληροφορίας που περιέχεται στις μεταβολές των ηλεκτρικών ιδιοτήτων του μέσου επικοινωνίας (κανάλι), τότε είναι σε θέση να επικοινωνούν μεταξύ τους.

Η προφανής διαφορά μεταξύ των ενσύρματων και ασύρματων δικτύων είναι ότι τα δεύτερα χρησιμοποιούν σήματα ραδιοσυχνότητας (Radio Frequency — RF), που δημιουργούνται εφαρμόζοντας εναλλασσόμενο ρεύμα σε μια κεραία για την παραγωγή ενός ηλεκτρομαγνητικού πεδίου (Electromagnetic - EM). Το πεδίο RF που προκύπτει χρησιμοποιείται από τις συσκευές για μετάδοση και λήψη. Στην περίπτωση των ασύρματων δικτύων, το μέσο επικοινωνίας είναι το πεδίο EM, δηλαδή, η περιοχή του χώρου που επηρεάζεται από την ηλεκτρομαγνητική ακτινοβολία. Όπως συμβαίνει και στα ενσύρματα δίκτυα, το πλάτος μειώνεται με την απόσταση, με αποτέλεσμα την υποβάθμιση της ισχύος του σήματος και τελικά της δυνατότητας επικοινωνίας.

1.2 Ραδιοφάσμα

Οι ασύρματες συσκευές περιορίζονται για να λειτουργήσουν σε μια ορισμένη ζώνη συχνότητας. Κάθε ζώνη έχει σχετικό *εύρος ζώνης*, το οποίο είναι απλά το διάστημα συχνότητας στη ζώνη.
Το εύρος ζώνης έχει αποκτήσει την έννοια του μέτρου της χωρητικότητας δεδομένων μιας σύνδεσης. Μαθηματικά, θεωρία πληροφοριών, και επεξεργασία σήματος μπορούν να χρησιμοποιηθούν για να αποδείξουν ότι υψηλό εύρος ζώνης μπορεί να χρησιμοποιηθεί για να διαβιβαστούν περισσότερες πληροφορίες. Σαν παράδειγμα, ένα αναλογικό κανάλι κινητής τηλεφωνίας απαιτεί ένα εύρος ζώνης 20 kHz. Σήματα τηλεόρασης είναι φυσικά πιο σύνθετα και έχουν ένα αντίστοιχα μεγαλύτερο εύρος ζώνης 6 MHz.

Η χρήση ενός ραδιοφάσματος ελέγχεται αυστηρά από τις ρυθμιστικές αρχές με διαδικασίες *χορήγησης αδειών*. Στις ΗΠΑ, ο κανονισμός γίνεται από την Επιτροπή Ομοσπονδιακών Επικοινωνιών (FCC). Η ευρωπαϊκή κατανομή εκτελείται από το γραφείο των Ευρωπαϊκών Ραδιοεπικοινωνιών του CEPT (ERO). Άλλη εργασία κατανομής γίνεται από την Διεθνή Ένωση Τηλεπικοινωνιών (ITU). Για να αποτραπούν οι επικαλύψεις συχνότητας των ραδιοκυμάτων, η συχνότητα διατίθεται μέσα σε ζώνες, οι οποίες είναι απλά φάσματα συχνοτήτων διαθέσιμων σε συγκεκριμένες εφαρμογές

1.3 Τι είναι το πρωτόκολλο IEEE 802.11

Το standard 802.11 είναι το πρώτο standard για WLAN και εώς τώρα το μοναδικό που βρίσκεται στην αγορά.Η υλοποίηση του standard ξεκίνησε το 1987 σαν μέρος του IEEE 802.4 token bus standard με τον αριθμό γκρουπ IEEE 802.4L. Το IEEE 802.4 πρωτόκολλο είναι το αντίστοιχο των IEEE 802.3 και IEEE 802.5 τα οποία έχουν σχεδιαστεί με γνώμονα το βιομηχανικό περιβάλλον. Ένα από τα βασικά κίνητρα για την ανάπτυξη των WLAN's ήταν για να χρησιμοποιηθούν από τη βιομηχανία στην επικοινωνία μεταξύ διαφόρων μηχανημάτων. Για αυτό το λόγο μεγάλες εταιρείες όπως η GM(General Motors) συμμετείχαν ενεργά στην ανάπτυξη του 802.4L ειδικά κατά τα πρώτα στάδια της ανάπτυξης του. Το 1990 η ομάδα εργασίας του 802.4L μετονομάστηκε σε IEEE 802.11 δημιουργώντας ένα ανεξάρτητο 802.11 standard ώστε να ορίσει το φυσικό στρώμα και το MAC στρώμα για WLANs. Το πρώτο IEEE 802.11 standard για ταχύτητες 1 και 2 Mbps ολοκληρώθηκε το 1997 υποστηρίζοντας DSSS , FHSS και φυσικό στρώμα διάχυτων υπέρυθρων ακτίνων (DFIR). Από την ολοκλήρωση αυτού του standard , καινούργιες υλοποιήσεις του φυσικού στρώματος που υποστηρίζουν 11Mbps χρησιμοποιώντας CCK (IEEE 802.11b) και 54Mbps χρησιμοποιώντας OFDM (IEEE 802.11a) έχουν υλοποιηθεί. Και οι τρεις αυτές εκδόσεις του 802.11 μοιράζονται το ίδιο στρώμα MAC που χρησιμοποιεί πρωτόκολλο Ανίχνευσης Φέροντος Μέσου Πολλαπλής Πρόσβασης με Αποφυγή Σύγκρουσης (Carrier Sense Multiple Access with Collision Avoidance - CSMA/CA) για αποθήκευση δεδομένων , μηχανισμό αίτησης αποστολής / αποδεκτής αποστολής (RTS/CTS) για να προσπεράσουν το πρόβλημα κρυμμένου τερματικού και έναν προαιρετικό μηχανισμό που λέγεται λειτουργία συντονισμού σημείων (PCF) για να υποστηρίξει εφαρμογές ευαίσθητες στην

απόκριση χρόνου. Το IEEE 802.11 standard υποστηρίζει τόσο WLAN's βασισμένα στη λογική του πελάτη – εξυπηρετητή όσο και ad hoc δίκτυα με ισότιμους peers.

Το IEEE 802.11 standard ήταν το πρώτο standard ασύρματων δικτύων που είχε να αντιμετωπίσει την πρόκληση να ορίσει ένα συστηματικό standard για ασύρματα ευρυζωνικά δίκτυα. Σε σύγκριση με τα ενσύρματα δίκτυα τύπου LAN , τα WLAN's λειτουργούν κάτω από αντίξοες συνθήκες μέσου μεταφοράς (αέρας) και έχουν μεγάλες απαιτήσεις σε φορητότητα και ασφάλεια. Το ασύρματο μέσο μεταφοράς έχει μεγάλους περιορισμούς στο εύρος ζώνης και περιοριστικούς κανονισμούς όσον αφορά τις συχνότητες που μπορεί να χρησιμοποιήσει. Επιπλέον , έχει το πρόβλημα της παρεμβολής από ανακλάσεις του σήματος (multipath fading). Το WLAN υπόκειται σε παρεμβολές από άλλα γειτονικά WLANs ή γενικά συσκευές ραδιοεπικοινωνίας ή μη (φούρνοι μικροκυμάτων , παλιά ασύρματα τηλέφωνα). Τα standard ασύρματης επικοινωνίας πρέπει να είναι σχεδιασμένα ώστε να υποστηρίζουν φορητότητα του χρήστη , χαρακτηριστικό που δεν υποστηρίζεται από κανένα άλλο standard τύπου LAN. Η ομάδα εργασίας του IEEE 802.11 έπρεπε να εξετάσει τη διαχείριση σύνδεσης , διαχείριση διασφάλισης σταθερότητας της σύνδεσης και διαχείριση εξοικονόμησης ενέργειας · κανένα από αυτά δεν υφίσταται σε κάποιο άλλο πρωτόκολλο της σειράς 802. Επίσης τα WLANs δεν έχουν φυσικά όρια (όριο του WLAN είναι τα σημεία όπου εξασθενεί τόσο το σήμα ώστε να είναι αδύνατη η πρόσβαση σε αυτό) και συνήθως επικαλύπτονται με γειτονικά WLANs έτσι η ομάδα που τυποποίησε τα standard έπρεπε να βρουν κάποιο τρόπο ώστε να οριστεί ένα ισχυρό επίπεδο ασφάλειας μεταξύ των ζεύξεων. Για όλους τους παραπάνω αναφερθέντες λόγους συν των διαφόρων ανταγωνιστικών standards χρειάστηκαν σχεδόν 10 χρόνια για την υλοποίηση του IEEE 802.11 χρόνος που είναι αρκετά μεγαλύτερος από αυτόν που απαιτήθηκε για άλλα standard τύπου 802 που σχεδιάστηκαν για ενσύρματα μέσα. Μόλις παρουσιάστηκε το γενικό πλαίσιο χρειάστηκε αρκετά μικρότερος χρόνος για να αναπτυχθούν οι επεκτάσεις IEEE 802.11b και 802.11a .

1.4 Προδιαγραφές 802.11

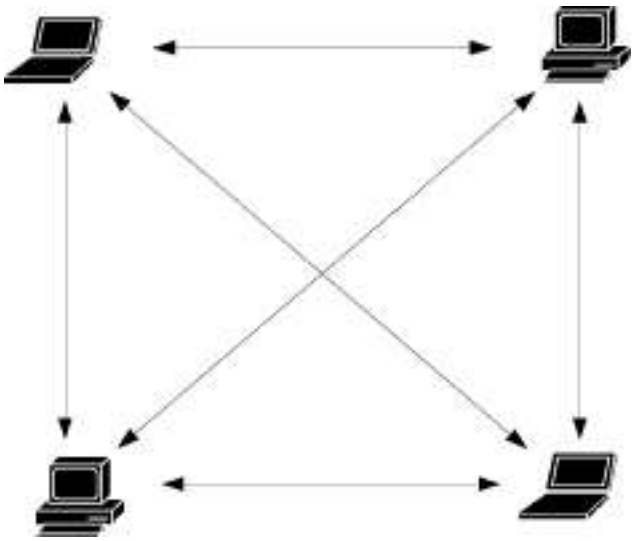
Το πρωτόκολλο 802.11 υποστηρίζει ρυθμούς μετάδοσης δεδομένων της τάξεως των 1Mbps και 2Mbps. Η μετάδοση του σήματος γίνεται είτε στην ISM ζώνη συχνοτήτων (2.4GHz – 2.4835GHz), είτε με υπέρυθρη ακτινοβολία μήκους κύματος 850nm. Για την μετάδοση του σήματος στην ISM ζώνη χρησιμοποιείται διαμόρφωση FSK 2 – επιπέδων για ρυθμούς 1Mbps και FSK 4 – επιπέδων για ρυθμούς 2Mbps. Για την επικοινωνία μέσω υπερύθρων χρησιμοποιείται διαμόρφωση PPM (Pulse Position Modulation). Για μεγαλύτερη ανθεκτικότητα στον θόρυβο στενής ζώνης το σήμα κωδικοποιείται με μεθόδους απλωμένου φάσματος. Το πρωτόκολλο υποστηρίζει την μέθοδο εναλλαγής συχνότητας (FHSS) και ευθείας ακολουθίας (DSSS) για αυτό το σκοπό. Η μέγιστη εκπεμπόμενη ισχύς καθορίζεται από τους περιορισμούς που υπάρχουν για την χρήση της ISM ζώνης συχνοτήτων και περιορίζεται στα 20dBm ενώ η ευαισθησία του δέκτη, ορίζεται από το πρωτόκολλο, ότι πρέπει να είναι μικρότερη ή ίση των –80dBm για FER της τάξης του 3%.

1.5 Αρχιτεκτονική

Το πρότυπο IEEE 802.11 παρέχει δύο διαφορετικές αρχιτεκτονικές για την επικοινωνία μεταξύ ασύρματων συσκευών: λειτουργία κατά περίπτωση (ad-hoc mode) και λειτουργία υποδομής (infrastructure mode). Στη συνέχεια παρουσιάζουμε κάθε τρόπο λειτουργίας ξεχωριστά.

Λειτουργία κατά περίπτωση (ad-hoc)

Η λειτουργία Ασύρματων Τοπικών Δικτύων κατά περίπτωση, επιτυγχάνει τη διασύνδεση ασύρματων συσκευών που είναι σε θέση να επικοινωνούν απ' ευθείας μεταξύ τους. Επομένως, στην αρχιτεκτονική αυτή, οι σταθμοί ομαδοποιούνται σε μια περιορισμένη γεωγραφική περιοχή. Η λειτουργία κατά περίπτωση είναι παρόμοια με τα δίκτυα ομοτίμων οντοτήτων (peer-to-peer networks), όπου κανένας κόμβος δεν απαιτείται, να παίζει το ρόλο του εξυπηρετητή. Οι διασυνδεδεμένες συσκευές στη λειτουργία κατά περίπτωση, αναφέρονται και με τον όρο **Ανεξάρτητο Σύνολο Βασικών Υπηρεσιών** (Independent Basic Service Set - IBSS). Η τοπολογία κατά περίπτωση φαίνεται στο Σχ. 1.1.

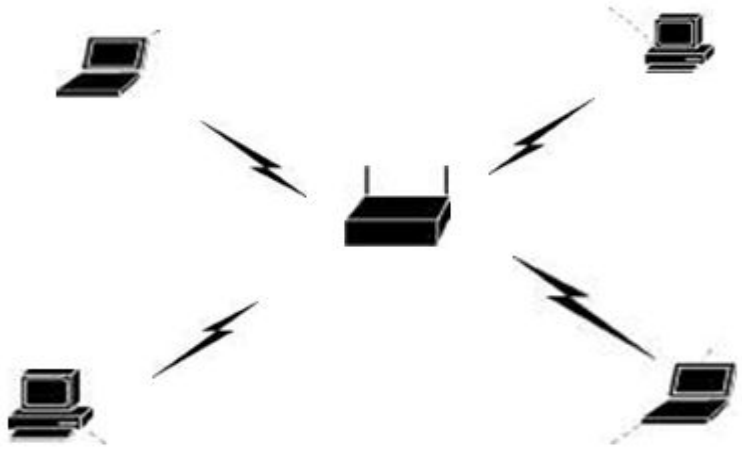


Σχήμα 1.1: Λειτουργία Ασύρματου Τοπικού Δικτύου κατά περίπτωση

Λειτουργία υποδομής

Η λειτουργία Ασύρματων Τοπικών Δικτύων υποδομής βασίζεται σε σταθερά **σημεία πρόσβασης** (access points), με τη βοήθεια των οποίων, καθίσταται δυνατή η επικοινωνία των ασύρματων κόμβων. Το δίκτυο υποδομής επιτυγχάνει την επέκταση του εύρους του ενσύρματου Τοπικού Δικτύου σε ασύρματες κυψέλες. Μια ασύρματη συσκευή είναι, σε θέση να μετακινείται από κυψέλη σε κυψέλη, δηλαδή από σημείο πρόσβασης σε σημείο πρόσβασης, διατηρώντας την πρόσβασή της στους πόρους του Τοπικού Δικτύου. Μια κυψέλη είναι η περιοχή που καλύπτεται από ένα

σημείο πρόσβασης και ονομάζεται **Σύνολο Βασικών Υπηρεσιών** (Basic Service Set — BSS). Το σύνολο όλων των κυψελών ενός δικτύου υποδομής ονομάζεται **Επεκτεταμένο Σύνολο Υπηρεσιών** (Extended Service Set - ESS). Η τοπολογιά υποδομής φαίνεται στο Σχ. 1.2.



Σχήμα 1.2: Λειτουργία Ασύρματου Τοπικού δικτύου υποδομής

1.6 Τεχνικά χαρακτηριστικά

Οι λειτουργίες που προδιαγράφονται από το πρότυπο IEEE 802.11 ανήκουν στο Φυσικό επίπεδο και το επίπεδο Ζεύξης Δεδομένων, ενώ τα δεδομένα των ανώτερων επιπέδων θεωρούνται ωφέλιμο φορτίο (payload). Τα πλαίσια (frames) που ορίζονται από το πρωτόκολλο διακρίνονται σε τρεις τύπους: **διαχείρισης** (management), **ελέγχου** (control) και **δεδομένων** (data). Γενικά, κάθε τύπος πλαισίου παρέχει μεθόδους προκειμένου οι ασύρματες συσκευές να εντοπίσουν, να συσχετιστούν (associate), να αποσυσχετιστούν (disassociate), και να επαληθεύσουν την ταυτότητα τους μεταξύ τους. Επιπρόσθετα, ορίζονται λειτουργίες ώστε να μεταβάλλεται ο ρυθμός μετάδοσης ανάλογα με το επίπεδο ισχύος του σήματος, καθώς επίσης, και λειτουργίες για την εξοικονόμηση ενέργειας.

Από το σύνολο των πληροφοριών που μεταδίδονται, μέσω των πλαισίων ελέγχου του πρωτοκόλλου IEEE 802.11, αξίζει να γίνει αναφορά στο **Αναγνωριστικό Συνόλου Υπηρεσιών** (Service Set Identifier - SSID). Πρόκειται για το αναγνωριστικό που διαθέτει κάθε ασύρματο δίκτυο (ή υποσύνολό του) και διακρίνεται σε IBSSID, BSSID και ESSID, ανάλογα με τον τύπο λειτουργίας που αναφέρεται,, IBSS, BSS και ESS, αντίστοιχα. Όταν λειτουργούν περισσότερα από ένα Ασύρματα Τοπικά Δίκτυα στον ίδιο χώρο, το SSID χρησιμοποιείται για την επιλογή του δικτύου με το οποίο θέλει να συνδεθεί μια ασύρματη συσκευή.

1.7 Παραλλαγές του 802.11

Το πρωτόκολλο IEEE 802.11 είναι στην πραγματικότητα ένα *σύνολο* προτύπων που προδιαγράφουν τη μετάδοση δεδομένων πάνω από Ασύρματα Τοπικά Δίκτυα. Τα πρότυπα αυτά είναι τα εξής:

i. 802.11 a – OFDM in 5GHz Band

Το 802.11a αποτελεί ένα πρωτόκολλο για το φυσικό επίπεδο ενός ασυρμάτου δικτύου το οποίο καθορίζει την λειτουργία αυτού στην ζώνη UNII των 5GHz. Χρησιμοποιείται διαμόρφωση ορθογώνιας διαίρεσης συχνότητας (OFDM) και υποστηρίζει ρυθμούς μετάδοσης μέχρι και 54Mbps. Λόγω της λειτουργίας του στην ζώνη UNII όπου υπάρχουν πολύ λιγότερες παρεμβολές από την ζώνη ISM και του υψηλότερου ρυθμού μετάδοσης προσφέρει πολύ καλύτερες επιδόσεις τόσο από το κλασσικό 802.11 όσο και από το νεότερο και ευρύτερα εξαπλωμένο 802.11b.

ii. 802.11 b – High Rate DSSS

Η ομάδα εργασίας 802.11b είχε αναλάβει την εργασία, να επεκτείνει τον τρόπο κωδικοποίησης DSSS του φυσικού επιπέδου του 802.11 ώστε να υποστηρίζει ρυθμούς μετάδοσης της τάξης των 5.5Mbps και 11Mbps. Για να το πετύχει αυτό, τροποποιήθηκε ο τρόπος διαμόρφωσης του σήματος. Έτσι για την επίτευξη των νέων ρυθμών χρησιμοποιήθηκε διαμόρφωση CCK, ενώ για τους ρυθμούς των 1Mbps και 2Mbps, ώστε να κρατηθεί η συμβατότητα με το 802.11, χρησιμοποιήθηκε διαμόρφωση DBPSK (Differential Binary) και DQPSK (Differential Quadratic) αντίστοιχα.

iii. 802.11 c – Bridge Op Procedures

Το 802.11c παρέχει απαραίτητες πληροφορίες για να διασφαλιστεί η σωστή λειτουργία των bridges. Οι πληροφορίες που περιέχονται σε αυτό το πρωτόκολλο χρησιμοποιούνται κυρίως από τους κατασκευαστές σημείων πρόσβασης ώστε να εξασφαλίζεται η διαλειτουργικότητά τους με συσκευές άλλων κατασκευαστών.

iv. 802.11 d – Global Harmonization

Η ομάδα εργασίας 802.11d έχει αναλάβει την εργασία να καθορίσει τις απαιτήσεις του φυσικού επιπέδου καθώς και να καταγράψει το νομικό πλαίσιο που

ισχύει για την χρησιμοποίηση ραδιοσυχνοτήτων σε διάφορες χώρες ώστε να μπορούν να κατασκευαστούν προϊόντα που θα λειτουργούν σε διάφορες γεωγραφικές περιοχές.

v. 802.11 e – MAC Enhancements for QoS

Χωρίς καλό QoS (Quality of Service) το αρχικό πρωτόκολλο 802.11 δεν βελτιστοποιεί την μετάδοση φωνής και video. Αυτό ακριβώς το μειονέκτημα έρχεται να καλύψει η ομάδα εργασίας 802.11e τροποποιώντας το υποεπίπεδο MAC και βελτιώνοντας το QoS του πρωτοκόλλου.

vi. 802.11 F – Inter Access Point Protocol

Η αρχική ομάδα εργασίας του 802.11 σκοπίμως δεν προσδιορίζει την επικοινωνία μεταξύ σημείων πρόσβασης με σκοπό την υποστηρίξει της περιαγωγής των χρηστών από ένα σημείο πρόσβασης σε ένα άλλο. Η επιλογή αυτή δίνει ευελιξία όταν χρησιμοποιούνται διάφορα distribution system. Το πρόβλημα, όμως που ανακύπτει είναι ότι τα σημεία πρόσβασης από διαφορετικούς κατασκευαστές μπορεί να μην λειτουργούν ομαλά μεταξύ τους όταν υποστηρίζουν λειτουργίες περιαγωγής. Το 802.11f έρχεται ακριβώς σε αυτό το σημείο, να φτιάξει μια προδιαγραφή που θα παρέχει στα σημεία πρόσβασης της απαραίτητες πληροφορίες για να γίνει μια περιαγωγή με επιτυχία και να εξασφαλιστεί η ομαλή λειτουργία του συστήματος. Το κεφαλαίο “F” στην ονομασία δείχνει ότι είναι μια προτεινόμενη πρακτική και όχι πρότυπο.

vii. 802.11 g – Union of .11a and .11b

Η παραλλαγή αυτή του 802.11 έχει ως αντικείμενο εργασίας να προσφέρει ρυθμούς μετάδοσης της τάξης των 54Mbps, όπως και το 802.11a διατηρώντας όμως την συμβατότητα με το διαδεδομένο 802.11b. Λειτουργεί στην ISM ζώνη συχνοτήτων όπως το 802.11b αλλά χρησιμοποιεί διαμόρφωση OFDM όπως το 802.11a για να πετύχει υψηλούς ρυθμούς μετάδοσης. Χάριν συμβατότητας με το 802.11b υποστηρίζεται και η διαμόρφωση CCK.

viii. 802.11 h – UNII for Europe

Η προδιαγραφή αυτή είναι συμπληρωματική του υποεπιπέδου MAC και συμμορφώνεται με τους ευρωπαϊκούς κανονισμούς για την χρήση της ζώνης συχνοτήτων στα 5GHz. Συγκεκριμένα οι ευρωπαϊκοί κανονισμοί απαιτούν για τις συσκευές που λειτουργούν σε αυτή την ζώνη συχνοτήτων να έχουν δυνατότητες ελέγχου εκπεμπόμενης ισχύος (Transmission Power Control) και δυναμικής επιλογής συχνότητας (Dynamic Frequency Selection).

ix. 802.11 i – Enhanced Security

Η προδιαγραφή αυτή έρχεται να καλύψει πολλά από τα κενά σε θέματα ασφαλείας που βρέθηκαν στο πρωτόκολλο κρυπτογράφησης WEP του 802.11. Ο αλγόριθμος RC4 της RCA που χρησιμοποιείται αποδείχτηκε ανεπαρκής, με πολλά σφάλματα και παραλήψεις, κάνοντας τα ασύρματα δίκτυα εύκολο στόχο σε διάφορα είδη επιθέσεων. Με την νέα προδιαγραφή καθορίζονται πρωτόκολλα για τα κλειδιά κρυπτογράφησης όπως τα TKIP (Temporal Key Integrity Protocol) και AES (Advanced Encryption Standard).

x. 802.11 j - Extensions for Japan (2004)

Ειδικά σχεδιασμένο για την Ιαπωνική αγορά. Τελειοποιήθηκε το 2004. Το πρωτόκολλο αυτό λειτουργεί στα 4.9 GHz όπως επίσης και στα 5GHz ώστε να συμμορφώνεται με τους Ιαπωνικούς κανόνες για λειτουργία ραδιοκυμάτων σε εσωτερικούς και εξωτερικούς χώρους.

Το 802.11j καθορίζει τις μεθόδους που επιτρέπουν στα APs να κινηθούν σε νέες συχνότητες ή να αλλάξουν το πλάτος των καναλιών για καλύτερη απόδοση ή χωρητικότητα -- παραδείγματος χάριν, για να αποφύγει τις παρεμβολές με άλλες ασύρματες εφαρμογές.

xi. 802.11 k - Radio resource measurement enhancements

Το IEEE 802.11k είναι ένα προτεινόμενο πρότυπο για τη διαχείριση των πόρων της ασύρματης επικοινωνίας.
Καθορίζει και προβάλλει τις πληροφορίες της ασύρματης σύνδεσης καθώς και του δικτύου για να διευκολύνει τη διαχείριση και τη συντήρηση ενός κινητού WLAN. Τα IEEE 802.11k και IEEE 802.11r είναι τα βασικά πρότυπα βιομηχανίας που αναπτύσσονται τώρα και θα επιτρέψουν τις μεταβάσεις Basic Service Set (BSS) σε περιβάλλον WLAN. Το πρότυπο 802.11k παρέχει τις πληροφορίες για να
βρεθεί το καλύτερο δυνατό σημείο πρόσβασης.

Το 802.11k προορίζεται να βελτιώσει τον τρόπο που η κυκλοφορία διανέμεται μέσα σε ένα δίκτυο. Σε ένα ασύρματο τοπικό LAN, κάθε συσκευή συνδέεται φυσιολογικά με το σημείο πρόσβασης (AP) που παρέχει το ισχυρότερο σήμα. Ανάλογα με τον αριθμό και τις γεωγραφικές θέσεις των συνδρομητών, αυτή η

ρύθμιση μπορεί μερικές φορές να οδηγήσει στην υπερβολική απασχόληση ενός AP και την υποεκμετάλλευση άλλων, με συνέπεια την υποβάθμιση της γενικής απόδοσης του δικτύου. Σε ένα δίκτυο που προσαρμόζεται στο 802.11k, εάν το AP που έχει το ισχυρότερο σήμα φορτωθεί έως τη μέγιστη χωρητικότητα του, τότε μια ασύρματη συσκευή συνδέεται σε ένα από τα υποχρησιμοποιούμενα APs. Ακόμα κι αν το σήμα είναι πιο αδύναμο, το γενικότερο throughput είναι μεγαλύτερο επειδή γίνεται αποδοτικότερη χρήση των πόρων του δικτύου.

xii. 802.11 m - Maintenance of the standard

Το IEEE 802.11m είναι μια πρωτοβουλία για να εκτελούνται συντηρήσεις, διορθώσεις, βελτιώσεις, διευκρινίσεις, και ερμηνείες εκδόσεων σχετικά με την οικογένεια προτύπων IEEE 802.11.

Η πρωτοβουλία 802.11m, αποκαλούμενη μερικές φορές "802.11 οικοκυρική" ή "καθαρισμός του 802.11" ξεκίνησε το 1999 από την υποομάδα m του IEEE που αποτελεί τμήμα της ομάδας εργασίας IEEE 802.11.

xiii. 802.11 n - Higher throughput improvements

Τον Ιανουάριο του 2004 η IEEE ανήγγειλε ότι έχει σχηματίσει μια νέα ομάδα εργασίας (TaskGroup n) για να αναπτύξει μια νέα τροποποίηση του 802.11 προτύπου για τα WLAN. Το πραγματικό throughput υπολογίζεται να φθάσει θεωρητικά τα 540 MBIT/S, δηλαδή μέχρι 40 φορές γρηγορότερο από το 802.11b, και περίπου 10 φορές γρηγορότερο από το 802.11a ή το 802.11g. Προβλέπεται επίσης ότι το 802.11n θα προσφέρει μια καλύτερη απόσταση λειτουργίας από τα τρέχοντα δίκτυα.

Υπήρξαν δύο ανταγωνιστικές προτάσεις του προτύπου 802.11n: Η WWiSE (World-Wide Spectrum Efficiency), που υποστηρίζεται από εταιρίες όπως η Broadcom, και η TGn Sync που υποστηρίζεται από τις Intel και Philips.

Οι ανταγωνίστριες TGn Sync και WWiSE, και μια τρίτη ομάδα, η MITMOT, ανακοίνωσαν στα τέλη Ιουλίου 2005 ότι θα συγχώνευαν τις αντίστοιχες προτάσεις τους ως ένα σχέδιο που θα στελνόταν στην IEEE το Σεπτέμβριο και μια τελική έκδοση θα υποβαλλόταν το Νοέμβριο. Η διαδικασία τυποποίησης αναμένεται να ολοκληρωθεί το δεύτερο μισό του 2006.

Το 802.11n αναπτύχθηκε με βάση τα προηγούμενα πρότυπα 802.11 προσθέτοντας το MIMO (multiple-input multiple-output). Το MIMO χρησιμοποιεί πολλαπλούς πομπούς και κεραίες λήψης για να επιτρέψει το αυξανόμενο throughput δεδομένων μέσω πολυπλεξίας και το αυξανόμενο εύρος με την εκμετάλλευση της χωρικής ποικιλομορφίας, ίσως μέσω κωδικοποιήσεων όπως η κωδικοποίηση Alamouti.

Η επιτροπή Enhanced Wireless Consortium (EWC) διαμορφώθηκε για να βοηθήσει έτσι ώστε να επιταχυνθεί η διαδικασία ανάπτυξης του 802.11n και να προωθήσει τις προδιαγραφές τεχνολογίας για τη διαλειτουργικότητα των ασύρματων προϊόντων τοπικού δικτύου (WLAN) επόμενης γενιάς.

xiv. 802.11 p - WAVE - Wireless Access for the Vehicular Environment

Το 802.11p που αναφέρεται και ως Wireless Access for the Vehicular Environment (WAVE) καθορίζει τον εμπλουτισμό του 802.11 έτσι ώστε να υποστηρίζει εφαρμογές έξυπνων μεταφορικων συστημάτων (Intelligent Transportation Systems (ITS). Αυτό περιλαμβάνει την ανταλλαγή στοιχείων μεταξύ των οχημάτων και μεταξύ των οχημάτων αυτών και της κατά μήκος του δρόμου υποδομής στη αδειοδοτημένη ITS μπάντα των 5,9 GHz.

Το 802.11p θα χρησιμοποιηθεί από το Υπουργείο Μεταφορών των Η.Π.Α για εφαρμογές όπως η είσπραξη διοδίων, υπηρεσίες ασφάλειας οχημάτων, και εμπορικές συναλλαγές μέσω των αυτοκινήτων. Το όραμα είναι ένα εθνικού επιπέδου δίκτυο που θα επιτρέπει τις επικοινωνίες μεταξύ των οχημάτων ή μεταξύ των οχημάτων και των διαφόρων σημείων πρόσβασης κατά μήκος του δρόμου. Η εργασία στηρίζεται στον προκάτοχό της, την ASTN a2213-O3.

Οι επίσημες προδιαγραφές του προτύπου αναμένεται να ανακοινωθούν τον Ιανουάριο του 2007.

xv. 802.11 r – Fast Roaming

Το 802.11r είναι μη εγκεκριμένο πρότυπο του IEEE 802.11 που προσδιορίζει τις γρήγορες BSS ("Basic Service Set") μεταβάσεις. Αυτό θα επιτρέψει τη σύνδεση από κινούμενα οχήματα, με γρήγορα handoffs από έναν σταθμό βάσης σε έναν άλλο σε ελάχιστο χρόνο. Τα Handoffs υποστηρίζονται από τις υλοποιήσεις "a", "b" και "g", αλλά μόνο για δεδομένα. Επίσης ο χρόνος handover είναι πάρα πολύ μεγάλος για να υποστηρίξει εφαρμογές όπως η φωνή και το βίντεο.

Η βασική εφαρμογή που προβλέπεται αυτήν την περίοδο για τα πρότυπα 802.11r είναι η μετάδοση φωνής μέσω διαδικτύου (Voice over IP (VOIP)) μέσω των κινητών τηλεφώνων που έχουν σχεδιαστεί ώστε να δουλεύουν με ασύρματα δίκτυα αντί των τυποποιημένων κυψελωτών δικτύων.

Αυτά τα ασύρματα κινητά τηλέφωνα-PDAs πρέπει να είναι σε θέση να αποσυνδεθούν γρήγορα από ένα σημείο πρόσβασης και να συνδεθούν σε ένα άλλο. Η καθυστέρηση που εμφανίζεται κατά τη διάρκεια του handoff δεν πρέπει να υπερβεί τα 50msec (το διάστημα που είναι ανιχνεύσιμο από το ανθρώπινο αυτί). Εντούτοις, οι τρέχουσες καθυστερήσεις περιαγωγής στα δίκτυα 802.11 υπολογίζονται κατά μέσο όρο σε εκατοντάδες msec. Αυτό μπορεί να οδηγήσει σε διακοπές στη μετάδοση, απώλεια σύνδεσης και υποβάθμιση της ποιότητας φωνής. Τα γρηγορότερα handoffs είναι απαραίτητα για την ευρύτερη χρήση της τεχνολογίας 802.11 για τη μετάδοση φωνής.

Ένα άλλο πρόβλημα με την τρέχουσα τεχνολογία 802.11 είναι ότι μια κινητή συσκευή δεν μπορεί να ξέρει εάν είναι διαθέσιμοι οι απαραίτητοι πόροι QoS σε ένα νέο σημείο πρόσβασης μέχρι να γίνει η μετάβαση. Κατά συνέπεια, δεν είναι δυνατό να είναι γνωστό από πριν εάν μια μετάβαση θα οδηγήσει σε ικανοποιητικότερη απόδοση εφαρμογής.

Το πρωτόκολλο 802.11r για να ελαχιστοποιήσει τις απώλειες σύνδεσης επιτρέπει σε έναν ασύρματο πελάτη πριν κάνει τη μετάβαση σε ένα νέο σημείο πρόσβασης να γνωρίζει την κατάσταση της ασφάλειας και του QoS. Οι γενικές αλλαγές στο πρωτόκολλο δεν εισάγουν νέες ευπάθειες ασφάλειας, πράγμα που

σημαίνει ότι διατηρείται η τρέχουσα κατάσταση των σταθμών βάσης και των σημείων πρόσβασης (APs).

xvi. 802.11 s - ESS Mesh Networking

Το 802.11s είναι μη εγκεκριμένο πρότυπο του IEEE 802.11 για τη δικτύωση του ESS Mesh. Προσδιορίζει μια επέκταση του IEEE 802.11 MAC για να λύσει το πρόβλημα διαλειτουργικότητας με τον καθορισμό μιας αρχιτεκτονικής και ενός πρωτοκόλλου που υποστηρίζουν εκπομπές multicast και unicast.

Πάνω σε αυτό το προτεινόμενο πρότυπο υπάρχουν διάφορες προτάσεις όπως η SEEMesh η οποία προτείνει την αναγνώριση παλιών καθώς και νέων τεχνολογιών ασύρματης δικτύωσης σε ένα δίκτυο μέσω των Mesh portals. Μια άλλη πρόταση είναι αυτή της Wi-Mesh η οποία προτείνει την επικοινωνία μεταξύ χρηστών ασύρματης τεχνολογίας ανεξάρτητα από την εταιρία παροχής των εξαρτημάτων.

xvii. 802.11 T - Wireless Performance Prediction (WPP)

Το IEEE 802.11T αναφέρεται επίσης ως η ασύρματη πρόβλεψη απόδοσης (Wireless Performance Prediction - WPP). Λαμβάνοντας υπόψη την πολυπλοκότητα της οικογένειας πρωτοκόλλων IEEE 802.11 ένας έλεγχος χαρακτηριστικών είναι ιδιαίτερα σημαντικός έτσι ώστε να εξακριβωθεί η απόδοση όπως και οι προδιαγραφές των προϊόντων. Το κεφαλαίο "T" στην ονομασία δείχνει ότι είναι μια προτεινόμενη πρακτική και όχι πρότυπο.

Ο στόχος του προγράμματος 802.11T είναι να παρασχεθεί ένα σύνολο μεθόδων μέτρησης, μετρικών απόδοσης, και προτεινόμενων δοκιμών που επιτρέπουν στους κατασκευαστές, στα ανεξάρτητα εργαστήρια δοκιμών, στους φορείς παροχής υπηρεσιών, και στους τελικούς χρήστες να μετρήσουν την απόδοση του τυποποιημένου εξοπλισμού και των δικτύων IEEE 802.11. Το πρόγραμμα προβλέπεται να ολοκληρωθεί τον Ιανουάριο του 2008.

xviii. 802.11 u - Interworking with External Networks

Το IEEE 802.11u είναι μια τροποποίηση του προτύπου IEEE 802.11 για να προσθέσει τα χαρακτηριστικά που βελτιώνουν την αλληλεπίδραση με εξωτερικά δίκτυα.

Το IEEE 802.11 υποθέτει ότι ένας χρήστης είναι εξουσιοδοτημένος από πριν για να χρησιμοποιήσει το δίκτυο. Το IEEE 802.11u καλύπτει τις περιπτώσεις όπου ο χρήστης δεν είναι εξουσιοδοτημένος από πριν. Ένα δίκτυο θα είναι σε θέση να επιτρέψει την πρόσβαση βασισμένη στη σχέση του χρήστη με ένα εξωτερικό δίκτυο (π.χ. συμφωνία περιαγωγής μεταξύ σημείων πρόσβασης), ή να υποδείξει ότι είναι δυνατή η απευθείας εγγραφή, ή να επιτρέψει την πρόσβαση σε ένα αυστηρά περιορισμένο σύνολο υπηρεσιών όπως οι κλήσεις έκτακτης ανάγκης.

Από την μεριά του χρήστη, ο στόχος είναι να βελτιωθεί η εμπειρία ενός χρήστη που ταξιδεύει και ανοίγει ένα laptop σε ένα ξενοδοχείο πολλά χιλιόμετρα μακριά από το σπίτι του. Αντί να του παρουσιαστεί ένας μακρύς κατάλογος με ανούσια SSIDs, θα μπορούσε να του παρουσιαστεί ένας κατάλογος δικτύων, οι υπηρεσίες που παρέχουν, και οι όροι κάτω από τους οποίους ο χρήστης θα μπορούσε να έχει πρόσβαση σε αυτά..

Οι προδιαγραφές απαιτήσεων του IEEE 802.11u περιέχουν τις απαιτήσεις στις περιοχές της εγγραφής, την επιλογή δικτύων, την υποστήριξη κλήσεων έκτακτης ανάγκης, την κατάτμηση της κίνησης των χρηστών, και την διαφήμιση υπηρεσιών. Το πρότυπο 802.11u είναι στο στάδιο αξιολόγησης των προτάσεών του.

xix. 802.11 v - Wireless Network Management

Το Ieee 802.11v είναι το πρότυπο της Διαχείρισης Ασύρματου Δικτύου (Wireless Network Management) για την οικογένεια προτύπων Ieee 802.11 . Η ομάδα εργασίας TGv δουλεύει σε μια τροποποίηση του Ieee 802.11 για να επιτρέψει τη διαμόρφωση των συσκευών των πελατών όταν συνδέονται σε δίκτυα 802.11. Το πρότυπο μπορεί να συμπεριλαμβάνει ένα κυψελοειδές σύστημα διαχείρισης. Το πρότυπο 802.11v είναι ακόμα στα αρχικά στάδια προτάσεων.

xx. 802.11 w - Protected Management Frames

Το Ieee 802.11w είναι το Πλαίσιο Προστατευμένης Διαχείρισης για την οικογένεια προτύπων Ieee 802.11 . Η ομάδα εργασίας TGw δουλεύει πάνω στη βελτίωση του Μέσου Στρώματος Ελέγχου Πρόσβασης (Medium Access Control layer) του 802.11 για να αυξήσει την ασφάλεια των πλαισίων διαχείρισης.

Τα ασύρματα δίκτυα στέλνουν πληροφορίες διαχείρισης συστήματος σε μη προστατευμένα πλαίσια, ενέργεια που τα καθιστά τρωτά. Αυτό το πρότυπο θα προστατεύσει από τη διάσπαση δικτύων, που προκαλείται από τα κακόβουλα συστήματα που πλαστογραφούν τα αιτήματα αποσύνδεσης και εμφανίζονται να στέλνονται από έγκυρο εξοπλισμό.

Αναμένεται ότι το 802.11w θα γίνει επέκταση του Ieee 802.11i ώστε να προσαρμόσει στο 802.11 πλαίσια διαχείρισης, καθώς επίσης και πλαίσια δεδομένων. Βέβαια αυτές οι επεκτάσεις θα αλληλεπιδρούν με τα πρότυπα Ieee 802.11r και Ieee 802.11u. Το πρότυπο 802.11w είναι στα αρχικά στάδια προτάσεων. Στόχος είναι να επικυρωθεί τον Μάρτιο του 2008.

xxi. 802.11 y - Contention Based Protocol (3.65-3.7GHz Operation in USA)

Το Ieee 802.11y είναι το Βασισμένο Στον Ανταγωνισμο Πρωτόκολλο (Contention Based Protocol) της οικογένειας προτύπων Ieee 802.11 . Τον Ιούλιο του 2005, η FCC άνοιξε τη χρήση της ζώνης συχνοτήτων 3.65-3.7GHz για δημόσια χρήση, που προηγουμένως χρησιμοποιούνταν από τα σταθερά δίκτυα δορυφορικών

υπηρεσιών. Η ομάδα εργασίας TGy θα δουλεύει πάνω σε τροποποιήσεις του Ieee 802.11 για τη λειτουργία ευζωνικών ασύρματων υπηρεσιών στη ζώνη 3.65-3.7GHz.

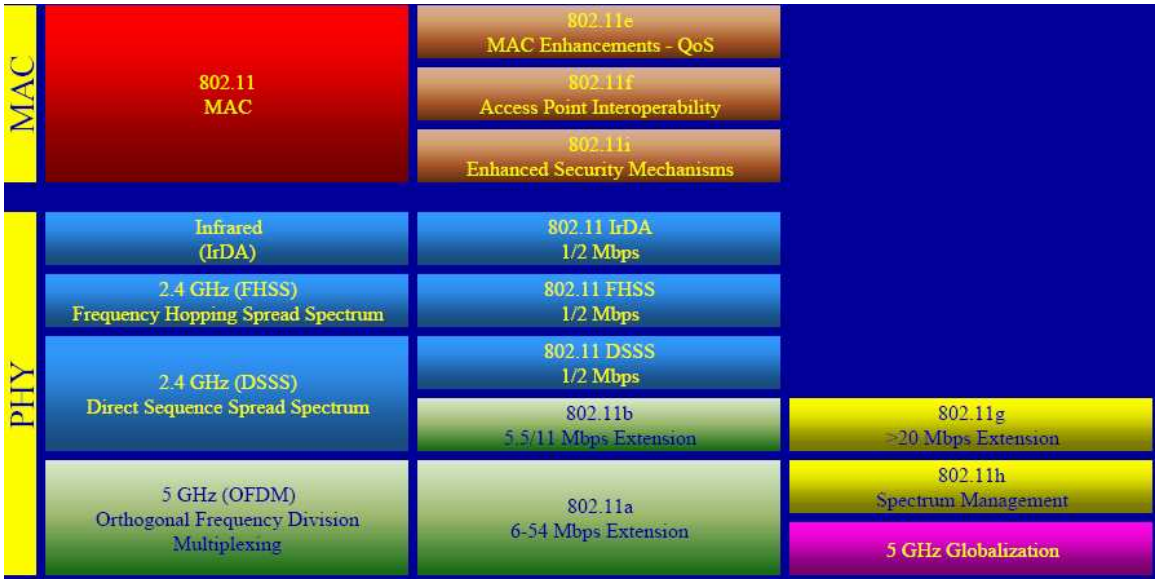
Το Ieee 802.11y παρέχει έναν τυποποιημένο μηχανισμό αποφυγής παρεμβολών, και επίσης προβλέπει μηχανισμό για την υιοθέτηση νέων συχνοτήτων στο μέλλον. Το πρότυπο 802.11y είναι στα αρχικά στάδια προτάσεων. (3/2006)

Σημείωση:

- *Οι χαρακτήρες -l- , -o- , και -q- , έχει αποφασιστεί ότι δεν θα χρησιμοποιηθούν για το συμβολισμό κάποιου προτύπου .*

- ***Προς αποφυγή σύγχυσης:** Δεν υπάρχει 802.11x πρότυπο ή ομάδα εργασίας , αυτός ο όρος απλά χρησιμοποιείται ανεπίσημα για να δείξει οποιαδήποτε τρέχοντα ή μελλοντικά 802.11 πρότυπα, σε περιπτώσεις όπου η περαιτέρω ακρίβεια δεν είναι απαραίτητη.*

Στο παρακάτω σχήμα παρουσιάζονται μερικές από τις παραλλαγές του 802.11 σε σχέση με την λειτουργία τους και την θέση τους στο μοντέλο αναφοράς OSI.



Σχήμα 1.3:Διάφορες παραλλαγές του 802.11 πρωτοκόλλου

1.8 Τα κυριότερα εμπορικά πρωτόκολλα σήμερα

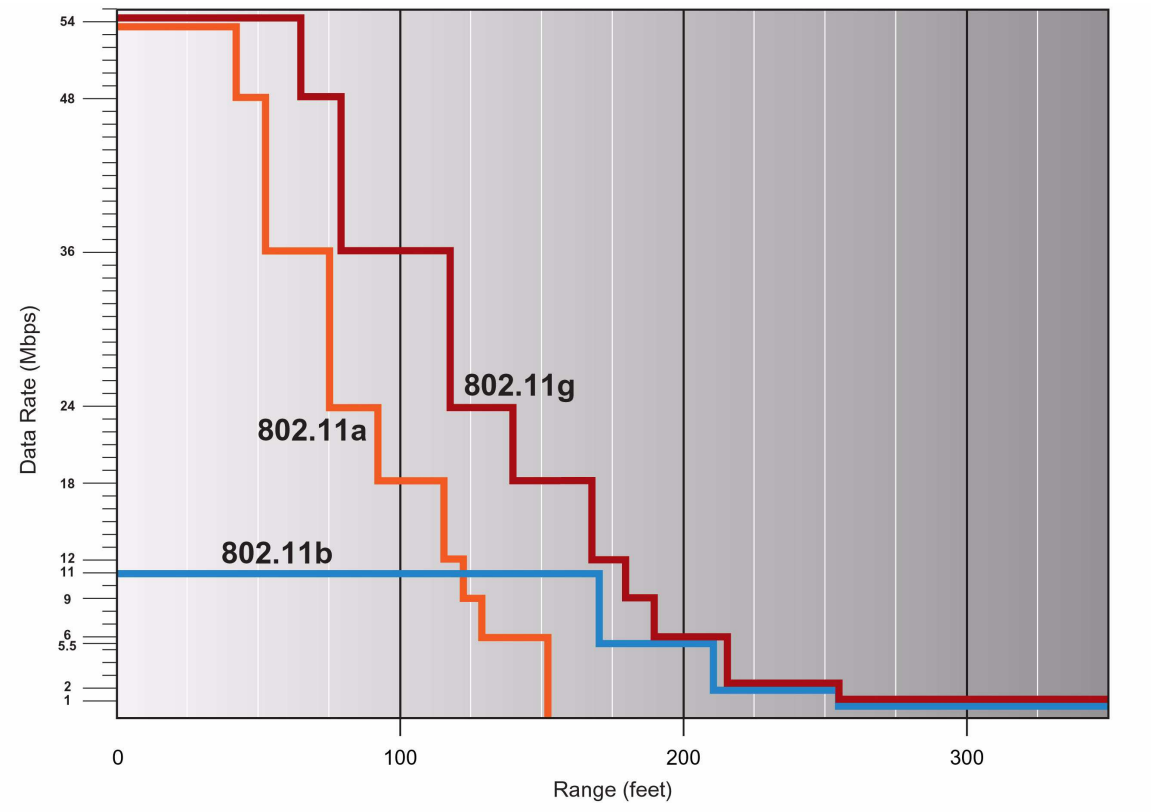
Σήμερα στην αγορά κυριαρχούν υλοποιήσεις βασισμένες στα 802.11a, 802.11b και 802.11g . Οι τεχνικές προδιαγραφές τους επισημαίνονται στον παρακάτω πίνακα:

	802.11a	*802.11b*	*802.11g*
Ακτίνα κάλυψης (εξωτερικοί χώροι)	30m@54Mbps 300m@6Mbps	120m@11Mbps 460@1Mbps	120m@54Mbps 460m@1Mbps
Ακτίνα κάλυψης (εσωτερικοί χώροι)	12m@54Mbps 91m@6Mbps	30m@11Mbps 91m@1Mbps	30m@54Mbps 91m@1Mbps
Bandwidth	54 Mbps	11 Mbps	54 Mbps
Συχνότητα	2.4 - 2.497 GHz	5.15-5.35GHz 5.425-5.675GHz 5.725-5.875GHz	2.4 – 2.497 GHz
Διαμόρφωση	CCK	OFDM	CCK & OFDM
Μέσο πραγματικό Throughput	4-5 Mbps	27 Mbps	20-25 Mbps
Ρυθμός μετάδοσης δεδομένων	1, 2, 5.5, 11 Mbps	6, 9, 12, 18, 24, 36, 48, 54 Mbps	CCK: 1, 2, 5.5, 11
Εύρος καναλιού	20 MHz	22 MHz	5, 10, and 20 MHz
Effective Isotropic Radiated Power (EIRP)	Lower U-NII: 22 dBm	Middle U-NII: 29 dBm	Upper U-NII: 35 dBm
Χωρητικότητα	64 users per access point	32 users per access point	64 users per access point
Αριθμός καναλιών	8 μη επικαλυπτόμενα	3 μη επικαλυπτόμενα	3 μη επικαλυπτόμενα

Το πρωτόκολλο 802.11 υποστηρίζει διάφορους ρυθμούς ταχυτήτων ώστε να επιτρέπει στους χρήστες να επικοινωνούν με την καλύτερη δυνατή ταχύτητα. Η επιλογή ρυθμού ταχύτητας είναι μια χρυσή τομή μεταξύ της λήψης του υψηλότερου δυνατού ρυθμού ταχύτητας προσπαθώντας να ελαχιστοποιήσει τον αριθμό λαθών επικοινωνίας. Όποτε υπάρχει λάθος στα απεσταλθέντα δεδομένα, το σύστημα ασύρματης επικοινωνίας πρέπει να ξοδέψει χρόνο ώστε να αναμεταδοθούν τα στοιχεία έως ότου μεταδοθούν επιτυχώς. Η κάρτα πρόσβασης του κάθε χρήστη 802.11 μόλις συνδεθεί με το σημείο πρόσβασης ακολουθεί μια διαδικασία για να επιλέξει το καλύτερο ποσοστό στοιχείων. Οι χρήστες του πρωτόκολλου 802.11g μπορούν να επιλέξουν ρυθμό μετάδοσης από τους διαθέσιμους με διαμόρφωση OFDM 54 ..48 ..36 ..24 ..18 ..12 ..9, και 6 Mbps, και τους ρυθμούς μετάδοσης με διαμόρφωση CCK 11, 5.5 , 2, και 1 Mbps.

Όσο η απόσταση από το σημείο πρόσβασης αυξάνεται, τα βασισμένα στο 802.11 προϊόντα προσαρμόζουν προς τα κάτω την ταχύτητα σύνδεσης για να διατηρήσουν τη σύνδεση. Το πρότυπο 802.11g έχει τα ίδια χαρακτηριστικά διάδοσης με το 802.11b, επειδή εκπέμπει στην ίδια ζώνη συχνότητας των 2.4-GHz. Επειδή τα προϊόντα 802.11b και 802.11g έχουν τα ίδια χαρακτηριστικά διάδοσης, οι υλοποιήσεις καρτών ασύρματης πρόσβασης και σημείων πρόσβασης παρέχουν κατά προσέγγιση την ίδια μέγιστη ακτίνα ραδιοκάλυψης στην ίδια ταχύτητα μεταφοράς. Επειδή τα ραδιοκύματα στα 5- GHZ δεν έχουν τα ίδια χαρακτηριστικά διάδοσης όπως στα 2.4-GHz, η ακτίνα ραδιοκάλυψης των προϊόντων βασισμένων στο 802.11a είναι περιορισμένη συγκριτικά με όσα είναι βασισμένα στο 802.11b ή 802.11g.

Η απόσταση του τερματικού από το σημείο πρόσβασης (access point) επηρρεάζει σημαντικά την αναμενόμενη ρυθμαπόδοση (throughput) της σύνδεσης. Η θεωρητική ρυθμαπόδοση για διάφορες αποστάσεις απεικονίζεται σχηματικά στο σχήμα 1.4



Σχήμα 1.4 Ρυθμαπόδοση των παραλλαγών του 802.11 σε συνάρτηση με την απόσταση

Κεφάλαιο 2

Πρωτόκολλα κρυπτογράφησης για Δίκτυα IEEE 802.11x

2.1 Γενικά περί ασφάλειας ασύρματων δικτύων

Όσο οι συσκευές wifi εισέβαλλαν σε όλο και περισσότερα δίκτυα, τόσο οι χρήστες τους , έβλεπαν πιο σοβαρά το ζήτημα της ασφάλειας των δεδομένων που διακινούσαν μέσω αυτών. Αναρίθμητες μελέτες, τόσο από κοινούς χρήστες, όσο και από την επιστημονική κοινότητα, βοήθησαν στο να ξεσκεπαστούν πολλές θεμελιώδεις ατέλειες στο μοντέλο ασφάλειας του πρωτοκόλλου. Θα προσπαθήσουμε να δώσουμε μια γενική εικόνα της όλης κατάστασης, προτείνοντας τελικά κάποιες λύσεις.

Η επιτροπή IEEE, για λόγους ασφάλειας και πιστοποίησης (authentication) χρηστών, όρισε το WEP (wired equivalent privacy), με σκοπό την ενθυλάκωση των πακέτων των δεδομένων για την επίτευξη ασφάλειας παρόμοιας με ένα ενσύρματο δίκτυο. Η υλοποίηση του WEP σε εμπορικές συσκευές άργησε να υποστηριχτεί απο όλους τους κατασκευαστές. Μια γρήγορη λύση για την υποκατάστασή του, ήταν η πιστοποίηση χρηστών μέσω λιστών επιτρεπόμενων MAC διευθύνσεων. Η MAC διεύθυνση είναι ένας μοναδικός δεκαεξαδικός αριθμός, που είναι «γραμμένος» στο υλικό κάθε δικτυακής συσκευής. Το Access Point κρατούσε μια λίστα με όλες τις διευθύνσεις MAC που ο διαχειριστής του δικτύου επέτρεπε να συνδεθούν. Αν η MAC μιας client συσκευής δεν ανήκε στη λίστα, αυτή η συσκευή δεν θα μπορούσε να συνδεθεί στο Access Point. Αυτή είναι μια πολύ αδύναμη μέθοδος πιστοποίησης στοιχείων των σταθμών πελατών. Κάποιος εκτός λίστας, με αρκετά δικαιώματα σε ένα unix-like λειτουργικό σύστημα, μπορεί με διάφορους τρόπους να αλλάξει την MAC διεύθυνση που παρουσιάζει στο δίκτυο, έτσι ώστε να μπορέσει να χρησιμοποιήσει μια MAC που να είναι αποδεκτή από το AP. Τέτοιες επιθέσεις ονομάζονται mac spoofing attacks. Χρησιμοποιώντας εξειδικευμένο «ανιχνευτικό» λογισμικό (network sniffer), που πολλές φορές είναι δωρεάν, μπορεί με μια απλή WiFi κάρτα και ένα λάπτοπ να φτιάξει μια λίστα με τις MAC διευθύνσεις που βλέπει ότι συνδέονται επιτυχώς στο Access Point-στόχο. Έτσι, αλλάζοντας την MAC διεύθυνσή του σε οποιαδήποτε από αυτές, έχει την δυνατότητα να συνδεθεί επιτυχώς στο δίκτυο, χωρίς κανείς να μπορεί να καταλάβει την διαφορά.

Το WEP ήταν η πρώτη σοβαρή προσπάθεια υπέρ της αύξησης της ασύρματης ασφάλειας. Δυστυχώς, ο σχεδιασμός του προτύπου, συνέπεσε χρονικά με την φρενίτιδα της κυβέρνησης των ΗΠΑ κατά της δημόσιας χρήσης συστημάτων ισχυρής κρυπτογράφησης, που σημαίνει μεγάλο μήκος κλειδιού. Έτσι το μήκος κλειδιού που υποστηρίζει το WEP, περιορίστηκε στα 40 ψηφία. Επιπλέον, ένα τέτοιο μήκος κλειδιού θα καθιστούσε το WEP ευκολότερο να υλοποιηθεί, καθώς η κατασκευή των MAC πλαισίων από το τότε υλικό ήταν ήδη μια διαδικασία που απαιτούσε μεγάλη υπολογιστική ισχύ, πόσο μάλλον η ενθυλάκωση τους με WEP. Η εισαγωγή μιας δυνατής κρυπτογράφησης θα επιβάρυνε ακόμη περισσότερο τις επιδόσεις των συσκευών. Καθώς όλοι είχαν πλέον καταλάβει ποσό τρωτό είναι ένα ανοιχτό δίκτυο, βιάστηκαν να υιοθετήσουν το πρότυπο αυτό.

Δύο επιστημονικές εργασίες όμως, από ομάδες του πανεπιστημίου του

Berkeley και του Maryland, έμελλαν να ταράξουν τα νερά για το πρότυπο, και να καταστήσουν εμφανή τα τρωτά του σημεία. Η εργασία της ομάδας του Berkeley καταδεικνύει τις αδυναμίες του προτύπου λόγω της συνεχούς επαναχρησιμοποίησης κλειδιών, ενώ η εργασία του Maryland θίγει της αδυναμίες στους μηχανισμούς πρόσβασης, ακόμη και αυτούς που λειτουργούν με βάση ΤΟ WEP. Άλλες εργασίες που ακολούθησαν πρότειναν τρόπους για την τοποθέτηση πλαστών πακέτων στην κίνηση του δικτύου, με αποκορύφωμα το άρθρο ενός μέλους της ομάδας 802.11 που μιλούσε για ΤΟ WEP σαν «ανασφαλές για οποιοδήποτε μήκος κλειδιού» («WEP:unsafe at any key length»). Όλες οι προηγούμενες εργασίες βασίζονταν σε σχεδιαστικές ατέλειες του προτύπου για να προτείνουν την ύπαρξη κενών ασφάλειας. Ο ίδιος ο αλγόριθμος κρυπτογράφησης(RC4 της RCA), παρόλαυτα, θεωρούνταν επαρκής και δεν είχε δεχθεί αμφισβήτηση. Τότε οι Scott Fluhrer, Itsik Mantin, και Adi Shamir, ανακάλυψαν ένα ελάττωμα του αλγόριθμου χρονοδρομολόγησης κλειδιών που καθιστούσε κάποια κλειδιά «αδύναμα». Ένας εισβολέας, θα μπορούσε να βρει το μυστικό κλειδί WEP, απλά συλλέγοντας αρκετά αδύναμα κλειδιά. Δεν δημοσίευσαν ωστόσο κάποια υλοποίηση των ευρημάτων τους. Δυστυχώς ή ευτυχώς, ακολούθησαν πολλοί που το έκαναν. Πάμπολλα προγράμματα ανοιχτού λογισμικού, όπως ΤΟ AirSnort έχουν την δυνατότητα να σπάσουν την κρυπτογράφηση WEP σε δευτερόλεπτα, δεδομένης μιας συλλογής αδύναμων κλειδιών του δικτύου - στόχος.

Η πραγματικότητα είναι ακόμη πιο οδυνηρή. Πολλές έρευνες σε περιοχές με μεγάλη πυκνότητα wifi δικτύων έχουν δείξει ότι μόνο ένα πολύ μικρό ποσοστό Access Points που ανιχνεύτηκαν, έχουν πράγματι ΤΟ WEP ενεργοποιημένο.

Το μεγαλύτερο ποσοστό των εταιρικών δικτύων, είναι ορθάνοιχτο σε «επισκέπτες». Μάλιστα η μη νόμιμη πρόσβαση σε ασύρματα δίκτυα είναι τόσο εκτεταμένη, που υπάρχουν web sites στα οποία συγκεντρώνονται οι συντεταγμένες ανοιχτών εταιρικών δικτύων. Τέτοιες ομάδες χρηστών χρησιμοποιούν προγράμματα όπως ΤΟ netstumbler για να ανακαλύπτουν όλα τα ασύρματα δίκτυα εντός της εμβέλειας της κεραίας του φορητού τους υπολογιστή, αλλά και να βλέπουν χρήσιμες πληροφορίες όπως ΤΟ SSID του Access Point, αν έχει ενεργοποιημένο ΤΟ WEP, αλλά και την ποιότητα της εκπομπής της κεραίας - στόχου. Μια βόλτα με αυτοκίνητο στους εμπορικούς δρόμους της Νέας Υόρκης, έχοντας ένα φορητό υπολογιστή, μια φτηνή wifi κάρτα και μια ακόμα φθηνότερη κεραία, μπορεί να αποδείξει την ύπαρξη τρυπών στα περισσότερα ασύρματα εταιρικά δίκτυα. Πολλοί έχουν αναγάγει την δραστηριότητα αυτή σε «σπορ», ενονόματι wardriving, επωφελούμενοι κυρίως απο την δωρεάν broadband σύνδεση στο διαδίκτυο που μπορεί να «προσφέρει» ένα απροστάτευτο δίκτυο. Η επίθεση parking lot, συνεπάγεται την χρήση της εμβελείας ενός wifi δικτύου σε συνδυασμό με κάποια τρύπα ασφαλείας, για την εισβολή στο δίκτυο αυτό από έναν ασφαλή για τον εισβολέα χώρο, όπως ο εταιρικός χώρος πάρκιν. Με μια δόση χιούμορ, πολλά άρθρα στο διαδίκτυο, για να ωθήσουν τους network administrators να αυξήσουν την ασφάλεια των ασύρματων δικτύων τους, ρωτούν: «μοιράζεστε την εταιρική σας σύνδεση στο ίντερνετ με εκείνο τον κύριο στο πάρκιν;».

Αυτό το είδος επίθεσης είναι μόνο μία από τις μεθόδους πρόκλησης κατάρρευσης σε ένα ασύρματο δίκτυο. Ένας αρκετά έξυπνος και δύσκολα αντιμετωπίσιμος τρόπος επίθεσης, είναι η ηθελημένη εκπομπή ψευδών πακέτων «αποσύνδεσης χρήστη»(disassociation/deauthentication packets) προς ΤΟ Access Point. Εφόσον ο εισβολέας συλλέξει τις MAC διευθύνσεις των σταθμών πελατών μιας κυψέλης, μπορεί να απλά να στείλει πολλά πακέτα αποσύνδεσης για κάθε μια MAC-

πελάτη. Το AP απλά δεν θα καταλάβει ότι τα πακέτα αυτά είναι κακόβουλα, και θα αποσυνδέσει όσους σταθμούς του ζητηθούν, προκαλώντας έτσι την κατάρρευση του δικτύου.

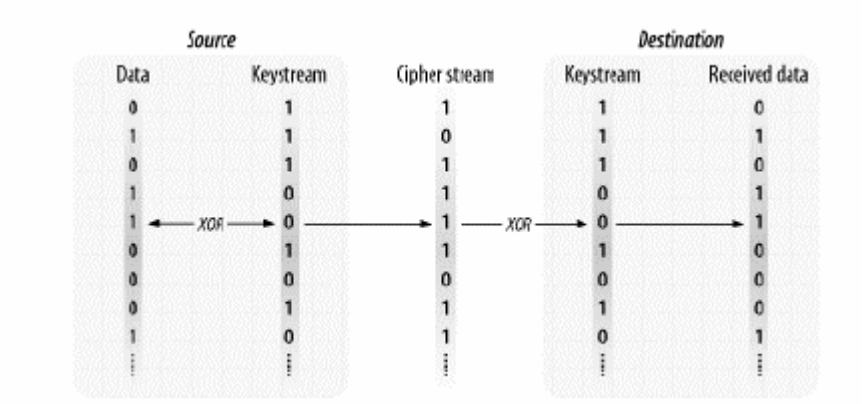
Όλα τα παραπάνω συνηγορούν ότι η προτυποποίηση της ασύρματης ασφάλειας, είναι μια εργασία σε εξέλιξη. Νέα πρότυπα μελετούνται, όπως το 802.11 i, που υπόσχονται μια καλύτερη λύση από ΤΟ WEP. Βέβαια ένας τέτοιος στόχος φαίνεται εύκολος, δεδομένης της πλήρους και πέρα για πέρα αποτυχίας του WEP πρωτοκόλλου. Πολλοί χρησιμοποιούν λύσεις λογισμικού που κρυπτογραφούν την κίνηση δεδομένων σε υψηλότερο δικτυακό επίπεδο, όπως ΤΟ IPsec, ΤΟ SSL κτλ.

2.2 Περιγραφή λειτουργίας του πρωτοκόλλου WEP

2.2.1 Κρυπτογραφικό υπόβαθρο του WEP

Πριν αναφερθούμε στο WEP είναι απαραίτητο να καλύψουμε κάποιες βασικές κρυπτογραφικές έννοιες.

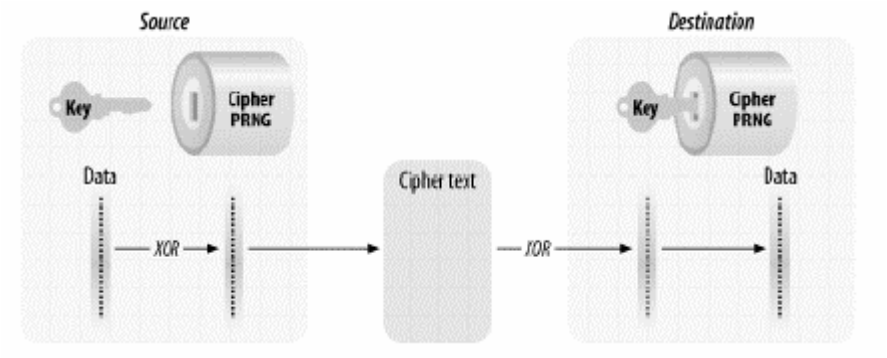
Για να προστατεύσει τα δεδομένα, το WEP απαιτεί τη χρήση του αλγόριθμου κρυπτογράφησης RC4 , ο οποίος είναι ένας συμμετρικός αλγόριθμος κρυπτογράφησης ακολουθίας (μυστικού κλειδιού). Γενικά μιλώντας, ένας αλγόριθμος κρυπτογράφησης ακολουθίας χρησιμοποιεί μια ακολουθία bits, αποκαλούμενη *ακολουθία κλειδιού (keystream)*. Το keystream συνδυάζεται κατόπιν με το μήνυμα για να παραγάγει το *κρυπτογράφημα (ciphertext)*. Για να ανακτήσει τον αρχικό μήνυμα, ο δέκτης επεξεργάζεται το κρυπτογράφημα με το ίδιο keystream. Ο RC4 χρησιμοποιεί αποκλειστικό Η (XOR) για να συνδυάσει το keystream και το κρυπτογράφημα. Το Σχήμα 2.1 επεξηγεί τη διαδικασία.



Σχήμα 2.1 Λειτουργία κρυπτογράφησης/ αποκρυπτογράφησης

Οι περισσότεροι αλγόριθμοι αποκρυπτογράφησης ακολουθίας λειτουργούν παίρνοντας ένα σχετικά μικρό μυστικό κλειδί και επεκτείνοντάς το στο ψευδοτυχαίο keystream που έχει το ίδιο μήκος με το μήνυμα. Αυτή η διαδικασία φαίνεται στο σχήμα 2.2. Η ψευδοτυχαία γεννήτρια αριθμού (PRNG) είναι ένα σύνολο κανόνων

που χρησιμοποιούνται για να επεκταθεί το κλειδί σε keystream. Για να ανακτήσουν τα δεδομένα, και οι δύο πλευρές πρέπει να μοιραστούν το ίδιο μυστικό κλειδί και να χρησιμοποιούν τον ίδιο αλγόριθμο για να επεκτείνουν το κλειδί σε μια ψευδοτυχαία ακολουθία.



Σχήμα 2.2 Λειτουργία κρυπτογράφησης/ αποκρυπτογράφησης

Επειδή η ασφάλεια του αλγόριθμου κρυπτογράφησης ακολουθίας στηρίζεται εξ' ολοκλήρου στην τυχαιότητα του keystream, ο σχεδιασμός της επέκτασης κλειδιού σε keystream είναι ύψιστης σημασίας. Όταν ο RC4 επιλέχτηκε από τη 802.11 ομάδα εργασίας, φαινόταν να είναι αρκετά ασφαλής. Αλλά έπειτα έρευνα που διεξήχθει απέδειξε αδυναμίες του RC4 που θα συζητηθούν αργότερα.

Ασφάλεια της κρυπτογράφησης ακολουθίας

Ένα αποκλειστικά τυχαίο keystream ονομάζεται one-time pad και είναι το μόνο γνωστό σενάριο κρυπτογράφησης που αποδεικνύεται από μαθηματική άποψη ότι παρέχει προστασία από ορισμένους τύπους επιθέσεων. Τα one-time pads δεν χρησιμοποιούνται συνήθως επειδή το keystream πρέπει να είναι εντελώς τυχαίο, να έχει το ίδιο μήκος με τα δεδομένα που θα προστατευθούν και δεν μπορεί ποτέ να επαναχρησιμοποιηθεί.

Οι επιτιθέμενοι δεν περιορίζονται στο να επιτεθούν στο υποκείμενο κρυπτογράφημα. Μπορούν να επιλέξουν να εκμεταλλευτούν οποιοδήποτε αδύνατο σημείο σε ένα κρυπτογραφικό σύστημα. Είναι εύκολο να γίνει κατανοητή η ανάγκη να επαναχρησιμοποιηθούν τα one-time pads. Τεράστιοι όγκοι υλικού κλειδιών είναι απαραίτητοι για να προστατεύσουν ακόμη και ένα μικρό ποσό δεδομένων, και αυτά τα pads πρέπει να διανεμηθούν ασφαλώς, το οποίο στην πράξη αποδεικνύεται να είναι μια σημαντική πρόκληση.

Η κρυπτογράφηση ακολουθίας είναι ένας συμβιβασμός μεταξύ της ασφάλειας και της πρακτικότητας. Η τέλεια τυχαιότητα (και τέλεια ασφάλεια) ενός one-time pad είναι ελκυστική, αλλά οι πρακτικές δυσκολίες και το κόστος που απαιτούνται για την παραγωγή και τη διανομή του υλικού κλειδιών αξίζει μόνο για τα σύντομα μηνύματα που απαιτούν την απώτατη ασφάλεια. Οι αλγόριθμοι αποκρυπτογράφησης ακολουθίας χρησιμοποιούν ένα λιγότερο τυχαίο keystream αλλά αρκετά τυχαίο για τις περισσότερες εφαρμογές.

Κρυπτογραφικές διαδικασίες WEP

Η ασφάλεια επικοινωνιών έχει τρεις σημαντικούς στόχους. Οποιοδήποτε πρωτόκολλο που προσπαθεί να εξασφαλίσει τα δεδομένα καθώς ταξιδεύουν μέσω ενός δικτύου πρέπει να βοηθά τους διαχειριστές δικτύων να επιτύχουν αυτούς τους στόχους.

Η εμπιστευτικότητα είναι ο όρος που χρησιμοποιείται για να περιγράψει τα δεδομένα που προστατεύονται ενάντια στην επέμβαση από αναρμόδια συμβαλλόμενα μέρη. Η *ακεραιότητα* σημαίνει ότι το στοιχείο δεν έχει τροποποιηθεί. Η *επικύρωση* υποστηρίζει οποιαδήποτε στρατηγική ασφάλειας επειδή μέρος της αξιοπιστίας των δεδομένων είναι βασισμένο στην προέλευσή τους. Οι χρήστες πρέπει να εξασφαλίσουν ότι τα δεδομένα προέρχονται από την πηγή που ισχυρίζονται ότι προέρχονται.

Τα συστήματα πρέπει να χρησιμοποιούν την επικύρωση για να προστατεύουν τα δεδομένα κατάλληλα. Εξουσιοδότηση και έλεγχος πρόσβασης και τα δύο εφαρμόζονται πάνω στην επικύρωση. Πριν να επιτραπεί η πρόσβαση σε ένα κομμάτι από δεδομένα, τα συστήματα πρέπει να ανακαλύψουν ποιος είναι ο χρήστης (επικύρωση) και εάν η πρόσβαση στην λειτουργία επιτρέπεται (εξουσιοδότηση).

Το WEP παρέχει τις διαδικασίες που βοηθούν στην επιτυχία αυτών των στόχων. Η κρυπτογράφηση των πλαισίων υποστηρίζει την εμπιστευτικότητα. Μια ακολουθία ελέγχου ακεραιότητας προστατεύει τα δεδομένα κατά τη μεταφορά και επιτρέπει στους δέκτες να επικυρώσουν ότι τα λαμβανόμενα δεδομένα δεν άλλαξαν κατά τη μεταφορά. Το WEP επίσης επιτρέπει την ισχυρότερη επικύρωση δημοσίου κλειδιού των σταθμών για τα σημεία πρόσβασης. Στην πράξη, το WEP έχει αδυναμίες σε όλες αυτές τις περιοχές. Η εμπιστευτικότητα μειώνεται από τις αδυναμίες του RC4 αλγόριθμου αποκρυπτογράφησης, ο έλεγχος ακεραιότητας ήταν κακώς σχεδιασμένος και η επικύρωση γίνεται για τις διευθύνσεις MAC των χρηστών, όχι για τους χρήστες τους ίδιους.

Το WEP πάσχει επίσης στο εξής. Κρυπτογραφεί τα πλαίσια καθώς διαπερνούν το ασύρματο μέσο. Τίποτα δεν γίνεται για να προστατεύσει τα πλαίσια στο συνδεμένο με καλώδιο βασικό δίκτυο, όπου είναι υποκείμενα οποιασδήποτε επίθεσης. Επιπλέον, το WEP έχει ως σκοπό να εξασφαλίσει το δίκτυο από τους εξωτερικούς εισβολείς. Μόλις ανακαλύψει ένας εισβολέας το κλειδί WEP, εν τούτοις, το ασύρματο μέσο γίνεται ισοδύναμο με ένα μεγάλο συνδεμένο με καλώδιο δίκτυο που πολλοί έχουν ελεύθερα πρόσβαση.

2.2.2 Ιδιότητες του αλγορίθμου WEP

Ο αλγόριθμος WEP έχει τις ακόλουθες ιδιότητες:

- *Είναι εύλογα ισχυρός:*

Η ασφάλεια που διατίθεται από τον αλγόριθμο στηρίζεται στη δυσκολία να ανακαλυφθεί το μυστικό κλειδί μέσω μιας σκληρής επίθεσης. Αυτό συσχετίζεται στη συνέχεια με το μήκος μυστικού κλειδιού και τη συχνότητα μεταβολής των κλειδιών. Το WEP επιτρέπει την αλλαγή του κλειδιού (k) και τη συχνή αλλαγή του IV.

- *Είναι αυτοσυγχρονιζόμενος:*

Το WEP είναι αυτοσυγχρονιζόμενο για κάθε μήνυμα. Αυτή η ιδιότητα είναι

κρίσιμη για έναν αλγόριθμο κρυπτογράφησης επιπέδου σύνδεσης δεδομένων, όπου υποθέτουμε την καλύτερη παράδοση και το ποσοστό απώλειας δεδομένων μπορεί να είναι υψηλό.

- *Είναι αποδοτικός:*

Ο αλγόριθμος WEP είναι αποδοτικός και μπορεί να εφαρμοστεί είτε στο υλικό είτε στο λογισμικό.

- *Μπορεί να είναι εξαγώγιμος:*

Κάθε προσπάθεια έχει καταβληθεί για να σχεδιασθεί η λειτουργία συστημάτων WEP ώστε να μεγιστοποιηθούν οι πιθανότητες της έγκρισης, από τον Τομέα Εμπορίου της Αμερικανικής Κυβέρνησης, της εξαγωγής από τις ΗΠΑ προϊόντων που περιέχουν εφαρμογές WEP.

- *Είναι προαιρετικό:*

Η εφαρμογή και η χρήση WEP είναι μια IEEE 802.11 επιλογή.

2.2.3 Θεωρία λειτουργίας WEP

Η διαδικασία μεταμφίεσης (δυαδικών) δεδομένων προκειμένου να κρυφτεί το περιεχόμενο πληροφοριών της καλείται *κρυπτογράφηση (encryption,* συμβολίζεται με E). Τα δεδομένα που δεν κρυπτογραφούνται αποτελούν το *plaintext* (συμβολίζεται με P) και τα δεδομένα που κρυπτογραφούνται αποτελούν το *cipher text* (συμβολίζεται με C).

Η διαδικασία μετατροπής του chiphertext σε plaintext καλείται *αποκρυπτογράφηση (dencryption, συμβολίζεται με D).* Ένας *αλγόριθμος κρυπτογράφησης ή cipher* είναι μια μαθηματική λειτουργία που χρησιμοποιείται για την κρυπτογράφηση ή αποκρυπτογράφηση δεδομένων. Οι σύγχρονοι αλγόριθμοι κρυπτογράφησης χρησιμοποιούν μια ακολουθία κλειδιού (που συμβολίζεται με k) για να τροποποιήσουν τα εξαγόμενα τους.

Η λειτουργία κρυπτογράφησης E ενεργεί επάνω στο P για να παραγάγει το C.

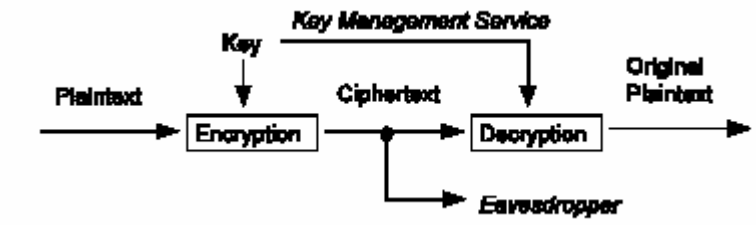
$$\mathbf{E}_k\,\mathbf{(P) = C}$$

Στην αντίστροφη διαδικασία η λειτουργία αποκρυπτογράφησης D ενεργεί επάνω στο C για να παραγάγει το P

$$D_k © = P$$

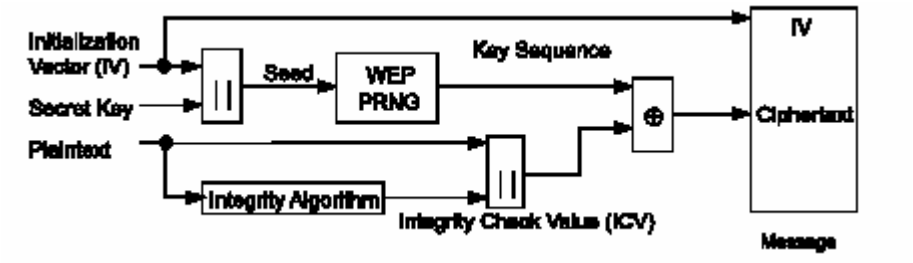
Όπως φαίνεται στο σχήμα 2.3 εάν το ίδιο κλειδί μπορεί να χρησιμοποιηθεί στην κρυπτογράφηση και αποκρυπτογράφηση τότε

$$D_k(E_k(P)) = P$$



Σχήμα 2.3 Ένα εμπιστευτικό κανάλι δεδομένων

Στον αλγόριθμο WEP ένα τμήμα plaintext γίνεται XORed με μια ψευδοτυχαία ακολουθία κλειδιού ίσου μήκους. Η ακολουθία κλειδιού παράγεται από τον αλγόριθμο WEP.Αναφερόμενοι στο σχήμα 2.4 και κοιτάζοντας από αριστερά προς τα δεξιά, η κρυπτογράφηση ξεκινά με ένα *μυστικό κλειδί* που είναι διανεμημένο στους συνεργαζόμενους STAs από μια εξωτερική υπηρεσία διαχείρισης κλειδιού. Ο WEP είναι ένας συμμετρικός αλγόριθμος στον οποίο το ίδιο κλειδί χρησιμοποιείται για κρυπτογράφηση και αποκρυπτογράφηση.



Σχήμα 2.4 Block Diagram WEP κρυπτογράφησης

Το μυστικό κλειδί συνδέεται με ένα *διάνυσμα έναρξης* (IV) και το αποτέλεσμα *(seed)* εισάγεται σε ένα PRNG. Ο PRNG παράγει μια ακολουθία κλειδιού *k* από ψευδοτυχαία octets ίσα στο μήκος με τον αριθμό octets δεδομένων που πρέπει να διαβιβαστούν στην εκτεταμένη MPDU συν 4 (δεδομένου ότι η ακολουθία κλειδιού χρησιμοποιείται για να προστατεύσει την *τιμή ελέγχου ακεραιότητας (Integrity Check Value* ICV) καθώς επίσης και τα δεδομένα). Δύο διαδικασίες εφαρμόζονται στο plaintext της MPDU. Για προστασία από αναρμόδια τροποποίηση δεδομένων, ένας αλγόριθμος ακεραιότητας λειτουργεί επάνω στο P για να παραγάγει ένα ICV. Η κρυπτογράφηση έπειτα ολοκληρώνεται έπειτα με μαθηματικό συνδυασμό της ακολουθίας κλειδιού με το plaintext που μετατράπηκε σε ICV. Το προϊόν της διαδικασίας είναι ένα *μήνυμα* που περιέχει το IV και το κρυπτογράφημα (cipher).

Ο WEP PRNG είναι το κρίσιμο συστατικό αυτής της διαδικασίας, δεδομένου ότι μετασχηματίζει ένα σχετικά σύντομο μυστικό κλειδί σε μια αυθαίρετα μακροχρόνια ακολουθία κλειδιού. Αυτό απλοποιεί πολύ την διαδικασία διανομής κλειδιού, καθώς μόνο το μυστικό κλειδί πρέπει να μεταδοθεί μεταξύ STAs. Το IV επεκτείνει την διάρκεια ζωής του μυστικού κλειδιού και παρέχει την ιδιότητα αυτοσυγχρονισμού του αλγορίθμου. Το μυστικό κλειδί παραμένει σταθερό ενώ τα IV αλλάζουν περιοδικά. Κάθε νέο IV καταλήγει σε ένα νέο seed και μια νέα ακολουθία κλειδιού, κατά συνέπεια υπάρχει μια ένα προς ένα αντιστοίχιση μεταξύ του IV και του k. Το IV μπορεί να αλλάξει τόσο συχνά όσο κάθε MPDU και, δεδομένου ότι ταξιδεύει με το μήνυμα, ο δέκτης θα είναι σε θέση πάντα να αποκρυπτογραφήσει οποιοδήποτε μήνυμα. Το IV διαβιβάζεται χωρίς ασφάλεια αφού δεν παρέχει σε έναν επιτιθέμενο οποιεσδήποτε πληροφορίες για το μυστικό κλειδί, και δεδομένου ότι η τιμή του πρέπει να μαθευτεί από τον παραλήπτη προκειμένου να εκτελεσθεί η αποκρυπτογράφηση.Όταν πρέπει να αποφασίσουμε πόσο συχνά πρέπει να αλλάζουν οι τιμές του IV, πρέπει να λάβουμε υπ' όψη μας ότι το περιεχόμενο κάποιων τμημάτων στις επικεφαλίδες των υψηλότερων στρωμάτων του πρωτοκόλλου καθώς επίσης και ορισμένες άλλες πληροφορίες ανώτερου στρώματος είναι σταθερά ή ιδιαίτερα προβλέψιμες. Όταν τέτοιες πληροφορίες διαβιβάζονται ενώ η

κρυπτογράφηση γίνεται με ένα συγκεκριμένο κλειδί και IV, ο ωτακουστής μπορεί εύκολα να καθορίσει ορισμένα τμήματα της ακολουθίας κλειδιού που παράγεται από αυτό το ζεύγος (κλειδί, IV). Εάν το ίδιο ζεύγος (κλειδί, IV) χρησιμοποιείται για διαδοχικά MPDUs, αυτή η επίδραση μπορεί ουσιαστικά να μειώσει το βαθμό μυστικότητας που παρέχεται από τον αλγόριθμο WEP, αφού επιτρέπει σε έναν ωτακουστή να ανακτήσει ένα υποσύνολο απ΄ τα δεδομένα του χρήστη χωρίς οποιαδήποτε γνώση του μυστικού κλειδιού. Η αλλαγή του IV μετά από κάθε MPDU είναι μια απλή μέθοδος για να διατηρούμε την αποτελεσματικότητα τουWEP σε αυτή την περίπτωση.

Ο αλγόριθμος WEP εφαρμόζεται στο σώμα του πλαισίου ενός MPDU. Η τριπλέτα (IV, σώμα πλαισίου, ICV) διαμορφώνει τα πραγματικά δεδομένα που στέλνονται στο πλαίσιο δεδομένων.

Για προστατευμένα από τα το WEP πλαίσια, τα πρώτα τέσσερα octets του σώματος πλαισίου περιέχουν το πεδίο IV για το MPDU. Ο PRNG seed είναι 64 bit. Τα bit 0 έως 23 του IV αντιστοιχούν στα bit 0 έως 23 του PRNG seed, αντίστοιχα. Τα bit 0 έως 39 του μυστικού κλειδιού αντιστοιχούν στα bit 24 έως 63 του PRNG seed, αντίστοιχα. Η αρίθμηση των octets του PRNG seed αντιστοιχεί σε αυτή του RC4 κλειδιού. Το IV ακολουθείται από το MPDU, το οποίο ακολουθείται από το ICV. Το WEP ICV είναι 32 bit.

Όπως δηλώνεται προηγουμένως, το WEP συνδυάζει το k με το P χρησιμοποιώντας XOR.

Αναφερόμενοι στο σχήμα 2.3 και κοιτάζοντας από αριστερά προς τα δεξιά η αποκωδικοποίηση ξεκινά με την άφιξη ενός μηνύματος. Ο IV του εισερχόμενου μηνύματος θα χρησιμοποιηθεί για να παραγάγει τη ακολουθία κλειδιού που είναι απαραίτητη για να αποκρυπτογραφηθεί το εισερχόμενο μήνυμα. Συνδυάζοντας το κρυπτογραφημένο κείμενο με την κατάλληλη ακολουθία κλειδιού παράγεται το αρχικό κείμενο (plaintext) και ο ICV. Η σωστή αποκωδικοποίηση θα ελεγχθεί με την εκτέλεση του αλγορίθμου ελέγχου ακεραιότητας στο ανακτημένο plaintext και συγκρίνοντας το παραγόμενο ICV’ με το ICV που διαβιβάζεται με το μήνυμα. Εάν το ICV’ δεν είναι ίδιο με το ICV, η λαμβανόμενη MPDU είναι λάθος και μια ένδειξη λάθους στέλνεται στη διαχείριση MAC. MSDUs με λανθασμένες MPDUs (λόγω της ανικανότητας αποκρυπτογράφησης) δεν θα περάσουν στο LLC.

Κλειδιά WEP

Για να προστατεύσουμε την κυκλοφορία από ισχυρές επιθέσεις αποκρυπτογράφησης, το WEP χρησιμοποιεί ένα σύνολο μέχρι τεσσάρων *προεπιλεγμένων κλειδιών*, και μπορεί επίσης να χρησιμοποιήσει κλειδιά ζευγών (pairwise), αποκαλούμενα *χαρτογραφημένα κλειδιά*, όταν επιτρέπονται.

Τα προεπιλεγμένα κλειδιά μοιράζονται μεταξύ όλων των σταθμών σε ένα σύνολο υπηρεσιών. Μόλις λάβει ένας σταθμός τα κλειδιά προεπιλογής για το σύνολο υπηρεσιών του, αυτό μπορεί να επικοινωνήσει με τη χρησιμοποίηση WEP.

Η επαναχρησιμοποίηση κλειδιών είναι συχνά μια αδυναμία των κρυπτογραφικών πρωτοκόλλων. Για αυτόν τον λόγο, το WEP έχει μια δεύτερη κατηγορία κλειδιών που χρησιμοποιούνται για pairwise επικοινωνίες. Αυτά τα κλειδιά μοιράζονται μόνο μεταξύ της επικοινωνίας δύο σταθμών. Οι δύο σταθμοί που μοιράζονται ένα κλειδί έχουν μια σχέση χαρτογράφησης κλειδιού

Μήκος κλειδιών WEP

Οι τυποποιημένες εφαρμογές WEP χρησιμοποιούν κοινά κλειδιά RC4 64 bit. Από τα 64 bit, τα 40 είναι ένα δημόσιο μυστικό. Οι προμηθευτές χρησιμοποιούν ποικίλα ονόματα για το τυποποιημένο WEP όπως: »βασικό WEP,» «802.11-συμβατό WEP,» «40-bit WEP,» «40+24-bit WEP» ή ακόμα και»64-bit WEP». Οι ανησυχίες για το μήκος κλειδιού που χρησιμοποιείται στο WEP έχουν ξεκινήσει από την έναρξή του. Τα προϊόντα που χρησιμοποιούν τα μυστικά κλειδιά 40-bit είναι πάντα εξαγώγιμα από τις Ηνωμένες Πολιτείες, και έτσι έχουν δημιουργηθεί αμφιβολίες για την ασφάλεια που παρέχει ένα τέτοιο κλειδί. Σε ένα καλά σχεδιασμένο κρυπτογραφικό σύστημα, η πρόσθετη ασφάλεια μπορεί να αποκτηθεί με τη χρησιμοποίηση ενός πιο μακροχρόνιου κλειδιού. Κάθε πρόσθετο bit διπλασιάζει τον αριθμό των πιθανών κλειδιών και θεωρητικά διπλασιάζει το χρονικό διάστημα που απαιτείται για μια επιτυχή επίθεση.

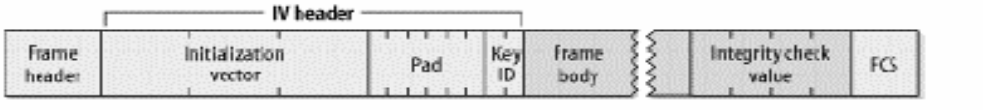
Για να έχουν το χρόνο για την τυποποίηση μιας καλύτερης λύσης από το WEP, το μεγαλύτερο μέρος της βιομηχανίας κινείται προς ένα 128-bit δημόσιο RC4 κλειδί. Αφού αφαιρεθούν 24 bit για το δημόσιο μυστικό συστατικό του RC4 κλειδιού, μόνο 104 bit είναι μυστικά. Ακόμα κι αν μόνο 104 bit είναι μυστικά, οι προμηθευτές αναφέρονται σε αυτό ως «128-bit WEP». Εφαρμογές με κλειδιά μεγαλύτερου μήκους δεν είναι εγγυημένο ότι θα είναι συμβατές γιατί κανένα πρότυπο για αυτές δεν υπάρχει. Τουλάχιστον ένας προμηθευτής χρησιμοποιεί 128 μυστικά bit, συν τα 24 του διανύσματος έναρξης, για ένα σύνολο 152 bit.

Το WEP, εντούτοις, δεν είναι ένα καλά σχεδιασμένο κρυπτογραφικό σύστημα, και τα πρόσθετα bit στο κλειδί δεν έχουν ιδιαίτερη σημασία. Η καλύτερη αποκαλυπτόμενη δημόσια επίθεση ενάντια στοWEP μπορεί να ανακτήσει το κλειδί στα δευτερόλεπτα όπως θα δούμε παρακάτω.

Πλαίσια WEP

Όταν χρησιμοποιείται το WEP το σώμα των πλαισίων επεκτείνεται από οκτώ bytes.

Τέσσερα bytes χρησιμοποιούνται για την επικεφαλίδα του σώματος του πλαισίου IV, και τέσσερα χρησιμοποιούνται για το ICV. Αυτά φαίνονται στο σχήμα 2.5.



Σχήμα 2.5 Επεκτάσεις πλαισίων WEP

Η επικεφαλίδα IV χρησιμοποιεί 3 bytes για το 24-bit IV, με το τέταρτο byte να χρησιμοποιείται για γέμισμα και προσδιορισμό κλειδιού (key identification). Όταν ένα προεπιλεγμένο κλειδί χρησιμοποιείται, το υποπεδίο key-ID προσδιορίζει το προεπιλεγμένο κλειδί που χρησιμοποιήθηκε για να κρυπτογραφήσει το πλαίσιο. Εάν χρησιμοποιείται μια σχέση χαρτογράφησης κλειδιού, το υποπεδίο key-ID είναι 0. Τα 6 bit γεμίσματος του τελευταίου byte πρέπει να είναι 0. Ο έλεγχος ακεραιότητας είναι ένας 32-bit, επισυνάπτεται στο σώμα του πλαισίου και προστατεύεται από RC4.

Κρυπτογραφικές ιδιότητες WEP

Η επαναχρησιμοποίηση keystream είναι η σημαντικότερη αδυναμία σε οποιοδήποτε κρυπτογραφικό σύστημα βασισμένο σε αλγόριθμο κρυπτογράφησης ακολουθίας.

Όταν τα πλαίσια κρυπτογραφούνται με το ίδιο RC4 keystream, το XOR των δύο κρυπτογραφημένων πακέτων είναι ισοδύναμο με το XOR των δύο πακέτων plaintext. Με την ανάλυση των διαφορών μεταξύ των δύο ακολουθιών από κοινού με τη δομή του σώματος πλαισίων, οι επιτιθέμενοι μπορούν να μάθουν για το περιεχόμενο των πλαισίων plaintext. Για να αποτρέψει την επαναχρησιμοποίηση keystream, το WEP χρησιμοποιεί το IV για να κρυπτογραφήσει διαφορετικά πακέτα με διαφορετικά RC4 κλειδιά.

Εντούτοις, το IV είναι μέρος της επικεφαλίδας πακέτων και δεν κρυπτογραφείται, έτσι οι ωτακουστές έχουν αρκετές πληροφορίες για τα πακέτα που κρυπτογραφούνται με το ίδιο RC4 κλειδί.

Τα προβλήματα εφαρμογής μπορούν να συμβάλουν στην έλλειψη ασφάλειας. Το 802.11 αναγνωρίζει ότι η χρησιμοποίηση του ίδιου IV για έναν μεγάλο αριθμό πλαισίων είναι επισφαλής και πρέπει να αποφευχθεί. Το πρότυπο επιτρέπει τη χρησιμοποίηση ενός διαφορετικού IV για κάθε πλαίσιο, αλλά αυτή δεν απαιτείται.

Το WEP ενσωματώνει έναν έλεγχο ακεραιότητας, αλλά ο αλγόριθμος που χρησιμοποιείται είναι ένας κυκλικός έλεγχος πλεονασμού (CRC). Οι CRCs μπορούν να ανιχνεύσουν τις αλλαγές ενός bit με υψηλή πιθανότητα, αλλά δεν είναι ασφαλείς κρυπτογραφικά. Κρυπτογραφικά ασφαλείς έλεγχοι ακεραιότητας είναι βασισμένοι σε απρόβλεπτες λειτουργίες. Με τις απρόβλεπτες λειτουργίες, εάν ο επιτιθέμενος αλλάζει ακόμη και ένα bit του πλαισίου, ο έλεγχος ακεραιότητας θα αλλάξει με απρόβλεπτο τρόπο. Η πιθανότητα ενός επιτιθεμένου να βρει ένα αλλαγμένο πλαίσιο με τον ίδιο έλεγχο ακεραιότητας είναι τόσο μικρή που δεν μπορεί να γίνει πραγματικά. Οι CRCs είναι απλά μαθηματικά, και είναι εύκολο να προβλεφθεί πώς η αλλαγή ενός μόνο bit έχει επιπτώσεις στο αποτέλεσμα του υπολογισμού CRC. (Αυτή η ιδιότητα χρησιμοποιείται συχνά από τα συμπιεσμένα δεδομένα για την επανάκτηση! Εάν μερικά συγκεκριμένα bit είναι λάθος, μπορούν μερικές φορές να προσδιοριστούν και να διορθωθούν με βάση μια τιμή CRC).

Διανομή κλειδιού

Όπως τόσα πολλά άλλα κρυπτογραφικά πρωτόκολλα βασισμένα στα συμμετρικά κλειδιά, το WEP πάσχει από το πρόβλημα της διανομής κλειδιού. Τα μυστικά κομμάτια του κλειδιού WEP πρέπει να διανεμηθούν σε όλους τους σταθμούς που συμμετέχουν σε ένα 802.11 σύνολο υπηρεσιών και ασφαλίζονται από WEP. Το 802.11 πρότυπο, εντούτοις, αποτυγχάνει να διευκρινίσει τον μηχανισμό διανομής κλειδιού. Το αποτέλεσμα είναι ότι οι προμηθευτές δεν έχουν κάνει τίποτα. Ο καθένας μας δακτυλογραφεί το κλειδί στον οδηγό της συσκευής ή έχει πρόσβαση σε συσκευές με το χέρι. Δυστυχώς, ο χειρωνακτικός καθορισμός από τον διαχειριστή συστημάτων είναι το περισσότερο μη εξελίσσιμο «πρωτόκολλο» σε χρήση.

Οι δυσκολίες ενός τέτοιου πρωτοκόλλου είναι:

Τα κλειδιά δεν μπορούν να θεωρηθούν μυστικά: όλα τα κλειδιά πρέπει να εισαχθούν στατικά στους οδηγούς software ή firmware στην ασύρματη κάρτα. Με κάθε τρόπο, το κλειδί δεν μπορεί να προστατευθεί από έναν τοπικό χρήστη που θέλει να το ανακαλύψει.

Εάν τα κλειδιά είναι προσιτά στους χρήστες, κατόπιν όλα τα κλειδιά πρέπει να αλλάζουν όποτε μέλη του προσωπικού φεύγουν από την επιχείρηση. Η γνώση κλειδιών WEP επιτρέπει σε έναν χρήστη να φτιάξει έναν 802.11 σταθμό και να ελέγχει παθητικά και να αποκρυπτογραφεί την κυκλοφορία χρησιμοποιώντας το μυστικό κλειδί. Το WEP δεν μπορεί να προστατεύσει ενάντια στα εξουσιοδοτημένα μέλη που έχουν επίσης το κλειδί.

Οι οργανισμοί με μεγάλο αριθμό εξουσιοδοτημένων χρηστών πρέπει να δημοσιεύσουν το κλειδί στους πληθυσμούς χρηστών και έτσι αυτό δεν παραμένει μυστικό.

2.2.4 Προβλήματα του WEP

Οι κρυπτογράφοι έχουν εντοπίσει πολλές αδυναμίες στο WEP. Οι σχεδιαστές καθόρισαν τη χρήση RC4, ο οποίος γίνεται αποδεκτός ευρέως ως ισχυρός κρυπτογραφικός αλγόριθμος κρυπτογράφησης. Οι επιτιθέμενοι, εντούτοις, δεν περιορίζονται σε μια πλήρως μετωπική επίθεση στους κρυπτογραφικούς αλγορίθμους. Μπορούν να επιτεθούν σε οποιοδήποτε αδύνατο σημείο στο κρυπτογραφικό σύστημα. Μέθοδοι για να ηττηθεί το WEP προκύπτουν από παντού. Ένας προμηθευτής κατασκεύασε σημεία πρόσβασης που παραθέτουν το μυστικό κλειδί WEP κατευθείαν με SNMP, που επιτρέπει σε έναν επιτιθέμενο να ζητήσει απλά το κλειδί. Το μεγαλύτερο μέρος των εκδόσεων, εν τούτοις, είναι αφιερωμένο στις αδυναμίες πέρα από τα λάθη εφαρμογής, οι οποίες είναι πολύ πιο δύσκολο να διορθωθούν.

Αδυναμίες σχεδιασμού

Οι αδυναμίες σχεδιασμού του WEP άρχισαν να φαίνονται όταν η ομάδα Ασφάλειας, Εφαρμογών, Επικύρωσης και Κρυπτογραφίας (ISAAC) του Πανεπιστημίου του Berkeley δημοσίευσε προκαταρκτικά αποτελέσματα βασισμένα στην ανάλυση του προτύπου WEP.

Κανένα από τα προβλήματα που προσδιορίζονται από τους ερευνητές δεν εξαρτάται από το σπάσιμο του RC4.

Παρουσιάζουμε μια περίληψη των προβλημάτων που βρέθηκαν:

1. Η χειρωνακτική διαχείριση κλειδιών είναι ένα ναρκοπέδιο προβλημάτων. Παραμερίζοντας τα λειτουργικά ζητήματα που προκύπτουν με τη διανομή των δημοσίων μυστικών στον πληθυσμό χρηστών, οι ανησυχίες ασφάλειας είναι εφιαλτικές. Το νέο υλικό κλειδιών πρέπει να διανεμηθεί σε μια καθορισμένη ημέρα σε όλα τα συστήματα ταυτόχρονα, και οι συνετές πρακτικές ασφάλειας θα έκλιναν έντονα προς τη νέα εισαγωγή κλειδιού όποτε οποιοσδήποτε που χρησιμοποιεί WEP αφήνει την επιχείρηση (το διαχειριστικό σώμα μπορεί, εντούτοις, να μην το κάνει

αυτό). Τα ευρέως διανεμημένα μυστικά τείνουν να γίνουν δημόσια κατά τη διάρκεια του χρόνου. Οι παθητικές επιθέσεις sniffing απαιτούν μόνο τα κλειδιά WEP, τα οποία είναι πιθανό να αλλαχτούν σπάνια. Μόλις ένας χρήστης λάβει τα κλειδιά WEP, οι επιθέσεις sniffing είναι εύκολες.

2. Παρά τις αξιώσεις προμηθευτών για το αντίθετο, το τυποποιημένο WEP προσφέρει ένα δημόσιο μυστικό από μόνο 40 bit. Οι εμπειρογνώμονες ασφάλειας έχουν εξετάσει από καιρό την επάρκεια του 40-bit ιδιωτικού κλειδιού, και πολλοί συστήνουν τα ευαίσθητα στοιχεία να προστατεύονται από τουλάχιστον 128-bit κλειδιά. Δυστυχώς, κανένα πρότυπο δεν έχει αναπτυχθεί για τα πιο μακροχρόνια κλειδιά, έτσι η διαλειτουργικότητα στα δίκτυα πολλών διαφορετικών υποκατασκευαστών με τα μακροχρόνια κλειδιά WEP δεν είναι εγγυημένη χωρίς μελλοντική εργασία του IEEE.

3.Οι αλγόριθμοι κρυπτογράφησης ακολουθίας είναι τρωτοί στην ανάλυση όταν επαναχρησιμοποιείται το keystream. Η χρήση του IV από το WEP πληροφορεί έναν επιτιθέμενο για την επαναχρησιμοποίηση keystream. Δύο πλαίσια που μοιράζονται το ίδιο IV σχεδόν βέβαια χρησιμοποιούν το ίδιο μυστικό κλειδί και keystream. Αυτό

το πρόβλημα γίνεται χειρότερο από τις φτωχές εφαρμογές, οι οποίες μπορούν να μην επιλέξουν τυχαία IVs. Η ομάδα του Berkeley προσδιόρισε μια εφαρμογή που αρχίζει με ένα IV 0 όταν η κάρτα εισάγεται και αυξάνει απλά το IV για κάθε πλαίσιο.

Επιπλέον, το IV διάστημα είναι αρκετά μικρό (λιγότερο από 17 εκατομμύρια), έτσι οι επαναλήψεις είναι εγγυημένες για τα πολυάσχολα δίκτυα.

4.Η σπάνια νέα εισαγωγή κλειδιών επιτρέπει στους επιτιθεμένους να συγκεντρώσουν ότι η ομάδα του Berkeley καλεί *λεξικά αποκρυπτογράφησης* δηλαδή μεγάλες συλλογές των πλαισίων που κρυπτογραφούνται με τα ίδια keystreams. Δεδομένου ότι περισσότερα πλαίσια με το ίδιο IV συσσωρεύονται, περισσότερες πληροφορίες είναι διαθέσιμες για τα πλαίσια ακόμα κι αν το μυστικό κλειδί δεν ανακτάται. Λαμβάνοντας υπόψη πόσο καταπονημένο το προσωπικό διαχείρισης συστημάτων και δικτύων είναι η σπάνια νέα εισαγωγή κλειδιών είναι ο κανόνας.

5.Το WEP χρησιμοποιεί ένα CRC για τον έλεγχο ακεραιότητας. Αν και η τιμή του ελέγχου ακεραιότητας κρυπτογραφείται από το RC4 keystream, οι CRCs δεν είναι κρυπτογραφικά ασφαλείς. Η χρήση ενός αδύναμου ελέγχου ακεραιότητας δεν αποτρέπει τους επιτιθεμένους από το να τροποποιούν διαφανώς πλαίσια.

6.Το σημείο πρόσβασης είναι σε προνομιούχο θέση να αποκρυπτογραφεί πλαίσια. Ένας σταθμός μπορεί να δεχθεί επίθεση με την εξαπάτηση του σημείου πρόσβασης στην αναμετάδοση των πλαισίων που κρυπτογραφήθηκαν από WEP. Τα πλαίσια που παραλαμβάνονται από το σημείο πρόσβασης θα αποκρυπτογραφούνταν και έπειτα θα αναμεταδίδονταν στο σταθμό του επιτιθεμένου. Εάν ο επιτιθέμενος χρησιμοποιεί WEP, το σημείο πρόσβασης θα κρυπτογραφούσε πρόθυμα το πλαίσιο χρησιμοποιώντας το κλειδί του επιτιθεμένου.

2.2.5 Το τελικό σπάσιμο του κλειδιού

Τον Αύγουστο του 2001, οι Scott Fluhrer, Itsik Mantin, και Adi Shamir δημοσίευσαν ένα έγγραφο με τον τίτλο »Αδυναμίες στο αλγόριθμο σχεδίασης κλειδιού RC4.» Στο τέλος του εγγράφου, οι συντάκτες περιγράφουν μια θεωρητική επίθεση σε WEP. Στην καρδιά της επίθεσης είναι μια αδυναμία στον τρόπο που ο

RC4 παράγει το keystream. Αυτό που προκύπτει είναι η δυνατότητα να ανακτηθεί το πρώτο byte του κρυπτογραφημένου ωφέλιμου φορτίου. Δυστυχώς, το 802.11 χρησιμοποιεί ενθυλάκωση LLC, και η cleartext τιμή του πρώτου byte είναι γνωστή ως 0xAA (το πρώτο byte της επικεφαλίδας SNAP). Επειδή το πρώτο byte του cleartext είναι γνωστό, το πρώτο byte του keystream μπορεί να προκύψει εύκολα από μια τετριμμένη λειτουργία XOR με το πρώτο κρυπτογραφημένο byte.

Οι επιθέσεις του εγγράφου στρέφονται σε μια κατηγορία αδύναμων κλειδιών που γράφονται στη μορφή (B+3):ff:N. Κάθε αδύναμο IV χρησιμοποιείται για να επιτεθεί σε ένα συγκεκριμένο byte του μυστικού τμήματος του RC4 κλειδιού. Τα bytes κλειδιού είναι αριθμημένα από το μηδέν. Επομένως, το αδύναμο IV που αντιστοιχεί στο byte μηδέν του μυστικού κλειδιού έχει τον τύπο 3:FF:N. Το δεύτερο byte πρέπει να είναι 0xFF. Η γνώση του τρίτου byte στο κλειδί απαιτείται, αλλά δεν χρειάζεται να έχει κάποια συγκεκριμένη αξία.

Ένα τυποποιημένο κλειδί WEP είναι 40 μυστικά bit, ή 5 bytes που αριθμούνται κατά συνέπεια από 0 έως 4. Τα αδύναμα IVs σε ένα δίκτυο που προστατεύεται από τυποποιημένο WEP πρέπει να έχουν ένα πρώτο byte που κυμαίνεται από 3 (B=0) έως 7 (B=4) και ένα δεύτερο byte 255. Το τρίτο byte πρέπει να σημειωθεί αλλά δεν είναι περιορισμένο σε κάποια συγκεκριμένη αξία. Υπάρχει 5 X 1 X 256=1,280 αδύναμα IVs στο πρότυπο δίκτυο WEP.

Είναι ενδιαφέρον να σημειωθεί ότι ο αριθμός αδύναμων κλειδιών εξαρτάται εν μέρει από το μήκος του RC4 κλειδιού που χρησιμοποιείται. Εάν το μέγεθος κλειδιού WEP αυξάνεται για πρόσθετη προστασία, το δίκτυο αδύναμου κλειδιού απαιτεί περισσότερα δεδομένα στην επίθεση. Τα περισσότερα εμπορικά προϊόντα χρησιμοποιούν ένα 128-bit δημόσιο RC4 κλειδί, έτσι ώστε να υπάρχουν πάνω από δύο φορές περισσότερα αδύναμα IVs. Ο πίνακας 2.1 παρουσιάζει τον αριθμό των αδύναμων IVs ως συνάρτηση του μυστικού μήκους κλειδιού.

Μυστικό μήκος κλειδιού	B+3 IV	Τιμές του στα αδύναμα (B+3:FF:N)	Αριθμός αδύναμων IVs	Ποσοστό των αδύναμων IV
40 bits		3<=B+3<8 (0<=B<5)	1280	0.008%
104 bits		3<=B+3<16 (0<=B<13)	3328	0.020%
128 bits		3<=B+3<19 (0<=B<16)	4096	0.024%

Πίνακας 2.1 Αριθμός των αδύναμων IVs σαν συνάρτηση του μήκους κλειδιού

Εφαρμόζοντας την θεωρία πιθανοτήτων οι Flurher, Mantin και Shamir προβλέπουν ότι περίπου 60 επιλυμένες περιπτώσεις απαιτούνται για να καθορίσουν ένα byte κλειδιού. Επιπλέον, και ίσως χειρότερα από όλα, η επίθεση κερδίζει ταχύτητα καθώς περισσότερα byte κλειδιού καθορίζονται. Συνολικά, λειτουργεί σε γραμμικό χρόνο. Ο διπλασιασμός του μήκους κλειδιού διπλασιάζει μόνο το χρόνο που χρειάζεται η επίθεση να πετύχει.

Με ένα τέτοιο αποπλανητικό αποτέλεσμα, ήταν μόνο ένα θέμα χρόνου προτού να χρησιμοποιηθεί για να γίνει επίθεση σε ένα πραγματικό σύστημα. Στις αρχές

Αυγούστου του 2001 οι Adam Stubblefield, John Ioannidis, και Avi Rubin εφάρμοσαν την επίθεση Fluhrer/Mantin/Shamir σε ένα πειραματικό, αλλά πραγματικό, δίκτυο με καταστρεπτική επίδραση. Στη δοκιμή τους, 60 επιλυμένες περιπτώσεις καθόριζαν συνήθως ένα byte κλειδιού και 256 επιλυμένες περιπτώσεις παρήγαγαν πάντα ένα πλήρες κλειδί. Χρειάστηκε λιγότερο από εβδομάδα για να γίνει η επίθεση, από την παραγγελία της ασύρματης κάρτας στην αποκατάσταση του πρώτου πλήρους κλειδιού. Η κωδικοποίηση της επίθεσης διήρκεσε μόνο μερικές ώρες. Η αποκατάσταση κλειδιού ολοκληρώθηκε μεταξύ πέντε και έξι εκατομμυρίων πακέτων, το οποίο είναι ένας μικρός αριθμός ακόμη και για ένα πολυάσχολο δίκτυο.

Η υποβολή έκθεσης σχετικά με μια επιτυχή επίθεση, εντούτοις, δεν είναι τίποτα σε σχέση με την κατοχή μιας δημόσιας βάσης κώδικα διαθέσιμης στη χρήση. Το βασικό σημείο της επίθεσης Fluhrer/Mantin/Shamir ήταν η εύρεση της RC4 αδυναμίας. Η εφαρμογή των συστάσεών τους δεν είναι πάρα πολύ δύσκολη. Τον Αύγουστο του 2001, ο Jeremy Bruestle και Blake Hegerle παρουσίασαν τοAirSnort, ένα open-source πρόγραμμα αποκατάστασης WEP.

2.2.6 Συμπεράσματα και συστάσεις

Το WEP είχε ως σκοπό να παρέχει τη σχετικά ελάχιστη προστασία στα πλαίσια στον αέρα. Δεν ήταν σχεδιασμένο για περιβάλλοντα που απαιτούν ένα υψηλό επίπεδο ασφάλειας και επομένως προσφέρει ένα συγκριτικά μικρότερο επίπεδο προστασίας. Η IEEE 802.11 ομάδα εργασίας έχει αφιερώσει μια ολόκληρη υποομάδα στην ασφάλεια. Η υποομάδα αυτή εργάζεται ενεργά σε ένα αναθεωρημένο πρότυπο ασφάλειας. Στο μεταξύ, μερικοί προμηθευτές προσφέρουν προσεγγίσεις που επιτρέπουν ισχυρότερη επικύρωση δημοσίου κλειδιού και τα τυχαία κλειδιά συνόδου, αλλά αυτές οι προσεγγίσεις είναι λύσεις μη γενικές που απευθύνονται μόνο σε ένα προμηθευτή.

Παραθέτονται τα εξής συμπεράσματα:

1.Το WEP δεν είναι χρήσιμο παρά μόνο για την προστασία ενάντια σε κοινές επιθέσεις σύλληψης της κίνησης πακέτων. Με το τελικό σπάσιμο τον Αύγουστο του 2001 και την επόμενη απελευθέρωση του δημοσίου κώδικα εφαρμογής, οι διαχειριστές ασφάλειας πρέπει να υποθέσουν ότι το WEP από μόνο του δεν προσφέρει καμία εμπιστευτικότητα. Επιπλέον, τα 802.11 δίκτυα δηλώνουν την ύπαρξη τους σε όλους. Είναι πολύ εύκολο να ανιχνευθούν από ένα laptop που χρησιμοποιεί απλά μια PC card IEEE 802.11.

2. Η χειρωνακτική διαχείριση κλειδιών είναι ένα σοβαρό πρόβλημα. Τα από άκρη σε άκρη (peer-to-peer) συστήματα δικτύωσης έχουν προβλήματα στον τομέα της διαχειριστικής εξελιξιμότητας και τοWEP το ίδιο. Να επεκτείνουν pairwise κλειδιά είναι ένα τεράστιο φορτίο για τους διαχειριστές συστημάτων και δεν προσφέρει πολλή επιπλέον ασφάλεια.

3. Όταν ένα μυστικό μοιράζεται ευρέως, παύει γρήγορα να είναι μυστικό. Το WEP εξαρτάται ευρέως από την διανομή του μυστικού κλειδιού. Οι χρήστες αλλάζουν και τα κλειδιά WEP πρέπει να αλλάζουν με κάθε αναχώρηση για να εξασφαλισθεί η προστασία που παρέχεται από WEP.

4. Τα δεδομένα που πρέπει να κρατηθούν εμπιστευτικά πρέπει να χρησιμοποιούν ισχυρά κρυπτογραφικά συστήματα σχεδιασμένα από την αρχή επάνω στην ασφάλεια. Οι προφανείς επιλογές είναι οι IPSec ή SSH. Η επιλογή μπορεί να

βασιστεί στην τεχνική αξιολόγηση, στην διαθεσιμότητα προϊόντων, στην πείρα των χρηστών, και σε μη τεχνικούς παράγοντες (θεσμική αποδοχή, τιμολόγηση και χορήγηση αδειών, και τα λοιπά).

5. Ποικίλα επίπεδα ανησυχίας είναι πιθανά για τις διαφορετικές θέσεις. Κατά τη χρησιμοποίηση του 802.11 για την επέκταση ενός LAN, οι μεγαλύτερες απειλές είναι πιθανό να βρεθούν στα μεγάλα γραφεία.

α. Οι μακρινοί τηλεργαζόμενοι πρέπει να προστατευθούν από ισχυρά συστήματα VPN όπως IPSec. Η χρησιμοποίηση 802.11 στις μακρινές θέσεις μπορεί να αυξήσει τον κίνδυνο παρεμπόδισης, αλλά οποιεσδήποτε μεταδόσεις από έναν πελάτη σε μια κεντρική περιοχή πρέπει ήδη να προστατεύονται χρησιμοποιώντας ένα ισχυρό σύστημα VPN. Οι επιτιθέμενοι μπορούν να είναι σε θέση να συλλάβουν πακέτα που ταξιδεύουν πέρα από ένα ασύρματο δίκτυο ευκολότερα, αλλά το IPSec σχεδιάστηκε για να λειτουργήσει σε ένα περιβάλλον όπου οι επιτιθέμενοι είχαν μεγάλα ποσά κρυπτογραφημένης κυκλοφορίας να αναλύσουν.

β. Τα μεγάλα γραφεία θέτουν μια πολύ μεγαλύτερη ανησυχία. Τα VPNs στα περιφερειακά γραφεία είναι από περιοχή σε περιοχή, προστατεύοντας μόνο από την άκρη του περιφερειακού γραφείου έως το σημείο πρόσβασης (AP) στα γραφεία έδρας. Οτιδήποτε μέσα στο απομακρυσμένο γραφείο δεν προστατεύεται από IPSec είναι τρωτό στο sniffing εάν άλλα μέτρα δεν λαμβάνονται.

6. Το να σταματήσεις τίποτα πιο σύνηθες από το sniffing πακέτων απαιτεί λογισμικό πελάτη που πραγματοποιεί ισχυρή κρυπτογραφική προστασία. Εντούτοις, απαιτεί επιπλέον εργασία ανάπτυξης του συστήματος και δοκιμής.

α. Μια τεχνολογία υψηλής ασφάλειας, διασωλήνωσης (tunneling) από σημείο σε σημείο μπορεί να είναι όλα όσα χρειάζεται μια επιχείρηση. Τα συστήματα Unix μπορούν να τρέξουν PPP πάνω σε SSH κανάλια, και μερικές λύσεις IPSec μπορούν να χρησιμοποιηθούν για να δημιουργήσουν tunneling από σημείο σε σημείο πέρα από το σημείο πρόσβασης.

β. Το IPSec προστατεύει επίσης πέρα από το LAN, το οποίο μπορεί να είναι σημαντικό. Είναι δυνατό ένας επιτιθέμενος να αποκτήσει πρόσβαση στο συνδεμένο με καλώδιο LAN όπου η κυκλοφορία δεν προστατεύεται πλέον από WEP.

7. Το WEP δεν προστατεύει τους χρήστες τον ένα από τον άλλο. Όταν όλοι οι χρήστες έχουν το κλειδί WEP, οποιαδήποτε κυκλοφορία μπορεί να αποκρυπτογραφηθεί εύκολα. Ασύρματα δίκτυα που πρέπει να προστατεύσουν τους χρήστες τον ένα από τον άλλο πρέπει να χρησιμοποιήσουν λύσεις VPN ή εφαρμογές με ισχυρή ενσωματωμένη ασφάλεια.

Είναι επικίνδυνο να υποτεθεί ότι τα πρωτόκολλα όπως IPSec και SSH είναι μαγικές σφαίρες που μπορούν να λύσουν τα προβλήματα ασφάλειας. Αλλά το γεγονός για τα ασύρματα δίκτυα είναι ότι δεν μπορούν να βασίζονται στο WEP για να παρέχουν ακόμη και την ελάχιστη ασφάλεια, και η χρησιμοποίηση IPSec ή SSH για να κρυπτογραφήσουν την κυκλοφορία βελτιώνει αρκετά την κατάσταση.

2.3 WPA - Ασύρματη Προστατευμένη Πρόσβαση

Το πρότυπο IEEE 802.Hi ανέπτυξε την Ασύρματη Προστατευμένη Πρόσβαση (Wi-Fi Protected Access - WPA) προκειμένου να καλυφθεί η ανάγκη για περισσότερη ασφάλεια από αυτή που παρέχει το WEP, χρησιμοποιώντας τις

δυνατότητες του υπάρχοντος εξοπλισμού ασύρματης δικτύωσης. Για το σκοπό αυτό, ορίστηκε το **Πρωτόκολλο Χρονικής Ακεραιότητας Κλειδιού** (Temporal Key Integrity Protocol - TKIP), το *οποίο* παρουσιάζεται παρακάτω. Το TKIP μπορεί να χρησιμοποιηθεί απλά με αναβάθμιση του λογισμικού των παλιότερων προϊόντων ασύρματης δικτύωσης.

2.3.1 Πρωτόκολλο χρονικής ακεραιότητας κλειδιού

Οι αδυναμίες του WEP, που είδαμε , μπορούν να συνοψιστούν στον πίνακα 2.1.

Το Πρωτόκολλο Χρονικής Ακεραιότητας Κλειδιού (TKIP) εισάγει μια σειρά μέτρων που αντιμετωπίζουν κάθε ένα από τα ελαττώματα αυτά. Παρόλο που δεν είναι δυνατό να γίνουν μεγάλες αλλαγές, όπως για παράδειγμα να τροποποιηθεί ο τρόπος υλοποίησης του RC4 σε hardware, εν τούτοις, προστίθενται μια σειρά από διορθωτικά εργαλεία γύρω από το υπάρχον hardware. Οι αλλαγές που εφαρμόζονται στο WEP για την υλοποίηση του TKIP παρατίθενται στον πίνακα 2.3, όπου οι αριθμοί σε παρένθεση υποδεικνύουν τις αδυναμίες του πίνακα 2.2 που αντιμετωπίζει η κάθε αλλαγή.

1.Η τιμή του IV είναι πολύ μικρή και δεν αποτρέπεται η επαναχρησιμοποίησή της.
2.Ο τρόπος παραγωγής των κλειδιών από το IV καθιστά το WEP ευάλωτο σε επιθέσεις αδύναμων κλειδιών.
3.Δεν υπάρχει αποτελεσματικός τρόπος εντοπισμού της τροποποίησης των μηνυμάτων (ακεραιότητα μηνυμάτων).
4.Το WEP χρησιμοποιεί το κύριο κλειδί και δεν προβλέπει την ανανέωση των κλειδιών.
5.Δεν παρέχεται προστασία από την αναπαραγωγή των μηνυμάτων.

Πίνακας 2.2: Οι Αδυναμίες του WEP

Σκοπός	Αλλαγή	Αδυναμίες που αντιμετωπίζονται
Ακεραιότητα μηνυμάτων	Προσθήκη πρωτοκόλλου ακεραιότητας μηνυμάτων που να αποτρέπει την τροποποίηση και να μπορεί να υλοποιηθεί με λογισμικό σε μικροεπεξεργαστή μικρής ισχύος.	(3)
Επιλογή και χρήση IV	Αλλαγή των κανόνων επιλογής των τιμών IV και επαναχρησιμοποίηση του IV ως μετρητή αναπαραγωγής.	(1) (3)
Κλειδί ανά Πακέτο	Αλλαγή του κλειδιού κρυπτογράφησης για κάθε πλαίσιο.	(1) (2) (4)
Μέγεθος IV	Αύξηση του μεγέθους του IV ώστε να αποτρέπεται η επαναχρησιμοποίησή του.	(1) (4)
Διαχείριση Κλειδιών	Προσθήκη μηχανισμού διάθεσης και αλλαγής των κλειδιών που εκπέμπονται.	(4)

Πίνακας 2.3: Αλλαγές από το WEP στο TKIP

Ακεραιότητα μηνυμάτων

Όπως έχει αναφερθεί, η ακεραιότητα μηνυμάτων αποτελεί σημαντική παράμετρος στο θέμα της ασφάλειας. Το WEP διαθέτει το ICV για τον εντοπισμό της τροποποίησης μηνυμάτων, το *οποίο,* όμως, δεν είναι αποτελεσματικό. Αν και δεν αποτελεί μέρος της ασφάλειας του TKIP, ωστόσο η τιμή του εξακολουθεί να υπολογίζεται.

Μια απλή μέθοδος εντοπισμού τροποποιήσεων, είναι ο συνδυασμός όλων των byte ενός μηνύματος για την παραγωγή μιας τιμής ελέγχου και η αποστολή αυτής μαζί με το μήνυμα. Η λαμβάνουσα πλευρά μπορεί να κάνει τον αντίστοιχο υπολογισμό και να συγκρίνει το αποτέλεσμα, το *οποίο* θα διαφέρει εφόσον αλλάξει κάποιο bit.

Αυτή η απλή προσέγγιση δεν είναι αποτελεσματική, καθώς ένας κακόβουλος χρήστης είναι σε θέση να υπολογίσει ξανά την τιμή ελέγχου ώστε να συμφωνεί με τις τροποποιήσεις του στο μήνυμα. Ωστόσο, η βασική ιδέα είναι ίδια: Συνδυασμός όλων των byte του μηνύματος για την παραγωγή μιας τιμής ελέγχου που καλείται Κώδικας Ελέγχου Ακεραιότητας (Message Integrity Code — MIC) και αποστολής της μαζί με το μήνυμα. Εν τούτοις, στην περίπτωση του TKIP, ο MIC υπολογίζεται χρησιμοποιώντας μια μη αντιστρέψιμη επεξεργασία σε συνδυασμό με ένα μυστικό κλειδί. Ως εκ *τούτου,* ο *επίδοξος* εισβολέας δεν είναι σε θέση να υπολογίζει εκ νέου την τιμή του MIC, εφόσον δε γνωρίζει το μυστικό κλειδί. Μόνο ο παραλήπτης μπορεί να υπολογίσει και να ελέγξει την τιμή.

Υπάρχουν πολλές ασφαλείς μέθοδοι για την παραγωγή του MIC, οι *οποίες* όμως, απαιτούν είτε την εισαγωγή νέων κρυπτογραφικών αλγορίθμων ή ταχείς υπολογισμούς πολλαπλασιασμού. Ωστόσο, οι μικροεπεξεργαστές στις περισσότερες υπάρχουσες κάρτες ασύρματης δικτύωσης δε διαθέτουν μεγάλη ισχύ. Και ενώ μια

προσέγγιση θα ήταν η μεταφορά του υπολογιστικού φόρτου στο λογισμικό του *οδηγού,* που αντέχουν οι επεξεργαστές των σύγχρονων προσωπικών υπολογιστών, ωστόσο η λύση αυτή δε μπορεί να εφαρμοστεί στα σημεία πρόσβασης, τα οποία, ως επί το πλείστον, δε διαθέτουν την απαιτούμενη επεξεργαστική ισχύ.

Συνεπώς, απαιτείται μια μέθοδος ασφαλής όσο οι ήδη γνωστές προσεγγίσεις, που να μην απαιτεί όμως, ούτε πολλαπλασιασμούς, ούτε νέους κρυπτογραφικούς αλγορίθμους. Μια καλή λύση συμβιβασμού δόθηκε από τον κρυπτογράφο Niels Ferguson με μια μέθοδο που ονόμασε Μιχάλη (Michael). Ο Μιχάλης είναι μια μέθοδος υπολογισμού του MIC που δε χρησιμοποιεί πολλαπλασιασμούς, παρά μόνο πράξεις ολίσθησης και πρόσθεσης. Ο Μιχάλης μπορεί να υλοποιηθεί από τα σύγχρονα σημεία πρόσβασης χωρίς να καταναλώνει ολόκληρη την υπολογιστική τους ισχύ. Ωστόσο, το κόστος της απλότητας είναι ότι ο Μιχάλης είναι ευάλωτος σε επιθέσεις ωμής δύναμης (brute force), κατά τις *οποίες ο επίδοξος* εισβολέας είναι σε θέση να κάνει πολλές αλλεπάλληλες *επιθέσεις* με ταχύ ρυθμό. Ο Μιχάλης αντιμετωπίζει την αδυναμία αυτή με την εισαγωγή της ιδέας των αντιμέτρων (countermeasures).

Η φιλοσοφία των αντιμέτρων είναι πολύ απλή: ανάπτυξη μιας αξιόπιστης μεθόδου εντοπισμού επιθέσεων και λήψης των κατάλληλων μέτρων. Το απλούστερο των αντιμέτρων είναι το κλείσιμο ολόκληρου του δικτύου όταν ανιχνευθεί μια επίθεση, ώστε ο *επίδοξος* εισβολέας να μην είναι σε θέση να κάνει επιπλέον απόπειρες.

Ο Μιχάλης επιτρέπει τον υπολογισμό της τιμής του MIC η οποία προστίθεται στο μήνυμα πριν την κρυπτογράφηση και ελέγχεται από τον παραλήπτη μετά την αποκρυπτογράφηση. Η τιμή αυτή, προσφέρει την ακεραιότητα μηνυμάτων που δεν παρέχει το WEP.

Ο Μιχάλης εφαρμόζεται στις MSDU καί όχι σε κάθε MPDU. Αυτό προσφέρει δύο πλεονεκτήματα. Κατ' αρχήν, όσον αφορά την πλευρά της ασύρματης συσκευής, επιτρέπει την υλοποίηση του υπολογισμού στον οδηγό της συσκευής που εκτελείται, στον υπολογιστή πριν την προώθηση της MSDU στην κάρτα ασύρματης δικτύωσης. Επιπλέον, περιορίζει το επιπρόσθετο κόστος, καθώς δεν απαιτείται η προσθήκη της τιμής του MIC σε κάθε θραύσμα (MPDU) του μηνύματος. Αντίθετα, η *κρυπτογράφηση* TKIP λαμβάνει χώρα στο επίπεδο της MPDU.

Ο Μιχάλης χρειάζεται, το δικό του μυστικό κλειδί, το *οποίο* πρέπει να είναι διαφορετικό από το μυστικό κλειδί που χρησιμοποιείται στην κρυπτογράφηση. Η εξαγωγή τέτοιων κλειδιών επιτυγχάνεται εύκολα παράγωντας χρονικά κλειδιά από το κύριο κλειδί.

2.3.2 Επιλογή και χρησιμοποίηση IV

Οι αδυναμίες στον τρόπο χρήσης του IV από WEP, συνοπτικά είναι οι εξής:

- Το IV είναι πολύ μικρό με αποτέλεσμα οι τιμές του να επαναχρησιμοποιούνται συχνά σε ένα δίκτυο με πολλή κίνηση.

- Το IV δεν είναι ειδικό για κάθε σταθμό και επομένως το ίδιο IV μπορεί να χρησιμοποιηθεί με το ίδιο μυστικό κλειδί από πολλαπλές ασύρματες συσκευές.

- Ο τρόπος που το IV εισάγεται, πριν από το κλειδί καθιστά το σύστημα ευάλωτο σε επιθέσεις αδύναμων κλειδιών (επιθέσεις FMS).

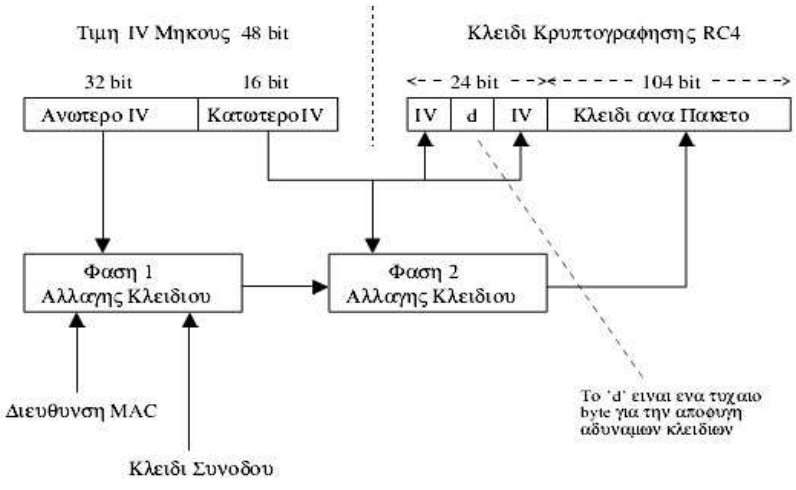
Στο πρότυπο του WEP, δεν υπάρχει η απαίτηση να αποφεύγεται η επαναχρησιμοποίηση του IV, σε αντίθεση με το TKIP. Η αύξηση του IV μπορεί να καθυστερεί τη σύγκρουση τιμών του IV, αυτή, ωστόσο, εμφανίζεται μετά από 16 εκατομμύρια πλαίσια. Ως εκ *τούτου,* το TKIP εισάγει νέους κανόνες όσον αφορά τη χρήση του IV. Ουσιαστικά, υπάρχουν τρεις διαφορές σε σύγκριση με το WEP:

1. Το μέγεθος του IV αυξάνεται από τα 24 στα 48 bit. Για την ακρίβεια προστίθενται 32 bit ακόμη, σχηματίζοντας ένα IV μήκους 56 bit. Ωστόσο, πρακτικά χρησιμοποιούνται μόνο τα 48 bit, καθώς ένα byte αξιοποιείται για την αποφυγή αδύναμων κλειδιών. Η αύξηση αυτή, εξαλείφει αποτελεσματικά τη σύγκρουση τιμών του IV, εν τούτοις, εξακολουθεί να υπάρχει η ανάγκη αποφυγής της χρήσης του ίδιου IV σε συνδυασμό με το ίδιο κλειδί από δύο διαφορετικές συσκευές.

Από την άλλη πλευρά, η αλλαγή αυτή εισάγει ορισμένα προβλήματα όσον αφορά την υλοποίηση. Όπως είναι γνωστό, το IV στο WEP προστίθεται μπροστά από το μυστικό κλειδί προκειμένου να σχηματιστεί το κλειδί κρυπτογράφησης του αλγορίθμου RC4. Ως εκ τούτου, με το συνδυασμό του IV των 24 bit και ενός μυστικού κλειδιού των 40 bit, παράγεται, ένα κλειδί RC4 μήκους 64 bit. Το hardware του παλιότερου εξοπλισμού υποθέτει αυτή τη δομή κλειδιού και δε μπορεί να αναβαθμιστεί ξαφνικά ώστε να υποστηρίζει το νέο κλειδί των 88 bit για τις ανάγκες του TKIP. Στο πλαίσιο αυτό, ακολουθείται η εξής προσέγγιση: αντί να σχηματιστεί ένα νέο κλειδί RC4 από την ένωση του μυστικού κλειδιού και του IV, το IV χωρίζεται σε δύο τμήματα. Τα πρώτα 16 bit του νέου IV επεκτείνονται κατάλληλα στα 24 ώστε να αποφεύγονται, γνωστά αδύναμα κλειδιά. Αυτή η τιμή μήκους 24 bit, χρησιμοποιείται όπως στα συστήματα WEP. Ωστόσο, αντί να ενωθεί με το μυστικό κλειδί, ένα νέο *ανάμεικτο* κλειδί" (mixed key) παράγεται από το συνδυασμό του μυστικού κλειδιού με τα 32 bit που απομένουν στο IV. Ο τρόπος με τον *οποίο* το IV μεγάλου μήκους ενσωματώνεται στο κλειδί, ονομάζεται αλλαγή κλειδιού ανά πακέτο, και παρουσιάζεται στο Σχ. 2.6. Τέλος, πρέπει να σημειωθεί ότι η παραπάνω προσέγγιση επιτυγχάνει δύο στόχους:

• Η τιμή του κλειδιού που χρησιμοποιείται στην κρυπτογράφηση RC4 είναι διαφορετική για κάθε τιμή του IV.

• Η δομή του κλειδιού του RC4 αποτελείται από το «παλιό» IV μήκους 24 bit και ένα πεδίο μυστικού κλειδιού των 104 bit.



Δημιουργία του Κλειδιού Κρυπτογράφησης RC4 στο TKIP

Σχήμα 2.6

2. Το IV αποκτά ένα δευτερεύοντα ρόλο ως μετρητής ακολουθίας για την προστασία από επιθέσεις αναπαραγωγής. Αυτού του είδους η προστασία δεν παρέχεται από το WEP, όπου ένας *επίδοξος* εισβολέας είναι σε θέση να καταγράψει ένα έγκυρο πακέτο και να το αναπαράγει αργότερα. Σε μια τέτοια επίθεση, ο κακόβουλος χρήστης δεν επιχειρεί να αποκρυπτογραφήσει το μήνυμα, ωστόσο, προσπαθεί να υποθέσει το ρόλο αυτού. Για παράδειγμα, καταγράφοντας τα μηνύματα κατά τη διάρκεια της διαγραφής ενός αρχείου, είναι θεωρητικά δυνατό, αναπαράγοντας τα, να διαγραφεί ένα αρχείο με το ίδιο όνομα, χωρίς να παραβιαστεί καν η κρυπτογράφηση. Η προστασία από την αναπαραγωγή έχει ακριβώς ως στόχο την αποφυγή χρήσης παλιών μηνυμάτων με τον τρόπο αυτό. Το TKIP παρέχει ένα σχετικό μηχανισμό που ονομάζεται, μετρητής ακολουθίας TKIP (TKIP Sequence Counter - TSC).

Στην πραγματικότητα, ο TSC και το IV είναι το ίδιο. Η τιμή αρχίζει πάντα από το μηδέν και αυξάνεται κατά ένα για κάΰε πακέτο που στέλνεται. Επειδή, είναι εγγυημένο ότι δεν πρόκειται, να επαναληφθεί η τιμή του IV για ένα *δοσμένο* κλειδί, η αναπαραγωγή μπορεί να αποφευχθεί αγνοώντας οποιαδήποτε μηνύματα παρουσιάζουν τιμή του TSC που έχει ήδη ληφθεί. Οι κανόνες αυτοί εξασφαλίζουν ότι δεν είναι δυνατή μια επίθεση που θα στηρίζεται στην αναπαραγωγή παλιότερων καταγεγραμμένων μηνυμάτων.

Ο απλούστερος τρόπος αποφυγής επιθέσεων αναπαραγωγής είναι η απόρριψη ληφθέντων μηνυμάτων στα οποία ο TSC δεν έχει αυξηθεί κατά 1 σε σχέση με το τελευταίο μήνυμα. Εν τούτοις, υπάρχουν αρκετοί πρακτικοί λόγοι που δεν επιτρέπουν αυτήν την προσέγγιση. Κατ' αρχήν, είναι δυνατό να χαθούν κάποια πλαίσια κατά τη μετάδοση λόγω παρεμβολών και θορύβου. Εξαιτίας ενός ενδεχόμενου χαμένου πλαισίου, όλα τα πλαίσια που θα ακολουθούσαν θα απορρίπτονταν λανθασμένα επειδή ο TSC δε θα είχε αυξηθεί κατά 1.

Ως εκ τούτου, πρέπει να υιοθετηθεί μια προσέγγιση που να λαμβάνει υπόψη της τις επαναμεταδόσεις. Σύμφωνα με το πρότυπο, πρέπει να επιβεβαιώνεται η λήψη των πλαισίων με σύντομα μηνύματα ACK. Αν δε ληφθεί επιβεβαίωση, το μήνυμα πρέπει να επαναμεταδοθεί θέτοντας ένα bit που να υποδεικνύει ότι πρόκειται για αντίγραφο. Όντας μήνυμα επαναμετάδοσης, πρέπει να έχει την ίδια τιμή TSC με το αρχικό. Στην πράξη, η προσέγγιση αυτή είναι αποτελεσματική επειδή η λαμβάνουσα πλευρά χρειάζεται ένα μόνο έγκυρο αντίγραφο του μηνύματος και δεν υπάρχει πρόβλημα να απορρίπτονται τυχόν αντίγραφα κατά τον έλεγχο του TSC από τον παραλήπτη. Το ενδεχόμενο επαναμετάδοσης υποδηλώνει ότι ίδιες τιμές του TSC δεν πρέπει να εκλαμβάνονται απαραίτητα ως απόπειρα επίθεσης.

Ανακύπτει ένα ακόμη δυσκολότερο πρόβλημα εξαιτίας μιας νέας έννοιας γνωστής ως έκρηξη-ack (burst-ack). Σύμφωνα με το αρχικό πρότυπο IEEE 802.11, κάθε πλαίσιο δεδομένων που στέλνεται, πρέπει να επιβεβαιωθεί ξεχωριστά. Ενώ, η απαίτηση αυτή φαίνεται αποτελεσματική, δεν είναι, ωστόσο, επαρκής, καθώς ο αποστολέας πρέπει να σταματάει και να περιμένει μήνυμα ACK προτού συνεχίσει. Η έννοια της έκρηξης-ack είναι να στέλνονται, διαδοχικά έως και 16 πλαίσια και στη συνέχεια να επιτρέπεται στον παραλήπτη να επιβεβαιώσει και τα 16 με ένα μήνυμα. Αν κάποια από τα μηνύματα δε ληφθούν επιτυχώς, ο παραλήπτης είναι σε θέση να υποδείξει ποια χρειάζονται επαναμετάδοση. Η έκρηξη-ack δεν είναι ακόμη μέρος του πρότυπου, εν τούτοις είναι πολύ πιθανό να συμπεριληφΰει στο μέλλον.

- ACCEPT: Ο TSC είναι ο μεγαλύτερος που έχει εμφανιστεί έως τώρα.

- REJECT: Ο TSC είναι μικρότερος του μέγιστου -16.
- WINDOW: Ο TSC είναι μικρότερος του μέγιστου, αλλά μεγαλύτερος από το κατώτερο όριο (μέγιστο -16).

3. Το IV παράγεται, κατάλληλα ώστε να αποφεύγονται ορισμένα αδύναμα κλειδιά, τα οποία καθιστούσαν το WEP ευάλωτο στην επίθεση FMS, που αποτελεί και τη μεγαλύτερη απειλή του προτύπου. Αυτή επιτρέπει την εξαγωγή του μυστικού κλειδιού παρακολουθώντας την κίνηση της δικτυακής κίνησης της ασύρματης ζεύξης με τη βοήθεια αυτοματοποιημένων εργαλείων.

Ο Ron Rivest, σχεδιαστής του RC4, πρότεινε τη μη χρησιμοποίηση των πρώτων 256 byte που παράγονται, από τον αλγόριθμο, προκειμένου να αντιμετωπιστεί αυτή η αδυναμία. Δεδομένου ότι το hardware του υπάρχοντος εξοπλισμού ασύρματης δικτύωσης δεν υποστηρίζει την προτεινόμενη λύση, το TKIP θέτει τους εξής στόχους:

- Προσπάθεια αποφυγής αδύναμων κλειδιών.
- Προσπάθεια επιπρόσθετης απόκρυψης του μυστικού κλειδιού.

Η επίθεση FMS βασίζεται στη δυνατότητα συλλογής πολλαπλών δειγμάτων πλαισίων που περιέχουν αδύναμα κλειδιά. Απαιτούνται μόλις 60 πλαίσια για να εξαχθούν τα πρώτα bit του ζητούμενου, ενώ η πλήρης αποκωδικοποίηση του κλειδιού μπορεί να γίνει μετά από λίγα εκατομμύρια πακέτα. Η προσέγγιση που υιοθετήθηκε από το TKIP είναι, η αλλαγή του μυστικού κλειδιού για κάθε πακέτο. Με τον τρόπο αυτό, ο εισβολέας δεν είναι σε θέση να συγκεντρώσει αρκετά δείγματα για να επιτεθεί σε κάποιο *δοσμένο* κλειδί.

Ένας επιπρόσθετος μηχανισμός άμυνας από την επίθεση FMS είναι η αποφυγή χρήσης αδύναμων κλειδιών. Το πρόβλημα είναι ότι κανείς δε γνωρίζει με ακρίβεια όλα τα αδύναμα κλειδιά. Ωστόσο, οι κρυπτογράφοι έχουν προσδιορίσει έναν τύπο κλειδιού που είναι αδύναμος. Αποδεικνύεται ότι θέτοντας κατάλληλα δύο bit του IV κατά τη φάση ανάμειξης κλειδιού, αποφεύγεται μια γνωστή κατηγορία αδύναμων κλειδιών.

Ορισμένοι κατασκευαστές έχουν τροποποιήσει την υλοποίηση του WEP ώστε να αποφεύγονται τιμές του IV που παράγουν αδύναμα κλειδιά. Εν τούτοις, προκύπτει ένα άλλο πρόβλημα με την προσέγγιση αυτή. Ως γνωστό, δεν υπάρχει επαρκής αριθμός τιμών του IV όταν αυτό έχει μήκος 24 bit. Μειώνοντας λοιπόν ακόμη περισσότερο το *σύνολο* τιμών του IV, περιορίζουμε το ένα πρόβλημα αλλά επιδεινώνουμε ένα άλλο. Στο TKIP δεν υπάρχει αυτός ο κίνδυνος, καθώς το μήκος του IV έχει διπλασιαστεί.

Η ενότητα αυτή, εστιάστηκε στις αλλαγές στον τρόπο χρήσης του IV από το TKIP. Συνοψίζοντας, υπάρχουν τρεις σημαντικές τροποποιήσεις: το μήκος αυξάνεται στα 48 bit, το IV χρησιμοποιείται ως μετρητής ακολουθίας (ο TSC), και το IV συνδυάζεται με το μυστικό κλειδί με περισσότερο *πολύπλοκο* τρόπο σε σχέση με το WEP. Η τελευταία αλλαγή επιτυγχάνει δύο στόχους: επιτρέπει την ενσωμάτωση του IV μήκους 48 bit που να υποστηρίζεται, στις παρούσες υλοποιήσεις hardware και επιπλέον αποτρέπει τη χρήση μιας γνωστής κατηγορίας αδύναμων κλειδιών. Οι τροποποιήσεις, όσον αφορά το IV, παρέχουν πολύ σημαντική επιπρόσθετη ασφάλεια σε σύγκριση με το WEP.

2.3.3 Λεπτομέρειες υλοποίησης του TKIP

Στην ενότητα αυτή, περιγράφεται λεπτομερέστερα ο τρόπος υλοποίησης του αλγορίθμου TKIP. Αρχικά, υποθέτουμε ότι τα κύρια κλειδιά (master keys) έχουν διανεμηθεί, ενώ τα αντίστοιχα κλειδιά συνόδου (session keys) έχουν παραχθεί και στις δύο πλευρές της επικοινωνιακής ζεύξης. Τα κύρια κλειδιά μπορεί ενδεχομένως να έχουν αποκτηθεί χρησιμοποιώντας κάποια από τις μεθόδους επαλήθευσης ταυτότητας των ανωτέρων στρωμάτων που βασίζεται στο EAP, ή εναλλακτικά να αποτελούν προμεριζόμενα (preshared) κλειδιά. Η τελευταία περίπτωση είναι ανάλογη με την προσέγγιση του WEP, όπου τα κλειδιά προεγκαθίστανται στις διάφορες συσκευές. Προφανώς, κάτι τέτοιο μπορεί να βρει εφαρμογή μόνο σε δίκτυα περιορισμένων διαστάσεων ή κατά τη λειτουργία τύπου ad-hoc. Στα πλαίσια του TKIP παράγονται τρεις τύποι κλειδιών:

1. Κλειδί για την προστασία της ανταλλαγής μηνυμάτων EAPOL-Key.
2. Κλειδί-Ζεύγος (pairwise) για την προστασία των ίδιων των μηνυμάτων με χρήση TKIP.
3. Ομαδικό κλειδί για την προστασία εκπομπών (broadcasts) που χρησιμοποιούν TKIP.

Από τα δεδομένα του κλειδιού-ζεύγους παράγονται τα χρονικά κλειδιά:

• Κλειδί Χρονικής Κρυπτογράφησης (128 bit): Αυτό χρησιμοποιείται, ως *είσοδος* στο στάδιο αλλαγής κλειδιών πριν την κρυπτογράφηση RC4.

• Κλειδί Χρονικού Επαληθευτή Ταυτότητας TX MIC: Αυτό χρησιμοποιείται σε συνδυασμό με τη μέθοδο επαλήθευσης ταυτότητας Μιχάλης για την παραγωγή του MIC στα πλαίσια που μεταδίδονται από τον επαληθευτή ταυτότητας (σημείο πρόσβασης σε ένα δίκτυο υποδομής).

• Κλειδί Χρονικού Επαληθευτή Ταυτότητας RX MIC: Αυτό χρησιμοποιείται σε συνδυασμό με τη μέθοδο Μιχάλης για την παραγωγή του MIC στα πλαίσια που μεταδίδονται από την οντότητα του supplicant (συνήθως αυτή είναι η κινητή συσκευή).

Όσον αφορά τα ομαδικά κλειδιά, μόνο οι δύο πρώτοι τύποι χρειάζεται να παραχθούν, καθώς οι εκπομπές (broadcasts) στέλνονται αποκλειστικά από τον επαληθευτή ταυτότητας και όχι από την οντότητα του supplicant.

Ο στόχος του TKIP είναι, όπως έχει αναφερθεί, η παροχή μηχανισμών ασφαλείας, αφενός για την εξασφάλιση της ακεραιότητας των λαμβανομένων δεδομένων, αφετέρου για την προστασία των δεδομένων που αποστέλλονται. Στα πλαίσια αυτά, το πρωτόκολλο υλοποιεί τα ακόλουθα:

- Παραγωγή και έλεγχος IV
- Παραγωγή και έλεγχος MIC

- Κρυπτογράφηση και αποκρυπτογράφηση

Η λειτουργία του TKIP κατά τη μετάδοση δεδομένων, φαίνεται στο Σχ. 2.7. Οι τέσσερις διεργασίες που χρησιμοποιεί το πρωτόκολλο είναι οι ακόλουθες:

1.Μιχάλης

2.Παραγωγή κλειδιών

3.IV/TSC

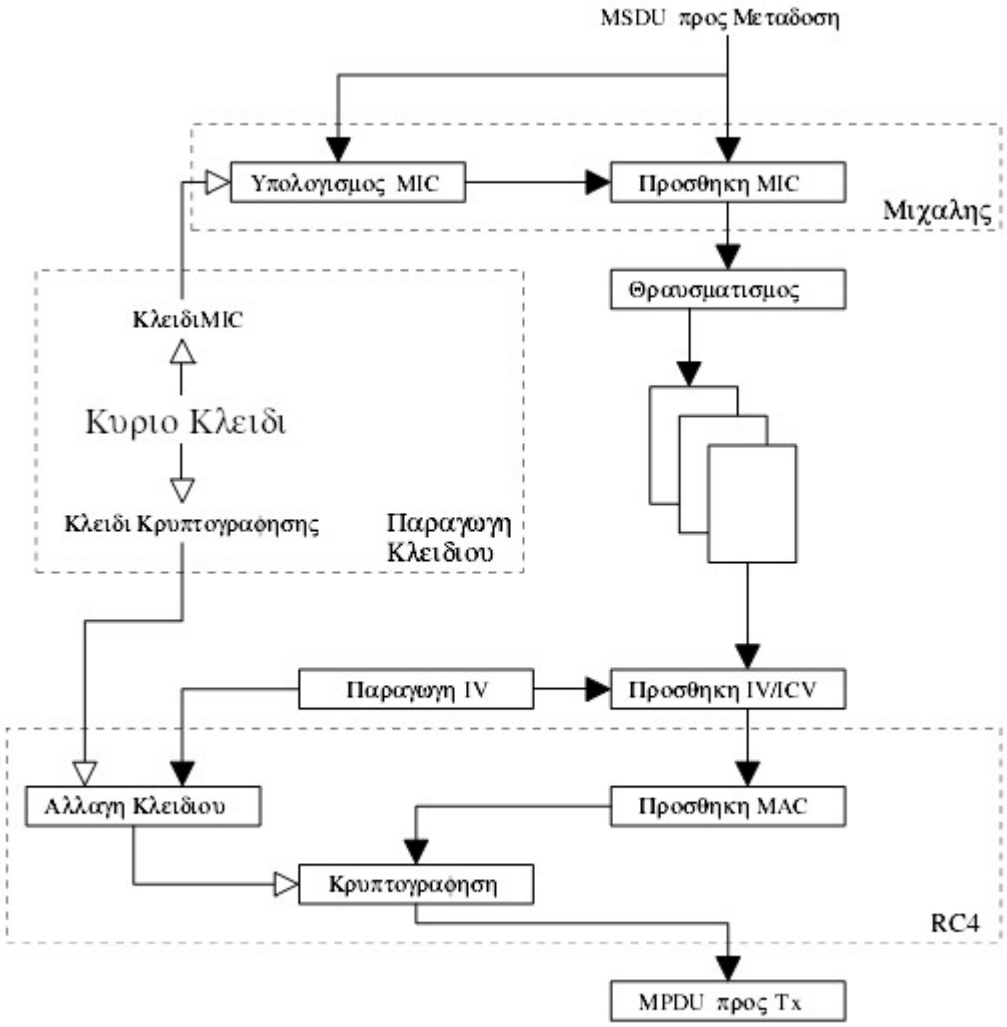
4.RC4

Ας σημειωθεί ότι η τιμή ελέγχου ακεραιότητας υπολογίζεται βάσει της MSDU και προστίθεται σε αυτή, πριν το θραυσματισμό. Ως αποτέλεσμα, τα byte της τιμής ελέγχου είναι παρόντα μόνο στην τελευταία MPDU και περιέχονται στα κρυπτογραφημένα δεδομένα. Η αρχική τιμή ελέγχου (του WEP), το ICV, εξακολουθεί να υπολογίζεται και να προστίθεται σε κάθε MPDU, παρόλο που δεν αποτελεί μέρος του ελέγχου ακεραιότητας πακέτων του TKIP.

Καθώς το MIC υπολογίζεται στο επίπεδο της MSDU, δεν είναι δυνατό να συμπεριληφθεί η τιμή του IV στον υπολογισμό του MIC για δύο λόγους. Κατ' αρχήν, επειδή η MSDU μπορεί να είναι θραυσματισμένη, ενδέχεται να χρησιμοποιούνται πολλαπλές τιμές του IV για την αποστολή των θραυσμάτων της MSDU. Επιπλέον, δεν επιτρέπεται η επιλογή της τιμής του IV, παρά μόνο μετά την αφαίρεση του θραύσματος από τις ουρές μετάδοσης. Στο μέλλον, προκειμένου να υποστηριχθούν πολυμεσικές εφαρμογές, το πρότυπο IEEE 802.11e μπορεί να διαθέτει μέχρι και οκτώ ουρές προτεραιότητας για τα εξερχόμενα πλαίσια και η σειρά με την οποία τα θραύσματα επιλέγονται για μετάδοση εξαρτάται από *πολλούς* παράγοντες που καθορίζονται, από περιορισμούς πραγματικού χρόνου και προτεραιότητες. Ως εκ *τούτου, οι* MSDU υψηλότερης προτεραιότητας ενδέχεται να προηγηθούν παλαιότερων MSDU ή ακόμη και να σταλούν μεταξύ θραυσμάτων των τελευταίων. Το TKIP διαθέτει ένα μόνο μετρητή IV ανά ζεύξη -όχι ανά ουρά- και επομένως η ανάθεση της τιμής του IV πρέπει να περιμένει μέχρι την τελευταία στιγμή, δηλαδή πριν την επιλογή ενός θραύσματος για μετάδοση. Συνεπώς, η τιμή δε μπορεί να είναι, γνωστή κατά τον υπολογισμό του MIC.

Ο υπολογισμός του MIC στο επίπεδο της MSDU, σε συνδυασμό με την έλλειψη προστασίας του IV, επιτρέπει σε ένα *επίδοξο* εισβολέα να «μπλοκάρει» ένα σταθμό αναπαράγοντας προηγούμενα πλαίσια με νέα τιμή του IV. Το πρόβλημα ανακύπτει καθώς το IV διπλασιάζεται, όπως ο μετρητής ακολουθίας TSC, προκειμένου να αποφευχθούν οι επιθέσεις αναπαραγωγής. Προφανώς, θα αποτύχει η αποκρυπτογράφηση τέτοιων ψευδεπίγραφων πλαισίων, τα οποία και θα απορριφθούν. Δεν αποτελούν απειλή ως προς την ακεραιότητα του πρωτοκόλλου, ωστόσο καθιστούν τα έγκυρά πλαίσια που ακολουθούν να φαίνονται σαν επίθεση αναπαραγωγής. Όταν ένα έγκυρο πλαίσιο καταφτάνει, ενδέχεται να απορριφθεί επειδή η τιμή του TSC έχει εξαντληθεί από τον επιτιθέμενο σταθμό. Συνεπώς, ανήκει στην κατηγορία των επιθέσεων άρνησης-υπηρεσιών (denial-of-service). Στον κόσμο των ασύρματων επικοινωνιών υπάρχουν *πολλοί* απλοί τρόποι που επιτυγχάνουν ακριβώς αυτό και δεν είναι δυνατό να αντιμετωπιστούν αποτελώντας μόνιμα μια πιθανή απειλή.

Υποτίθεται ότι το τμήμα Κρυπτογράφησης, όπως παρουσιάζεται στο Σχ. 2.7, υλοποιεί τον ίδιο αλγόριθμο κρυπτογράφησης RC4 που χρησιμοποιείται και στο WEP. Οι περισσότεροι κατασκευαστές έχουν υλοποιήσει το τμήμα αυτό με τέτοιο τρόπο ώστε να μην είναι δυνατή η τροποποίησή του μέσω αναβαθμίσεων firmware.



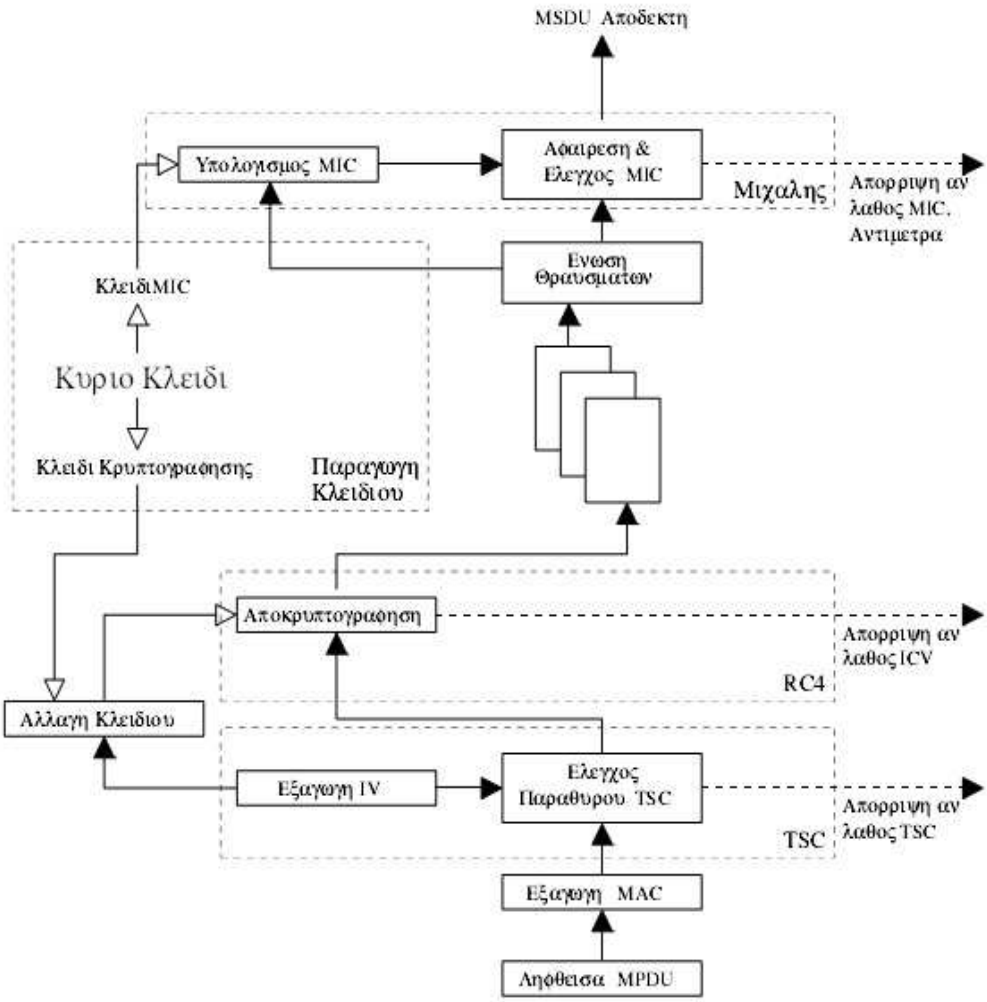
Λειτουργία του TKIP κατά τη Μετάδοση

Ο υπάρχων εξοπλισμός WEP συχνά περιλαμβάνει μηχανισμό hardware για την αρχικοποίηση του κουτιού-S του RC4. Η αδυναμία αλλαγής της συγκεκριμένης μονάδας, αποτέλεσε και το μεγαλύτερο πρόβλημα κατά το σχεδιασμό του TKIP.

Σχήμα 2.7

Η διαδικασία λήψης δεν είναι η ακριβώς αντίστροφη αυτής της μετάδοσης. Κατ' αρχήν, η αποκρυπτογράφηση δεν είναι η πρώτη λειτουργία. Αντίθετα, ο TSC (που προκύπτει από το IV) ελέγχεται για την προστασία από αναπαραγωγές. Ας σημειωθεί ότι η τιμή του ICV ελέγχεται και χρησιμοποιείται για την απόρριψη του πακέτου. Δεν πρόκειται αυστηρά για έναν έλεγχο ακεραιότητας , ωστόσο αποτελεί μια γρήγορη ένδειξη για την επιτυχία ή μη της αποκρυπτογράφησης: Η αποκρυπτογράφηση ενός πακέτου με λανθασμένο κλειδί ή με χρήση μη έγκυρων τιμών του IV παράγει πάντα λανθασμένη τιμή του ICV.

Το MIC ελέγχεται μετά τη λήψη όλων των θραυσμάτων και τη σύνθεσή τους στην MSDU. Ας σημειωθεί ότι αν το MIC αποτύχει, δε θα απορριφθεί μόνο η MSDU, αλλά, επιπλέον, ενδέχεται να ενεργοποιηθούν αντιμέτρα. Αν και θεωρητικά δυνατό, είναι εξαιρετικά απίθανο να υπάρξουν λάθη κατά τη μετάδοση, τέτοια που να επιτρέψουν σε ένα πλαίσιο να περάσει τον έλεγχο CRC και στη συνέχεια να αποκρυπτογραφηθεί για να παράγει ένα αποδεκτό ICV. Σε περίπτωση αποτυχίας του MIC , είναι σίγουρο ότι έχει προηγηθεί σκόπιμη τροποποίηση και όχι τυχαία σφάλματα μετάδοσης ή παρεμβολές.



Λειτουργία του TKIP κατά τη Λήψη

Σχήμα 2.8

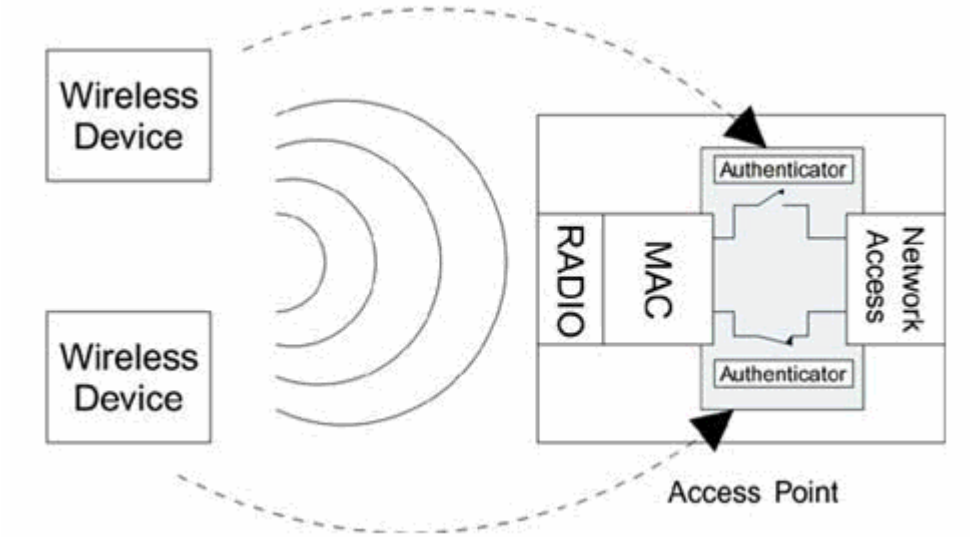
2.3.4 Το 802.1X

Για να αντιμετωπιστούν οι ανεπάρκειες του WEP σχετικά με την επικύρωση εξετάζονται λύσεις βασισμένες στην προδιαγραφή 802.1X, η οποία είναι η ίδια βασισμένη στο IETF Εκτεταμένο Πρωτόκολλο Επικύρωσης (EAP). Το EAP σχεδιάστηκε με γνώμονα την ευελιξία και έχει χρησιμοποιηθεί ως βάση για διάφορες επεκτάσεις επικύρωσης δικτύων.

Το IEEE 802.1X είναι πολύ απλό στην έννοια. Ο σκοπός του είναι να εφαρμόσει τον έλεγχο πρόσβασης στο σημείο στο οποίο ένας χρήστης ενώνεται στο δίκτυο. Διαιρεί το δίκτυο σε τρεις οντότητες.

- Τους Supplicants, που θέλουν να συνδεθούν στο δίκτυο
- Τον Authenticator, που ελέγχει την πρόσβαση
- Τον Κεντρικό Υπολογιστή Επικύρωσης (Authentication Server), ο οποίος λαμβάνει τις αποφάσεις έγκρισης

Το σημείο στο οποίο ένας χρήστης συνδέεται με το δίκτυο καλείται θύρα (port). Ένα δίκτυο μπορεί να έχει πολλές θύρες παραδείγματος χάριν, σε ένα switched LAN hub κάθε σύνδεσμος (connector) Ethernet θα ήταν μια θύρα. Υπάρχει μια ένα προς ένα σχέση μεταξύ supplicant και θύρας, και κάθε θύρα έχει ένα σχετικό authenticator για να ελέγξει την κατάστασή της. Υπάρχει μια πολλοί προς ένας σχέση μεταξύ των θυρών και του κεντρικού υπολογιστή επικύρωσης. Με άλλα λόγια, ένας ενιαίος κεντρικός υπολογιστής επικύρωσης είναι συνήθως αρμόδιος για πολλές θύρες, κάθε μια όμως έχει το δικό της authenticator. Η χρησιμοποίηση του 802.1X στα ασύρματα δίκτυα φαίνεται παρακάτω στο σχήμα 2.9.



Σχήμα 2.9 IEEE 802.1X θύρες σε ένα σημείο πρόσβασης

Το 802.1X έχει παρόλα' αυτά προβλήματα. Μια πρόσφατη ερευνητική έκθεση προσδιόρισε αρκετά προβλήματα με την προδιαγραφή. Το πρώτο σημαντικό πρόβλημα είναι ότι το 802.1X δεν παρέχει ένα τρόπο να εγγυηθεί την αυθεντικότητα και την ακεραιότητα οποιωνδήποτε πλαισίων στο ασύρματο δίκτυο. Τα πλαίσια στα ασύρματα δίκτυα μπορούν εύκολα να πειραχτούν ή να καταστραφούν εντελώς, και το πρωτόκολλο δεν παρέχει έναν τρόπο να σταματήσουν εύκολα ή ακόμα και να ανιχνευθούν τέτοιες επιθέσεις. Το δεύτερο σημαντικό πρόβλημα είναι ότι το 802.1X είχε ως σκοπό να επιτρέψει στο δίκτυο να επικυρώσει το χρήστη. Υπονοείται στο σχέδιο του πρωτοκόλλου ότι οι χρήστες θα συνδεθούν μόνο με το "σωστό" δίκτυο. Στα συνδεδεμένα με καλώδιο δίκτυα, το να συνδεθείς με το σωστό δίκτυο είναι τόσο απλό όσο το να ακολουθήσεις το καλώδιο. Η πρόσβαση στην καλωδίωση βοηθά τους χρήστες να προσδιορίσουν το "σωστό" δίκτυο. Σε ένα ασύρματο δίκτυο, δεν υπάρχουν σαφείς φυσικές συνδέσεις, και έτσι άλλοι μηχανισμοί πρέπει να

σχεδιαστούν για να αποδείξουν τα δίκτυα την ταυτότητά τους (ή, ακριβέστερα, την ταυτότητα του ιδιοκτήτη τους) στους χρήστες. Το 802.1X είχε ως σκοπό να συλλέξει τις πληροφορίες επικύρωσης από τους χρήστες και να χορηγεί ή να αρνείται την πρόσβαση βασισμένο σε εκείνες τις πληροφορίες. Δεν είχε ως σκοπό να βοηθήσει τα δίκτυα να παρέχουν τα πιστοποιητικά στους χρήστες, έτσι ώστε η λειτουργία να μην εξετάζεται από το 802.1X.

2.4 Πρωτόκολλο Επεκτάσιμης Επαλήθευσης Ταυτότητας

Στην ενότητα αυτή, παρουσιάζεται το Πρωτόκολλο Επεκτάσιμης Επαλήθευσης Ταυτότητας (Extensible Authentication Protocol - EAP). Το EAP περιλαμβάνει ένα *σύνολο* μηνυμάτων που χρησιμοποιείται κατά την έναρξη και το κλείσιμο των διαπραγματεύσεων που πραγματοποιούνται από όλες τις μεθόδους επαλήθευσης ταυτότητας των ανωτέρων στρωμάτων. Επιπλέον, το EAP επιτρέπει σε δύο πλευρές να ανταλλάξουν τις πληροφορίες που αφορούν τη συγκεκριμένη μέθοδο επαλήθευσης ταυτότητας που επιθυμούν να εφαρμόσουν. Το περιεχόμενο των μεθόδων αυτών δεν ορίζεται στο EAP. Ακριβώς αυτή η δυνατότητα του EAP να διεκπεραιώνει μέρος της επικοινωνίας με προτυποποιημένο τρόπο και το υπόλοιπο με ειδικό για κάθε μέθοδο τρόπο, αποτελεί το κλειδί της επεκτασιμότητας του πρωτοκόλλου. Αναφερόμαστε σε αυτά τα ειδικά μηνύματα ως ενδιάμεσα, επειδή παρουσιάζονται μετά την έναρξη και πριν τον τερματισμό.

Μεγάλος αριθμός αυτών των ενδιάμεσων μηνυμάτων μπορούν να *ανταλλαχθούν* μέχρι να ολοκληρωθεί η επαλήθευση ταυτότητας. Ο λόγος για τον οποίο το EAP είναι επεκτάσιμο είναι ότι οι λεπτομέρειες αυτών των ειδικών μηνυμάτων ορίζονται στα αντίστοιχα κείμενα Request For Comment — RFC. Για παράδειγμα, υπάρχει ειδικό RFC σχετικό με τη χρήση Ασφάλειας Επιπέδου Μεταφοράς πάνω από το EAP (EAP-TLS) και άλλο για το Σηραγγώδες TLS (EAP-TTLS). Το γεγονός αυτό επιτρέπει και την ανάπτυξη νέων μεθόδων οι *οποίες* μπορούν να υλοποιηθούν στα υπάρχοντα συστήματα.

Στο EAP ορίζονται τέσσερις τύποι μηνυμάτων που μπορούν να σταλούν:

- **Request:** Χρησιμοποιείται για την αποστολή μηνυμάτων από τον επαληθευτή ταυτότητας στην οντότητα του supplicant
- **Response:** Χρησιμοποιείται για την αποστολή μηνυμάτων από την οντότητα του supplicant στον επαληθευτή ταυτότητας
- **Success:** Στέλνεται, από τον επαληθευτή ταυτότητας ως ένδειξη παροχής πρόσβασης
- **Failure:** Στέλνεται από τον επαληθευτή ταυτότητας ως ένδειξη άρνησης πρόσβασης

Ας σημειωθεί ότι τα μηνύματα αυτά ορίζονται σε σχέση με τον επαληθευτή ταυτότητας. Ωστόσο, στο σενάριο του IEEE 802.IX, ο επαληθευτής ταυτότητας προωθεί τα μηνύματα στον εξυπηρετητή επαλήθευσης ταυτότητας, που συνήθως χρησιμοποιεί το RADIUS. Στην περίπτωση αυτή, ο εξυπηρετητής επαλήθευσης ταυτότητας είναι αυτός που παράγει μηνύματα request, success και failure, ενώ ο επαληθευτής ταυτότητας απλά τα αναμεταδίδει στην οντότητα του supplicant.

Τα μηνύματα request και response υποδιαιρούνται επιπλέον με βάση *το* πεδίο Τύπος του EAP. Το πεδίο αυτό υποδεικνύει το είδος της πληροφορίας που μεταφέρεται στο μήνυμα EAP. Οι πρώτοι έξι τύποι ορίζονται στο πρότυπο, ενώ όλοι οι υπόλοιποι έχουν κρατηθεί για τις μεθόδους επαλήθευσης ταυτότητας. Ο πιο σημαντικός από τους βασικούς τύπους είναι ο Identity (ταυτότητα) με τιμή 1. Συνήθως, αυτός χρησιμοποιείται, στη φάση έναρξης του EAP: το μήνυμα EAP-Request/Identity στέλνεται από τον επαληθευτή ταυτότητας σε ένα νέο supplicant. Ο τελευταίος απαντά με το μήνυμα EAP-Response/Identity, το οποίο περιέχει το όνομα χρήστη ή κάποιο άλλο αναγνωριστικό κατάλληλο για τον εξυπηρετητή επαλήθευσης ταυτότητας.

Οι τιμές του πεδίου Τύπος που είναι υψηλότερες του 6 είναι μοναδικές για κάθε μέθοδο επαλήθευσης ταυτότητας. Ωστόσο, η χρήση του συγκεκριμένου πεδίου δεν έχει πάντα την ίδια έννοια. Γενικά, υποδεικνύει τη μέθοδο επαλήθευσης ταυτότητας. Για παράδειγμα ένα μήνυμα με τιμή του πεδίου Τύπος ίση με 2 ονομάζεται, Notification (ανακοίνωση) και χρησιμοποιείται προκειμένου να εμφανιστεί κάποιο μήνυμα κειμένου στο χρήστη. Ένα μήνυμα με τιμή 3 στο εν λόγω πεδίο, ονομάζεται NAK και χρησιμοποιείται όταν γίνεται μια αίτηση για μέθοδο επαλήθευσης ταυτότητας που δεν υποστηρίζεται.

Στα πλαίσια του IEEE 802.IX μια αίτηση τύπου Identity αποτελεί συνήθως το πρώτο μήνυμα που στέλνεται και στο *οποίο* ο supplicant απαντά με πληροφορίες σχετικές με την ταυτότητά του. Μια πολύ απλοποιημένη διαδικασία επαλήθευσης ταυτότητας θα μπορούσε να έχει ως εξής:

1.EAP-Identity request (από τον επαληθευτή ταυτότητας)

2.EAP-Identity response (από την οντότητα του supplicant)

3.EAP-Success (από τον επαληθευτή ταυτότητας)

Ουσιαστικά στην απλή αυτή περίπτωση, η συσκευή δεν έχει επαληθεύσει την ταυτότητά της, καθώς ο επαληθευτής την αποδέχεται 'τυφλά'. Από την άλλη πλευρά, η απόδειξη αυθεντικότητας ·θα μπορούσε να παρέχεται με κάποιο άλλο μηχανισμό. Για παράδειγμα, η ταυτότητα ίσως να παράγεται από μια έξυπνη κάρτα (smart card) που μεταβάλλεται κάθε δευτερόλεπτο, όντας συγχρονισμένη με τον εξυπηρετητή επαλήθευσης ταυτότητας. Η μέθοδος αυτή αναφέρεται συχνά ως *κωδικός εισόδου μιας χρήσης* (one-time password). Η κενή επαλήθευση αυτού του τύπου, μπορεί να βρει εφαρμογή σε απλά ασύρματα τοπικά δίκτυα, τα οποία διαθέτουν ήδη εγκατεστημένα μυστικά κλειδιά (προμεριζόμενα κλειδιά), και στηρίζονται στην κρυπτογράφηση για την επίτευξη της ασφάλειας.

Καθώς η ανταλλαγή EAP-Identity μπορεί να θεωρηθεί από μόνη της ως μια *ολοκλη*ρωμένη μέθοδος επαλήθευσης ταυτότητας, όταν χρησιμοποιείται και μια άλλη *μέθοδος,* όπως για παράδειγμα η ασφάλεια επιπέδου μεταφοράς, τότε πρακτικά εκτελούνται δύο μέθοδοι στη σειρά. Αυτή η έννοια της **σειριακής επαλήθευσης ταυτότητας** έχει υιοθετηθεί στο πρότυπο EAP και επιτρέπει την εφαρμογή οποιουδήποτε αριθμού μεθόδων πριν το τελικό μήνυμα EAP-Success ή EAP-Failure. Η δυνατότητα αυτή, επιτρέπει στον πελάτη να επαληθευτεί από το δίκτυο προτού αποκαλύψει την ταυτότητα του.

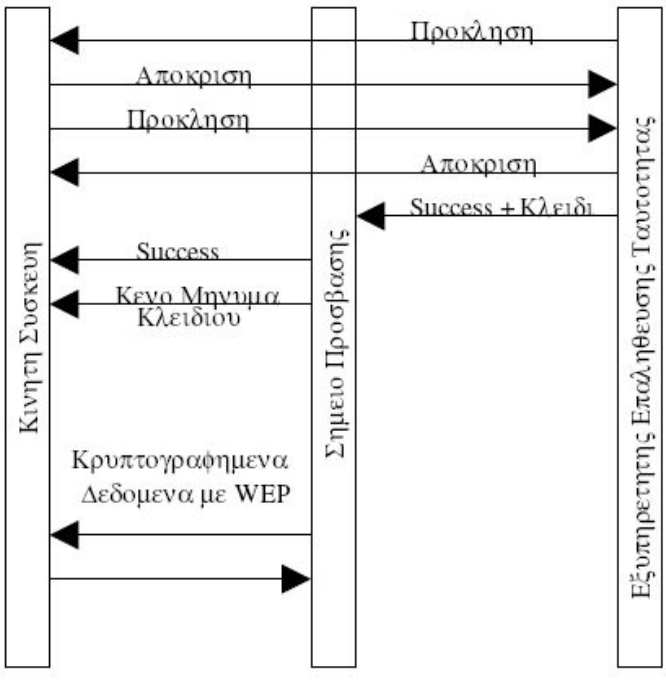
2.5 Ελαφρύ EAP (LEAP)

Το Ελαφρύ EAP (Lightweight EAP — LEAP), παρόλο που αποτελεί ένα ιδιοκτησιακό πρωτόκολλο που αναπτύχθηκε από τη Cisco, ωστόσο η ευρεία του χρήση οδήγησε και άλλους κατασκευαστές να το υποστηρίζουν στους εξυπηρετητές RADIUS.

Συνεπές με το μοντέλο IEEE 802.1X, το LEAP χωρίζει το σύστημα σε τρεις οντότητες: supplicant, επαληθευτής ταυτότητας και εξυπηρετητής επαλήθευσης ταυτότητας. Ο supplicant βρίσκεται, στην κινητή συσκευή, ενώ ο επαληθευτής ταυτότητας στο σημείο πρόσβασης. Ο εξυπηρετητής επαλήθευσης ταυτότητας υλοποιείται από ένα εξυπηρετητή RADIUS. Για τη μεταφορά των κλειδιών χρησιμοποιούνται κάποια ιδιοκτησιακά γνωρίσματα του RADIUS.

Το LEAP είναι ένα πρωτόκολλο αμφίδρομης πρόκλησης - απόκρισης που βασίζεται σε ένα μεριζόμενο μυστικό κλειδί μεταξύ του εξυπηρετητή επαλήθευσης ταυτότητας και της κινητής συσκευής και όχι του σημείου πρόσβασης. Στηρίζεται γενικά στο MS-CHAPvl, το οποίο χρησιμοποιείται συνήθως για απομακρυσμένη επαλήθευση ταυτότητας μέσω dial-up. Σε αντίθεση με το συμβατικό MS-CHAP, η επαλήθευση ταυτότητας είναι αμοιβαία, με ξεχωριστές προκλήσεις να εκδίδονται από τον εξυπηρετητή επαλήθευσης ταυτότητας και την κινητή συσκευή. Στο πλαίσιο αυτό, δεν εξασφαλίζεται, η αυθεντικότητα του ίδιου του σημείου πρόσβασης. Αν ένα μη εξουσιοδοτημένο σημείο πρόσβασης μπορούσε με κάποιο τρόπο να αποκτήσει πρόσβαση στο ενσύρματο δίκτυο με σύνδεση στον εξυπηρετητή επαλήθευσης ταυτότητας, θα μπορούσε να δράσει ως 'ενδιάμεσος' (man in the middle) στη διαδικασία επαλήθευσης ταυτότητας. Ωστόσο, το σημείο πρόσβασης πρέπει να διαθέτει ήδη εγκαταστημένη σχέση εμπιστοσύνης με τον εξυπηρετητή επαλήθευσης ταυτότητας προκειμένου να λάβει το κλειδί κρυπτογράφησης συνόδου, επομένως ένα παράνομο σημείο πρόσβασης δε θα ήταν σε θέση να στείλει ή να λάβει κρυπτογραφημένα δεδομένα από την κινητή συσκευή.

Μόλις ολοκληρωθεί η αμοιβαία επαλήθευση ταυτότητας, το κλειδί κρυπτογράφησης συνόδου στέλνεται στο σημείο πρόσβασης μέσα σε ένα γνώρισμα RADIUS. Αυτό το γνώρισμα κρυπτογραφείται χρησιμοποιώντας ένα μεριζόμενο μυστικό μεταξύ του σημείου πρόσβασης και του εξυπηρετητή. Ο πελάτης υπολογίζει επίσης ένα αντίγραφο του κλειδιού συνόδου. Το κλειδί δε μεταδίδεται μέσω της ασύρματης ζεύξης αλλά υπολογίζεται βάσει μιας τυχαίας τιμής. Το σημείο πρόσβασης σηματοδοτεί μια επιτυχημένη επαλήθευση ταυτότητας με μήνυμα EAPOL-Success προς την κινητή συσκευή. Στη συνέχεια ενεργοποιεί την κρυπτογράφηση στέλνοντας ένα μήνυμα EAPOL-Key. Ακολουθούν τα βήματα της όλης διαδικασίας, ενώ σχηματικά παρουσιάζεται στο Σχ. 2.10:



Σχήμα 2.10 Ακολουθία μηνυμάτων LEAP

1. Ο εξυπηρετητής επαλήθευσης ταυτότητας στέλνει μια τυχαία ακολουθία χαρακτήρων στην κινητή συσκευή ως πρόκληση. Η κινητή συσκευή πρέπει να αποδείξει ότι γνωρίζει το κλειδί στέλνοντας μια ακολουθία χαρακτήρων που προκύπτει από την πρόκληση.

2.Η κινητή συσκευή στέλνει μια πρόκληση στον εξυπηρετητή επαλήθευσης ταυτότητας, ο οποίος πρέπει επίσης να αποκριθεί σωστά.

3.Ο εξυπηρετητής επαλήθευσης ταυτότητας παράγει και στέλνει ένα κλειδί συνόδου στο σημείο πρόσβασης με το μήνυμα EAP-Success ενθυλακωμένο σε RADIUS.

4.Το σημείο πρόσβασης ειδοποιεί την κινητή συσκευή σχετικά με την επαλήθευση ταυτότητας χρησιμοποιώντας το μήνυμα EAPOL-Success.Στο σημείο αυτό ο πελάτης υπολογίζει το κλειδί συνόδου που απαιτείται.

5.Το σημείο πρόσβασης στέλνει ένα μήνυμα EAPOL-Key για την ενεργοποίηση της κρυπτογράφησης. Ας σημειωθεί ότι δε στέλνεται το πραγματικό κλειδί, αλλά απλά ένα μήνυμα γνωστοποίησης.

6.Η κινητή συσκευή και το σημείο πρόσβασης επικοινωνούν χρησιμοποιώντας κρυπτογράφηση WEP.

Στην ασύρματη πλευρά, το LEAP χρησιμοποιεί το IEEE 802.IX και το EAPOL, Στην ενσύρματη πλευρά, το LEAP χρησιμοποιεί το EAP πάνω από RADIUS.

. Το LEAP αρχικά χρησιμοποιούσε το WEP, το οποίο παρουσιάζει αρκετές αδυναμίες. Ωστόσο, η δυνατότητα του LEAP να παράγει προσωρινά κλειδιά συνόδου μειώνει σε κάποιο βαθμό την αποτελεσματικότητα των επιθέσεων. Επιπλέον, το LEAP χρησιμοποιεί το πρωτόκολλο MS-CHAPvl, το οποίο είναι ευάλωτο σε μερικές επιθέσεις με λεξικό. Συνολικά, όμως, το LEAP παρέχει σχετική ασφάλεια παρουσιάζοντας τα εξής πλεονεκτήματα:

- Αμοιβαία επαλήθευση ταυτότητας
- Προσωρινά κλειδιά συνόδου
- Κεντρικοποιημένη διαχείριση κλειδιών

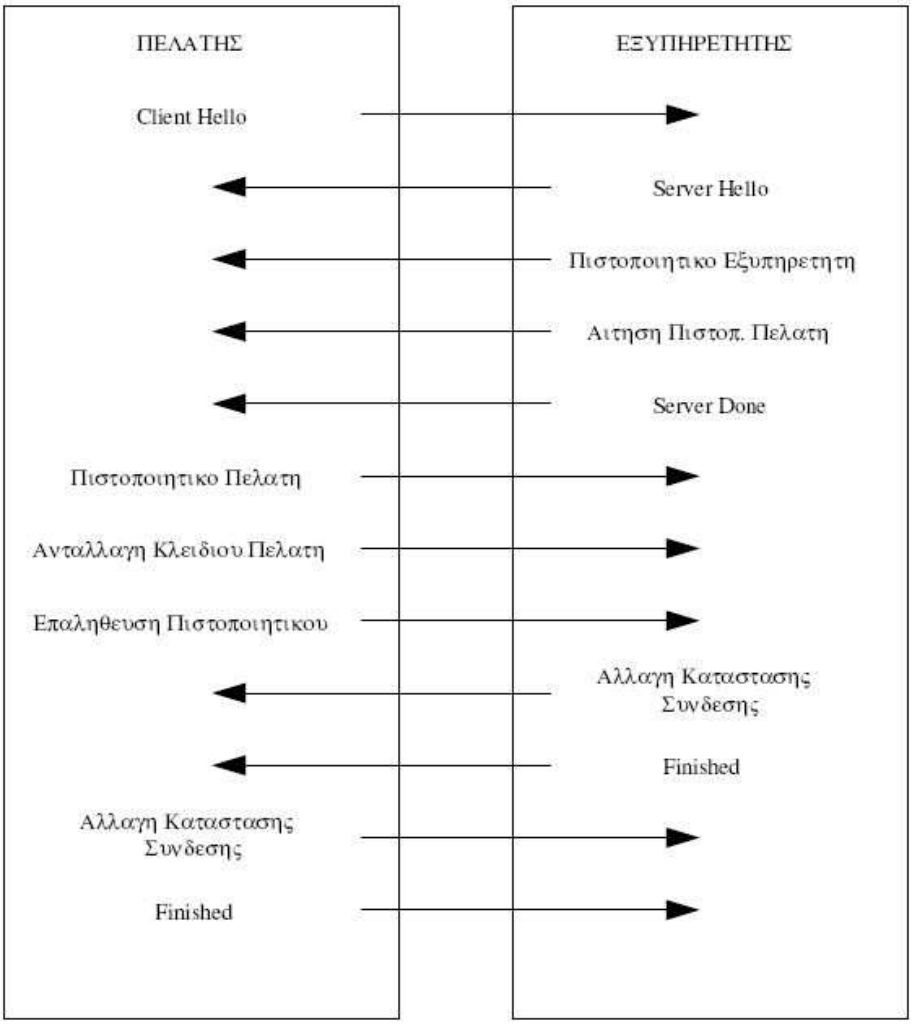
2.6 Ασφάλεια Επιπέδου μεταφοράς και EAP

Το πρωτόκολλο Ασφάλειας Επιπέδου Μεταφοράς (Transport Layer Security - TLS) προσφέρει περισσότερες υπηρεσίες από αυτές που απαιτούνται στα πλαίσια του TSN/RSN. Πιο συγκεκριμένα παρέχει μηχανισμούς επαλήθευσης ταυτότητας, κρυπτογράφησης και συμπίεσης δεδομένων. Τόσο το TSN, όσο και το RSN, διαθέτουν δικές τους μεθόδους κρυπτογράφησης, όπως είναι το TKIP και το AES-CCMP αντίστοιχα, ενώ στις προδιαγραφές τους δεν ανήκει η χρήση συμπίεσης των

δεδομένων. Αντίθετα, η μέθοδος επαλήθευσης ταυτότητας του TLS είναι ιδανική για το μοντέλο του EAP/IEEE 802.1X.

Γενικές αρχές του TLS

Η σχέση μεταξύ των δύο πλευρών που επικοινωνούν, εγκαθίσταται στο TLS με τη σύναψη μιας χειραψίας. Αυτή περιλαμβάνει μια σειρά μηνυμάτων που ανταλλάσσονται με καθορισμένη σειρά και φαίνεται στο Σχ. 2.11. Μπορούμε να παρατηρήσουμε ότι κατά την έναρξη της χειραψίας, οι δυο πλευρές στέλνουν μηνύματα χαιρετισμού (Client Hello/Server Hello), ενώ πριν το τέλος της, ελέγχεται η εγκυρότητα κάθε μηνύματος.



Σχήμα 2.11 Χειραψια TLS

Η διαδικασία της χειραψίας του TLS επιτυγχάνει τρεις στόχους:

1.Την επαλήθευση ταυτότητας του εξυπηρετητή (και προαιρετικά του πελάτη).

2.Την παραγωγή ενός μυστικού κύριου κλειδιού (master key) για τη σύνοδο.

3. Την αρχικοποίηση και ενεργοποίηση κρυπτογραφικής λειτουργίας για την προστασία των επικοινωνιών.

Στα πλαίσια του TSN/RSN, οι μόνες λειτουργίες του TLS που απαιτούνται, είναι η επαλήθευση ταυτότητας και η παραγωγή του κύριου κλειδιού, καθώς, όπως αναφέρθηκε, διαθέτουν δικές τους κρυπτογραφικές μεθόδους. Το TSN/RSN λαμβάνει το κύριο κλειδί που παράγεται από το TLS και από αυτό υπολογίζει ένα σύνολο κλειδιών που χρησιμοποιεί για την κρυπτογράφηση της ασύρματης ζεύξης. Με αυτόν τον τρόπο, το TLS ενσωματώνεται στο μοντέλο κατά IEEE 802.IX και λειτουργεί πάνω από το EAP, όπως θα δούμε αναλυτικά στη συνέχεια.

2.7 EAP-TLS

Το TLS σχεδιάστηκε για να λειτουργεί στο στρώμα πάνω από ένα αξιόπιστο πρωτόκολλο μεταφοράς γενικά, και όχι αποκλειστικά πάνω από το TCP/IP. Έτσι, στα πλαίσια των TSN/RSN, το TLS λειτουργεί πάνω από το EAP.
Το EAP αρχίζει και ολοκληρώνεται πάντα με την ίδια ακολουθία. Συνήθως, ανταλλάσσεται ένα μήνυμα αίτησης/απόκρισης EAP-Identity. Στη συνέχεια στέλνεται μια σειρά αιτήσεων και αποκρίσεων μηνυμάτων EAP που σχετίζονται με τη συγκεκριμένη μέθοδο επαλήθευσης ταυτότητας και αναγνωρίζονται από το πεδίο Τύπος κάθε μηνύματος. Τελικά, ένα μήνυμα EAP-Success/Fail στέλνεται ανάλογα με την έκβαση. Η γενική μορφή ενός μηνύματος EAP απεικονίζεται, στο Σχ. 2.12.

Κωδικος	Αναγνωριστικο	Μηκος	Τυπος	Δεδομενα Αιτησης / Αποκρισης

Σχήμα 2.12: Μορφή Μηνύματος EAP

Στην περίπτωση του TLS, το RFC ορίζει ότι το πεδίο Τύπος για τις αιτήσεις και αποκρίσεις του EAP παίρνει την τιμή 13. Μόνο οι πελάτες και οι εξυπηρετητές που υποστηρίζουν το EAP-TLS θα επιχειρήσουν να αποκωδικοποιήσουν αυτά τα μηνύματα. Επιπλέον, ορίζονται δύο νέα πεδία που ακολουθούν το Τύπος. Τα πεδία αυτά είναι τα Σημαίες και Μήκος, όπως φαίνεται στο Σχ. 2.13.

Κωδικος	Αναγνωριστικο	Μηκος	'13'	Σημαιες	Μηκος	Δεδομενα EAP–TLS

Σχήμα 2.13: Μορφή Μηνύματος EAP-TLS

Το πρώτο πεδίο Μήκος αναφέρεται στο μήκος του πλαισίου EAP, ενώ το δεύτερο στο μήκος του πακέτου EAP-TLS. Τα πακέτα αυτά μπορεί να είναι αρκετά μεγάλα σε μέγεθος, υπερβαίνοντας το μέγιστο μέγεθος ενός μηνύματος EAP. Σε μια τέτοια περίπτωση, το πακέτο EAP-TLS θραυσματίζεται και στέλνεται διαδοχικά. Η δεύτερη τιμή του πεδίου Μήκος, αναφέρεται συνολικά στο μήνυμα TLS και όχι στο τρέχον πλαίσιο. Μάλιστα, το δεύτερο πεδίο Μήκος είναι προαιρετικό και συνήθως παραλείπεται όταν τα δεδομένα του EAP-TLS χωρούν στο τρέχον πλαίσιο.

Το πεδίο Σημαίες περιλαμβάνει τρία bit:

- Σημαία Μήκους: Υποδεικνύει την παρουσία ή μη του πεδίου Μήκος
- Σημαία Θραυσμάτων: Ενεργοποιείται όταν ακολουθούν θραύσματα.
- Σημαία Έναρξης: Σηματοδοτεί την έναρξη της χειραψίας

Η ακολουθία των μηνυμάτων που ανταλλάσσονται κατά τη χειραψία του EAP-TLS παρουσιάζονται στο Σχ. 2.14. Έχει υποτεθεί ότι ο εξυπηρετητής έχει αρχίσει την επικοινωνία του με τον πελάτη μέσω κάποιας μεθόδου, όπως για παράδειγμα με ένα μήνυμα EAP-Start. Τα βήματα έχουν ως εξής:

1. {request} Αυτή είναι η αρχή της συναλλαγής EAP. Ο εξυπηρετητής ζητά την ταυτότητα του πελάτη.

2. {response} Εδώ ο πελάτης στέλνει ένα μήνυμα με την ταυτότητα του. Για εταιρικό περιβάλλον, θα μπορούσε να προσδιοριστεί η ταυτότητα του ιδιοκτήτη του πιστοποιητικού του πελάτη που θα σταλεί. Αν ο πελάτης δεν προτίθεται να στείλει πιστοποιητικό, μπορεί να στείλει ένα ανώνυμο αναγνωριστικό, για παράδειγμα η ακολουθία ' anonymous'.

3. {request} Ο εξυπηρετητής στέλνει μια κενή αίτηση EAP-TLS με τη σημαία έναρξης ενεργοποιημένη. Αυτή είναι και η μοναδική περίπτωση που η σημαία αυτή τίθεται.

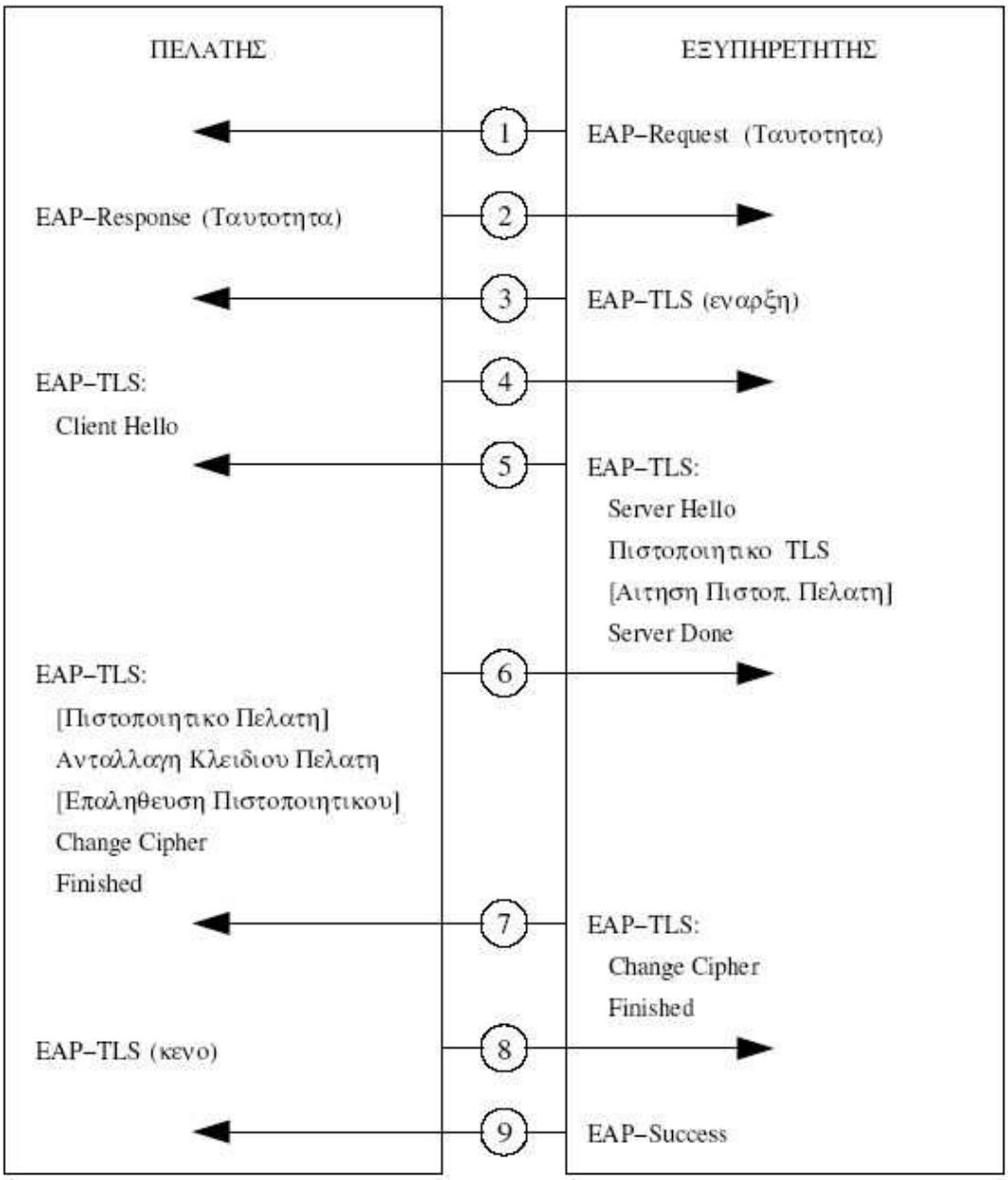
4. {response} Ο πελάτης στέλνει μήνυμα Client Hello το οποίο περιλαμβάνει τις ίδιες πληροφορίες με το σύνηθες TLS.

5. {request} Ο εξυπηρετητής στέλνει δύο ή τρία μηνύματα TLS σε μία μόνο αίτηση: το Server Hello, προαιρετικά την αίτηση για πιστοποιητικό πελάτη, και το μήνυμα τερματισμού του εξυπηρετητή.

6. {response} Ο πελάτης απαντά τώρα με πολλά μηνύματα TLS σε μία μόνο απόκριση:

- Πιστοποιητικό πελάτη (αν ζητηθεί)
- Προ-κύριο μυστικό του μηνύματος ανταλλαγής κλειδιού
- Πληροφορίες επαλήθευσης πιστοποιητικού πελάτη
- Αλλαγή κρυπτογραφήματος
- Τερματισμός

Παρατηρούμε ότι ο πελάτης δημιουργεί το προ-κύριο μυστικό, υπολογίζει το κύριο μυστικό και ενεργοποιεί το κρυπτογράφημα στο ίδιο βήμα. Ωστόσο, πρέπει να σημειωθεί ότι ολόκληρο το μήνυμα EAP στέλνεται μέσα στην αρχική κρυπτογραφική ακολουθία, η οποία είναι συνήθως ανοικτή, δηλαδή χωρίς κρυπτογράφηση. Η ακολουθία αυτή δεν ενεργοποιείται προτού ολοκληρωθούν τα μηνύματα EAP.



Σχήμα 2.14 Χειραψία EAP-TLS

7.{request} Ο εξυπηρετητής στέλνει όλα τα μηνύματα που απομένουν σε μία μόνο

αίτηση EAP.

8.{response} Ο πελάτης δεν έχει επιπλέον πληροφορίες να στείλει αλλά απαιτείται από το πρωτόκολλο να αποκριθεί και στο πλαίσιο αυτό απαντά με ένα κενό μήνυμα EAP-Response.

9.Τελικά για την ολοκλήρωση της χειραψίας EAP, ο εξυπηρετητής στέλνει ένα μήνυμα EAP-Success, υποθέτοντας ότι όλα έχουν πάει καλά. Αν οποιοδήποτε από τα βήματα είχαν αποτύχει, ο εξυπηρετητής θα είχε στείλει μήνυμα EAP-Failure στο σημείο που εντοπίστηκε το πρόβλημα.

Η χρήση του EAP αποτελεί κλειδί στην υλοποίηση του TLS στο TSN ή το RSN. Κατ' αρχήν, συνεπάγεται, ότι δε χρειάζεται διεύθυνση IP, επομένως η ασύρματη συσκευή μπορεί να ανταλλάξει μηνύματα EAP με το σημείο πρόσβασης και να πραγματοποιήσει τη χειραψία προτού της δοθεί πρόσβαση στο ενσύρματο δίκτυο. Το σημείο πρόσβασης δεν απαιτείται να υποστηρίζει το πρωτόκολλο TLS για την ολοκλήρωση της συναλλαγής, εφ' όσον έχει στη διάθεση του έναν εξυπηρετητή επαλήθευσης ταυτότητας για να του στείλει τα μηνύματα EAP. Το σημείο πρόσβασης μπορεί να περιμένει για μήνυμα EAP-Success το οποίο σηματοδοτεί την άδεια πρόσβασης στο δίκτυο.

Ο τρόπος με το οποίο το σημείο πρόσβασης στέλνει τα μηνύματα EAP στον εξυπηρετητή επαλήθευσης ταυτότητας έγκειται, στη χρήση του RADIUS. Πρόκειται για ένα πρωτόκολλο που επιτρέπει την επικοινωνία με τον εξυπηρετητή επαλήθευσης ταυτότητας. Έχει επεκταθεί σε μεγάλο βαθμό σε σχέση με τον αρχικό του σχεδιασμό, ωστόσο οι βασικές αρχές δεν έχουν μεταβληθεί. Μία από τις κύριες επεκτάσεις του σε σχέση με τα TSN/RSN, αποτελεί η υποστήριξη της προώθησης των αιτήσεων και αποκρίσεων EAP απ' ευθείας στον εξυπηρετητή.

2.8 Προστατευμένο EAP (PEAP)

Το Προστατευμένο EAP (Protected EAP — PEAP), όπως δηλώνει και το όνομά του, παρέχει έναν ασφαλή μηχανισμό για τις διαδικασίες του EAP. Το αρχικό κίνητρο ήταν να εξασφαλιστεί η ασφάλεια των κωδικών πρόσβασης των χρηστών προστατεύοντας τους από επιθέσεις με λεξικό. Για να επιτευχθεί αυτό, κάθε σύνοδος EAP είναι απόλυτα μυστική από τους επίδοξους εισβολείς.

Αρχικά πρέπει να εξεταστούν οι αδυναμίες σε επίπεδο ασφαλείας του EAP. Υπάρχει ο κεντρικός μηχανισμός επαλήθευσης ταυτότητας μεταξύ του πελάτη και του εξυπηρετητή. Ο μηχανισμός αυτός μπορεί να χρησιμοποιεί μέθοδο TLS και να θεωρείται ασφαλής, όπως έχουμε ήδη αναφέρει. Ωστόσο, αυτό που είναι κοινό σε όλες τις μεθόδους EAP είναι η φάση EAP-Identity και τα μηνύματα EAP-Success ή EAP-Fail στο τέλος. Σε αυτές τις φάσεις συναντώνται και οι αδυναμίες στην ασφάλεια:

- Επειδή το μήνυμα EAP-Identity δεν προστατεύεται,, μπορεί να υποκλαπεί, αποκαλύπτοντας την ταυτότητα του χρήστη που επιχειρεί να συνδεθεί.

- Το μήνυμα EAP-Success/Fail δεν προστατεύεται και θα μπορούσε να υποκλαπεί.

Μία λύση και στα δύο αυτά προβλήματα θα ήταν να πραγματοποιούνται οι διαπραγματεύσεις του EAP μέσα σε μία απόρρητη κρυπτογραφημένη σήραγγα (tunnel). Αν υπάρχει ασφαλής σύνδεση μεταξύ του πελάτη και του εξυπηρετητή, τότε οι διαπραγματεύσεις του EAP μπορούν να λάβουν χώρα με αρκετή ασφάλεια και η ταυτότητα του πελάτη δε θα αποκαλυφθεί. Ταυτόχρονα η ευελιξία που προσφέρει το EAP δε χάνεται, καθώς όλες οι μέθοδοι επαλήθευσης ταυτότητας ανώτερων στρωμάτων εξακολουθούν να μπορούν να χρησιμοποιηθούν. Αυτή είναι η βασική ιδέα του PEAP: όλες οι διαπραγματεύσεις του EAP προστατεύονται.

Το απόρρητο (privacy) και η αυθεντικότητα (authenticity) αποτελούν βασικές αρχές της ασφάλειας. Το απόρρητο έχει την έννοια ότι προστατεύεται η μυστικότητα της επικοινωνίας. Η αυθεντικότητα σημαίνει ότι δύο (ή περισσότερες) πλευρές μπορούν να αποδείξουν αμοιβαία την ταυτότητά τους. Στόχος του EAP αποτελεί η αυθεντικότητα: Πρωτόκολλο Επεκτάσιμης Επαλήθευσης Ταυτότητας. Στόχος του PEAP είναι να εξασφαλιστεί το απόρρητο κατά τη διαδικασία επαλήθευσης ταυτότητας. Για την επίτευξη και των δύο στόχων, αρχικά εξασφαλίζουμε το απόρρητο χωρίς αυθεντικότητα, και στη συνέχεια πραγματοποιείται η επαλήθευση ταυτότητας χρησιμοποιώντας την απόρρητη σύνδεση. Η προσέγγιση που περιγράφηκε αποτελείται από δύο φάσεις:

α) Κατά την πρώτη φάση, το EAP χρησιμοποιείται συμβατικά για την εγκατάσταση ασφαλούς σύνδεσης με τη βοήθεια του TLS. Μόνο η ταυτότητα του εξυπηρετητή επαληθεύεται σε αυτή τη φάση.

β) Κατά τη δεύτερη φάση, η ασφαλής σύνδεση χρησιμοποιείται για την πραγματοποίηση των διαπραγματεύσεων του EAP, στα πλαίσια των οποίων, λαμβάνει χώρα πλήρης επαλήθευση ταυτοτήτων.

Το TLS είναι η μέθοδος που έχει επιλεγεί για την εξασφάλιση του απορρήτου κατά την πρώτη φάση. Ωστόσο, μόλις το ασφαλές κανάλι εγκατασταθεί, οποιαδήποτε μέθοδος που υποστηρίζεται από το EAP θα μπορούσε να χρησιμοποιηθεί για τις διαπραγματεύσεις· δεν πρέπει να είναι απαραίτητα το TLS.

Πρέπει να τονιστεί ότι, η πρώτη φάση του PEAP περιλαμβάνει μέρος των διαδικασιών που εξασφαλίζουν την αυθεντικότητα ο εξυπηρετητής απαιτείται πάντα να αποδεικνύει την ταυτότητά του. Αυτό μπορεί να γίνει με τη χρήση κάποιου πιστοποιητικού. Με τον τρόπο αυτό επιτρέπει στον πελάτη να είναι σίγουρος για τη νομιμότητα του εξυπηρετητή. Αυτό είναι ιδιαίτερα σημαντικό για τα ασύρματα τοπικά δίκτυα γιατί είναι σχετικά εύκολο να εγκατασταθούν σημεία πρόσβασης τα οποία να διαφημίζουν ψευδώς ότι ανήκουν σε κάποιο έγκυρο δίκτυο.

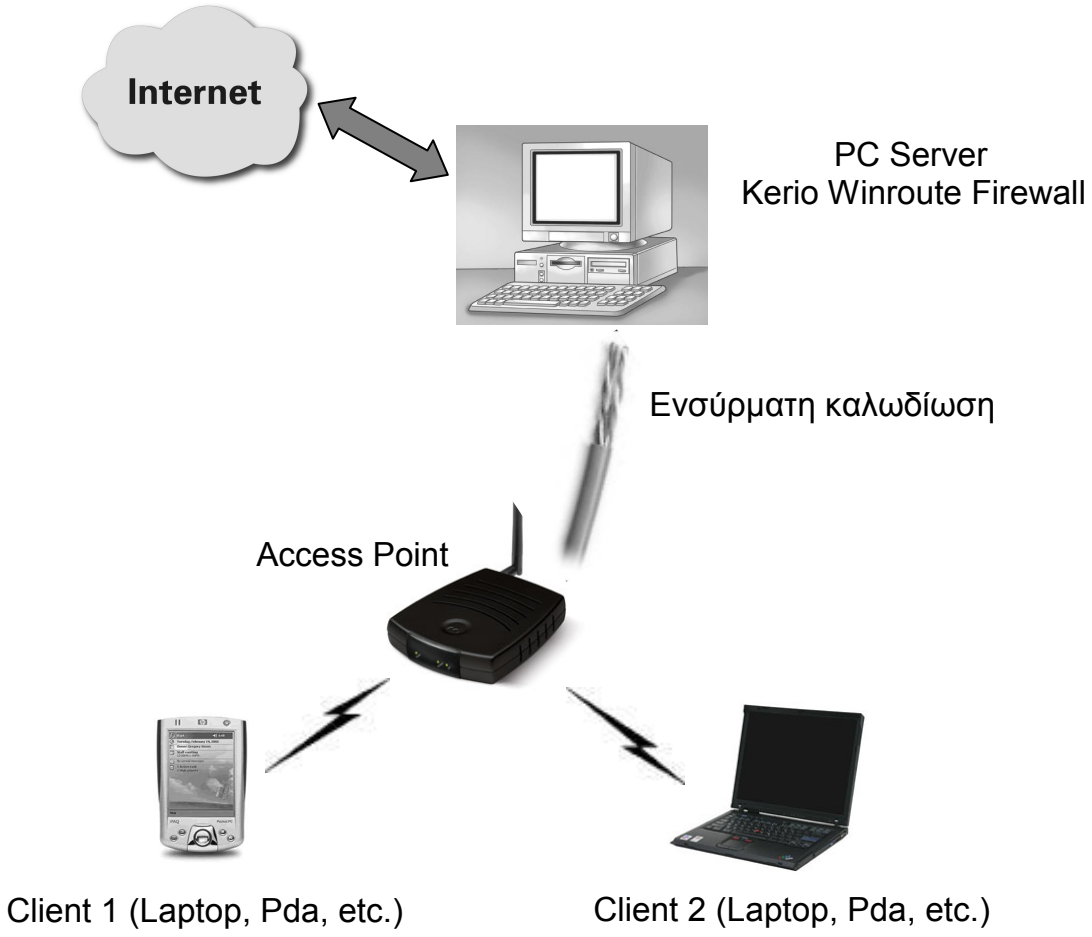
ΚΕΦΑΛΑΙΟ 3

3.1 Υλοποίηση Δικτύου WLAN

Σε αυτό το κεφάλαιο θα περιγράψουμε την σχεδίαση και υλοποίηση ενός ασύρματου δικτύου με τεχνολογία 802.11g στο χώρο του ΤΕΙ Χανιών . Στις επόμενες ενότητες, αναλύεται η αρχιτεκτονική του, οι λειτουργίες του, καθώς και οι μηχανισμοί πρόσβασης και διαχείρισής του.

Εισαγωγή

Η διάταξη μας αποτελείται από ένα σημείο πρόσβασης που ενώνεται ενσύρματα με έναν υπολογιστή που διαθέτει κάρτα δικτύου και αναλαμβάνει το ρόλο του firewall (Σχήμα 3.1). Με τη χρήση του firewall η κυκλοφορία απομονώνεται και διοχετεύεται μέσω ενός σταθερού σημείου εισόδου, και μπορούν να εφαρμοστούν τα πρόσθετα στρώματα της ασφάλειας μέσω της χρήσης ενός ιδεατού ιδιωτικού δικτύου ή πρόσθετων απαιτήσεων επικύρωσης.



Σχήμα 3.1

Hardware

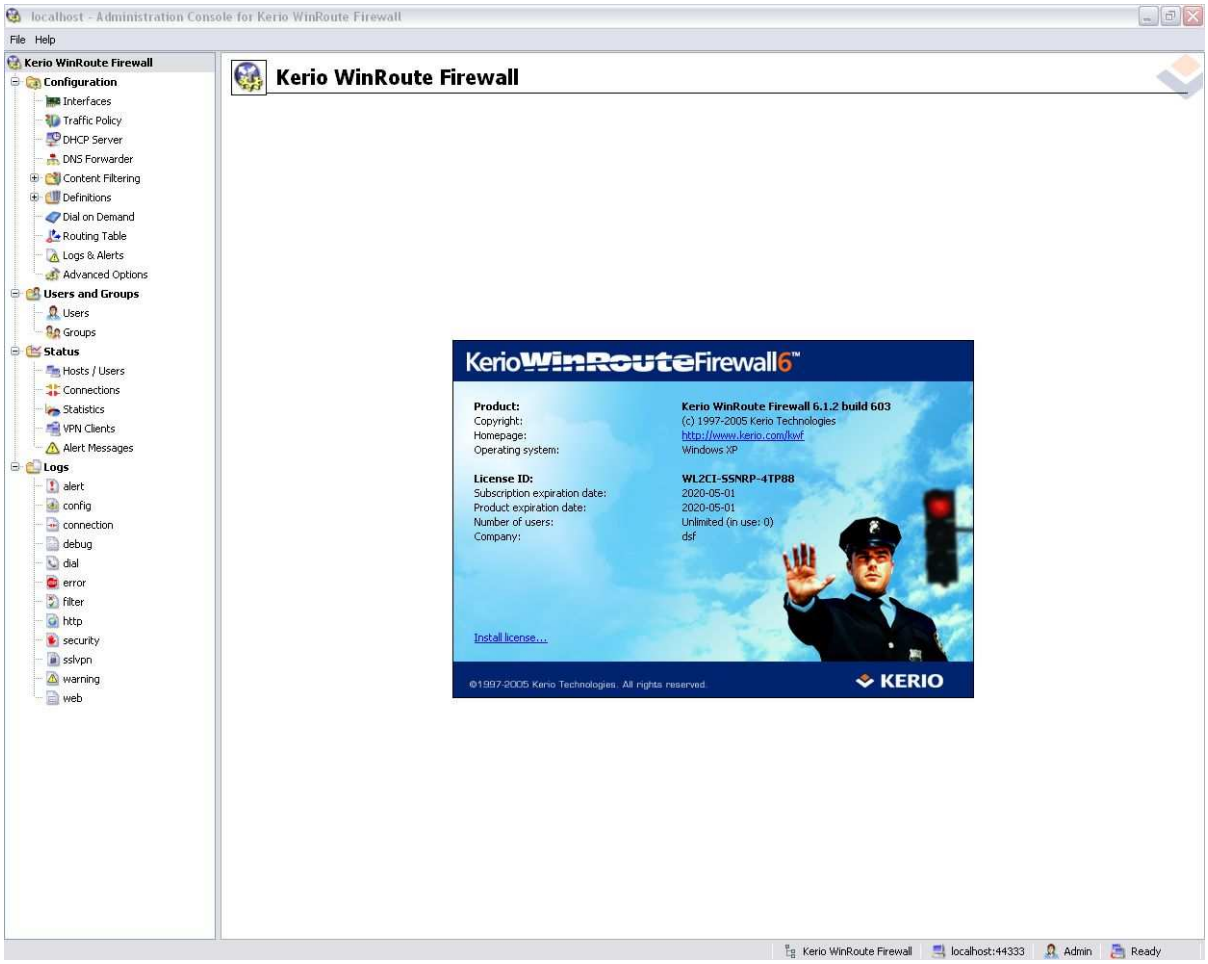
Για την υλοποίηση του ασύρματου δικτύου μας, χρησιμοποιήθηκε ένας υπολογιστής ως server και ένα Access Point. Στον υπολογιστή εγκαταστάθηκαν δυο κάρτες δικτυού. Η μια κάρτα συνδέει τον server με το εσωτερικό δίκτυο του ΤΕΙ ενώ η άλλη χρησιμοποιείται για την ενσύρματη δικτύωση με το Access Point. Για δοκιμές επίσης χρησιμοποιήθηκε ένας υπολογιστής με μια wireless κάρτα δικτύου ο οποίος είχε αναλάβει το ρόλο του πελάτη.

Software

Στον Server εγκαταστάθηκε το λειτουργικό windows xp professional sp2. Την προστασία από ιούς , trojans και net attacks ανέλαβε το Kaspersky anti virus. Το Kerio winroute με το οποίο θα ασχοληθούμε στη συνέχεια ανέλαβε την παροχή ip διευθύνσεων στους πελάτες (Dhcp server), την πιστοποίηση (authentication), τον έλεγχο κίνησης (traffic control) καθώς και τη διαχείριση (administration) του δικτύου.

3.2 Περιγραφή του Kerio Winroute Firewall

Στην ενότητα αυτή παρουσιάζονται συνοπτικά οι ρυθμίσεις που έγιναν στο Kerio winroute firewall.



Σχήμα 3.2 Αρχική σελίδα Kerio Winroute Firewall

3.2.1 Ανάθεση IP διευθύνσεων μέσω Dhcp server

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

Το πρωτόκολλο είναι ουσιαστικά ένα λογισμικό που τρέχει σε έναν υπολογιστή και κανονίζει όλα τα θέματα επικοινωνίας με αυτόν τον υπολογιστή και άλλους που χρησιμοποιούν αυτό το πρωτόκολλο ως γλώσσα. Για να δουλέψει το ίδιο λογισμικό σε τόσους πολλούς υπολογιστές υπάρχει η ανάγκη να το ξεκινήσουμε σε κάθε υπολογιστή με τις αντίστοιχες παραμέτρους για αυτόν και για τη θέση του στο δίκτυο. Η αρχικοποίηση (initialisation) αυτή μπορεί να γίνει κατά τη διάρκεια του φορτώματος (αν το πρωτόκολλο είναι συγχωνευμένο στο λειτουργικό σύστημα) ή με την κλήση του πρωτοκόλλου από κάποια εφαρμογή (αν το πρωτόκολλο υπάρχει στην εφαρμογή). Οι παράμετροι αυτές μπορούν να οριστούν τοπικά, για κάθε υπολογιστή ξεχωριστά. Κάτι τέτοιο όμως δημιουργεί αρκετά προβλήματα:

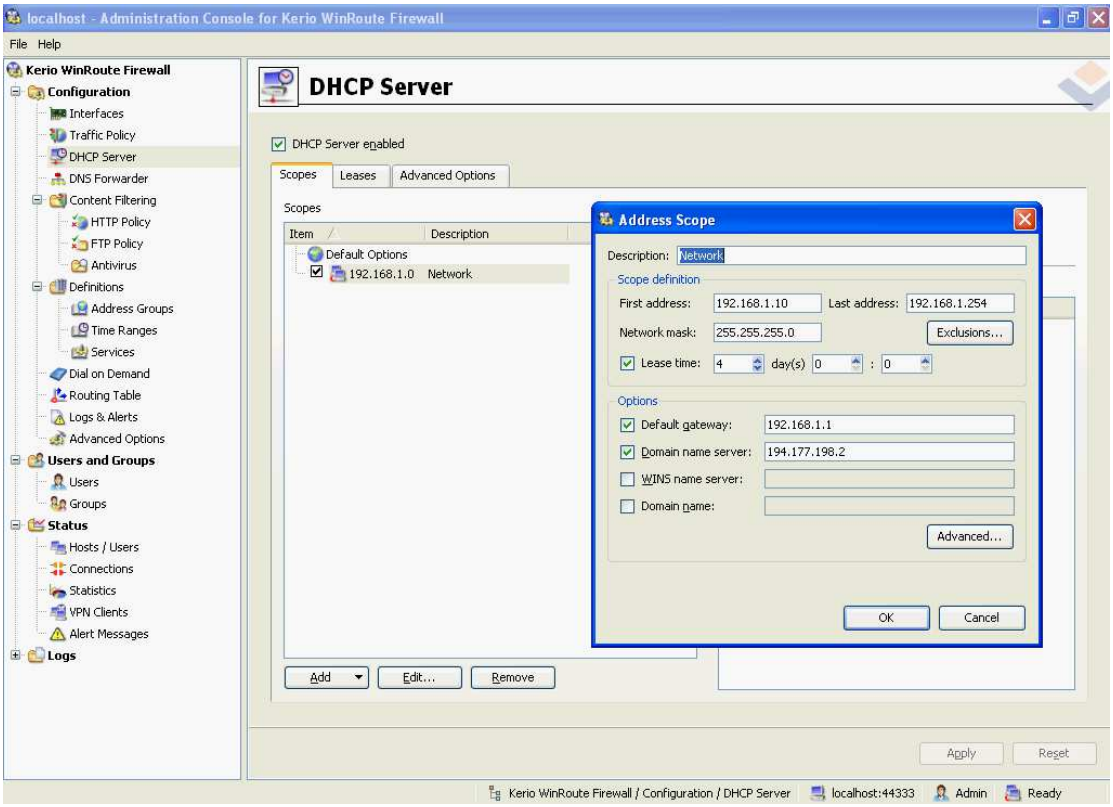
- Χρειάζεται πάρα πολύ εργασία από τον διαχειριστή του δικτύου η οποία είναι χρονοβόρα και επιρρεπής σε λάθη.
- Το να διατηρούνται οι παράμετροι ενημερωμένες χρειάζεται συνεχή δουλειά η οποία αυξάνεται γεωμετρικά με τις αλλαγές που συμβαίνουν στο δίκτυο, ειδικά αν υπάρχουν υπολογιστές που αλλάζουν συνεχώς θέση (π.χ. φορητοί Η/Υ).
- Η αλλαγή μίας παραμέτρου κοινής για τους υπολογιστές σε ένα subnet (π.χ. τοπική διεύθυνση ενός router) απαιτεί αλλαγές σε κάθε υπολογιστή.
- Μερικά μηχανήματα μπορεί να λειτουργούν ως τερματικά. Κάτι τέτοιο σημαίνει ότι δεν έχουν αποθηκευτικό χώρο για να κρατήσουν τις ρυθμίσεις.
- Σε περιπτώσεις έλλειψης διευθύνσεων ή ενός δικτύου που αλλάζει συνέχεια είναι χάσιμο χρόνου να δίνουμε σε έναν μη σταθερό υπολογιστή μόνιμη διεύθυνση. Μία καλύτερη προσέγγιση θα ήταν να χρησιμοποιούνται ομάδες διευθύνσεων από ομάδες υπολογιστών. Η «χειροκίνητη» ρύθμιση τέτοιου είδους δεν παρέχει εύκολο τρόπο για να γίνει αυτό.

Όλοι αυτοί οι λόγοι οδήγησαν στην ανάγκη για έναν αυτόματο μηχανισμό διαχείρισης των TCP/IP πρωτοκόλλων. Ο DHCP είναι αυτή τη στιγμή ο πιο προηγμένος μηχανισμός για να γίνεται αυτό.

Για να είναι η σύνδεση στο δίκτυο όσο το δυνατόν περισσότερο αυτοματοποιημένη και να μη γίνονται πολλές ρυθμίσεις από τη πλευρά του πελάτη ενεργοποιήσαμε το dhcp server του Kerio winroute firewall με την εξής διαδικασία(σχήμα 3.3):

Από το μενού **configuration** επιλέγουμε **dhcp server.** Στη συνέχεια στη σελίδα που εμφανίζεται δεξιά ενεργοποιούμε την επιλογή **dhcp server enabled**. Έπειτα κάνουμε **add scope** και εισάγουμε το εύρος διευθύνσεων 192.168.1.10 – 192.168.1.254, ενώ ως gateway ορίζουμε τη διεύθυνση της κάρτας δικτύου που συνδέεται με το Access Point.

Επίσης δίνουμε στο πεδίο **Domain Name Server** τη διεύθυνση DNS του ΤΕΙ 194.177.198.2.Επιβεβαιώνουμε τις επιλογές μας πατώντας **OK** και στη συνέχεια **APPLY**.



Σχήμα 3.3 Ρυθμίσεις και ενεργοποίηση DHCP server

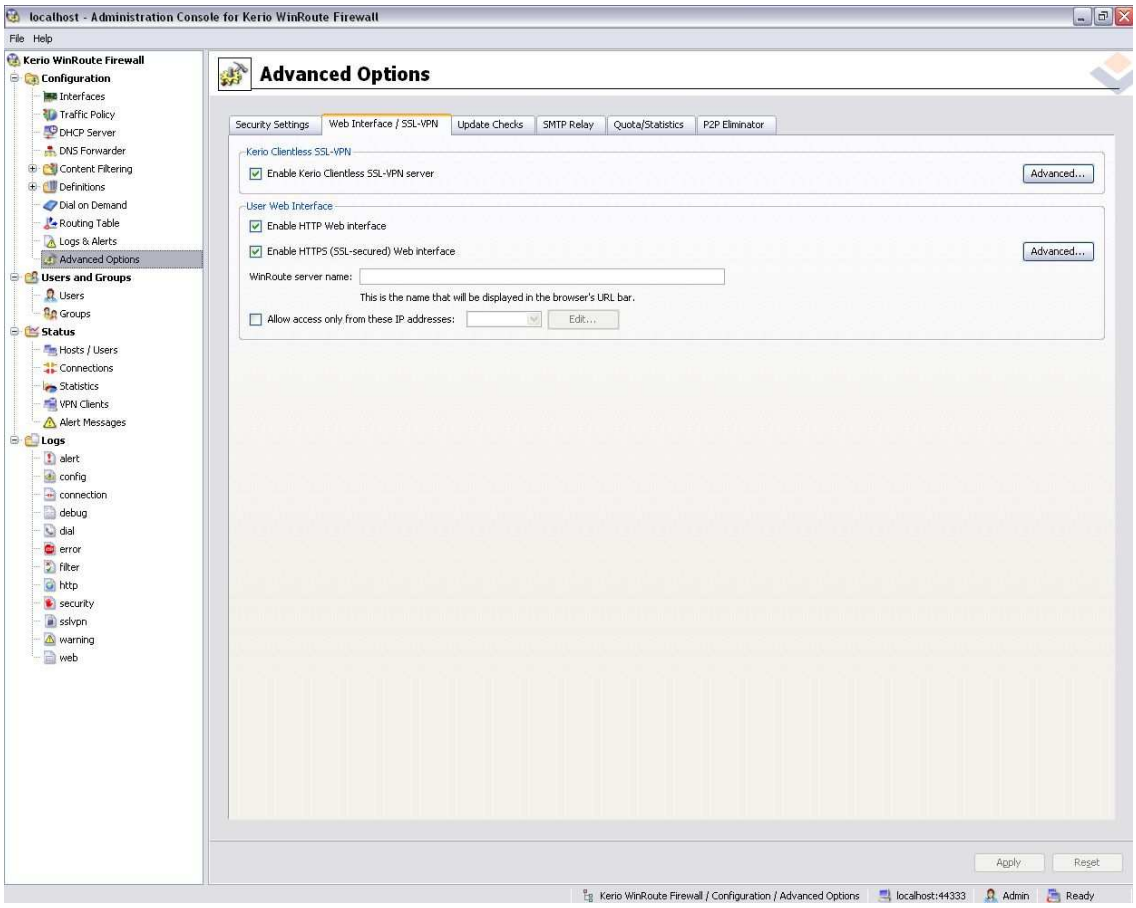
3.2.2 Δημιουργία και πιστοποίηση λογαριασμών χρηστών

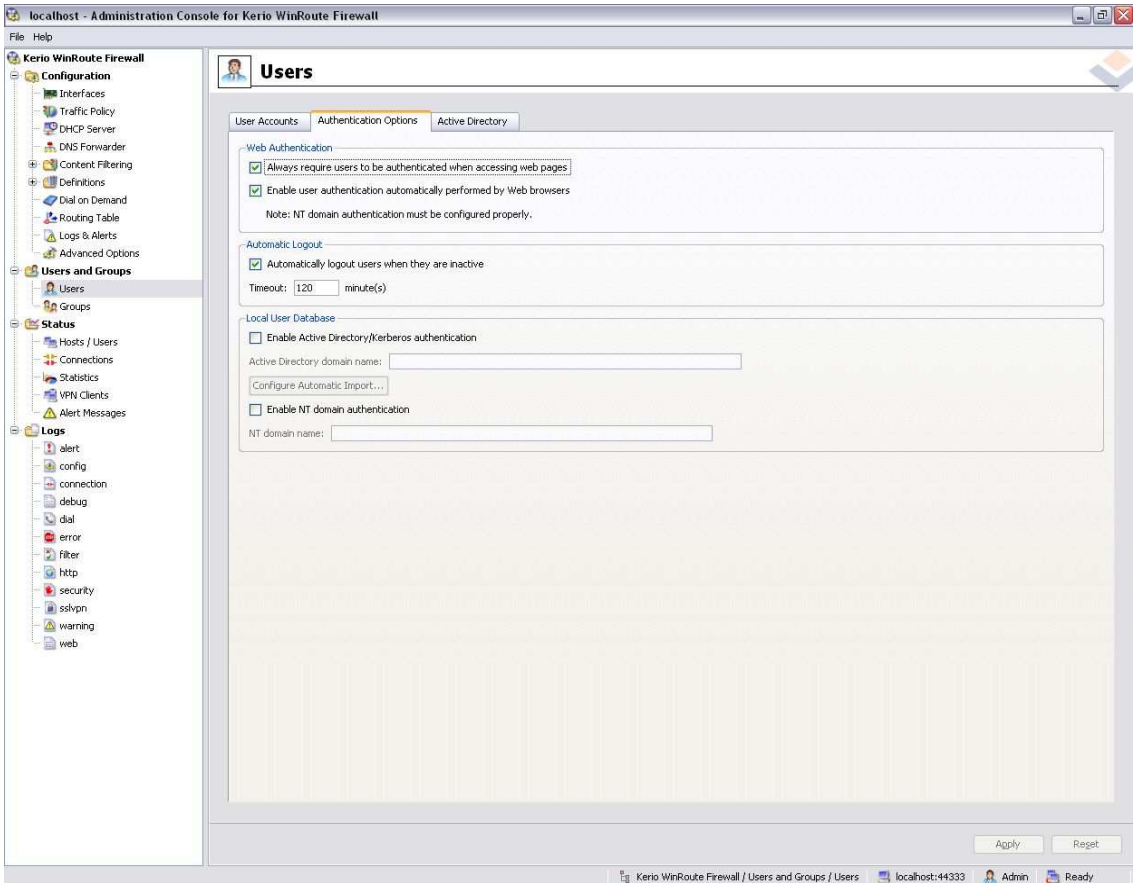
Το πρώτο βήμα για την παροχή υπηρεσιών ασύρματου δικτύου είναι αναμφίβολα η πιστοποίηση του κινητού τερματικού. Με τη χρήση διαφόρων μεθόδων πιστοποιούμε την ταυτότητα του χρήστη και επικυρώνουμε την φυσική υπόσταση προτού τον εξουσιοδοτήσουμε να χρησιμοποιήσει υπηρεσίες του δικτύου. Υπάρχουν πολλοί τρόποι για να γίνει η πιστοποίηση από τους οποίους στο δικό μας δίκτυο επιλέχτηκε η πιστοποίηση εισόδου με χρήση τοπικού κωδικού πρόσβασης.

Μέσω αυτής της μεθόδου ο διακομιστής πρόσβασης χρησιμοποιεί την τοπική του βάση δεδομένων για την πιστοποίηση των χρηστών. Αυτή η βάση δεδομένων περιέχει ζεύγη όνομα χρήστη – κωδικού πρόσβασης τα οποία συγκρίνει με την είσοδο του χρήστη. Ακολουθεί η διαδικασία ενεργοποίησης του web authentication και η δημιουργία λογαριασμών χρηστών.

Από το μενού **configuration** επιλέγουμε **advanced options** και στην καρτέλα **Web interface/SSL-VPN** κάνουμε ‘τικ’ τις επιλογές **enable http web interface** και **enable https (SSL-secured) web interface** και πατάμε **apply**.Επίσης από το μενου **users and groups** επιλέγουμε **users** και στη καρτέλα **authentication options**

κάνουμε ‘τικ’στις επιλογες **always require users to be authenticated when accessing web pages** και **enable user authentication automatically performed by web browsers.**





Σχήμα 3.4 Ενεργοποίηση Web Authentication

Για τη δημιουργία λογαριασμών χρηστών ακολουθείται η εξής διαδικασία:
Από το κεντρικο μενου επιλογων του Winroute επιλεγουμε **users and groups**, εν συνεχεία **users** και **add.**

Σχημα 3.5

1. Στην πρώτη καρτέλα που εμφανίζεται δίνουμε τα στοιχεία του χρήστη-πελάτη καθώς και τον επιθυμητό συνδυασμό username/password (σχήμα 3.5). Επίσης κάτω από την επικεφαλίδα **domain template** έχουμε την επιλογή να φτιάξουμε κάποιο προφίλ για τον συγκεκριμένο χρήστη (να του δώσουμε για παράδειγμα κάποια παραπάνω προνόμια) ή να χρησιμοποιήσουμε το προεπιλεγμένο προφίλ.

2. Στην επόμενη καρτέλα που εμφανίζεται έχουμε την επιλογή να εντάξουμε το χρήστη σε κάποιο group που προϋπάρχει και υπακούει σε συγκεκριμένους κανόνες (σχήμα 3.6)

Σχήμα 3.6

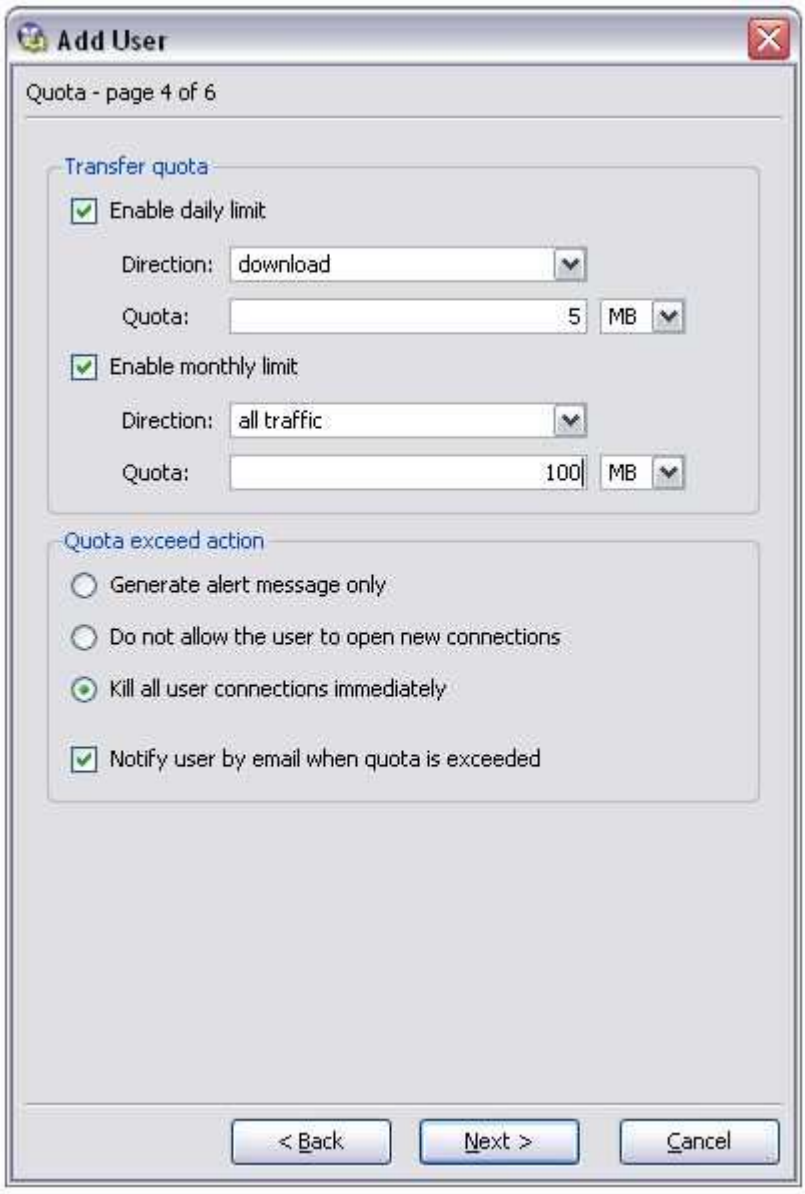
3. Στην τρίτη καρτέλα μπορούμε να δώσουμε δικαιώματα διαχειριστή στο χρήστη η να τον περιορίσουμε σε απλό επισκέπτη (σχήμα 3.7). Μπορούμε για παράδειγμα να του επιτρέψουμε η να του απαγορέψουμε τη χρήση P2P προγραμμάτων.

Σχήμα 3.7

4. Στην επόμενη καρτέλα υπάρχει μια πολύ σημαντική λειτουργία. Κάτω από την επικεφαλίδα **transfer quota** μπορούμε να ενεργοποιήσουμε ημερήσιο ή μηνιαίο όριο. Αναλυτικά μπορούμε να ορίσουμε το ανώτατο upload ή download ή και το σύνολο της κίνησης για το αντίστοιχο διάστημα. Όταν ο χρηστής ξεπεράσει το όριο που έχουμε θέσει τότε υπάρχουν 3 επιλογές που μπορούμε να 'τικάρουμε' κάτω από την επικεφαλίδα **quota exceed action** και να γίνει η αντίστοιχη ενέργεια:

- **Generate alert message only** (το πρόγραμμα προειδοποιεί το διαχειριστή ότι ο χρήστης έχει ξεπεράσει το όριο)

- **Do not allow the user to open new connections** (δεν επιτρέπει στο χρήστη να κάνει νέες συνδέσεις)



Σχήμα 3.8

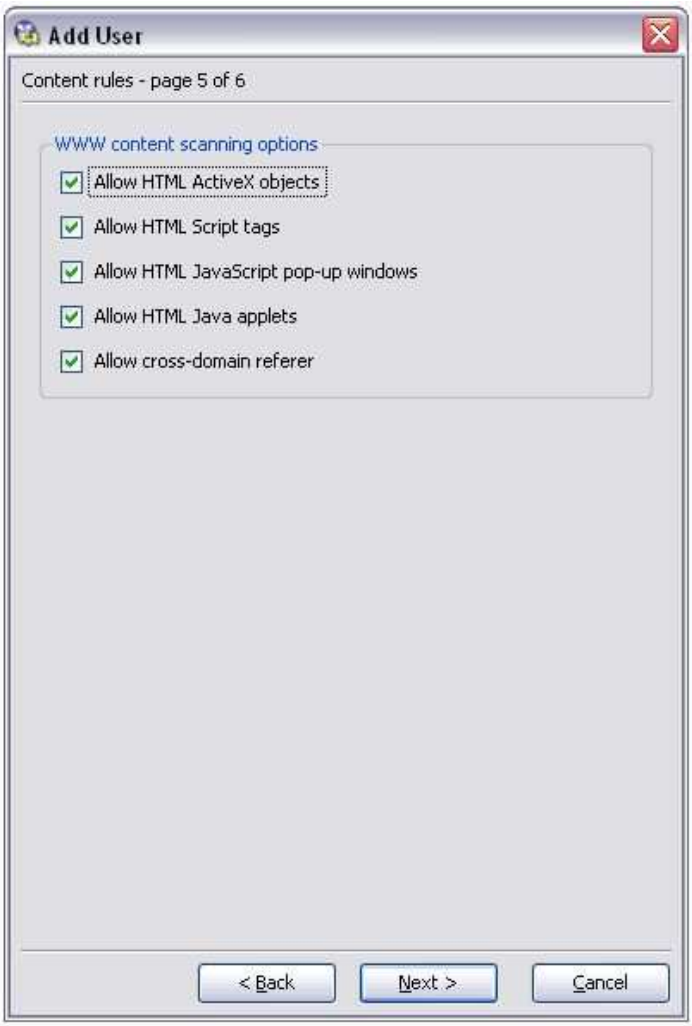
- **Kill all user connections immediately** (κλείνει όλες τις συνδέσεις του χρήστη)

Τέλος υπάρχει και η επιλογή **notify user by email when quota exceeded** με την οποία ειδοποιείται ο χρήστης όταν το όριο του έχει ξεπεραστεί(σχήμα 3.8).

5. Στην πέμπτη σελίδα εμφανίζονται οι επιλογές που έχουν σχέση με τα επιτρεπόμενα περιεχόμενα των WWW σελίδων. Διάφορες σελίδες χρησιμοποιούν ActiveX αντικείμενα, java applets η scripts επικίνδυνα για τον υπολογιστή του χρήστη. Από αυτή την καρτέλα έχουμε την δυνατότητα να τα απενεργοποιήσουμε (σχήμα 3.9).

6. Στην έκτη και τελευταία σελίδα της δημιουργίας νέου λογαριασμού χρήστη μπορούμε να ορίσουμε ότι χρήστης θα συνδέεται αυτόματα αν επισκεφτεί το δίκτυο μας από συγκεκριμένη IP (**Automatic Login-Specific host IP Addresses**) (σχήμα 3.10).

Τέλος ολοκληρώνουμε τη διαδικασία δημιουργίας νέου λογαριασμού χρήστη πατώντας finish και apply.



Σχήμα 3.9

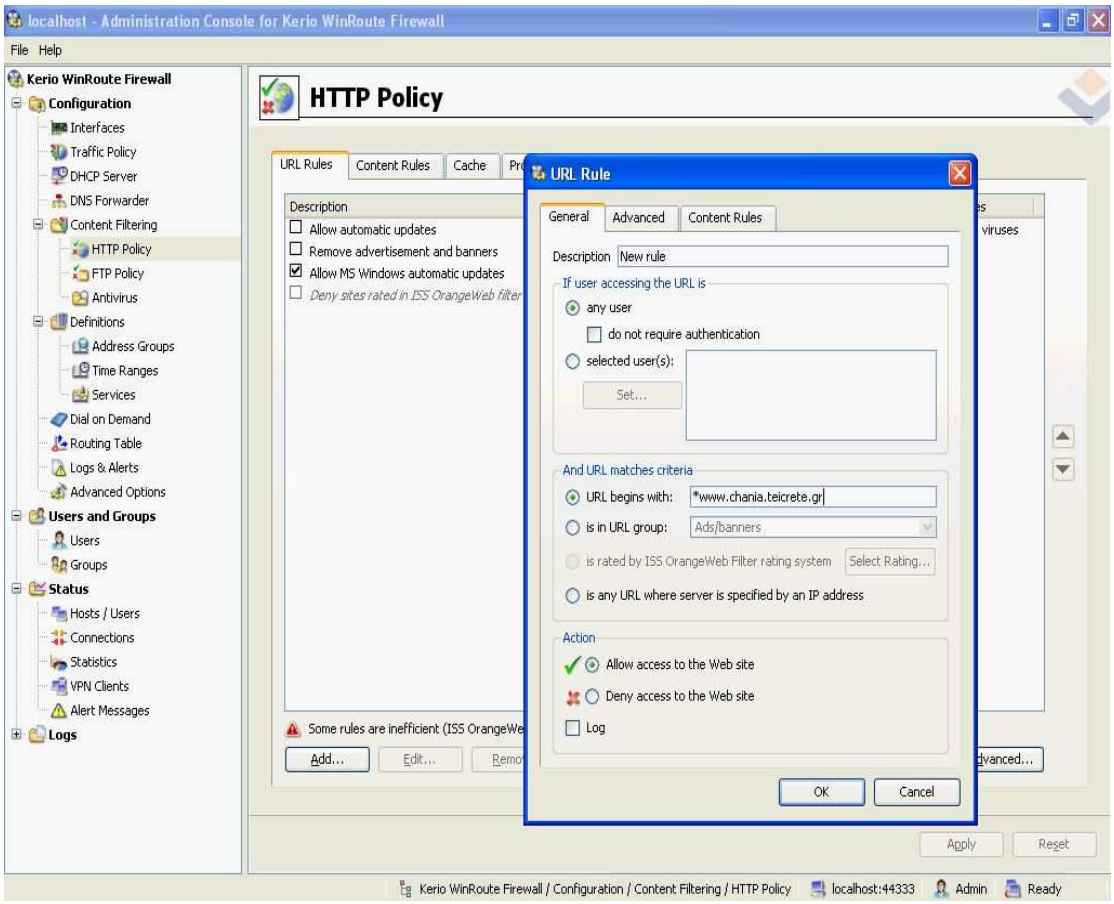
Σχήμα 3.10

3.2.3 Http Policy

Ένα άλλο χαρακτηριστικό του προγράμματος που θα πρέπει να τονίσουμε είναι ότι μπορούμε να απαγορέψουμε την εμφάνιση συγκεκριμένων σελίδων οι οποίες έχουν κριθεί ακατάλληλες για τους επισκέπτες του δικτύου. Επίσης μπορούμε να επιλέξουμε ορισμένες σελίδες που ο χρήστης μπορεί να επισκεφτεί χωρίς να απαιτηθεί η πιστοποίηση του. Για παράδειγμα η ελεύθερη πρόσβαση στην ιστοσελίδα και στον mail sever του ΤΕΙ ή ακόμα και σε κάποια μηχανή αναζήτησης.
Ακολουθεί περιγραφή της διαδικασίας:

Από το κεντρικό μενού **configuration** κάτω από την υποκατηγορία **content filtering** επιλέγουμε **http policy.** Στο παράθυρο που εμφανίζεται, στην καρτέλα **url rules** επιλέγουμε **add.**Εισάγουμε την σελίδα στο πεδίο **URL begins with:** και στη συνέχεια στο πεδίο **action** επιλέγουμε **allow access to the web site** ή **deny access to the web site** ανάλογα με το αν θέλουμε να επιτρέψουμε ή να απαγορέψουμε την χρήση της(σχήμα 3.11).

Ακόμα από το πρόγραμμα δίνεται η δυνατότητα περισσότερων επιλογών πάνω στην πολιτική εμφάνισης ιστοσελίδων π.χ πρόσβαση συγκεκριμένες μόνο ώρες που ορίζονται από τον διαχειριστή, πρόσβαση από συγκεκριμένο εύρος IP διευθύνσεων.



Σχήμα 3.11

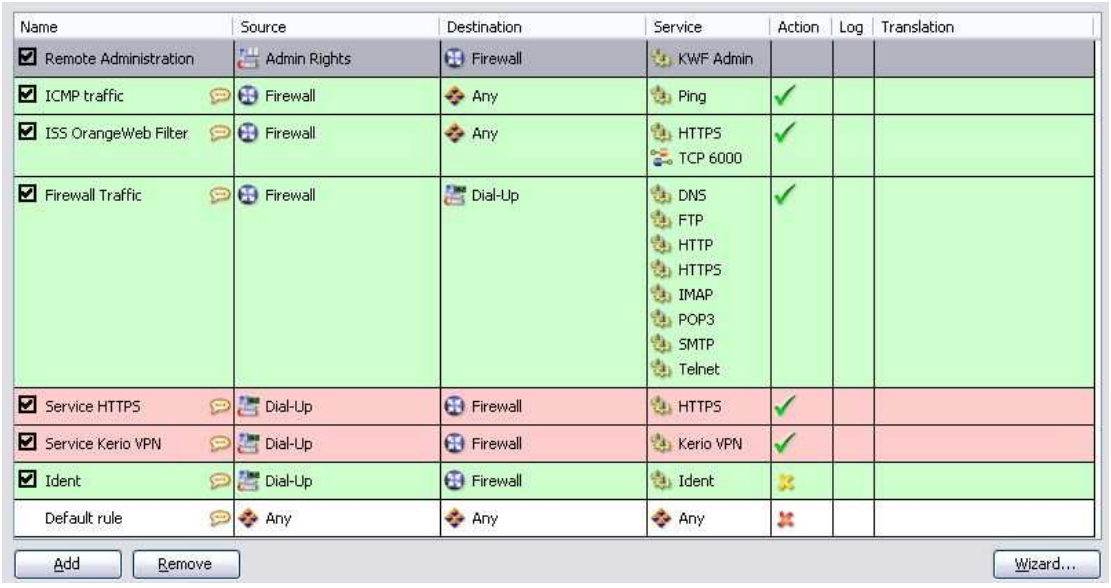
3.2.4 Απομακρυσμένη διαχείριση

Καθώς το δίκτυό επεκτείνεται μέσω συνδέσεων με μακρινά γραφεία, εγκαταστάσεις και άλλα υποδίκτυα πρέπει να υπάρχει ευκολία στη διαχείριση του. Γίνεται εύκολα κατανοητό ότι δεν θα πρέπει να απαιτείται η φυσική παρουσία του διαχειριστή στο χώρο του server.Παρόλα αυτά ο server θα πρέπει να είναι εύκολα προσβάσιμος οποιαδήποτε στιγμή χρειαστεί η επέμβαση του διαχειριστή.

Το **Kerio winroute** παρέχει μια κονσόλα για απομακρυσμένη διαχείριση την **Kerio Administration console**. Οι δυνατότητες διαχείρισης που προσφέρει μπορούν να αυτοματοποιήσουν διάφορες λειτουργίες όπως συντήρηση, ενημερώσεις και αναφορές.

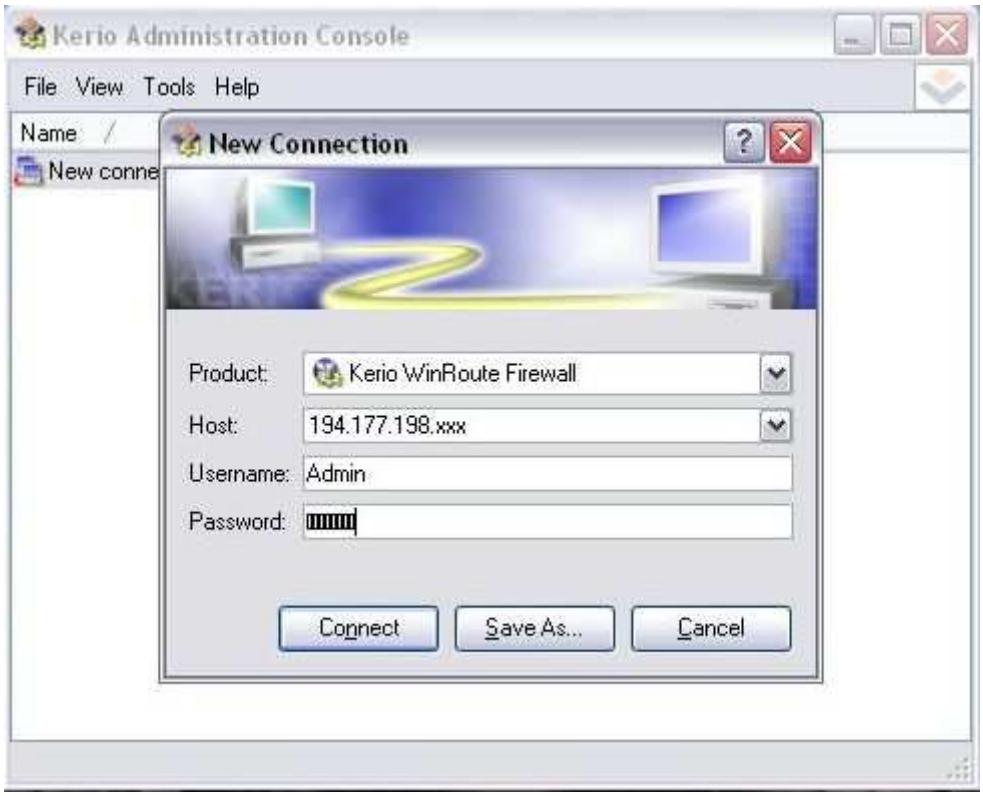
Για να εκμεταλλευτούμε αυτή τη δυνατότητα ακολουθούμε μια διαδικασία η οποία χωρίζεται σε δυο μέρη. Το πρώτο μέρος προετοιμάζει το server για την απομακρυσμένη διαχείριση, ενώ το δεύτερο απαιτεί απλά την εγκατάσταση της κονσόλας Kerio Administration στον υπολογιστή του client-διαχειριστή.

Αναλυτικότερα, από το μενού **configuration** επιλέγουμε **traffic policy** και στη συνέχεια **add** για να προσθέσουμε τον κανόνα που θα μας επιτρέψει την απομακρυσμένη διαχείριση. Σε αυτόν τον κανόνα δίνουμε τις παραμέτρους όπως φαίνονται στο παρακάτω σχήμα (σχήμα 3.12). Στην κατηγορία **Service** επιλέγουμε **KWF Admin**, στην κατηγορία **Destination** επιλέγουμε **Firewall** και στο **Source** έχουμε την δυνατότητα να ορίσουμε πρόσβαση από μια μόνο IP διεύθυνση, ένα εύρος IP διευθύνσεων ή ακόμα και από όλο το δίκτυο. Περιορίζοντας τη δυνατότητα πρόσβασης στην κονσόλα διαχείρισης από συγκεκριμένες IP διευθύνσεις μειώνουμε τον κίνδυνο κακόβουλων επιθέσεων στο δίκτυο.



Σχήμα 3.12

Στον υπολογιστή του client απαιτείται απλά η εγκατάσταση του Kerio Administration Console. Στο πεδίο Host εισάγουμε την IP διεύθυνση του server και στη συνέχεια τα username και password στα αντίστοιχα πεδία (σχήμα 3.13).



Σχήμα 3.13

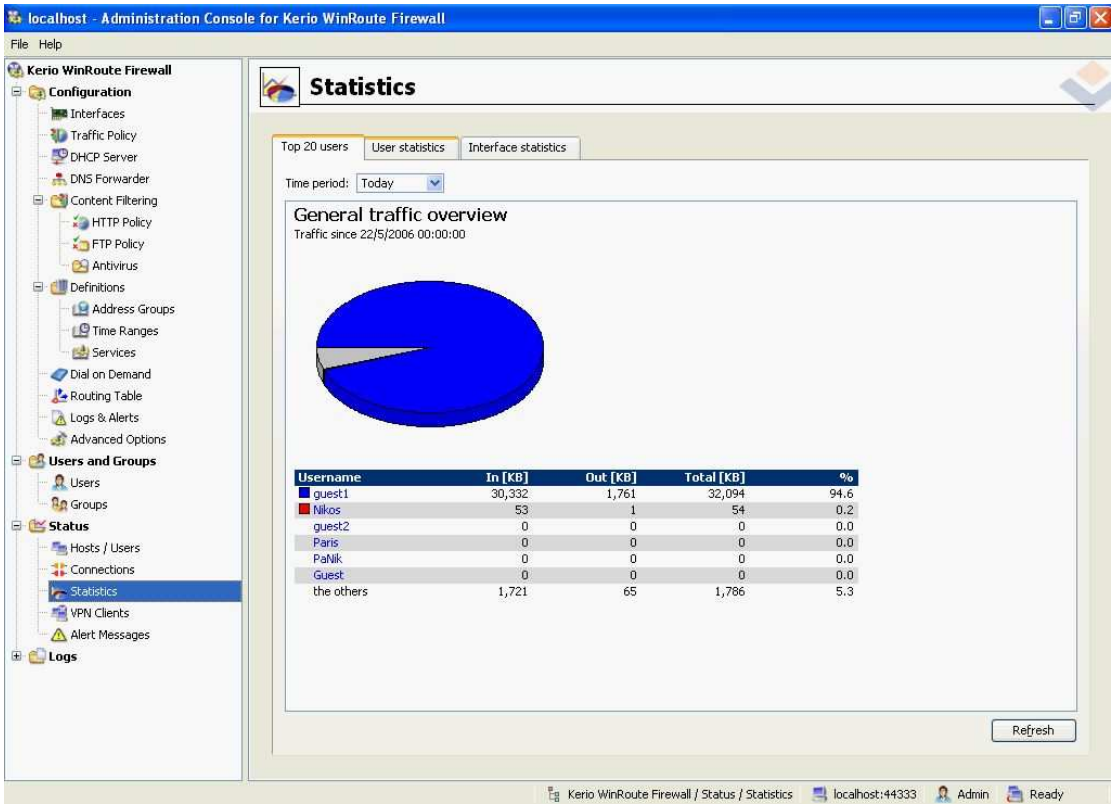
Με την ολοκλήρωση της διαδικασίας ο απομακρυσμένος διαχειριστής έχει όλες τις επιλογές που θα είχε αν βρισκόταν μπροστά στην οθόνη του server χωρίς να μετακινηθεί από τον υπολογιστή του.

3.2.5 Λήψη στατιστικών στοιχείων μέσω του Kerio

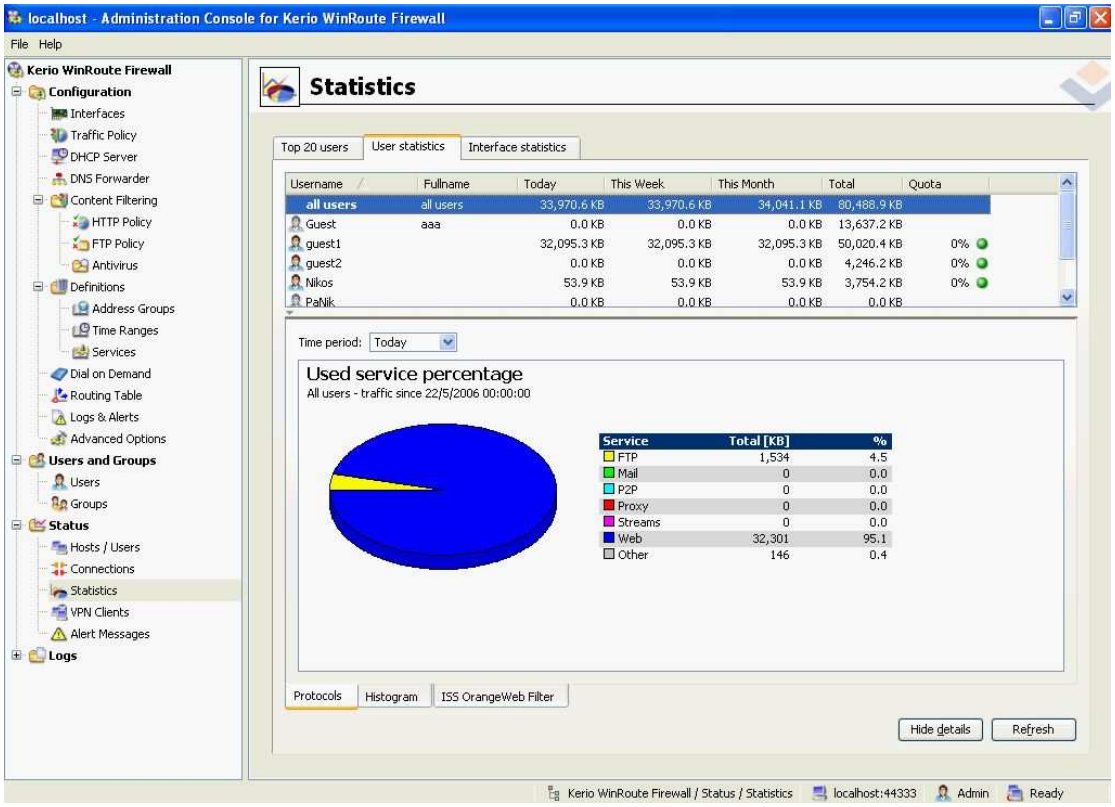
Η συνεχής παρακολούθηση του δικτύου βοηθά στην αντιμετώπιση προβλημάτων πριν αυτά δημιουργηθούν, στην αποδοτικότερη διαχείριση του, στην καλύτερη κατανομή του διαθέσιμου bandwidth ή και στη μελέτη της χρήσης του. Το Kerio winroute προσφέρει πληθώρα στατιστικών στοιχείων προσβάσιμων από το περιβάλλον του.

Από το μενού Status επιλέγοντας statistics στις αντίστοιχες καρτέλες μπορούμε να δούμε το Top 20 χρηστών με βάση την κίνηση τους (παρέχεται και το ποσοστό χρήσης επί της συνολικής κίνησης δικτύου) σχήμα 3.14, αναλυτικά στοιχεία χρήσης για τον κάθε χρήστη ξεχωριστά (έχουμε την κίνηση για κάθε κατηγορία χρήσης όπως ftp, mail, p2p, proxy, streams, web, other) σχήμα 3.15 και το ιστόγραμμα συνολικής κίνησης δικτύου (σχήμα 3.16).

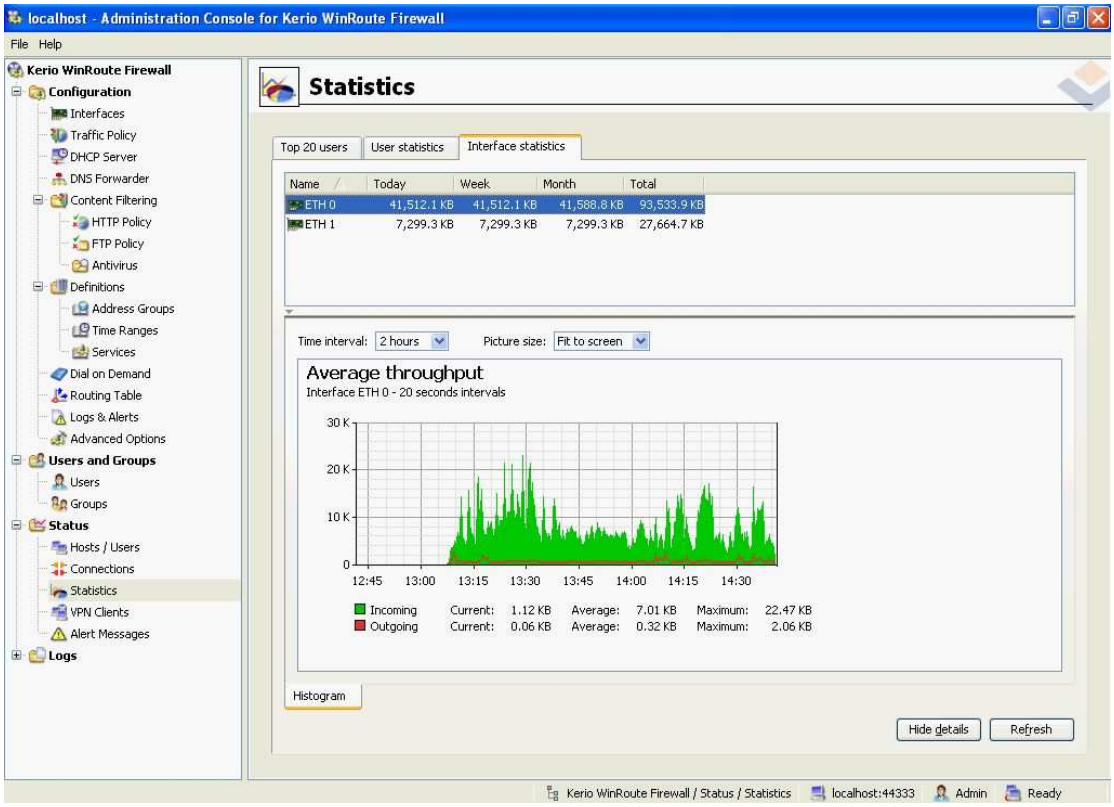
Ακολουθούν σχηματικά παραδείγματα απεικόνισης για κάθε μια από τις προαναφερθείσες κατηγορίες.



Σχήμα 3.14 – Top 20 users



Σχήμα 3.15 – User Statistics



Σχήμα 3.16 – Interface Statistics

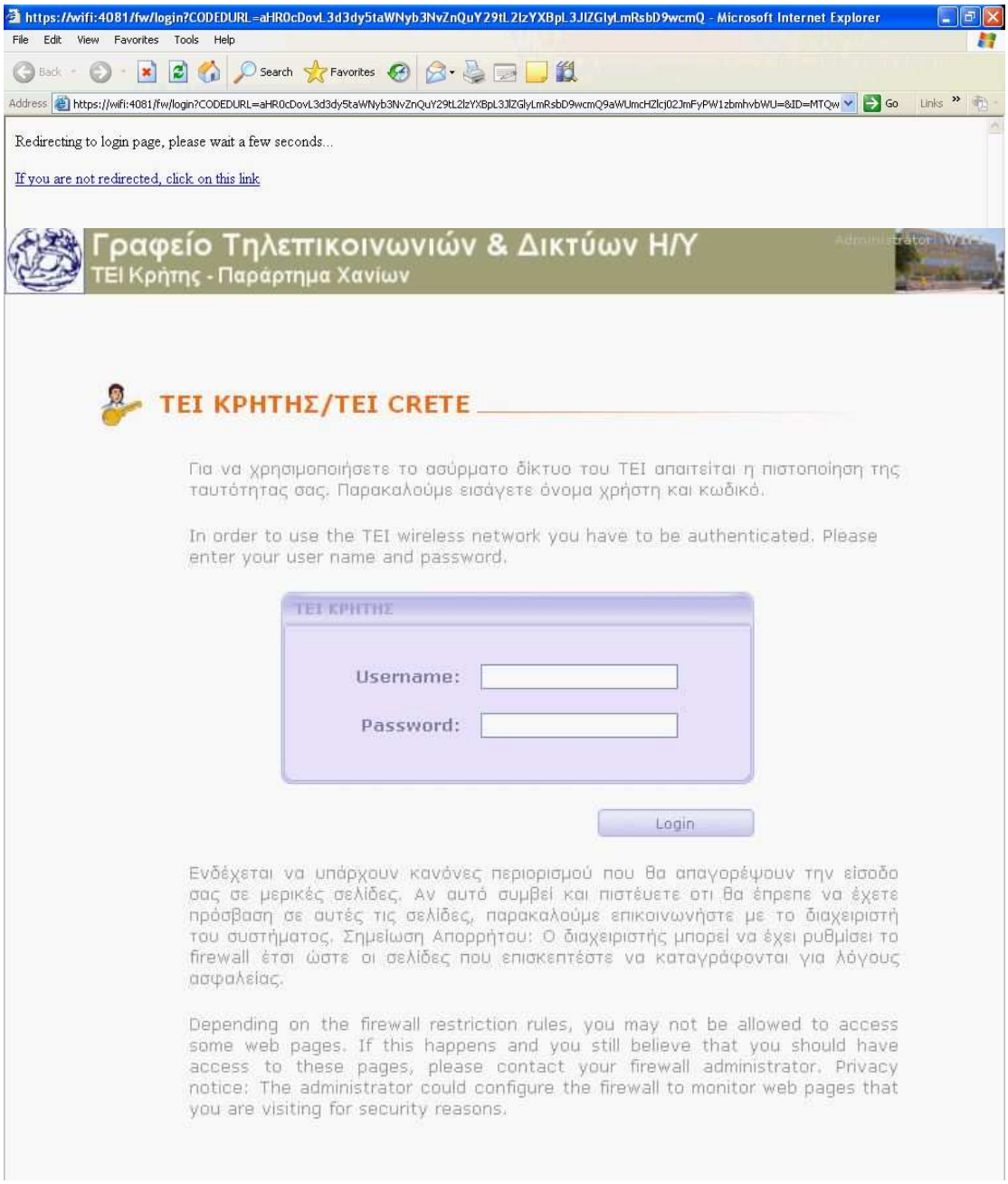
3.3 Περιήγηση – Εργαλεία Χρήστη και λογισμικό Kerio

Έως τώρα εξετάσαμε το δίκτυο από την πλευρά του διαχειριστή και περιγράψαμε τις ρυθμίσεις που πρέπει να γίνουν. Επίσης κάναμε μια σύντομη αναφορά στα εργαλεία που έχει στα χέρια του ο διαχειριστής για την εποπτεία και διαχείριση του δικτύου. Σε αυτή την ενότητα θα εξετάσουμε το δίκτυο από την πλευρά του χρήστη-πελάτη.

Κάθε χρήστης που εισέρχεται στο πεδίο εμβέλειας του access point και εφόσον συνδεθεί με αυτό, αποκτά αυτόματα IP της μορφής 192.168.1.xxx από το DHCP pool. Στην ουσία, το μόνο που θα χρειαστεί να κάνει ο χρήστης είναι να ρυθμίσει τον υπολογιστή του έτσι ώστε να γίνεται αυτόματη απόδοση IP όταν χρειαστεί. Θα πρέπει όμως να αναγνωρισθεί προκειμένου να του ανατεθούν δικαιώματα πρόσβασης. Αυτό γίνεται μέσω ενός μηχανισμού captive portal. Ο μη πιστοποιημένος χρήστης που επιχειρεί να περιηγηθεί στο διαδύκτιο ανακατευθύνεται σε μια ειδική Web σελίδα όπου απαιτείται το όνομα και ο κωδικός πρόσβασής του για να αποκτήσει το δικαίωμα εξουσιοδοτημένης χρήσης. Ας δούμε ένα παράδειγμα:

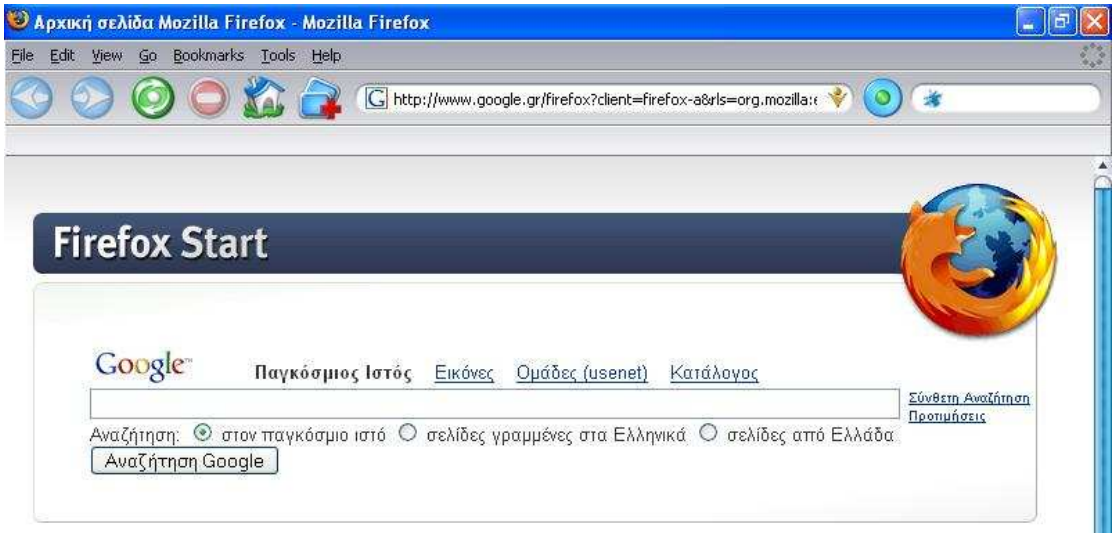
1) Ο χρηστής πληκτρολογεί τη σελίδα που θέλει να επισκεφτεί (σχήμα 3.16)
2) Γινεται ανακατεύθυνση στη σελίδα πιστοποίησης (σχήμα 3.17)
3) Ο χρήστης πληκτρολογεί όνομα και κωδικό πρόσβασης (σχήμα 3.18)
4) Εφόσον γίνει η πιστοποίηση ο χρήστης μπορεί να συνεχίσει ελεύθερα την περιήγηση του. (σχήμα 3.19)

Σχήμα 3.16 - Βήμα 1 από 4



Σχήμα 3.17 - Βήμα 2 από 4

Σχήμα 3.18 – Βήμα 3 από 4



Σχήμα 3.19 - Βήμα 4 από 4

Ο χρήστης μέσω του συνδέσμου index page στη σελίδα πιστοποίησης έχει πρόσβαση σε ένα μενού όπου μπορεί να βρει διάφορα στοιχεία του λογαριασμού του (σχήμα 3.20). Μπορεί για παράδειγμα να δει διάφορα στατιστικά χρήσης, τις σελίδες που υπάρχουν στη λίστα περιορισμένης πρόσβασης ή απλά να αποσυνδεθεί από το δίκτυο.

Σχήμα 3.20 – Μενού επιλογών χρήστη

Όπως βλέπουμε στο σχήμα 3.21, ο χρήστης έχει πλήρη εικόνα του λογαριασμού του και μπορεί ανά πάσα στιγμή να αντλήσει πολύτιμα στοιχεία. Για παράδειγμα μπορεί να δει τα όρια στο bandwidth που ενδεχομένως του έχει επιβάλει ο διαχειριστής του συστήματος. Έτσι μπορεί να περιορίσει τη χρήση του δικτύου αν δει ότι ο λογαριασμός του πλησιάζει το όριο της επιτρεπόμενης χρήσης. Άλλα χαρακτηριστικά που μπορεί να δει είναι η χρονική διάρκεια που είναι συνδεδεμένος, τα συνολικά bytes που έχει στείλει και λάβει, τα μπλοκαρισμένα δεδομένα από το φίλτρο του εργαλείου διαχείρισης και τα ημερήσια, εβδομαδιαία και μηνιαία όρια bandwidth που του έχουν επιβληθεί.


User Statistics - [guest1]
Login information
Your username: guest1
Your IP address: localhost
Login duration: 00:00:48
Logged in via: SSL
Traffic statistics
Today Total
Bytes sent: 1.74 MB 2.79 MB
Bytes received: 29.83 MB 46.28 MB
WWW requests sent: 1768 2961
Content filter statistics
Today Total
Blocked Java applets: 0 0
Blocked Pop-Up windows: 0 0
Blocked scripts: 0 0
Blocked ActiveX: 0 0
Blocked referers: 0 0
Transfer quota statistics
Limit Used Percentage
Daily quota: - 31.57 MB -
Weekly quota: - 31.57 MB -
Monthly quota: - 31.57 MB -
The total statistics counted since: Mon Apr 03 13:10:52 2006

Σχήμα 3.21

ΚΕΦΑΛΑΙΟ 4

Μελέτη παροχής LBS σε WLANs

4.1 Γενικά περί εντοπισμού θέσης

Τα ασύρματα τοπικά δίκτυα (WLANs) έχουν επεκταθεί επιτυχώς στα εταιρικά δίκτυα και τα δίκτυα πανεπιστημιουπόλεων. Επιπλέον, πολλοί φορείς παροχής υπηρεσιών Διαδικτύου (ISPs) παρέχουν τις ασύρματες υπηρεσίες πρόσβασης διαδικτύου με την εγκατάσταση των σημείων πρόσβασης (APs) σε δημόσια hotspot , όπως οι αερολιμένες, τα καταστήματα καφέ, και τα συνεδριακά κέντρα. Περισσότερες υπηρεσίες θα παρασχεθούν στα δημόσια hotspot. Όπως στα κυψελοειδή συστήματα τηλεπικοινωνιών, οι υπηρεσίες Location-based (LBSs) θα είναι από τις υπηρεσίες που θα εφαρμοστούν στα hotspot.Οι υπηρεσίες Location-based είναι υπηρεσίες που παρέχουν πληροφορίες για τη θέση σε έναν κινητό χρήστη σύμφωνα με τους τρέχοντες γεωμετρικούς τόπους όταν ο κινητός χρήστης έχει πρόσβαση σε ένα WLAN. Αυτήν την περίοδο, δεν υπάρχει καμία τυποποιημένη λύση στη διαχείριση γεωμετρικών τόπων IEEE 802.11 στις υπόδομές WLAN. Επομένως, μια αποτελεσματική τεχνική προσδιορισμού θέσης απαιτείται για την παροχή LBSs στα hotspot. Τα hotspot βρίσκονται συνήθως σε εσωτερικά περιβάλλοντα. Η περιοχή κάλυψης ενός εσωτερικού IEEE 802.11 AP είναι συνήθως μικρή, συγκρινόμενη με τα κυψελοειδή συστήματα τηλεπικοινωνιών. Επομένως, εάν ξέρουμε σε ποιο AP συνδέεται ένας κινητός χρήστης έπειτα εμείς μπορούμε να πούμε ότι η κινητή συσκευή είναι στη γειτονιά του AP. Εάν η κινητή συσκευή προσπαθεί να έχει πρόσβαση σε LBS, είναι πρακτικό για τις LBS να παρασχεθούν οι εξαρτώμενες από τη θέση πληροφορίες βασισμένες στη θέση του AP. Αυτή η προσέγγιση προσδιορισμού θέσης από την εγγύτητα είναι πολύ παρόμοια με την προσέγγιση ταυτότητας στα κυψελοειδή συστήματα τηλεπικοινωνιών. Ο προσδιορισμός θέσης όμως είναι πρακτικότερος στα hotspot,δεδομένου ότι η περιοχή κάλυψης ενός τυπικού AP είναι μικρότερη.

Σε ένα IEEE 802.11 WLAN, προτού να χορηγηθεί σε μια κινητή συσκευή η πρόσβαση στο δίκτυο, η κινητή συσκευή θα κάνει αρχικά μια σύνδεση με το κοντινότερο AP. Αυτό μπορεί να ολοκληρωθεί από την υπηρεσία σύνδεσης (association service) που καθορίζεται από το IEEE 802.11, το οποίο καθορίζει επίσης τις υπηρεσίες αποσύνδεσης(diassociation) και επανασύνδεσης (reassociation). Οι υπηρεσίες αποσύνδεσης θα χρησιμοποιηθούν όταν προηγούμενες συνδέσεις πρόκειται να τερματιστούν. Μια αποσύνδεση συμβαίνει συνήθως όταν μια κινητή συσκευή κλείνεται ή όταν απομακρύνεται από ένα AP. Η υπηρεσία επανασύνδεσης χρησιμοποιείται για να διατηρήσει μια ασύρματη σύνδεση όταν κινείται μια κινητή συσκευή από ένα AP σε προς ένα άλλο. Κάθε AP θα διατηρήσει τις πληροφορίες σύνδεσης για τη διαχείριση των ασύρματων συνδέσεων. Οι πληροφορίες σύνδεσης που φυλάσσονται σε ένα AP προσδιορίζουν ποιες κινητές συσκευές είναι συνδεδεμένες με το AP Ως εκ τούτου, μπορούμε να καθορίσουμε τις τρέχουσες θέσεις των κινητών συσκευών εάν μπορούμε να λάβουμε τις πληροφορίες σύνδεσης από τα APs. Οι πληροφορίες σύνδεσης στα APs είναι μέρος σημαντικών πληροφοριών διαχείρισης δικτύων. Γενικά, τα APs υποστηρίζουν το απλό πρωτόκολλο διαχείρισης δικτύων -Simple Network Management Protocol-(SNMP) για την παροχή των πληροφοριών διαχείρισης δικτύων με έναν τυποποιημένο

τρόπο. Στα περισσότερα APs, οι πληροφορίες σύνδεσης που απαιτούνται για τον προσδιορισμό θέσης μπορούν να ληφθούν μέσω του SNMP. Θα παρουσιάσουμε μια αποτελεσματική τεχνική προσδιορισμού θέσης βασισμένη στις παγίδες SNMP (ανακοινώσεις) που εκπέμπονται από τα APs.

Πολλές υπηρεσίες εφαρμογής Διαδικτύου έχουν ως σκοπό να είναι βασισμένες στο WEB. Εάν οι LBSs μπορούν να εφαρμοστούν ως εφαρμογή web, ο web browser σε μια κινητή συσκευή θα είναι το μόνο απαραίτητο λογισμικό για να έχει πρόσβαση στις πληροφορίες που εξαρτώνται από τη θέση . Αυτό θα διευκολύνει την επέκταση LBSs σε ετερογενές PDAs και σε φορητές συσκευές. Επομένως, ενδιαφερόμαστε για την ανάπτυξη LBSs βασισμένου στο WEB. Όταν ένας χρήστης χρησιμοποιεί έναν web browser για να έχει πρόσβαση σε βασισμένες στο WEB LBSs, οι LBSs μπορούν να ανακτήσουν τη διεύθυνση IP της κινητής συσκευής του χρήστη από τα αιτήματα HTTP. Κατόπιν, οι LBSs θα πρέπει να βρούν την τρέχουσα θέση της κινητής συσκευής από τη διεύθυνση IP της. Αφ' ετέρου, τα περισσότερα AP εξετάζει τις MAC διευθύνσεις για να προσδιορίσουν την ταυτότητα των κινητών συσκευών.

Ουσιαστικά, τα APs είναι συσκευές 2 στρωμάτων. Οι πληροφορίες σύνδεσης που αποθηκεύονται σε κάθε AP καταγράφουν μόνο τις MAC διευθύνσεις των συνδεδεμένων κινητών συσκευών. Επομένως, αφότου λάβουμε τη IP διεύθυνση μιας κινητής συσκευής από έναν web server, πρέπει έπειτα να πάρουμε την αντίστοιχη MAC διεύθυνση. Κατά συνέπεια, ο προσδιορισμός θέσης μπορεί να εκτελεσθεί με την εύρεση των πληροφοριών σύνδεσης με τη MAC διεύθυνση . Επομένως, για να επιτρέψουμε LBSs σε περιβάλλοντα WWW, θα παρουσιάσουμε επίσης ένα σχέδιο χαρτογράφησης IP-to-MAC διευθύνσεων. Εάν γνωρίζουμε μια IP διεύθυνση, το σχέδιο χρησιμοποιεί το SNMP για να ψάξει την αντίστοιχη MAC διεύθυνση στον πίνακα διευθύνσεων που διατηρείται σε έναν δρομολογητή (router). Συνεπώς, η χαρτογράφηση διευθύνσεων μαζί με τον προσδιορισμό θέσης καθιστά πιθανή την LBS ,σε περιβάλλοντα βασισμένα στο WEB στα Hotspot.

Μια προσέγγιση προσδιορισμού θέσης WLAN απαιτεί την πρόσβαση στις πληροφοριες διαχείρισης στα APs και στους δρομολογητές. Για να μην είναι εμφανής οι λεπτομέρειες του προσδιορισμού θέσης και της χαρτογράφησης διευθύνσεων, προτείνεται ένα γενικευμένο πλαίσιο υπηρεσιών web για LBSs στα Hotspot. Στο πλαίσιο αυτό , ένας κεντρικός υπολογιστής (server) χρησιμοποιείται για να εκτελεί τον προσδιορισμό θέσης και την χαρτογράφηση των διευθύνσεων. Ο κεντρικός υπολογιστής θέσης παρέχει τις πληροφορίες θέσης μέσω των WEB υπηρεσιών. Η υπηρεσία LB χρησιμοποιεί τις WEB υπηρεσίες για να πάρει τις πληροφορίες θέσης των κινητών συσκευών. Συνεπώς, LBSs μπορούν να αναπτυχθούν ανεξάρτητα μέσω του πλαίσιο WEB υπηρεσιών.

4.2 Σχετική εργασία

Οι LBSs αναπτύχθηκαν κυρίως στα κυψελοειδή τηλεφωνικά δίκτυα. Έχουν αναπτυχθεί διάφορες τεχνικές προσδιορισμού θέσης για τα κυψελοειδή συστήματα. Επιπλέον, για συγκεκριμένες LBSs εφαρμογές, χρησιμοποιούνται διάφορα συστήματα θέσης με ιδιαίτερο υλικό αισθητήρων όπως η ραδιοσυχνότητα (RF) και διάφορα εξαρτήματα GPS. Η χρήση των παραπάνω υλικών έχει το πλεονέκτημα της μεγαλύτερης ακρίβειας στον προσδιορισμό θέσης. Εντούτοις, η χρήση τέτοιου υλικού μπορεί να αυξήσει το κόστος της εφαρμογής και να περιορίσει την επέκταση LBSs. Ένας πρακτικός τρόπος να υποστηριχθεί ο προσδιορισμός θέσης για LBSs σε WLANs είναι η χρήση των τεχνικών προσδιορισμού θέσης απλά με τη βοήθεια του

IEEE 802.11. Παρακάτω, περιγράφουμε δύο σημαντικές προσεγγίσεις του προσδιορισμού θέσης χωρίς οποιαδήποτε ενίσχυση του ιδιαίτερου υλικού εκτός από το ίδιο το WLAN.

4.3.1 Προσέγγιση βασισμένη σε RSS

Διάφορες προηγούμενες μελέτες χρησιμοποίησαν την ισχύ των λαμβανόμενων σημάτων μια κινητής συσκευής για να συμπεράνουν την τρέχουσα θέση του.Ο τριγωνισμός (Triangulation) είναι η πιο κοινή τεχνολογία για τις προσεγγίσεις προσδιορισμού θέσης βασισμένες στις λαμβανόμενες δυνάμεις σημάτων (RSSs). Θεωρητικά, ο τριγωνισμός μπορεί να χρησιμοποιηθεί για να καθορίσει τη γεωγραφική θέση μιας κινητής συσκευής ακριβέστερα, εάν οι αποστάσεις μεταξύ των κινητών συσκευών και των APs μπορούν να υπολογιστούν ακριβώς από την ισχύ των σημάτων. Δυστυχώς, πιθανόν λόγω των παρεμποδίσεων και του φαινόμενου της εξασθένισης του σήματος μέσω των πολλαπλών διαδρομών στα εσωτερικά περιβάλλοντα, υπάρχει αξιοσημείωτη απόκλιση στην ισχύ των σημάτων που λαμβάνονται από μια κινητή συσκευή στο ίδιο χωρικό σημείο. Επομένως, ο τριγωνισμός βασιζόμενος στις μεταβλητές ισχύς σημάτων μπορεί να δώσει ανακριβή αποτελέσματα. Το ελάττωμα αυτό μπορεί να ξεπεραστεί με την χρήση μιας βάσης δεδομένων με τα στοιχεία της ισχύς των σημάτων, που έχουν μετρηθεί νωρίτερα σε κάθε πιθανή θέση. Κατόπιν, η θέση ενός κινητού χρήστη μπορεί να προκύψει με την εύρεση της πλέον πιθανής θέσης της οποίας τα αντίστοιχα στοιχεία ισχύος σήματος έχουν την καλύτερη αντιστοιχία με αυτά που βρίσκονται στη βάση δεδομένων και έχουν ληφθεί νωρίτερα. Αυτό το είδος τεχνικής προσδιορισμού θέσης καλείται **RSS-based location fingerprinting.**Αυτή η μέθοδος χρειάζεται κουραστικές μετρήσεις της ισχύος των σημάτων σε όλες τις περιοχές κάλυψης.
Επιπλέον, και ο τριγωνισμός αλλά και η RSS-based location fingerprinting απαιτούν την πυκνότερη εγκατάσταση APs για να εξασφαλίσουν ότι κάθε θέση είναι μέσα στη περιοχή κάλυψης τουλάχιστον τριών APs. Μια τέτοια διαμόρφωση APs είναι ασυνήθιστη σε hotspot.Εκτός αυτού, οι προσεγγίσεις RSS-based απαιτούν ένα πρόσθετο λογισμικό σε κάθε κινητή συσκευή για να εκτελέσουν τη συλλογή και τον υπολογισμό της ισχύος των σημάτων από τα APs.

4.3.2 Προσεγγίσεις βασισμένες στο δίκτυο

Αντίθετα από τις προηγούμενες τεχνικές RSS-based , διάφορες προσεγγίσεις καθορίζουν τη θέση μιας κινητής συσκευής με την εύρεση του AP με το οποίο συνδέεται η κινητή συσκευή. Οι Koo sgm πρότειναν μια βασισμένη στο δίκτυο προσέγγιση, αποκαλούμενη προσέγγιση RADIUS, βασισμένη στη χρήση ενός RADIUS server. Η Remote Authentication Dial-In User Service (RADIUS) είναι μια υπηρεσία που παρέχει την επικύρωση, την έγκριση, και τους λογαριασμούς χρηστών για την πρόσβαση στο δίκτυο. Η προσέγγιση RADIUS υποθέτει ότι ένας RADIUS server χρησιμοποιείται για να κάνει επικύρωση στους χρήστες WLAN. Κάθε κινητή συσκευή που προσπαθεί να έχει πρόσβαση στο WLAN θα στείλει ένα αίτημα επικύρωσης σε ένα AP. Το AP διαβιβάζει έπειτα το αίτημα στον RADIUS server. Στην περίπτωση μιας επιτυχούς επικύρωσης, η ώρα, η ταυτότητα του AP, και η MAC

διεύθυνση της κινητής συσκευής θα καταγραφούν στο log file του RADIUS server. Με την επιθεώρηση του log file, η προσέγγιση RADIUS μπορεί να καθορίσει με ποιο AP είναι συνδεδεμένη μια κινητή συσκευή. Για λόγους απόδοσης, συστήθηκε ο προσδιορισμός θέσης να εφαρμόζεται στον RADIUS server.Δεδομένου ότι το format του log file RADIUS δεν είναι τυποποιημένο, μπορεί να ποικίλει σε διαφορετικούς RADIUS servers. Επιπλέον, η προσέγγιση RADIUS δεν ισχύει για LBSs σε WLANs που δεν χρησιμοποιούν RADIUS για τις επικυρώσεις.

Μια άλλη βασισμένη στο δίκτυο προσέγγιση είναι η χρήση του SNMP στον προσδιορισμό θέσης. Σε μια προηγούμενη προσέγγιση SNMP, ένα πρόγραμμα καταγραφής SNMP χρησιμοποιήθηκε για να ρωτάει και να λαμβάνει τις MAC διευθύνσεις που παρατηρούνται από το AP.

Ουσιαστικά, τα APs διαμορφώνονται ως διαφανείς γέφυρες. Για την αποστολή των πλαισίων, οι διευθύνσεις της MAC που φαίνονται από ένα AP θα αποθηκευτούν στον πίνακα αποστολής του AP. Γενικά, μια MAC διεύθυνση μπορεί να αποθηκευτεί στον πίνακα αποστολής για 15 έως 20 λεπτά ακόμα κι αν η αντίστοιχη συσκευή έχει σταματήσει μια σύνδεση με το AP. Δεδομένου ότι μια κινητή συσκευή μπορεί να περιπλανηθεί μεταξύ APs, είναι δυνατό η ίδια MAC διεύθυνση να εμφανίζεται σε διάφορα APs. Αυτό μπορεί να περιπλέξει τη διαδικασία προσδιορισμού θέσης χρησιμοποιώντας την προσέγγιση SNMP. Επιπλέον, η περιοδική καταγραφή από το SNMP μπορεί να καταναλώσει μεγάλη ποσότητα πόρων δικτύου και μπορεί να οδηγήσει σε μεγάλους χρόνους απόκρισης.

4.3.3 Χαρτογράφηση διευθύνσεων

Και η προσέγγιση RADIUS αλλά και η χρήση προσέγγισης SNMP χρησιμοποιούν τις MAC διευθύνσεις των κινητών συσκευών για να εκτελέσουν τον προσδιορισμό θέσης. Όπως περιγράφεται προηγουμένως, μόνο οι IP διευθύνσεις των κινητών συσκευών μπορούν να ληφθούν από LBSs στα περιβάλλοντα WWW. Επομένως, απαιτούνται οι χαρτογραφήσεις IP-to-MAC διευθύνσεων. Δύο προσεγγίσεις για τη χαρτογράφηση IP-to-MAC προτάθηκαν **:** η προσέγγιση DHCP και η προσέγγιση SNMP. Στην προσέγγιση DHCP, το log file του DHCP server για ένα WLAN χρησιμοποιείται για να παρέχει τις χαρτογραφήσεις διευθύνσεων. Όποτε ένας DHCP server ορίζει επιτυχώς μια IP διεύθυνση σε μια κινητή συσκευή, η διεύθυνση IP καθώς επίσης και η MAC διεύθυνση της κινητής συσκευής θα καταγραφούν στο log file. Επομένως, οι χαρτογραφήσεις IP-to-MAC μπορούν να ληφθούν με την επιθεώρηση του log file. Δεδομένου ότι δεν υπάρχει κανένα τυποποιημένο format για το log file ενός DHCP server, η προσέγγιση DHCP εξαρτάται επίσης από μια ιδιαίτερη εφαρμογή του DHCP server. Επιπλέον, θα υπάρξουν πολλαπλάσιοι DHCP servers που διανέμονται στα δίκτυα εάν υπάρχουν πολλά hotspot. Αυτό θα περιπλέξει την αναζήτηση των MAC διευθύνσεων.

Μια άλλη προσέγγιση είναι η χρήση του SNMP. Μια προηγούμενη προσέγγιση SNMP εφαρμόστηκε σε ένα απλό LAN ή ένα σύνολο εικονικών LANs (VLANs).Πρέπει εξ αρχής να γνωρίζουμε τις πύλες προεπιλογής (default gateways) του LAN και των VLANs. Οι ερωτήσεις SNMP στέλνονται σε αυτές τις πύλες προεπιλογής για να βρουν την εναποθηκευμένη MAC διεύθυνση σε μια δεδομένη IP διεύθυνση. Σε μια πύλη προεπιλογής, οι χαρτογραφήσεις των IP διευθύνσεων και των MAC διευθύνσεων μπορούν να βρεθούν στον πίνακα network-to-media που ονομάζεται ipNetToMediaTable. Τα hotspot διανέμονται συνήθως σε διαφορετικά τμήματα δικτύων. Κατά συνέπεια, μπορούν να υπάρξουν πολλές πύλες προεπιλογής.

Η προηγούμενη προσέγγιση SNMP δεν εξέτασε πώς να βρεί αποτελεσματικά τις MAC διευθύνσεις μεταξύ των πολυάριθμων πυλών προεπιλογής.

4.4 Μια νέα προσέγγιση SNMP

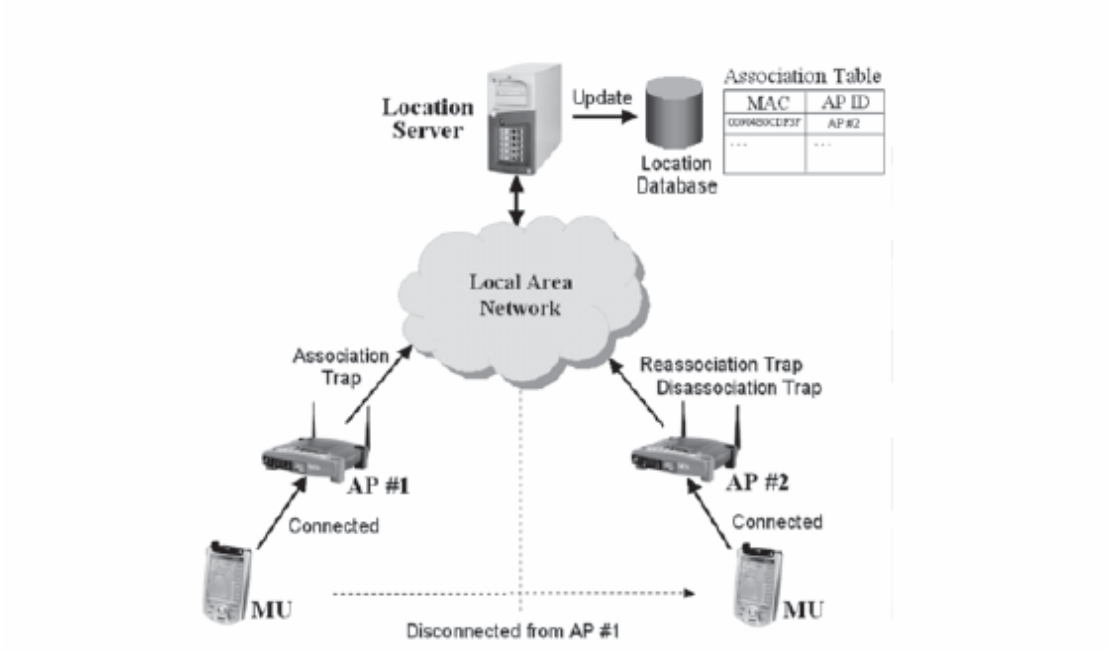
Η ανεξαρτησία πλατφορμών είναι ένας σημαντικός παράγοντας για να διευκολύνει την ευρεία χρήση LBSs στα hotspot. Οι προσεγγίσεις RSS-based για τον προσδιορισμό θέσης εξαρτώνται από τη πλατφόρμα, δεδομένου ότι απαιτείται εξειδικευμένο λογισμικό στους κινητούς πελάτες. Η προσέγγιση RADIUS μπορεί μόνο να υιοθετηθεί σε WLANs που χρησιμοποιούν επικυρώσεις RADIUS. Επιπλέον, επίσης εξαρτάται από πλατφόρμα, δεδομένου ότι πρέπει να ενσωματωθεί σε μια ιδιαίτερη εφαρμογή ενός RADIUS server.Μεταξύ των προηγούμενων προσεγγίσεων, η προσέγγιση SNMP είναι η πιο πολλά υποσχόμενη για να επιτύχει την ανεξαρτησία πλατφορμών. Εντούτοις, όπως περιγράφεται προηγουμένως, η περιοδική καταγραφή από το SNMP μπορεί να δημιουργήσει μεγάλη κίνηση σήματος και να οδηγήσει στην κακή απόδοση. Παρακάτω, θα προτείνουμε μια εναλλακτική λύση για τον προσδιορισμό θέσης βασισμένη στο μηχανισμό παγίδων του SNMP. Η προτεινόμενη λύση δεν απαιτεί οποιαδήποτε περιοδική καταγραφή εάν τα APs έχουν την ικανότητα της αποστολής των παγίδων SNMP για να εκθέσουν τα γεγονότα σχετικά με την σύνδεση στα APs.

Παίρνοντας πληροφορίες συσχετισμού από τις παγίδες SNMP

Προτού να επιτραπεί σε μια κινητή συσκευή να στείλει τα μηνύματα στοιχείων μέσω ενός AP, η κινητή συσκευή θα συνδεθεί αρχικά με το AP. Αυτό μπορεί να ολοκληρωθεί από την υπηρεσία σύνδεσης (association service) που διευκρινίζεται από το IEEE 802.11, το οποίο διευκρινίζει επίσης τη υπηρεσία επανασύνδεσης και την υπηρεσία αποσύνδεσης. Η υπηρεσία επανασύνδεσης επικαλείται για να επιτρέψει σε μια τρέχουσα σύνδεση να μεταφερθεί από ένα AP σε ένα άλλο. Η υπηρεσία αποσύνδεσης επικαλείται όποτε μια υπάρχουσα ένωση πρόκειται να ολοκληρωθεί. Κάθε AP θα κρατήσει τις πληροφορίες σύνδεσης για να διατηρήσει τις ασύρματες συνδέσεις μέσα στο AP Κατά συνέπεια, οι πληροφορίες σύνδεσης είναι σημαντικές για τη διαχείριση WLANs. Οι συνδέσεις σε ένα AP μπορούν να ποικίλουν με το χρόνο, δεδομένου ότι οι κινητές συσκευές μπορούν ελεύθερα να εισέλθουν ή να εξέλθουν από την περιοχή κάλυψης του AP. Δηλαδή η σύνδεση, η αποσύνδεση, και η επανασύνδεση είναι υπηρεσίες που μπορεί να πραγματοποιηθούν συχνά. Για την αποτελεσματική διαχείριση αυτών των υπηρεσιών, πολλά APs είναι σε θέση να στέλνουν τις παγίδες SNMP (ανακοινώσεις) στον διαχειριστή δικτύου όταν επικαλείται οποιαδήποτε από τις παραπάνω υπηρεσίες. Πράγματι, το IEEE 802.11 συστήνει ότι πρέπει να σταλεί μια παγίδα SNMP όταν εμφανίζεται μια αποσύνδεση. Για την αποτελεσματική διαχείριση των συνδέσεων, πολλά APs υψηλού επιπέδου, όταν πραγματοποιούνται συνδέσεις και αποσυνδέσεις στέλνουν παγίδες SNMP. Κατά συνέπεια, η ικανότητα της εκπομπής παγίδων σχετικών με την σύνδεση είναι ένα κοινό χαρακτηριστικό γνώρισμα που βρίσκεται στα περισσότερα APs. Οι πληροφορίες που φέρονται σε μια παγίδα σχετική με τη σύνδεση περιλαμβάνουν τη MAC διεύθυνση της κινητής συσκευής που εμπλέκεται

στην υπηρεσία διαδικασίας σύνδεσης. Η IP διεύθυνση του AP που στέλνει την παγίδα βρίσκεται και αυτή στον τομέα διευθύνσεων ενός μηνύματος παγίδων SNMP. Με την ερμηνεία των παγίδων που στέλνονται από όλα τα APs, μπορούμε να καθορίσουμε με ποιο AP συνδέεται ή αποσυνδέεται μια κινητή συσκευή.

Το σχήμα 4.1 επεξηγεί την προσέγγιση παγίδων SNMP. Στην προσέγγισή αυτή, μόνο ένας server θέσης απαιτείται στο ενσύρματο δίκτυο. Ο server θέσης είναι αρμόδιος για τη λήψη των παγίδων και την εκτέλεση των προσδιορισμών θέσης. Κάθε AP διαμορφώνεται έτσι ώστε όλες οι παγίδες να σταλούν στον server θέσης. Στον server θέσης, ένα πρόγραμμα λαμβάνει ασύγχρονα τις εισερχόμενες παγίδες από τα APs. Ο server θέσης περιέχει επίσης μια βάση δεδομένων θέσης για να αποθηκεύει τις πληροφορίες θέσης. Στη βάση δεδομένων θέσης, ένας πίνακας AP χρησιμοποιείται για να αποθηκεύει τις πληροφορίες για κάθε AP, συμπεριλαμβανομένου του προσδιοριστικού του (ID), της IP διεύθυνσης, και μιας περιγραφής θέσης. Επιπλέον, ένας πίνακας σύνδεσης αποθηκεύει τις τρέχουσες πληροφορίες σύνδεσης από όλα τα APs. Κάθε καταγραφή στον πίνακα σύνδεσης περιλαμβάνει τη MAC διεύθυνση της κινητής συσκευής και την ταυτότητα (ID) του AP που είναι συνδεδεμένη η κινητή συσκευή.



Σχήμα 4.1

Ο πίνακας σύνδεσης ενημερώνεται σύμφωνα με τους ακόλουθους λαμβανόμενους τύπους παγίδων:

i) **Παγίδα σύνδεσης.** Εισαγωγή ενός νέου αρχείου για να αποθηκευτεί η MAC διεύθυνση της κινητής συσκευής και η ταυτότητα του AP που έστειλε την παγίδα.

ii) **Παγίδα επανασύνδεσης.** Ενημέρωση του ID του AP του αρχείου σύνδεσης σε αντιστοιχία με τη MAC διεύθυνση που παρουσιάζεται στη παγίδα επανασύνδεσης.

iii) **Παγίδα αποσύνδεσης.** Διαγραφή του αρχείο σύνδεσης που αντιστοιχεί στη MAC διεύθυνση που παρουσιάζεται στην παγίδα αποσύνδεσης.

Αυτές οι αναπροσαρμογές που προκαλούνται από τις παγίδες σχετικές με την σύνδεση μπορούν να κρατούν τις πληροφορίες σύνδεσης πολύ ενημερωμένες. Οι ίδιες οι πληροφορίες σύνδεσης αποκαλύπτουν το σημείο όπου μια κινητή συσκευή έχει πρόσβαση σε ένα WLAN. Επομένως, με την εξέταση του πίνακα σύνδεσης, μπορούμε εύκολα να καθορίσουμε την τρέχουσα κατά προσέγγιση θέση οποιασδήποτε κινητής συσκευής. Αυτή η προσέγγιση του προσδιορισμού θέσης χρησιμοποιεί μόνο τις πληροφορίες σύνδεσης που φέρονται στις παγίδες SNMP. Κατά συνέπεια, η προσέγγιση παγίδων SNMP δεν θα προκαλέσει την πρόσθετη κυκλοφορία όπως υφίσταται στην προηγούμενη προσέγγιση καταγραφής SNMP. Επιπλέον, οι πληροφορίες σύνδεσης που συλλέγονται από τις παγίδες SNMP είναι πάντα οι πιο ενημερωμένες , ενώ οι εναποθηκευμένες MAC διευθύνσεις που χρησιμοποιούνται στην προσέγγιση καταγραφής SNMP μπορούν να είναι ανακριβείς. Ως εκ τούτου, έχει αναπτυχθεί επιτυχώς μια αποτελεσματική μέθοδος προσδιορισμού θέσης WLAN με τη βοήθεια των παγίδων σχετικών με τη σύνδεση.

4.5 Χαρτογράφηση διευθύνσεων IP σε MAC

Από τις πληροφορίες σύνδεσης , ο server θέσης λαμβάνει τη MAC διεύθυνση μιας κινητής συσκευής. Αφ' ετέρου, μια υπηρεσία LB παίρνει τη IP διεύθυνση μιας κινητής συσκευής από ένα αίτημα HTTP. Κατά συνέπεια, υπηρεσίες LB θα χρησιμοποιήσουν τις IP διευθύνσεις των κινητών συσκευών για να ζητήσουν από τον server θέσης να βρει τις θέσεις τους. Ως εκ τούτου, χρειαζόμαστε ακόμα μια χαρτογράφηση IP-to-MAC διευθύνσεων για τον προσδιορισμό θέσης. Ουσιαστικά, τα APs είναι συσκευές 2 στρωμάτων , οι οποίες δεν θα ανακτήσουν το πεδίο IP διευθύνσεων στην επιγραφή ενός IP πακέτου. Επομένως, δεν μπορούμε να λάβουμε τη διεύθυνση IP μιας κινητής συσκευής άμεσα από τα APs. Στην πραγματικότητα, η IP διεύθυνση μιας κινητής συσκευής θα φανεί από το δρομολογητή προεπιλογής του υποδικτύου όπου βρίσκεται η κινητή συσκευή. Όταν μια κινητή συσκευή έχει μια ασύρματη σύνδεση με ένα AP, η κινητή συσκευή και το AP είναι μέσα στο ίδιο υποδίκτυο. Επομένως, ο δρομολογητής προεπιλογής του AP θα είναι επίσης μια από τις κινητές συσκευές. Αρχικά, ξέρουμε ποια APs περιλαμβάνονται στα hotspot. Κατά συνέπεια, με την εξέταση των πινάκων δρομολόγησης εκείνων των APs, μπορούμε να καθορίσουμε τους δρομολογητές προεπιλογής που θα είναι αρμόδιοι για την αποστολή των IP πακέτων από τα WLANs. Επιπλέον, με την εξέταση των διαμορφώσεων των IP διευθύνσεων των APs, μπορούμε να ξέρουμε τα υποδίκτυα όπου βρίσκονται τα APs Αυτά τα υποδίκτυα είναι επίσης αυτά όπου μπορούν να εμφανιστούν οι κινητές συσκευές. Δεδομένου ότι λαμβάνουμε τη IP διεύθυνση μιας κινητής συσκευής από LBS, θα καθορίσουμε αρχικά το υποδίκτυο που περιέχει την κινητή συσκευή. Κατόπιν, προσδιορίζουμε το δρομολογητή προεπιλογής του υποδικτύου. Τέλος, βρίσκουμε τη MAC διεύθυνση της κινητής συσκευής στο δρομολογητή.

Για να υποστηρίξουμε τις παραπάνω διαδικασίες για τις χαρτογραφήσεις διευθύνσεων, προετοιμάζουμε έναν πίνακα υποδικτύου στη βάση δεδομένων θέσης. Ο πίνακας υποδικτύου αποτελείται από τέσσερις τομείς: Subnet ID, Subnet Mask, Default_Router, και Interface_Index. Κάθε αρχείο στον πίνακα υποδικτύου δείχνει ένα υποδίκτυο που θα μπορούσε να περιέχει τις κινητές συσκευές. Το Subnet ID μαζί με το Subnet_Mask καθορίζουν ένα υποδίκτυο. Ο τομέας Default Router δείχνει το δρομολογητή προεπιλογής του υποδικτύου. Ο δρομολογητής προεπιλογής μπορεί να

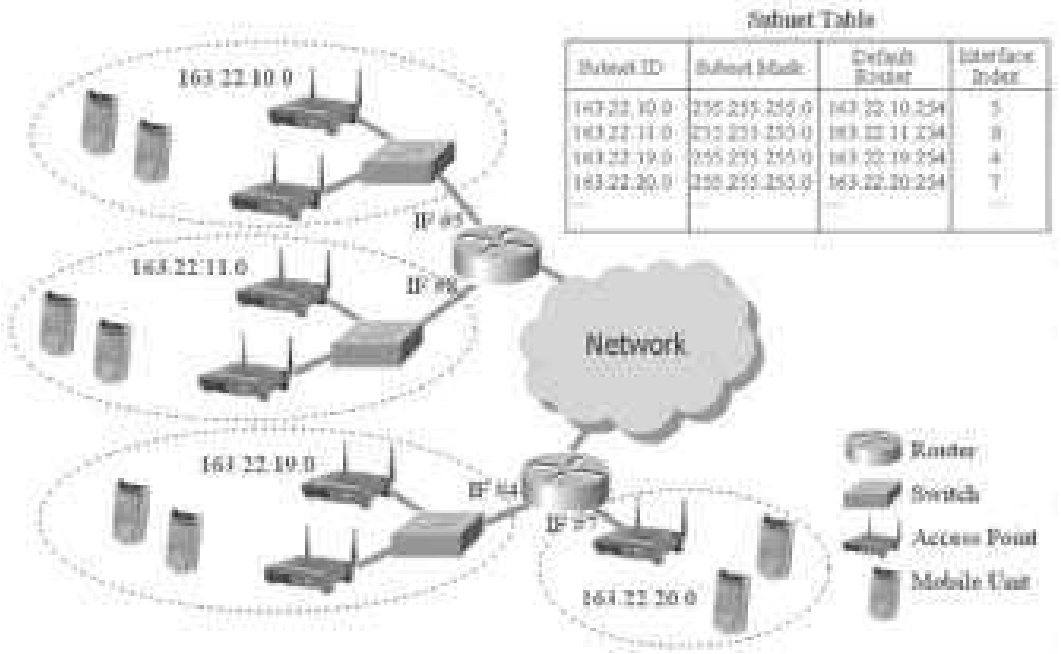
έχει διάφορες διεπαφές δικτύων. Το Interface Index χρησιμοποιείται για να προσδιορίσει τη διεπαφή δικτύων που συνδέεται με το υποδίκτυο. Ο πίνακας υποδικτύου μπορεί να χτιστεί βασισμένος στη βάση πληροφοριών διαχείρισης - management information base - (MIB) που αποθηκεύεται σε APs. Αρχικά, για κάθε AP, στέλνουμε ένα αίτημα SNMP στο AP για να πάρουμε τη μάσκα υποδικτύου. Η μάσκα υποδικτύου είναι διαθέσιμη στο αντικείμενο ipAdEntNetMask του πίνακα ipAddrTable, που καθορίζεται στο MIB II. Η αποκτηθείσα μάσκα υποδικτύου θα αποθηκευτεί στον τομέα Subnet_Mask ενός νέου αρχείου στον πίνακα υποδικτύου. Αφότου καθοριστεί η Subnet_Mask, ο τομέας Subnet_ID τίθεται από το λογικό -ΚΑΙ- της μάσκας υποδικτύου και της IP διεύθυνσης του AP.

Μετά από αυτό, πρέπει περαιτέρω να καθορίσουμε τον προεπιλεγμένο δρομολογητή του υποδικτύου. Για ένα AP, ο προεπιλεγμένος δρομολογητής του υποδεικνύεται στον πίνακα δρομολόγησης, ο οποίος μπορεί να ανακτηθεί από το SNMP. Στον πίνακα *ipRouteTable του* MIB II, (δηλ. ο πίνακας δρομολόγησης), η εγγραφή με τιμή " 0.0.0.0 " στο αντικείμενο *ipRouteDest* δείχνει μια προεπιλεγμένη διαδρομή. Η τιμή του αντικειμένου *ipRouteNextHop* στην είσοδο προεπιλεγμένων διαδρομών θα είναι η διεύθυνση IP του προεπιλεγμένου δρομολογητή. Κατά συνέπεια, ο τομέας Default_Router καθορίζεται. Κατόπιν, επίσης από το SNMP, καθορίζουμε την τιμή του τομέα Interface_Index από το MIB που αποθηκεύεται στον προεπιλεγμένο δρομολογητή. Στον πίνακα *ipAddrTable*, που καθορίζεται στο MIB II του προεπιλεγμένου δρομολογητή, βρίσκουμε μια εγγραφή που αντιστοιχεί στην IP διεύθυνση του προεπιλεγμένου δρομολογητή. Το Interface Index τίθεται στην τιμή του αντικειμένου *ipAdEntI - fIndex*. Αφότου έχουμε επισκεφτεί όλα τα APs μέσω του SNMP, όλα τα υποδίκτυα έχουν βρεθεί και χτίζεται ο πίνακας υποδικτύου. Το σχήμα 4.2 απεικονίζει μια χαρακτηριστική διαμόρφωση WLAN και τον αντίστοιχο πίνακα υποδικτύου του. Παρακάτω, επιδεικνύουμε πώς η χαρτογράφηση διευθύνσεων IP-to-MAC γίνεται με την βοήθεια του πίνακα υποδικτύου. Έχοντας υπόψη μας την IP διεύθυνση μιας κινητής συσκευής, ψάχνουμε τον πίνακα υποδικτύου για να βρούμε το υποδίκτυο που περιέχει τη δεδομένη IP διεύθυνση. Καθώς το υποδίκτυο βρίσκεται, αναγνωρίζουμε τον προεπιλεγμένο δρομολογητή ο οποίος έχει τη MAC διεύθυνση της κινητής συσκευής. Η MAC διεύθυνση θα είναι στον πίνακα *ipNetToMediaTable* του δρομολογητή. Ο πίνακας *ipNetToMediaTable*, που καθορίζεται στο MIB II, συντάσσεται κατά περιεχόμενο διεπαφών και IP διεύθυνση. Επομένως, με τη χρησιμοποίηση της τιμής Interface_Index που αποθηκεύεται στον πίνακα υποδικτύου και τη γνωστή IP διεύθυνση ως προσδιοριστικό περίπτωσης, μπορούμε να χρησιμοποιήσουμε ένα απλό SNMP get-request για να λάβουμε το αντικείμενο *ipNetToMediaPhys Address* στον πίνακα *ipNetToMediaTable*. Η τιμή που θα λάβουμε θα είναι η MAC διεύθυνση της κινητής συσκευής που παρατηρείται από το προεπιλεγμένο δρομολογητή.

4.6 Χρήση ιδιωτικών διευθύνσεων IP

Είναι πιθανό σε ένα WLAN hotspot ότι σε μια κινητή συσκευή ορίζεται μια ιδιωτική IP διεύθυνση λόγω των περιορισμένων διαθέσιμων IP διευθύνσεων. Κατά συνέπεια, οι κινητές συσκευές σε διαφορετικά WLAN hotspots μπορεί να έχουν την ίδια ιδιωτική IP διεύθυνση. Αυτό υπονοεί ότι δεν μπορούμε να προσδιορίσουμε μια μοναδική κινητή συσκευή άμεσα από την ιδιωτική IP διεύθυνση της. Συνήθως, οι LBSs βρίσκονται στο δημόσιο Διαδίκτυο. Για να χρησιμοποιήσει LBSs, μια

κινητή συσκευή με ιδιωτική IP διεύθυνση πρέπει να έχει μια μεταφρασμένη δημόσια IP διεύθυνση μέσω μιας NAT (Network Address Translation) συσκευής. Η χρήση των ιδιωτικών IP διευθύνσεων μπορεί να περιπλέξει την ανωτέρω IP–σε-MAC χαρτογράφηση διευθύνσεων, επειδή η IP διεύθυνση μιας κινητής συσκευής που αναγνωρίζεται από μια LBS είναι διαφορετική από την πραγματική ιδιωτική IP διεύθυνση που χρησιμοποιείται από την κινητή συσκευή σε ένα WLAN Hotspot. Η IP διεύθυνση μιας κινητής συσκευής που φαίνεται από τον προεπιλεγμένο δρομολογητή της είναι ιδιωτική, ενώ η LBS ξέρει μόνο τη μεταφρασμένη IP διεύθυνση της κινητής συσκευής. Επομένως, εάν εφαρμόζονται οι ιδιωτικές IP διευθύνσεις αλλά και NAT μέσα σε WLAN hotspots, χρειαζόμαστε επίσης χαρτογράφηση IP διευθύνσεων από δημόσια-σε-ιδιωτική πριν εκτελεστεί η ανωτέρω χαρτογράφηση διευθύνσεων Ip-σε-MAC.



Σχημα 4.2 – Διαμόρφωση WLAN και ο πίνακας υποδικτύων

4.7 Χαρτογράφηση διευθύνσεων IP από δημόσια -σε-ιδιωτική

Υπάρχουν διάφοροι τρόποι μετάφρασης διευθύνσεων δικτύων που υποστηρίζονται στις τρέχουσες συσκευές NAT. Συνήθως , μια ιδιωτική IP διεύθυνση μεταφράζεται σε μια δημόσια. Μια εναλλακτική προσέγγιση είναι η μετάφραση ενός συνόλου ιδιωτικών IP διευθύνσεων στις ίδιες δημόσιες διευθύνσεις IP αλλά με διαφορετικά ports. Αυτό ονομάζεται NAPT (Network Address Port Translation).Εάν χρησιμοποιούμε NAPT, τότε πρέπει να ξέρουμε το τρέχων port που χρησιμοποιείται από την κινητή συσκευή που προσπαθεί να χρησιμοποιήσει τη LBS. Σε αυτήν την περίπτωση, η LBS θα πρέπει να γνωρίζει το χρησιμοποιούμενο

port και να το στείλει μαζί με τη διεύθυνση IP της κινητής συσκευής στον διακομιστή θέσης. Γενικά, μια LBS υλοποιημένη σαν εφαρμογή web, δεν γνωρίζει τον αριθμό των port μιας σύνδεσης HTTP. Επομένως, εξετάζουμε μόνο τις βασικές μεταφράσεις διευθύνσεων δικτύου. Δηλαδή η ιδιωτική διεύθυνση IP μιας κινητής συσκευής θα δεσμευθεί σε μια μοναδική δημόσια διεύθυνση IP. Για να παρέχει τη χαρτογράφηση διευθύνσεων IP από δημόσια -σε- ιδιωτική, ο διακομιστής θέσης διατηρεί αρχικά τις πληροφορίες διευθύνσεων της IP pool για κάθε συσκευή NAT που περιλαμβάνεται στα WLAN hotspots που παρέχουν LBSs. Η IP pool για μια NAT συσκευή είναι το σύνολο δημόσιων διευθύνσεων IP που μπορούν να αποδοθούν από την συσκευή NAT. Συνήθως, μόνο μια συσκευή NAT απαιτείται για δίκτυα μέσα στον ίδιο ιδιωτικό χώρο διευθύνσεων. Επομένως, ο αριθμός συσκευών NAT είναι συνήθως μικρός. Επάνω στη λήψη της δημόσιας διεύθυνσης IP μιας κινητής συσκευής από μια LBS, ο διακομιστής θέσης καθορίζει σε ποια address pool ανήκει η διεύθυνση IP. Εάν υπάρχει μια address pool που περιέχει τη διεύθυνση IP, ανακαλύπτουμε ποια συσκευή NAT εκτελεί τη μετάφραση διευθύνσεων για την κινητή συσκευή. Κατόπιν, με την αποστολή ενός μηνύματος ερώτησης διευθύνσεων με τη δημόσια διεύθυνση IP, ο διακομιστής θέσης ζητά την αντίστοιχη ιδιωτική διεύθυνση IP από την συσκευή NAT. Κατά συνέπεια, γίνεται η χαρτογράφηση διευθύνσεων από δημόσια -σε- ιδιωτική, και ακολουθεί η χαρτογράφηση διευθύνσεων IP-σε-MAC. Είναι πιθανό η δημόσια διεύθυνση IP της κινητής συσκευής να μην είναι σε καμία address pool. Σε αυτήν την περίπτωση, ξέρουμε ότι η κινητή συσκευή βρίσκεται στο δημόσιο Διαδίκτυο. Κατά συνέπεια, δεν απαιτείται η χαρτογράφηση διευθύνσεων από δημόσια -σε- ιδιωτική, και μπορούμε να χρησιμοποιήσουμε τη δημόσια διεύθυνση IP για να εκτελέσουμε την χαρτογράφηση διευθύνσεων IP-σε-MAC.

Συνήθως στους δρομολογητές ενσωματώνονται λειτουργίες NAT. Οι περισσότεροι δρομολογητές υποστηρίζουν το SNMP. Κατά συνέπεια, ο πίνακας μετάφρασης διευθύνσεων NAT που αποθηκεύεται σε έναν δρομολογητή μπορεί να γίνει προσβάσιμος μέσω του SNMP. Παραδείγματος χάριν, οι περισσότεροι δρομολογητές Cisco με λειτουργίες NAT υποστηρίζουν το NAT MIB. Το *natAddrBindTable* στο NAT MIB φυλάσσει τις πληροφορίες χαρτογράφησης μεταξύ των δημόσιων και ιδιωτικών διευθύνσεων. Επομένως, μπορούμε να χρησιμοποιήσουμε το SNMP για να εφαρμόσουμε την ερώτηση διευθύνσεων από το διακομιστή θέσης προς μια συσκευή NAT. Στην περίπτωση της απουσίας υποστήριξης SNMP στις συσκευές NAT, ένα ειδικό πρωτόκολλο απαιτείται για να παρέχει την ερώτηση διευθύνσεων.

4.8 Αναγνωρίζοντας APs με ιδιωτικές IP διευθύνσεις

Ένα άλλο ζήτημα στη χρήση των ιδιωτικών διευθύνσεων είναι ότι τα APs καθώς επίσης και οι προεπιλεγμένοι δρομολογητές τους μπορούν επίσης να βρίσκονται σε ιδιωτικά δίκτυα. Επομένως, περισσότερα από ένα AP μπορούν να έχουν την ίδια ιδιωτική διεύθυνση IP. Κατά συνέπεια, κατά τη λήψη μιας παγίδας σχετικής με τη σύνδεση (association-related trap) από ένα AP, ο διακομιστής θέσης δεν μπορεί να καθορίσει το AP από το πεδίο διεύθυνσης του trap message. Αυτό φέρνει δυσκολίες στον καθορισμό της τρέχουσας θέσης μιας κινητής μονάδας. Γενικά, τοποθετούμε τον διακομιστή θέσης στο δημόσιο Διαδίκτυο για να τον καταστήσουμε προσιτό από τις LBSs. Κατά συνέπεια, ένα trap message που στέλνεται στον διακομιστή θέσης θα διαβιβαστεί επίσης μέσω μιας συσκευής NAT. Το πεδίο

source ip address στην επικεφαλίδα IP της παγίδας θα αλλάξει σε μια δημόσια, ενώ το πεδίο agent address παραμένει αμετάβλητο. Επομένως, ο διακομιστής θέσης θα λάβει και τις δημόσιες και ιδιωτικές διευθύνσεις ενός AP. Όπως στην ανωτέρω από δημόσια-σε-ιδιωτική χαρτογράφηση διευθύνσεων, μπορούμε να χρησιμοποιήσουμε τη δημόσια διεύθυνση IP για να καθορίσουμε την συσκευή NAT διαβιβάζοντας την παγίδα. Δεδομένου ότι είναι αδύνατο δύο APs με την ίδια ιδιωτική διεύθυνση IP να στέλνουν τις παγίδες μέσω της ίδιας συσκευής NAT, μπορούμε να προσδιορίσουμε ένα AP από την ιδιωτική IP διεύθυνση του και την συσκευή NAT.

Οι προεπιλεγμένοι δρομολογητές των APs μπορούν επίσης να βρίσκονται σε ιδιωτικά δίκτυα. Ο διακομιστής θέσης θα έχει πρόσβαση σε αυτούς από το δημόσιο Διαδίκτυο. Για να διαχειρίζεται από δημόσια δίκτυα, κάθε δρομολογητής πρέπει να είναι προσιτός έχοντας μιας στατική δημόσια διεύθυνση IP, η οποία μπορεί να ρυθμιστεί σε μια συσκευή NAT. Η διεύθυνση IP πρέπει επίσης να είναι γνωστή εκ των προτέρων από τον διακομιστή θέσης, ο οποίος αποθηκεύει τη διεύθυνση IP στο πεδίο Default_Router του πίνακα υποδικτύου της βάσης δεδομένων θέσης.

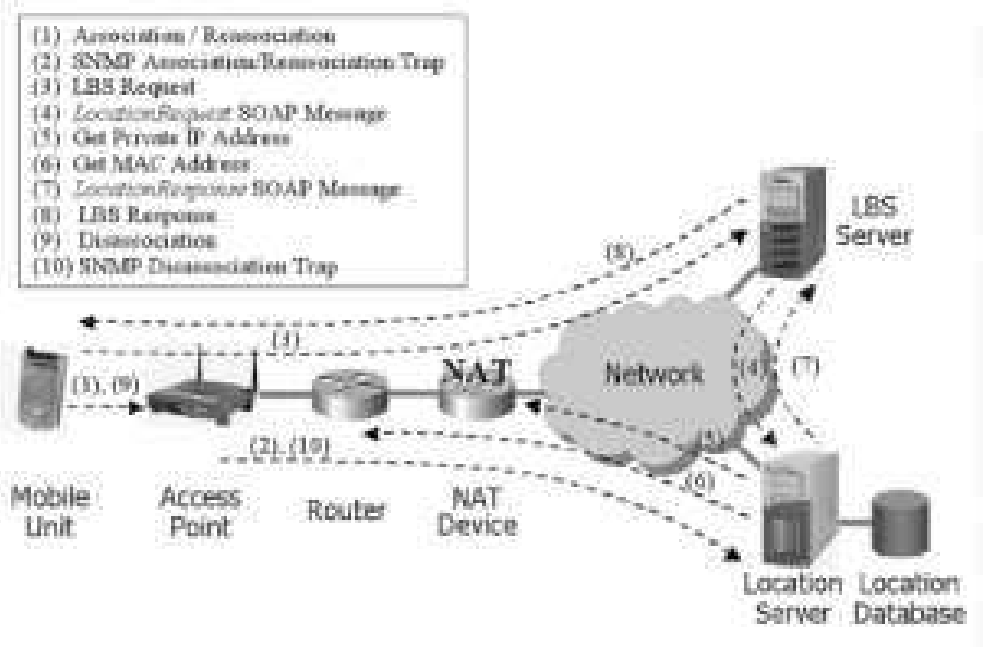
4.9 Ένα πλαίσιο υπηρεσιών ιστού για WLAN LBSs

Για να υπάρξει ένας τυποποιημένος τρόπος ανάπτυξης LBSs στα περιβάλλοντα WWW, προτείνεται ένα πλαίσιο υπηρεσιών Ιστού για LBSs σε WLAN hotspots. Το πλαίσιο υπηρεσιών Ιστού, όπως φαίνεται στο σχήμα 4.3, αποτελείται από τις κινητές μονάδες, WLAN APs με τους προεπιλεγμένους δρομολογητές προεπιλογής, τις συσκευές NAT, τους διακομιστές web, και έναν διακομιστή θέσης με μια βάση δεδομένων θέσης. Οι κινητές μονάδες είναι εκείνες οι κινητές συσκευές που ζητούν LBSs μέσω των web browsers. Τα WLAN APs με τους προεπιλεγμένους δρομολογητές τους παρέχουν μαζί τις απαραίτητες πληροφορίες διαχείρισης για τους προσδιορισμούς θέσης. Αυτό το πλαίσιο περιλαμβάνει επίσης τις συσκευές NAT για να επιτρέψει τη χρήση των ιδιωτικών διευθύνσεων IP. Εάν τα WLANs βρίσκονται στο δημόσιο Διαδίκτυο, τότε δεν απαιτούνται συσκευές NAT. Οι LBSs βρίσκονται σε web servers. Ο διακομιστής θέσης είναι το μέρος όπου εκτελείται ο προσδιορισμός θέσης. Όλες οι πληροφορίες θέσης αποθηκεύονται στη βάση δεδομένων θέσης. Το σχέδιο του πλαισίου υπηρεσιών ιστού λαμβάνει υπόψη τις περισσότερες πιθανές διαμορφώσεις των WLAN hotspots. Ακόμα υπάρχουν μερικοί περιορισμοί. Κατ' αρχάς, ο προεπιλεγμένος δρομολογητής ενός AP πρέπει να είναι επίσης ο ίδιος με εκείνο των κινητών συσκευών που έχουν πρόσβαση στο WLAN μέσω του AP. Δεύτερον, εάν εφαρμόζεται NAT, η ιδιωτική διεύθυνση IP της κινητής συσκευής πρέπει να αντιστοιχίζεται σε μια μοναδική δημόσια διεύθυνση IP. Επιπλέον, ο προσδιορισμός θέσης μπορεί να αυξήσει τη λανθάνουσα κατάσταση (latency) που υφίσταται σε LBSs. Πρόσθετη κυκλοφορία θα εισαχθεί επίσης στα συνδεμένα ενσύρματα δίκτυα.

Για την παροχή ενός τυποποιημένου τρόπου ώστε να έχουμε πρόσβαση στις πληροφορίες θέσης, σχεδιάζουμε μια υπηρεσία ιστού στον διακομιστή θέσης. Η υπηρεσία ιστού παρέχει τις υπηρεσίες ερώτησης θέσης χρησιμοποιώντας το SOAP (Simple Object Access Protocol). Οι διακομιστές δικτύου μπορούν να λάβουν τις πληροφορίες θέσης μέσω μηνυμάτων SOAP. Το SOAP είναι ένα πρωτόκολλο

βασισμένο στο XML για την ανταλλαγή των πληροφοριών σε web περιβάλλοντα. Το πρωτόκολλο SOAP μεταξύ διακομιστών δικτύου και του διακομιστή θέσης υλοποιείται πάνω σε HTTP. Στο προτεινόμενο πλαίσιο υπηρεσιών ιστού, καθορίζονται δύο μηνύματα SOAP. Το μήνυμα SOAP *LocationRequest*, που στέλνεται από τους διακομιστές δικτύου, περιέχει μια ενιαία παράμετρο την *muIP* για να φέρει τη διεύθυνση IP μιας κινητής μονάδας η θεση της οποίας πρόκειται να καθοριστεί Το μήνυμα SOAP *LocationResponse*, σταλμένο από το διακομιστή θέσης, χρησιμοποιείται για να επιστρέψει το αποτέλεσμα ενός προηγούμενου αιτήματος θέσης. Το μήνυμα SOAP *LocationResponse* περιλαμβάνει δύο παραμέτρους: *muIP* και *θέση*. Η παραμετρος *muIP* είναι η ίδια όπως στο μήνυμα SOAP *LocationRequest*. Η παράμετρος *θέσης* δείχνει την τρέχουσα θέση της κινητής μονάδας.

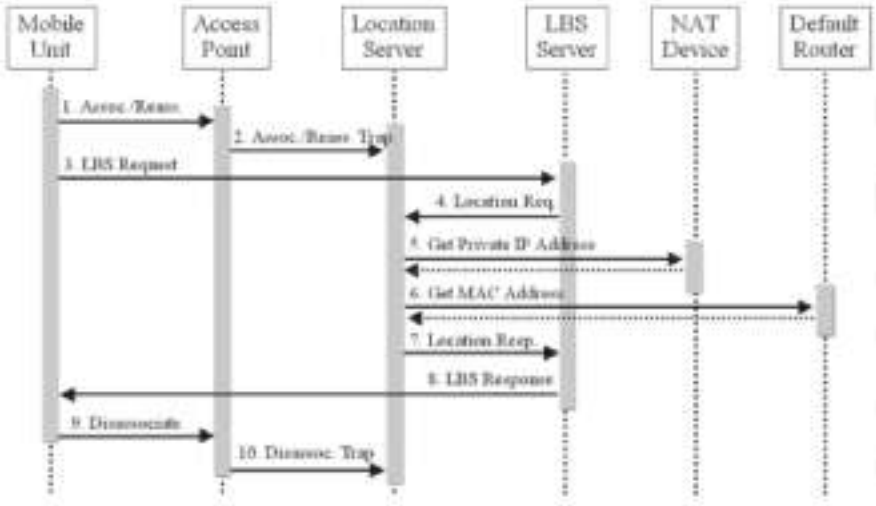
Το σχήμα 4.3 επεξηγεί τις αλληλεπιδράσεις μεταξύ των συστατικών του πλαισίου υπηρεσιών ιστού. Το σχήμα 4.4 είναι το διάγραμμα ακολουθίας του πλαισίου υπηρεσιών ιστού, όπως περιγράφεται παρακάτω.



Σχήμα 4.3 – Ένα πλαίσιο υπηρεσιών ιστού για WLAN LBSs

1. Μια κινητή μονάδα συνδέεται (reassociation) με ένα AP.
2. Αφότου γίνεται η σύνδεση (reassociation), το AP στέλνει μια παγίδα σύνδεσης SNMP (SNMP association trap) στον διακομιστή θέσης. Ο διακομιστής θέσης αποθηκεύει τη διεύθυνση MAC της κινητής μονάδας με την ταυτότητα του AP στον πίνακα συσχετισμού της βάσης δεδομένων θέσης.
3. Η κινητή μονάδα χρησιμοποιεί έναν web browser για να έχει πρόσβαση στη LBS σε έναν διακομιστή δικτύου. Το αίτημα για μια LBS στέλνεται μέσω ενός αιτήματος HTTP.
4. Ο διακομιστής δικτύου εξάγει τη IP διεύθυνση της κινητής μονάδας από το αίτημα HTTP και στέλνει έπειτα ένα μήνυμα SOAP *LocationRequest* στον διακομιστή θέσης.

5. Με τη λήψη ενός μηνύματος SOAP *LocationRequest*, ο διακομιστής θέσης παίρνει τη δημόσια διεύθυνση IP της κινητής μονάδας, και βρίσκει την address pool που περιέχει τη διεύθυνση IP. Εάν βρεθεί η address pool, καθορίζεται η συσκευή NAT που κάνει μετάφραση της διεύθυνσης IP της κινητής μονάδας. Κατόπιν, με την αποστολή ενός μηνύματος ερώτησης διευθύνσεων στη συσκευή NAT, ο διακομιστής θέσης λαμβάνει την τρέχουσα ιδιωτική διεύθυνση IP της κινητής μονάδας. Εάν ο διακομιστής θέσης δεν μπορεί να βρει την address pool που περιέχει τη δημόσια διεύθυνση IP, η κινητή μονάδα βρίσκεται στο δημόσιο Διαδίκτυο. Κατά συνέπεια, η δημόσια διεύθυνση IP είναι η αρχική διεύθυνση IP της κινητής συσκευής.
6. Μετά από τον καθορισμό της αρχικής διεύθυνσης IP της κινητής μονάδας, ο διακομιστής θέσης αναφέρεται στον πίνακα υποδικτύου στη βάση δεδομένων θέσης για να καθορίσει το προεπιλεγμένο δρομολογητή της διεύθυνσης IP. Κατόπιν, ο διακομιστής θέσης στέλνει ένα SNMP get-request στον προεπιλεγμένο δρομολογητή για να αποκτηθεί η αντίστοιχη διεύθυνση MAC.
7. Αφότου λαμβάνεται η διεύθυνση MAC της κινητής μονάδας, ο διακομιστής θέσης αναφέρεται στον πίνακα συσχετισμού για να καθορίσει το AP με το οποίο συνδέεται η κινητή μονάδα. Κατόπιν, ο διακομιστής θέσης στέλνει τις καθορισμένες πληροφορίες θέσης στον διακομιστή δικτύου μέσω ενός μηνύματος SOAP *LocationResponse*.
8. Ο διακομιστής δικτύου λαμβάνει τις πληροφορίες θέσης από το λαμβανόμενο μήνυμα SOAP και προετοιμάζει έπειτα τις πληροφορίες εξαρτώμενες από τη θέση για την κινητή μονάδα σε μια ιστοσελίδα. Η ιστοσελίδα στέλνεται έπειτα στην κινητή μονάδα μέσω μιας απάντησης HTTP.
9. Η κινητή μονάδα διαχωρίζεται από το AP.
10.Το AP στέλνει μια παγίδα αποσύνδεσης SNMP στον διακομιστή θέσης. Ο διακομιστής θέσης στη συνέχεια διαγράφει την έγγραφη για την κινητή συσκευή από



τον πίνακα συσχετισμού.

Σχημα 4.4 – Διαγραμμα ακολουθιας του πλαισιου υπηρεσιων ιστου για WLAN LBSs

Το πλαίσιο υπηρεσιών ιστού για WLAN LBSs δεν χρειάζεται την υποστήριξη πρόσθετων υπηρεσιών, όπως οι RADIUS και DHCP servers στις προηγούμενες προσεγγίσεις. Το πλαίσιο είναι επίσης ανεξάρτητο από τις διαμορφώσεις των WLAN hotspots, ανεξάρτητα από το πώς τα APs συνδέονται με το ενσύρματο δίκτυο. Επιπλέον, το πλαίσιο υπηρεσιών ιστού παρέχει μια ομοιόμορφη προσέγγιση για την πρόσβαση των πληροφοριών θέσης με τη βοήθεια

μιας τυποποιημένης διεπαφής SOAP. Επομένως, LBSs μπορούν να αναπτυχθούν ανεξάρτητα χωρίς να εξεταστούν οι λεπτομέρειες της θέσης.

4.10 Συμπεράσματα

Στην προσπάθεια μας να εξετάσουμε το κατά πόσο είναι δυνατή η υλοποίηση κάποιου είδους LBSs στο χώρο του ΤΕΙ Χανίων βρεθήκαμε αντιμέτωποι με αρκετά προβλήματα. Κυριότερο εκ των προβλημάτων ήταν η ελλιπής βιβλιογραφία πάνω στην διαδικασία υλοποίησης τέτοιων υπηρεσιών. Έτσι αποφασίσαμε να ξεκινήσουμε τη μελέτη με ότι πληροφορίες μπορέσαμε να αντλήσουμε από διάφορες πήγες. Επίσης το AP που είχαμε στη διάθεση μας δεν ξέραμε κατά πόσο είναι ικανό να συνεργαστεί με το Simple Network Management Protocol (SNMP) μιας και δεν αναφερόταν κάτι σχετικό στο εγχειρίδιο που το συνόδευε και η προσπάθεια μας για βοήθεια - υποστήριξη από την εταιρία παραγωγής του δεν απέδωσε.

Εφόσον η υλοποίηση LBSs δεν ήταν δυνατή κάτω από τις υπάρχουσες συνθήκες και μέσα στα προβλεπόμενα χρονικά όρια, αποφασίστηκε με τη σύμφωνη γνώμη του επιβλέποντα καθηγητή να γίνει απλά αναφορά επί του θέματος. Έχουμε την πεποίθηση ότι λαμβάνοντας κάποιος υπόψη το προτεινόμενο πλαίσιο και έχοντας συμβατό εξοπλισμό, θα έχει πολύ πιο εύκολο έργο στην προσπάθεια του να υλοποιήσει τέτοιου είδους υπηρεσίες στο υπάρχον WLAN.

ΚΕΦΑΛΑΙΟ 5

Αποτελέσματα ραδιοκάλυψης του WLAN

5.1 Πληροφορίες WLAN - Μετρήσεις, βελτιστοποίηση απόδοσης

Με την παρουσίαση των ασύρματων τεχνολογιών δικτύωσης, οι διαχειριστές δικτύων αντιμετωπίζουν μια δύσκολη πρόκληση. Όχι μόνο πρέπει να εξετάσουν πώς να εφαρμόσουν με ασφάλεια τα ασύρματα δίκτυα στην επιχείρησή τους, αλλά πρέπει επίσης να μετριάσουν τους κινδύνους που συνδέονται με τα AP εξαπάτησης (rogue APs) και τις παρεμβολές από άλλες συσκευές που χρησιμοποιούν το ίδιο φάσμα συχνότητας. Δυστυχώς, αυτό απαιτεί εκπαίδευση και εργαλεία που δεν είναι πάντα εύκολο να αγοραστούν, ειδικά για τις μικρότερες επιχειρήσεις με χαμηλό προϋπολογισμό.

Μια τυπική ερώτηση που θα μπορούσε να γίνει είναι : "γιατί θα έπρεπε να με ενδιαφέρει τι άλλο χρησιμοποιεί το φάσμα 2.4GHz (ή 5.8GHz);" Κατ' αρχάς, όταν στήνεται και αναπτύσσεται ένα ασύρματο δίκτυο, είναι σημαντικό να είναι γνωστό τι άλλο χρησιμοποιεί το ίδιο φάσμα συχνότητας. Εάν εκείνο το φάσμα είναι διαποτισμένο με ενέργεια από άλλες ασύρματες συσκευές, όπως Bluetooth συσκευές, ασύρματα τηλέφωνα, και άλλα, το ασύρματο δίκτυο δεν θα λειτουργήσει όπως αναμένεται. Δεύτερον, και το πιο σημαντικό, υπάρχουν διάφορες συσκευές επικοινωνίας που μπορούν να λειτουργήσουν στο ανοικτό φάσμα συχνοτήτων και μπορούν να παρέχουν στον επιτιθέμενο, είσοδο με πλάγιο τρόπο (backdoor entry) σε μια ανυποψίαστη επιχείρηση.

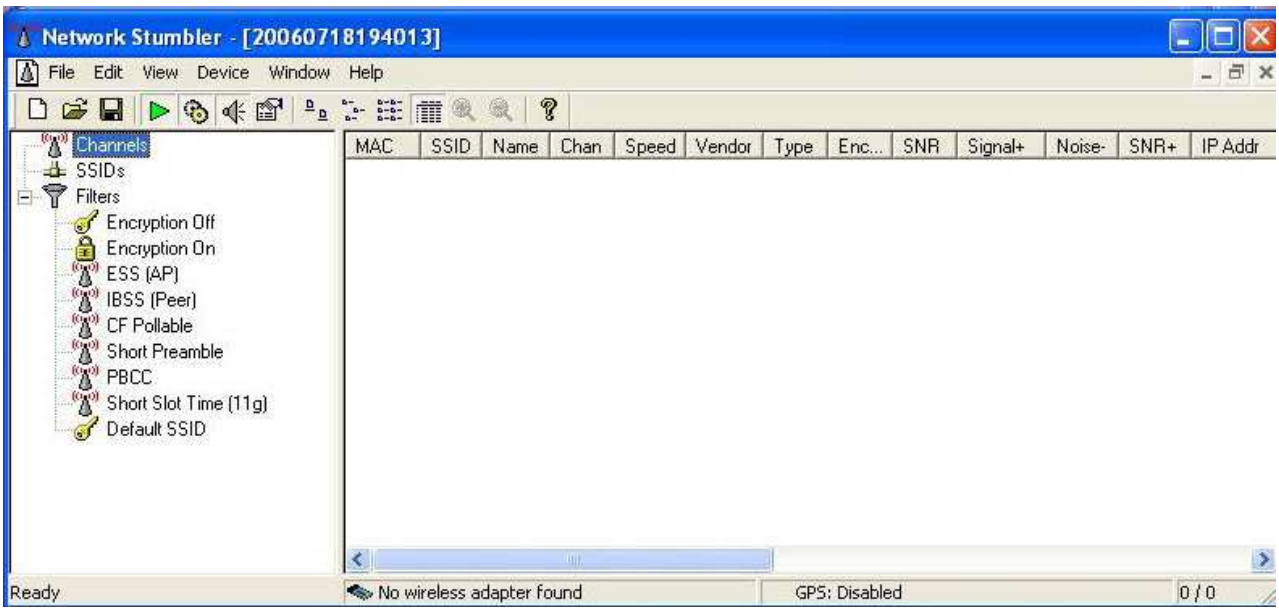
Το NetStumbler του Mario Milner ήταν ο πρώτος ανιχνευτής για hotspots, και ο καλύτερος. Παρέχει τις περισσότερες πληροφορίες για ένα hotspot σε μια εύκολα κατανοητή μορφή, και είναι ελεύθερο στους χρήστες(freeware). Η βασική λειτουργία είναι βασισμένη στο να κάνει hopping μεταξύ των 14 διαθέσιμων καναλιών και να παρακολουθεί την κυκλοφορία. Το πρόγραμμα αυτό μπορεί είτε ενεργά να στείλει αιτήματα ελέγχων, στα οποία ένα σημείο πρόσβασης θα αποκριθεί, ή μπορεί απλά να «ακούσει» τα ραδιοκύματα. Εδώ θα πρέπει να τονιστεί ότι το πρόγραμμα λειτουργεί χρησιμοποιώντας το πρωτόκολλο 802.11 (στρώμα OSI 1 "2).

Μόλις εγκαταστήσουμε το NetStumbler (σχήμα 5.1 και 5.2), μπορούμε να ψάξουμε για ασύρματα δίκτυα και τη δύναμη των σημάτων τους, να επιθεωρήσουμε ποια κανάλια χρησιμοποιούνται, και να τα συγκρίνουμε έπειτα με ανταγωνιστικά δίκτυα για να παρακολουθήσουμε τις παρεμβολές. Μπορούμε να κατεβάσουμε από το internet τη μικρή αυτή εφαρμογή και να την εγκαταστήσαμε σε λιγότερο από πέντε λεπτά. Κανένα άλλο πρόγραμμα δεν παρέχει τόση λεπτομερή πληροφόρηση. Αυτό το περιεκτικό εργαλείο έρευνας έχει 22 στήλες που παρουσιάζουν τη δύναμη του σήματος, την κρυπτογράφηση, το θόρυβο, και πολλά άλλα. Στον πίνακα 5.1 μπορούμε να δούμε την ποικιλία πληροφοριών που μπορούμε να αντλήσουμε.

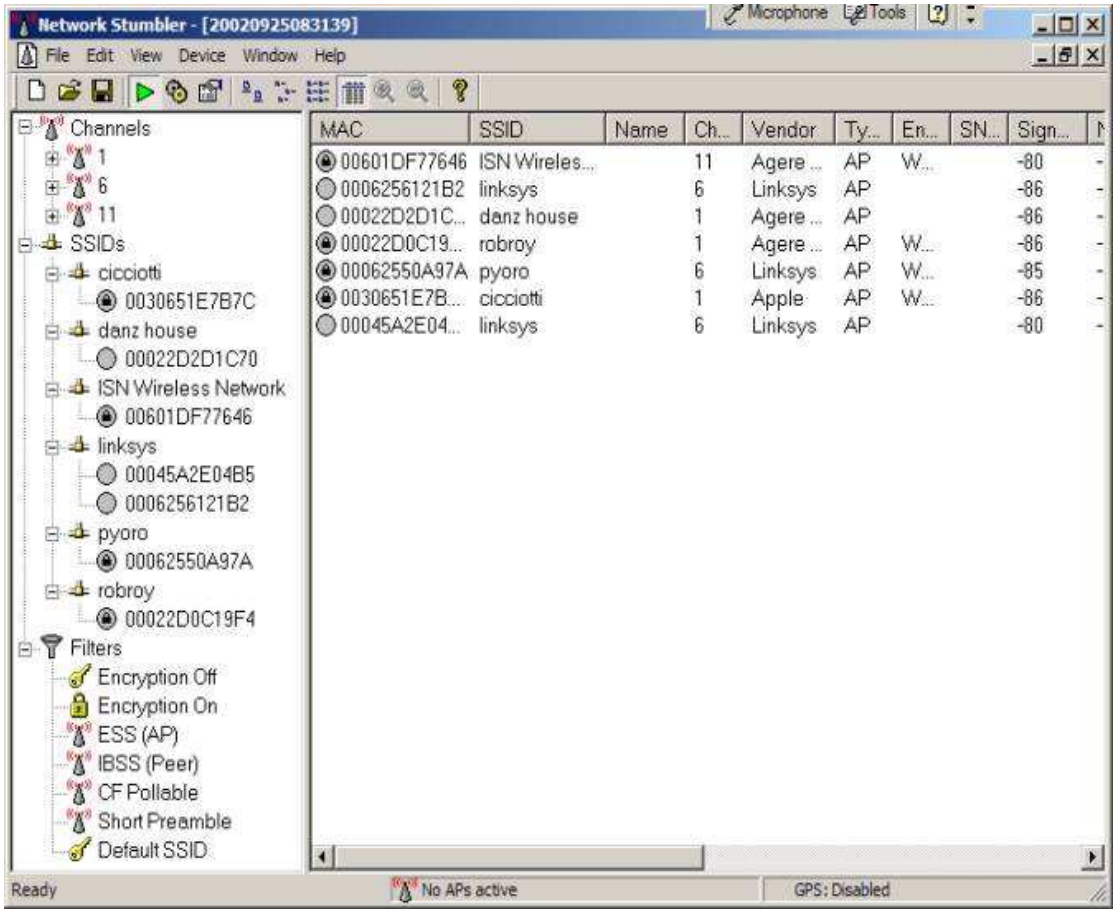
MAC	Κώδικας διευθύνσεων μηχανών. Μια μοναδική διεύθυνση για κάθε συσκευή Ethernet. Προηγείται ένα κυκλικό εικονίδιο που αλλάζει με βάση παράγοντες όπως η δύναμη του σήματος και η κωδικοποίηση.
SSID	Καθορισμένο προσδιοριστικό υπηρεσιών γνωστό και ως "όνομα δικτύου."
Name	Όνομα σημείου πρόσβασης. Συχνά είναι κενό, δεδομένου ότι δεν χρησιμοποιείται από όλες τις εταιρίες ασύρματου εξοπλισμού.
Chan	Ο αριθμός του καναλιού που λειτουργεί το δίκτυο. Στις επικοινωνίες 802.11b, 1 έως 14.
Speed	Η αναφερόμενη μέγιστη ταχύτητα του δικτύου, σε μεγαμπίτ ανά δευτερόλεπτο (Mbps).
Vendor	Όνομα του κατασκευαστή εξοπλισμού ή άλλο προσδιοριστικό εμπορικού σήματος.
Type	Τύπος δικτύου: είτε AP για σημείο πρόσβασης, είτε peer για peer-to peer.
Encryption	Εάν η ασύρματη κίνηση κρυπτογραφείται στο δίκτυο από τις ασύρματες συσκευές, χαρακτηρίζεται ως WEP.
SNR	Η αναλογία σήματος προς θόρυβο RF. Μετρημένη σε microvolt decibels (dBm). Ενεργή μόνο όταν βρισκόμαστε στην εμβέλεια ενός δικτύου.
Signal+	Το μέγιστο σήμα RF που εντοπίστηκε από τη συσκευή δικτύου σε dBm.
Noise-	Ο ελάχιστος θόρυβος RF που αναφέρθηκε στη συσκευή σε dBm.
SNR+	Η μέγιστη RF αναλογία σήματος προς θόρυβο που αναφέρθηκε στη συσκευή σε dBm.
IP Addr	Η αναφερόμενη διεύθυνση πρωτοκόλλου Διαδικτύου (Internet Protocol), εάν υπάρχει.
Subnet	Οποιοδήποτε αναφερόμενο υποδίκτυο IP, εάν υπάρχει.
Latitude	Το γεωγραφικό πλάτος όπως αναφερθηκε από το δέκτη GPS όταν το NetStumbler είδε το δίκτυο.
Longitude	Το γεωγραφικό μήκος όπως αναφέρθηκε από το δέκτη GPS όταν το NetStumbler είδε το δίκτυο.
First Seen	Ο χρόνος στον οποίο το NetStumbler πρωτοείδε το δίκτυο.

Last Seen	Ο χρόνος στον οποίον είδε το NetStumbler τελευταία φορά το δίκτυο.
Signal	Το τρέχον επίπεδο σήματος RF σε dBm. Ενεργό μόνο όταν βρισκόμαστε στην εμβέλεια ενός δικτύου.
Noise	Το τρέχον επίπεδο θορύβου RF σε dBm. Ενεργό μόνο όταν βρισκόμαστε στην εμβέλεια ενός δικτύου.
Flags	Σημαίες (flags) 802.11 από το δίκτυο σε δεκαεξαδικό κώδικα(Base 16).
Beacon Interval	Το διάστημα της ραδιομετάδοσης αναγνωριστικών σημάτων από το AP.
Distance	Η απόσταση στην οποία βρισκόμασταν όταν υπήρχε το καλύτερο SNR.

Πινακας 5.1 - Επεξήγηση των στηλών αναφοράς



Σχημα 5.1 - Το περιβάλλον του προγράμματος μετά την εγκατάσταση



Σχήμα 5.2 - Τυπική απεικόνιση αποτελεσμάτων μετά την αναζήτηση

Το απλό περιβάλλον απαριθμεί τη μέθοδο κρυπτογράφησης που χρησιμοποιείται, όπως WEP ή WPA , αλλά δεν επιδεικνύει περισσότερη λεπτομέρεια για τα χαρακτηριστικά γνωρίσματα ασφάλειας. Η ανικανότητα του NetStumbler ώστε να συνδεθεί στο ασύρματο δίκτυο και η έλλειψη λεπτομέρειας είναι τα μόνα πραγματικά μείον στο προϊόν.

Το πρόγραμμα χρησιμοποιείται συνήθως για:

- Wardriving
- Επαλήθευση της διαμόρφωσης δικτύου
- Εύρεση των θέσεων με κακή κάλυψη στα WLANs
- Ανίχνευση των αιτιών ασύρματων παρεμβολών
- Ανίχνευση μη εξουσιοδοτημένων AP ("rogue AP")
- Στόχευση κατευθυντικών κεραιών για συνδέσεις μεγάλων αποστάσεων μεταξύ WLANs

Ακολουθεί σύντομη αναφορά και παράδειγμα χρήσης με τις απαραίτητες ρυθμίσεις για κάθε μια από τις βασικές λειτουργίες του προγράμματος.

5.2.1 Διαδικασία Wardriving

"Wardriving" ονομάζεται η διαδικασία της ανίχνευσης και του εντοπισμού ασύρματων δικτύων. Το NetStumbler είναι ένα πολύ δημοφιλές εργαλείο για wardriving, εξαιτίας της ευκολίας στη χρήση του (και επιπρόσθετα εξαιτίας της συνεργασίας του με GPS).

- Ενεργοποιούμε το "Auto Reconfigure", για να εξασφαλίσουμε ότι θα βρεθούν όσο το δυνατόν περισσότερα ασύρματα LANs.
- Για να αποφύγουμε τη σύνδεση με τα δίκτυα που παρατηρούμε, πηγαίνουμε στο Network Control Panel και βγάζουμε την επιλογή TCP/IP από την κάρτα ασύρματου LAN μας.
- Προτείνεται η χρήση ενός δέκτη GPS.

5.2.2 Έλεγχος διαμόρφωσης του τοπικού ασύρματου LAN

Ένας διαχειριστής εταιρικού δικτύου χρειάζεται τη διαβεβαίωση ότι το ενσύρματο τοπικό LAN δεν εκτίθεται σε αναρμόδιους χρήστες. Αυτό μπορεί συχνά να συμβεί όταν οι χρήστες στήνουν δικό τους ασύρματο LAN για ευκολία. Τέτοια ασύρματα LANs έχουν συχνά ελάχιστη ή καμία ασφάλεια, γεγονός το οποίο θέτει έναν κίνδυνο για ολόκληρο το τοπικό LAN. Ο διαχειριστής του δικτύου μπορεί να χρησιμοποιήσει το NetStumbler για να ανιχνεύσει την παρουσία τέτοιων ασύρματων LANs εξαπάτησης (rogue).

- Ενεργοποιούμε το "Auto Reconfigure", για να εξασφαλίσουμε ότι θα βρεθούν όσο το δυνατόν περισσότερα ασύρματα LANs.
- Εάν το LAN μας χρησιμοποιεί DHCP, σιγουρευόμαστε ότι το DHCP είναι ενεργοποιημένο στην κάρτα ασυρμάτου δικτύου μας. Θα είμαστε σε θέση έπειτα να πούμε εάν τα δίκτυα που βρίσκουμε συνδέονται με το δίκτυό μας.

5.2.3 Επαλήθευση κάλυψης του ασύρματου LAN

Ο διαχειριστής ενός ασύρματου LAN μπορεί να χρησιμοποιήσει το NetStumbler για να ελέγξει αν μια περιοχή καλύπτεται ικανοποιητικά από ένα σήμα καλής ποιότητας. Το NetStumbler μπορεί επίσης να χρησιμοποιηθεί για να δούμε πόσο μακριά επεκτείνεται η περιοχή κάλυψης πέρα από το προοριζόμενο όριό της.

- Ρυθμίζουμε την κάρτα ασύρματου δικτύου με το SSID και τις άλλες παραμέτρους του δικτύου που θέλουμε να ελέγξουμε.
- Απενεργοποιούμε το "Auto Reconfigure", έτσι ώστε μόνο το επιθυμητό SSID να είναι ορατό.

5.2.4 Έρευνα περιοχών

Κατά την εγκατάσταση ενός WLAN ή την ανίχνευση λαθών, είναι σημαντικό να επιλεχτούν οι θέσεις και τα κανάλια κατά τέτοιο τρόπο ώστε οι παρεμβολές να ελαχιστοποιούνται. Μια έρευνα περιοχής τυπικά περιλαμβάνει την εύρεση των υπαρχόντων στοιχείων (φούρνοι μικροκυμάτων, ασύρματα τηλέφωνα, ραδιοπομποί) που χρησιμοποιούν τις ίδιες ραδιοσυχνότητες με το ασύρματο LAN. Μια έρευνα πρέπει να γίνεται πριν την εγκατάσταση ενός νέου ασύρματου LAN, και έπειτα οι επόμενες έρευνες πρέπει να εκτελούνται μετά από την εγκατάσταση. Μια πλήρης έρευνα περιοχής απαιτεί ειδικό υλικό όπως μια συσκευή ανάλυσης φάσματος RF, αλλά και το NetStumbler μπορεί επίσης να χρησιμοποιηθεί ως τμήμα μιας τέτοιας έρευνας.

- Ενεργοποιούμε το "Auto Reconfigure", για να εξασφαλίσουμε ότι θα βρεθούν όσο το δυνατόν περισσότερα ασύρματα LANs.
- Χρησιμοποιούμε μια κάρτα ασύρματου δικτύου που αναφέρει τα επίπεδα θορύβου. Τα υψηλά επίπεδα θορύβου είναι μια από τις τυπικές ενδείξεις παρεμβολών.
- Μια έρευνα μετά την εγκατάσταση θα πρέπει να συμπεριλάβει επαλήθευση κάλυψης, η οποία μπορεί να εκτελεσθεί με το "Auto Reconfigure" απενεργοποιημένο.
- Για να αποφύγουμε τη χρήση δικτύων που παρατηρούμε και δεν μας ανήκουν , πηγαίνουμε στο Network Control Panel και βγάζουμε την επιλογή TCP/IP από την κάρτα ασύρματου δικτύου.

5.2.5 Προσδιορισμός θέσης κεραιών

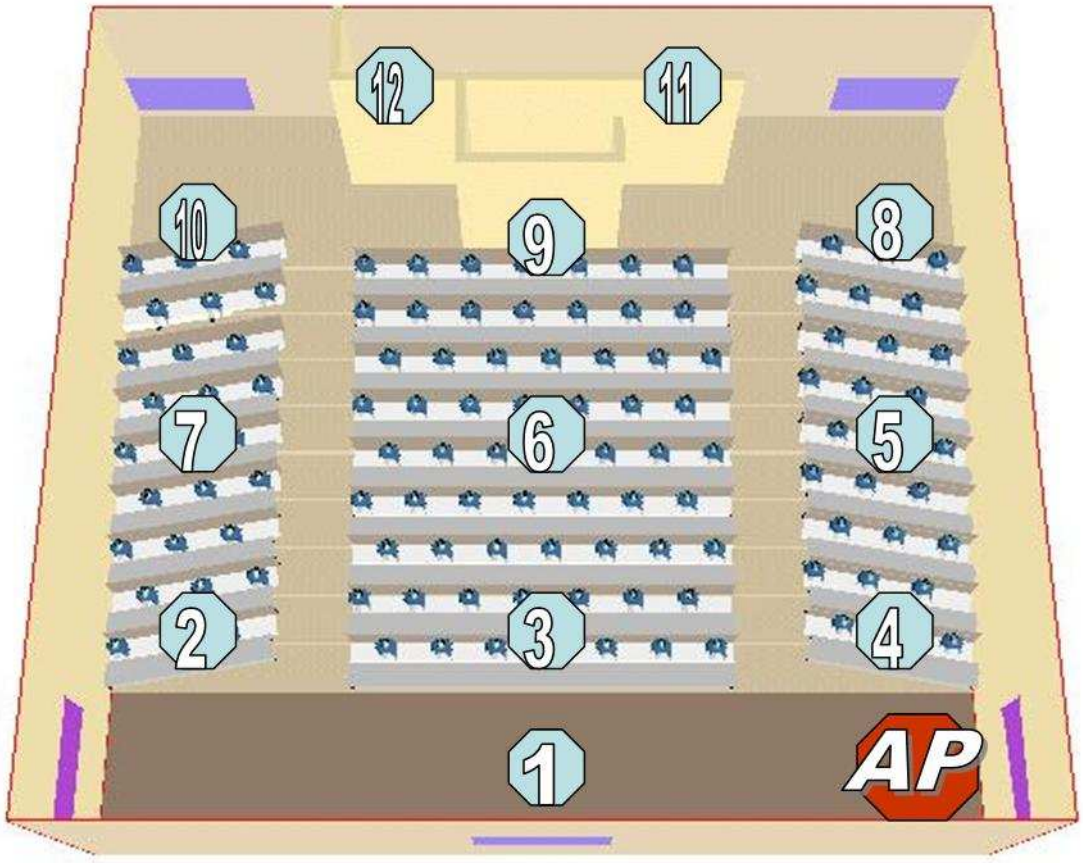
Κατά το στήσιμο μιας κεραίας, το NetStumbler μπορεί να χρησιμοποιηθεί ώστε να βοηθήσει για τη βέλτιστη θέση και στόχευση της κεραίας.

- Συνδέουμε την κεραία με ένα ασύρματο AP (ή μια WLAN κάρτα σε IBSS λειτουργία)
- Ρυθμίζουμε την κάρτα ασύρματου δικτύου με το SSID και τις άλλες παραμέτρους του απομακρυσμένου δικτύου.
- Απενεργοποιούμε το "Auto Reconfigure", έτσι ώστε μόνο το επιθυμητό SSID να είναι ορατό.

5.3.1 Μετρήσεις σε πραγματικό περιβάλλον

Μετά την παρουσίαση του περιβάλλοντος του προγράμματος Netstumbler και την σύντομη αναφορά στις κυριότερες λειτουργίες του, προχωρούμε στην συγκέντρωση μετρήσεων και στο σχολιασμό αυτών. Αυτό που κάναμε στην ουσία είναι η λειτουργία που περιγράφεται στο κεφάλαιο 5.2.3, δηλαδή επαλήθευση κάλυψης του ασυρμάτου δικτύου.

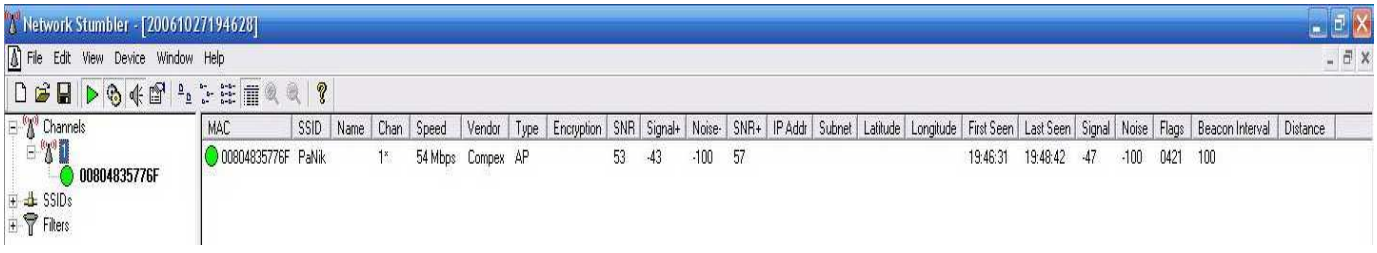
Περιβάλλον μετρήσεων: Ο server με το αντίστοιχο AP εγκαταστάθηκε στο χώρο του αμφιθεάτρου του ΤΕΙ Χανίων και συνδέθηκε με το ενσύρματο δίκτυο του ιδρύματος. Μετρήσεις ελήφθησαν σε διάφορες θέσεις του αμφιθεάτρου οι οποίες απεικονίζονται στο σχεδιάγραμμα 5.3. Στο σχήμα αυτό επίσης φαίνεται η θέση του



AP.

Σχήμα 5.3 - Σχεδιάγραμμα του αμφιθεάτρου του ΤΕΙ Χανίων

Διαδικασία μετρήσεων: Για την λήψη των μετρήσεων χρησιμοποιήθηκε ένας φορητός υπολογιστής στον οποίο είχε εγκατασταθεί το πρόγραμμα netstumbler. Ο χρήστης του υπολογιστή χρησιμοποίησε το το πρόγραμμα για να πάρει μετρήσεις στις θέσεις 1 έως 12. Ξεκινώντας από τη θέση 1 ελήφθησαν μετρήσεις σε όλες τις θέσεις ολοκληρώνοντας τη διαδικασία στη θέση 12. Αφού έγινε καταγραφή των μετρήσεων σε κάθε θέση ξεχωριστά **(σχήμα 5.4),** δημιουργήθηκε ο πίνακας ο οποίος συγκεντρώνει το σύνολο των μετρήσεων για ευκολία ανάλυσης και σχολιασμού (πίνακας 5.5).



Σχήμα 5.4 – Παράδειγμα της μπάρας μετρήσεων οι οποίες λαμβάνονται σε κάθε δεδομένη στιγμή μέτρησης

	1	2	3	4	5	6	7	8	9	10	11	12
MAC	00804835 776F	0080483 5776F	0080483 5776F	0080483 5776F	0080483 5776F	0080483 5776F	0080483 5776F	0080483 5776F	0080483 5776F	0080483 5776F	0080483 5776F	0080483 5776F
SSID	PaNik	PaNik	PaNik	PaNik	PaNik	PaNik	PaNik	PaNik	PaNik	PaNik	PaNik	PaNik
Chan	1*	1*	1*	1*	1*	1*	1*	1*	1*	1*	1*	1*
Speed	54 Mbps	54 Mbps	54 Mbps	54 Mbps	54 Mbps	54 Mbps	54 Mbps	54 Mbps	54 Mbps	54 Mbps	54 Mbps	54 Mbps
Vendor	Compex	Compex	Compex	Compex	Compex	Compex	Compex	Compex	Compex	Compex	Compex	Compex
Type	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP	AP
SNR	53	44	52	40	46	38	34	36	40	33	31	21
Signal+	-43	-43	-43	-43	-43	-43	-43	-43	-43	-43	-43	-43
Noise-	-100	-100	-100	-100	-100	-100	-100	-100	-100	-100	-100	-100
SNR+	57	57	57	57	57	57	57	57	57	57	57	57
First Seen	19:46:31	19:46:31	19:46:31	19:46:31	19:46:31	19:46:31	19:46:31	19:46:31	19:46:31	19:46:31	19:46:31	19:46:31
Last Seen	19:48:42	19:49:58	19:50:51	19:51:46	19:53:35	19:54:47	19:56:10	19:57:43	19:58:30	19:59:17	20:01:43	20:03:22
Signal	-47	-56	-48	-60	-54	-62	-66	-64	-60	-67	-69	-79
Noise	-100	-100	-100	-100	-100	-100	-100	-100	-100	-100	-100	-100
Flags	0420	0420	0420	0420	0420	0420	0420	0420	0420	0420	0420	0420
Beacon Interval	100	100	100	100	100	100	100	100	100	100	100	100

5.5 - Συγκεντρωτικός πίνακας μετρήσεων

5.3.2 Ανάλυση μετρήσεων

Ξεκινούμε την ανάλυση των μετρήσεων κάνοντας μια σύντομη αναφορά στις κατηγορίες μετρήσεων που εσκεμμένα δεν συμπεριλάβαμε στον πίνακα που παρουσιάζεται παραπάνω. Οι κατηγορίες αυτές είναι οι: Name, Encryption, Ip Addr, Subnet, Latitude, Longitude, Distance.

Name: όπως έχει αναφερθεί στην στήλη αυτή θα φαινόταν το όνομα του AP στην περίπτωση που αυτό προβλεπόταν από την εταιρία κατασκευης του. Στην περίπτωση μας η στήλη ήταν κενή.

Encryption: κατά την διαδικασία λήψης των μετρήσεων δεν χρησιμοποιήθηκε κάποιο encryption έτσι αυτή η στήλη ήταν επίσης κενή.

Ip Addr: στη συγκεκριμένη στήλη εμφανίζεται η IP του υπολογιστή στην περίπτωση που έχει συνδεθεί σε κάποιο δίκτυο.

Subnet: εδώ αντίστοιχα εμφανίζεται το υποδικτυο στο οποίο έχει συνδεθεί ο client.

Latitude, Longitude, Distance: για τη λήψη μετρήσεων στις τρεις αυτές κατηγορίες απαιτείται η σύνδεση του υπολογιστή με κάποια συσκευή GPS. Και οι τρεις αυτές κατηγορίες αναφέρονται σε μετρικές αποστάσεις και γεωγραφικό προσδιορισμό της θέσης του υπολογιστή-πελάτη ως προς το AP.

Συνεχίζουμε την ανάλυση κάνοντας αναφορά στις κατηγορίες οι οποίες έχουν μικρότερη σημασία σε σχέση με άλλες, στις οποίες θα δώσουμε μεγαλύτερο βάρος στο τελευταίο μέρος της ανάλυσης. Οι κατηγορίες αυτές είναι οι εξής: MAC, SSID, CHAN, Speed, Vendor, Type, Flags και Beacon Interval.

Στην στήλη MAC εμφανίζεται η διεύθυνση MAC του AP το οποίο έχει εντοπίσει το netstumbler και στη στήλη SSID το αντίστοιχο όνομα δικτυού το οποίο εκπέμπει το AP και το οποίο έχει καθοριστεί από τον διαχειριστή του δικτύου. Στην κατηγορία CHAN εμφανίζεται το κανάλι το οποίο χρησιμοποιεί το AP για να εκπέμψει δεδομένα. Στη συγκεκριμένη περίπτωση το κανάλι που χρησιμοποιείται είναι το κανάλι 1. Υπάρχουν 13 διαθέσιμα κανάλια λειτουργίας με βάση τις ευρωπαϊκές προδιαγραφές, 11 με βάση τις αμερικάνικες και 14 με βάση τις ιαπωνικές. Εάν υπήρχαν σε λειτουργία κι αλλά AP θα μπορούσαμε να αποφύγουμε τυχόν προβλήματα overlapping παρατηρώντας τη στήλη αυτή και επιλέγοντας για τα AP κανάλια που απέχουν αρκετά MHz μεταξύ τους (για παράδειγμα εφόσον υπάρχει ήδη ένα AP που λειτουργεί στο κανάλι 1 αν χρησιμοποιούσαμε και δεύτερο AP θα επιλέγαμε γι'αυτό κάποιο κανάλι μετά το 6ο). Στη στήλη Speed αναφέρεται η ανώτατη δυνατή ταχύτητα δικτύου που στην περίπτωση μας είναι τα 54Mbps όπως προβλέπεται από την τεχνολογία 802.11g. Η εταιρία κατασκευής του AP εμφανίζεται στην στήλη Vendor. Ακόμα στη στήλη Type βλέπουμε τον τύπο του δικτύου το οποίο εμφανίζεται ως AP (θα μπορούσε να αναφέρεται ως peer to peer αν είχαμε απευθείας ασύρματη δικτύωση δυο υπολογιστών χωρίς τη μεσολάβηση AP). Η στήλη Beacon Interval παρουσιάζει το διάστημα που μεσολαβεί μεταξύ της αναμετάδοσης των αναγνωριστικών σημάτων από το AP. Στα περισσότερα AP ο προεπιλεγμένος ρυθμός είναι 10 σήματα ανά δευτερόλεπτο, κάτι που συμβαίνει και στη δική μας περίπτωση (αναφέρεται ο αριθμός 100, που είναι σε ms, άρα σε ένα δευτερόλεπτο εκπέμπονται 10 σήματα). Τελειώνουμε την αναφορά στις μικρότερης σημασίας κατηγορίες με τη στήλη Flags στην οποία το πρόγραμμα netstumbler αναφέρει σε κωδικοποιημένη μορφή πληροφορίες για το δίκτυο μας όπως τον τύπο κωδικοποίησης και τον τύπο δικτύου, πληροφορίες που μπορούμε εξάλλου να αντλήσουμε και από τις ανάλογες στήλες.

Περνάμε στο τελευταίο μέρος των μετρήσεων. Εδώ βρίσκουμε μετρήσεις πολύ πιο σημαντικές ουσιαστικά για ένα ασύρματο δίκτυο αφού αναφέρονται στο εκπεμπόμενο σήμα, στο θόρυβο, και στον λόγο σήματος θορύβου. Τις μετρήσεις αυτές βρίσκουμε στις εξής στήλες: SNR, Signal+, Noise-, SNR+, Signal, Noise.

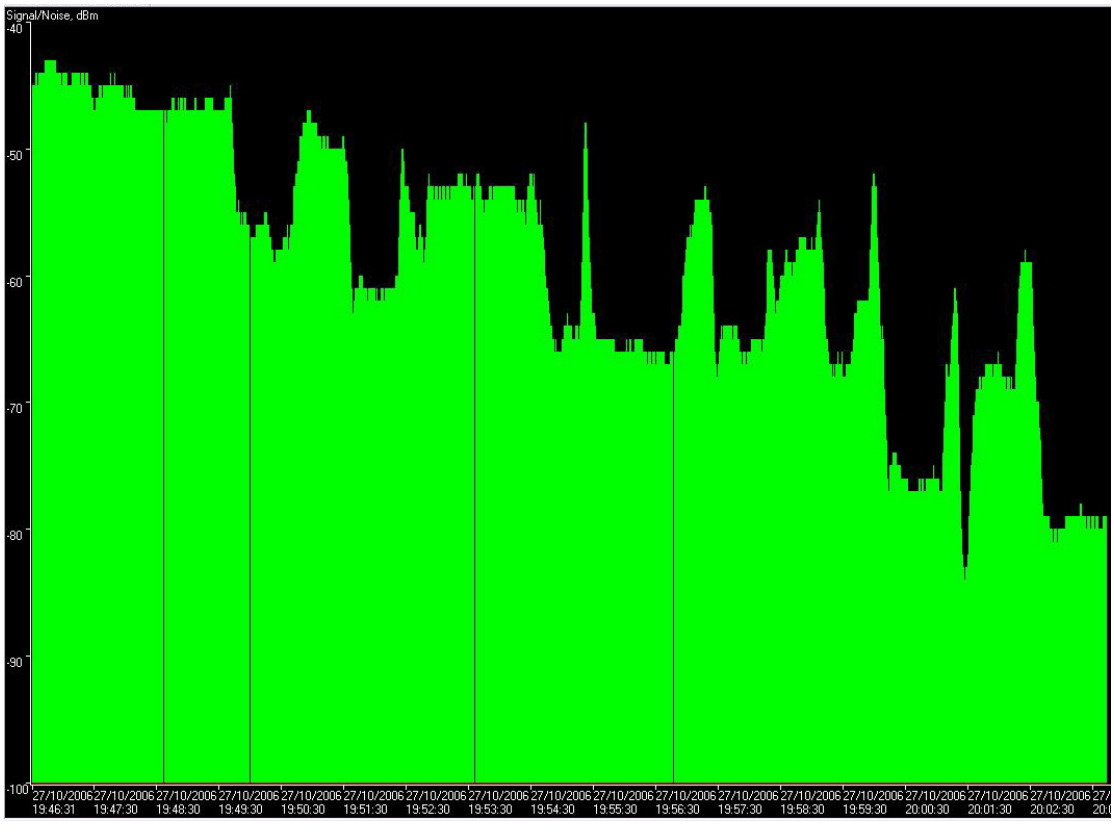
SNR: Στη συγκεκριμένη στήλη αναγράφεται η αναλογία σήματος-θορύβου που εντοπίστηκε στο υπό μελέτη δίκτυο. Για κάθε ένα από τα δώδεκα σημεία το πρόγραμμα λαμβάνοντας υπόψη τη στάθμη του σήματος στο συγκεκριμένο σημείο έκανε την σύγκριση με μια τυπική τιμή θορύβου και υπολόγισε έτσι το SNR.

Noise: Στη συγκεκριμένη στήλη κανονικά αναφέρεται η στάθμη του θορύβου στο δίκτυο. Όμως λόγω του ότι η κάρτα ασυρμάτου δικτυού που υπήρχε στον φορητό υπολογιστή δεν βρισκόταν στη λίστα συμβατότητας του προγράμματος netstumbler, δεν υπήρχαν πραγματικές μετρήσεις για τη στάθμη αυτή. Αντ' αυτού για τον υπολογισμό του SNR το πρόγραμμα χρησιμοποίησε την τυπική τιμή των -100dbm.

Noise-: Η ελάχιστη στάθμη θορύβου κατά τη διάρκεια των μετρήσεων. Κι εδώ ως τιμή παίρνουμε ενδεικτικά τα -100dbm λόγω ασυμβατότητας του hardware με το πρόγραμμα μετρήσεων.

Signal+: Στη στήλη αυτή μπορούμε να δούμε ότι η μέγιστη στάθμη σήματος ήταν -43dbm. Να σημειώσουμε εδώ ότι η τιμή αυτή δεν εμφανίζεται σε κανένα από τα 12 σημεία για τα οποία έχουμε συγκεντρώσει μετρήσεις όμως το πρόγραμμα ξεκίνησε να λαμβάνει μετρήσεις πριν από τη θέση 1, δηλαδή όταν ο υπολογιστής βρισκόταν μεταξύ του AP και της θέσης 1. Έτσι δικαιολογείται αυτή η τιμή μιας και η απόσταση από το AP ήταν πολύ μικρή.

SNR+: Εδώ βλέπουμε την μέγιστη τιμή του λογού σήματος θορύβου. Έχουμε ως δεδομένα όπως είδαμε νωρίτερα τη μέγιστη τιμή σήματος που είναι -43dbm και τη μέγιστη στάθμη του θορύβου που είναι -100dbm. Όπως γνωρίζουμε ο λόγος SNR ισούται με: SNR=Signal-Noise. Έτσι SNR=-43dbm-(-100)=57dbm.



Σχήμα 5.6 – Γραφική απεικόνιση σήματος

Signal: Σε αυτή την κατηγορία βλέπουμε τη στάθμη του σήματος σε κάθε ένα από τα 12 σημεία μετρήσεων. Εδώ όπως είναι λογικό παρατηρούμε μια σταδιακή εξασθένιση όσο απομακρυνόμαστε από το AP προς το βάθος του αμφιθεάτρου. Έτσι τα -47 έως -56dbm της πρώτης σειράς γίνονται -64 έως -67 στις πίσω σειρές του αμφιθεάτρου και φτάνουν τα -79dbm στο πάνω διάζωμα, στον χώρο πάνω από τις σκάλες. Στο σχήμα 5.6 βλέπουμε μια γραφική απεικόνιση της μεταβολής του σήματος κατά τη διάρκεια της μελέτης. Κάποιες κορυφές και βυθίσεις που παρατηρούμε στο γράφημα οφείλονται στην μετακίνηση του υπολογιστή που έλαβε τα δεδομένα μεταξύ των σημείων μετρήσεων.

5.3.3 - Συμπεράσματα

Λαμβάνοντας υπόψη μας τα παραπάνω δεδομένα μπορούμε να πούμε αρχικά ότι το αμφιθέατρο καλύπτεται απόλυτα από το AP όσον αφορά τη ραδιοκάλυψη. Ακόμα και η χαμηλότερη τιμή σήματος που έφτασε τα -79dbm στη θέση 12 είναι ικανοποιητική για μια τυπική κάρτα λήψης WIFI. Συγκεκριμένα οι κάρτες ασυρμάτου δικτύου ανάλογα με τη στάθμη του σήματος που λαμβάνουν ρυθμίζουν ανάλογα το data rate. Ας πάρουμε για παράδειγμα τις τυπικές τιμές της ευαισθησίας λήψης μιας κάρτας:

- -94 dBm στο 1 Mbps
- -91 dBm στα 2 Mbps
- -87 dBm στα 5.5 Mbps
- -82 dBm στα 11 Mbps

Αν ερμηνεύσουμε τα παραπάνω, για να δουλέψει στα 11Mbps η κάρτα θα πρέπει να λάβει μια ελάχιστη στάθμη σήματος -82dBm. Για χαμηλότερη στάθμη σήματος θα υποβαθμίσει την σύνδεση σε κάποιο από τα χαμηλότερα data rates. Αν το σήμα πέσει κάτω από τα -94 dBm η επικοινωνία θα διακοπεί. Επειδή πολλοί κατασκευαστές δεν αναφέρουν την ευαισθησία λήψης καλό θα ήταν να θεωρούμε μια συντηρητική τιμή γύρω στα -76dBm για data rate 11Mbps.

Πρακτικά, τα ραδιοκύματα συμπεριφέρονται απρόβλεπτα σε διάφορες συνθήκες. Για παράδειγμα έχουμε τα multipath effects (τα ραδιοκύματα αντανακλώνται σε διάφορα αντικείμενα και αυξάνουν ή μειώνουν το λαμβανόμενο σήμα.). Όσο πιο μακριά βρίσκεται ο πομπός από τον δέκτη και μεσολαβούν διάφορα αντικείμενα, τόσο αυξάνονται αυτά τα φαινόμενα. Τοίχοι, άνθρωποι, ηλεκτρονικός εξοπλισμός, βροχή/χιόνι/πάγος/ομίχλη μπορούν να μειώσουν το σήμα. Μια διακύμανση γύρω στα 10dB στη στάθμη του σήματος είναι απόλυτα φυσιολογική στο περιβάλλον ενός σπιτιού η ενός γραφείου.

Ένας άλλος σημαντικός παράγοντας είναι ο θόρυβος. Για να χρησιμοποιήσουμε ένα απλό παράδειγμα, ο θόρυβος είναι ραδιοσυχνότητες ¨σκουπίδια¨ που ο δεκτής ¨ακούει¨ αλλά θα πρέπει να απορρίψει. Πηγές θορύβου μπορεί να είναι άλλα δίκτυα wireless, ασύρματα τηλέφωνα, φούρνοι μικροκυμάτων, ραδιοπομποί, ιατρικός εξοπλισμός. Όπως και τα άλλα ράδιο-φαινόμενα ο θόρυβος μπορεί να έχει μεγάλη διακύμανση. Μια τυπική περιοχή έχει γύρω στα -95dBm θόρυβο. Ένα ασύρματο τηλέφωνο που δουλεύει στα 2.4GHz μπορεί να παράγει

ακόμα και -50dBm θόρυβο και να δημιουργήσει προβλήματα σε ένα ασύρματο δίκτυο.

Για να λειτουργήσει ένα ασύρματο δίκτυο η στάθμη του σήματος που λαμβάνει το δίκτυο θα πρέπει να είναι υψηλότερη από τη στάθμη του λαμβανομένου θορύβου. Ας δούμε ένα παράδειγμα: Έστω ότι έχουμε μια τιμή σήματος -75dBm σε κάποιο σημείο του αμφιθεάτρου. Όπως αναφέραμε νωρίτερα μεταβολές της τάξης των 10dB είναι απόλυτα φυσιολογικές. Έτσι έστω ότι μια άλλη μέρα η λαμβανομένη τιμή στο ίδιο σημείο είναι -85dBm. Έχουμε αναφέρει και μια τυπική τιμή θορύβου που είναι -95dBm. Αν μια πηγή θορύβου ανεβάσει την τιμή του λαμβανομένου θορύβου στα -78dBm τότε θα έχουμε προβλήματα στο ασύρματο δίκτυο που αρχικά θα οδηγήσουν σε μείωση του data rate και στη συνέχεια ίσως και στην διακοπή της σύνδεσης.

Αναφέραμε το παραπάνω παράδειγμα για να δείξουμε ότι η ποιότητα ενός ασυρμάτου δικτύου εξαρτάται από διάφορους παράγοντες. Μεταβολές εξαρτώμενες από εξωτερικούς παράγοντες μπορούν να επηρεάσουν το δίκτυο και να δημιουργήσουν προβλήματα. Έτσι για παράδειγμα στη θέση 12 του αμφιθεάτρου μπορεί κάποια στιγμή το SNR να είναι τέτοιο ώστε να μην επιτρέπει την αξιόπιστη σύνδεση. Όλα αυτά βέβαια είναι σχετικά μιας και κατά τη διάρκεια των δοκιμών λάβαμε ικανοποιητικές τιμές σήματος ακόμα και στην περίμετρο του αμφιθεάτρου, έξω από την κεντρική αίθουσα, φτάνοντας μέχρι και τη βιβλιοθήκη του ιδρύματος και το φωτοτυπικό κέντρο πριν διακοπεί η σύνδεση μας.

Βιβλιογραφία

[1] O' Reilly, Matthew Gast "*802.11 Wireless Networks: The Definitive Guide"* (Second Edition April 2005)

[2] Addison Wesley, John Edney and William A. Arbaugh *"Real 802.11 Security: Wi-Fi Protected Access and 802.11i" (2003)*

[3] O' Reilly, Bruce Potter, Bob Fleck *"802.11 Security"* (First Edition December 2002)

[4] McGraw-Hill, Frank Ohrtman and Konrad Roeder *"Wi-Fi Handbook: Building 802.11b Wireless Networks"* (2003)

[5] John Wiley & Sons , Ltd "*Enabling location-based services in wireless LAN hotspots*"(2005)

[6] NetStumbler User Manual http://www.netstumbler.com/downloads/netstumblerinstaller_0_4_0.exe (November 2006)

[7] Kerio Winroute Manual and guides http://www.kerio.com/supp_kwf_manual.html (November 2006)

[8] CISCO Capacity Coverage & Deployment Considerations for IEEE 802.11g http://www.cisco.com/application/pdf/en/us/guest/products/ps430/c1244/ccmigration_09186a00801d61a3.pdf (November 2006)

[9] EAP-TLS Deployment Guide for Wireless LAN Networks
http://www.cisco.com/warp/public/cc/pd/sqsw/sq/tech/acstl_wp.pdf (November 2006)

[10] IEEE 802.11
http://en.wikipedia.org/wiki/802.11g (November 2006)