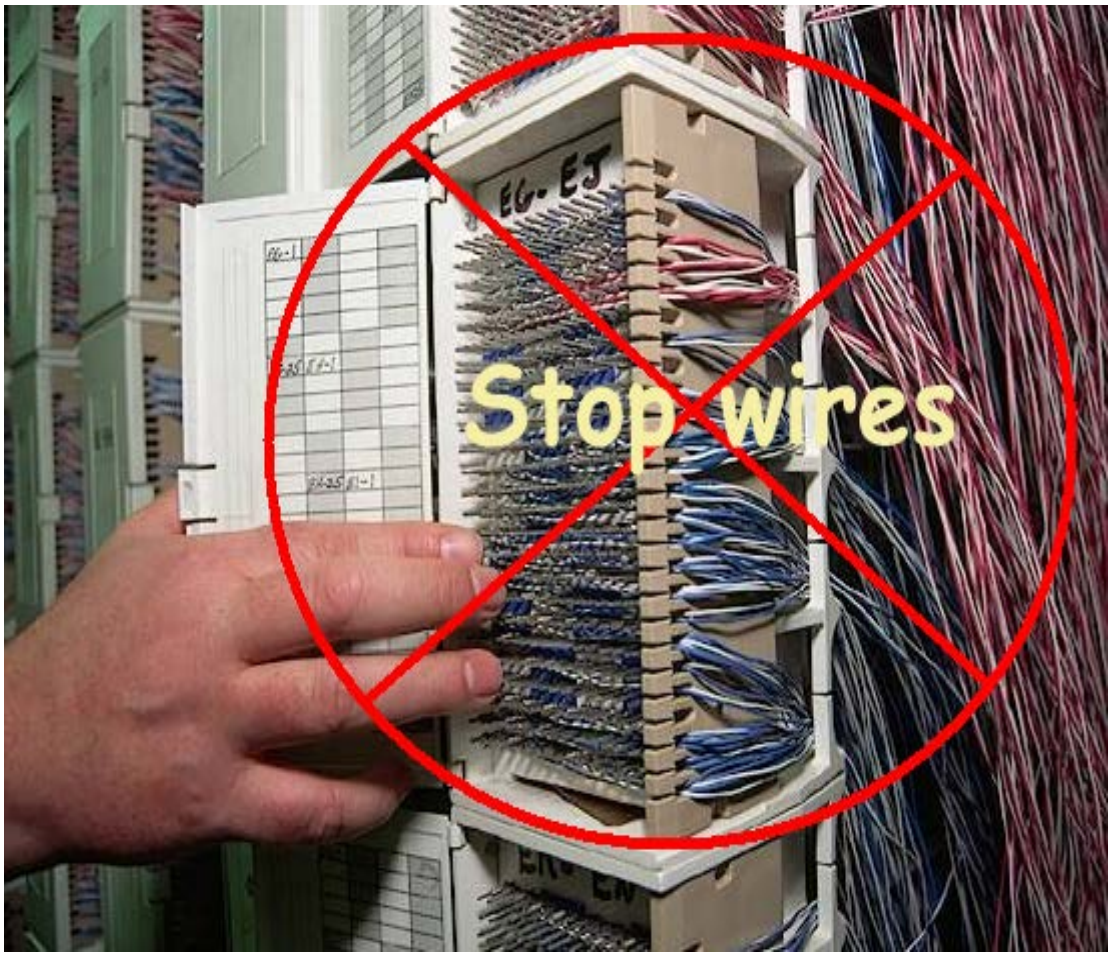
ΤΕΙ ΗΠΕΙΡΟΥ
ΤΜΗΜΑ ΤΗΛΕΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΔΙΟΙΚΗΣΗΣ



ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ:ΣΧΕΔΙΑΣΗ ΚΑΙ ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΗ ΑΣΥΡΜΑΤΟΥ ΤΟΠΙΚΟΥ ΔΙΚΤΥΟΥ

ΕΙΣΗΓΗΤΕΣ:ΧΡΗΣΤΟΥ ΛΑΜΠΡΟΣ-ΛΕΟΝΤΙΟΥ ΔΗΜΟΣΘΕΝΗΣ
ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ:ΤΣΙΑΝΤΗΣ ΛΕΩΝΙΔΑΣ

ΑΡΤΑ ΙΟΥΝΙΟΣ 2006

ΠΕΡΙΕΧΟΜΕΝΑ ΕΡΓΑΣΙΑΣ

ΕΙΣΑΓΩΓΗ

ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ-ΤΙ ΕΙΝΑΙ;

Ένας πολύ απλός και εύκολα κατανοητός ορισμός για τα ασύρματα δίκτυα (wireless networks) είναι δίκτυα στα οποία η πληροφορία δε μεταφέρεται μέσω καλώδιων, επιτρέπωντας έτσι ευελιξία στο χρήστη για ανταλλαγή δεδομένων. Αν θέλουμε όμως να είμαστε λίγο πιο ακριβής θα λέγαμε ότι είναι ο τύπος δικτύου όπου χρησιμοποιούνται υπέρυθρα, υπεριώδη ή ραδιο κύματα για να συνδέσουν τα υπολογιστικά συστήματα στο δίκτυο.

ΓΙΑΤΙ ΝΑ ΤΑ ΧΡΗΣΙΜΟΠΟΙΗΣΩ:

Ζώντας σε μια εποχή ραγδαίας τεχνολογικής προόδου όπου η διάδοση της πληροφορίας γίνεται με ασύληπτη ταχύτητα θα ήταν μάλλον περιττό (και έξω από το στόχο αυτής της εργασίας) να κάνουμε μια εκτενή αναφορά στο κεντρικό ρόλο που παίζουν τα δίκτυα στην ανάπτυξη αυτή. Αρκεί να πούμε ότι στην εποχή μας η μετάδοση της πληροφορίας, η αναταλλαγή δεδομένων η επικοινωνία βασίζεται αποκλειστικά στα δίκτυα (Internet, τηλεφωνία…). Για να μιλήσουμε και με αριθμούς σε μια καταγραφή που έγινε 30 Σεπτεβρίου του 2004 οι εγγεγραμμένοι χρήστες του internet έφταναν τους 812.931.592 ανθρώπους από όλο το κόσμο στοιχεία που μας δίνουν το μέγεθος και το ρόλο των δικτύων στην εποχή μας. Έχει υπολογιστεί ότι η ποσότητα της πληροφορίας που διακινείται παγκόσμια διπλασιάζεται κάθε 6 με 7 χρόνια. Η χρήση

των υπολογιστών και η νέα τεχνολογία δικτύων είναι απαραίτητη για την ταχύτατη επεξεργασία, οργάνωση και αποστολή αυτού του όγκου πληροφορίας. Επιπλέον, η εδραίωση των δικτύων, έχει επιφέρει δραστικές αλλαγές και στις υπηρεσίες που προσφέρονται, με αποτέλεσμα να έχουν εμφανιστεί πληθώρα από δικτυακές εφαρμογές και καινούργιες υπηρεσίες.

Όμως γιατι στραφήκαμε στα ασύρματα δίκτυα; Τι παραπάνω μας προσφέρουν σε σχέση με τα ενσύρματα; Παρακάτωπαρουσιάζονται δέκα τέσσερις καλοί λόγοι για να χρησιμοποιήσουμε ασύρματα δίκτυα.

I. Τα ασύρματα δίκτυα είναι μια απλή γρήγορη και ευέλικτη πρόταση που έχει όλα τα πλεονεκτήματα της ενσύρματης δικτύωσης και προσφέρεται σε χαμηλό κόστος χωρίς να σε περιορίζει σε μια σταθερή και αμετάβλητη εγκατάσταση.
II. Τα ασύρματα δίκτυα δίνουν λύση εκεί που η τοποθέτηση καλωδίων είναι ανεπιθύμητη ή ακόμα πολύ δύσκολο να πραγματοποιηθεί. Πιθανόν αυτό να συμβαίνει σε κάποιο περιορισμένο χώρο γραφείου, ή ακόμα εκεί όπου κάποιο φυσικό όριο δεν επιτρέπει την τοποθέτηση καλωδίων.
III. Για ομάδες εργαζομένων οι οποίοι χρειάζονται να επικοινωνούν και να συνεργάζονται από διαφορετικό τόπο σε διαφορετική χρονική στιγμή τα ασύρματα δίκτυα αποτελούν μια πολύτιμη λύση.
IV. Μπορούμε σίγουρα να φανταστούμε πόσο χρόνο θα κέρδιζε κάποιος αν ακόμα και στην καφετέρια είχε την δυνατότητα να διαβάσει το ηλεκτρονικό του ταχυδρομείο.
V. Τα ασύρματα δίκτυα είναι επιπλέον δίκτυα πολύ εύκολο να επεκταθούν και να εξυπηρετήσουν περισσότερο κόσμο.
VI. Εκτός από τη επεκτασιμότητα ένα ασύρματο δίκτυο είναι πολύ εύκολο να αλλάξει την τοποθεσία που βρίσκεται (relocate).
VII. Επίσης ένα ασύρματο δίκτυο είναι πολύ εύκολο να συνδεθεί σε κάποιο άλλο (πιθανόν ενσύρματο) δίκτυο για κάποια επείγουσα εργασία.

VIII. Όταν το δικτυο σου δεν έχει καλώδιο είναι εύκολο να μεταφέρεις τον υπολογιστή σου να καταγράφεις δεδομένα και να τα στέλνεις αμέσως προς επεξεργασία.

IX. Με τα ασύρματα δίκτυα είναι εξαιρετικά ευέλικτο να μοιράζεσαι μια σύνδεση στο internet ή και άλλους πόρους.

X. Τα ασύρματα δίκτυα σου δίνουν τη δυνατότητα να υλοποιείς εύκολα οποιαδήποτε κινητή υπηρεσία (mobile service).

XI. Οι χρήστες μπορούν να μετακινούνται εντός της **εμβέλειας** του ασύρματου δικτύου,δηλαδή σε χώρο που θα έχουν επαρκές σήμα, διατηρώντας την συνδεσιμότητα τους με αυτό. Αυτό έχει σαν αποτέλεσμα την μεγαλύτερη παραγωγικότητα - αποτελεσματικότητα στο εργασιακό περιβάλλον και όχι μόνο.

XII. Τα ασύρματα δίκτυα μπορούν να διαρθρωθούν σε ένα πλήθος από τοπολογίες, ώστε να ταιριάξουν στις απαιτήσεις των εφαρμογών. Οι τοπολογίες αλλάζουν εύκολα και επεκτείνονται από απλά δίκτυα με μικρό αριθμό χρηστών, ως μεγάλες δομές δικτύων με εκατοντάδες χρήστες και δυνατότητα περιαγωγής (roaming).

XIII. Όσο αναπτύσσεται η τεχνολογία γίνεται δυνατή η μετάδοση μεγαλύτερων ρυθμών δεδομένων. Ήδη ο μέγιστος ρυθμός μετάδοσης δεδομένων, από τα 2Mbps που μπορούσαν να επιτευχθούν αρχικά, έφτασε σήμερα σε ταχύτητες πάνω από 100Mbps ενώ ήδη έχουν εξαγγελθεί ακόμα μεγαλύτερες ταχύτητες.

XIV. Ένα ασύρματο δίκτυο κατάλληλα διαμορφωμένο μπορεί να έχει μεγάλη αξιοπιστία. Έτσι μπορεί να σχεδιαστεί έτσι ώστε να μπορεί να εργάζεται όταν συμβαίνουν διακοπές ρεύματος και να περιλαμβάνει πολλές εναλλακτικές διαδρομές.

ΠΟΥ ΔΕΝ ΧΡΕΙΑΖΕΤΑΙ Η ΑΣΥΡΜΑΤΗ ΔΙΚΤΥΩΣΗ

Η χρήση ασύρματης τεχνολογίας, σε καμία περίπτωση δεν παραγκωνίζει τις λύσεις ενσύρματης δικτύωσης. Οι δύο οικογένειες τεχνολογιών είναι συμπληρωματικές και όχι ανταγωνιστικές. Δεν πρέπει να γίνεται χρήση της ασύρματης τεχνολογίας στις ακόλουθεςπεριπτώσεις:

• Όταν ο χρήστης έχει κατευθείαν εύκολη πρόσβαση στο ενσύρματο δίκτυο, για παράδειγμα η σύνδεση ενός δύο υπολογιστών που βρίσκονται δίπλα δίπλα σε ένα γραφείο με ένα απλό ethernet καλώδιο.

• Στις περιπτώσεις όπου ο χρήστης - εφαρμογή απαιτεί αρκετά μεγάλο ρυθμό μετάδοσης, όπου δεν μπορεί να καλυφθεί από το ασύρματο δίκτυο. Έτσι για παράδειγμα εάν θέλουμε μία διασύνδεση με ρυθμό 1Gbps, μπορούμε να την υλοποιήσουμε με πολύ χαμηλό κόστος με συσκευές που να υποστηρίζουν Gigabit Ethernet και την κατάλληλη καλωδίωση. Η ασύρματη τεχνολογία δεν προβλέπεται να φτάσει ποτέ αυτές τις ταχύτητες.Επιπλέον ήδη έχουν κυκλοφορήσει λύσεις ενσύρματης δικτύωσης που φτάνουν στα 10Gbps αν και δεν είναι κοινή ακόμα η χρήση τους.

• Σε δίκτυα που απαιτούν μεγάλο βαθμό ασφαλείας, οι ενσύρματες λύσεις είναι σαφώς καλύτερες. Σε ένα καλώδιο το οποίο είναι προστατευμένο κάτω από ψευδοπατώματα, δεν είναι δυνατή η φυσική πρόσβαση στο καλώδιο προκειμένουνα γίνει υποκλοπή. Αντίθετα, στην περίπτωση ασύρματης υλοποίησης, επειδή δεν είναι δυνατό να περιορίσουμε τα ραδιοκύματα, είναι εύκολο να γίνει ανίχνευση της μεταδιδόμενης πληροφορίας. Σε περίπτωση δε, που η πληροφορία δεν είναι κωδικοποιημένη μπορεί να γίνει ανάκτηση της. Για να φτάσουν σε παρόμοιο βαθμό ασφαλείας τα ασύρματα δίκτυα, πρέπει να εφαρμοστούν σε αυτά περίπλοκες τεχνικές αυθεντικοποίησης και κωδικοποίησης και μάλιστα σε επίπεδο εφαρμογής. Άλλωστε αυτός είναι και ένας από τους λόγους που δεν χρησιμοποιούνται σε κρίσιμες στρατιωτικές εφαρμογές οι συμβατικές ασύρματες τεχνολογίες (για παράδειγμα επικοινωνία συσκευών, εφαρμογών, προσωπικού, σε ένα πολεμικό πλοίο ή εντός μιας στρατιωτικής βάσης).

• Σε περιοχές που έχουν μεγάλο ηλεκτρομαγνητικό θόρυβο, γεγονός που έχει ωςαποτέλεσμα προβληματικές και μη αξιόπιστες συνδέσεις.

ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ

Η έννοια του ασύρματου δικτύου και ποιο συγκεκριμμένα της ασύρματης επικοινωνίας δεν είναι νέα ιδέα. Ήδη από το 1901 ο Ιταλός φυσικός Γουλιέλμος Μαρκόνι επέδειξε στο κοινό έναν ασύρματο τηλέγραφο ανάμεσα στα πλοία και στη ξηρά. Ως κώδικα ο Μαρκόνι χρησιμοποίησε το κώδικα μορς (οι τελείες και οι παύλες είναι άλλωστε δυαδικό σύστημα). Τα σύγχρονα ψηφιακά ασύρματα έχουν βέβαια πολύ καλύτερη απόδοση, αλλά η βασική ιδέα είναι η ίδια. Συνεχίζοντας την αναδρομή μετά τον Marconi, τα πρώτα ασύρματα δίκτυα που εμφανίστηκαν ήταν τα ραδιοδίκτυα δεδομένων (Data) τεχνολογίας TCP/IP. Οι πρώτες τεχνικές μεταγωγής πακέτων αναπτύχθηκαν γύρω στο 1964, ενώ ο όρος "Packet" προτάθηκε από τον D. W. Davies του National Physical Laboratory της Μεγ. Βρετανίας. Οι έρευνες του εργαστηρίου αυτού οδήγησαν στο σημερινό διεθνές δημόσιο δίκτυο μεταγωγής πακέτων X.25, ενώ το ίδιο έτος ο οργανισμός ARPA (Advanced Research Projects Agency) των Η.Π.Α. άρχισε να χρηματοδοτεί τα προγράμματα που οδήγησαν στη δημιουργία του ARPAnet (πυρήνα του σημερινού Internet) το 1969.
Η τεχνολογία των ασυρμάτων δικτύων μετάδοσης πακέτων άρχισε να αναπτύσσεται στην δεκαετία 1970-1980, αν και η μεγάλη ανάπτυξή της συμπίπτει με την διάδοση των μικροϋπολογιστών στην δεκαετία 1980-1990. Εδώ αξίζει να αναφέρουμε ότι το πρώτο ολοκληρωμένο ασύρματο LAN κατασκευάστηκε στο πανεπιστήμιο της Χαβάης στα πλαίσια ενός project που λέγονταν *ALOHANET*. Λόγω των ιδιαίτερων χαρακτηριστικών του μέσου μεταδόσεως τα ασύρματα δίκτυα χρησιμοποιούν εξειδικευμένα πρωτόκολλα για το υποεπίπεδο πρόσβασης μέσου (Medium Access Control) και το επίπεδο σύνδεσης δεδομένων (Data Link

Layer) και συχνά και για ανώτερα επίπεδα (π.χ. δρομολόγηση πακέτων).
Σήμερα είναι διαθέσιμος ένας αριθμός από καινούργιες συσκευές και προϊόντα ασύρματης επικοινωνίας που βασίζονται σε νέες τεχνολογίες και νέα πρότυπα. Τα τελευταία χρόνια οι κινητοί υπολογιστές (notebook, laptop, palmtop) είναι διαθέσιμοι και ελκυστικοί για το ευρύ κοινό, αφού έχουν πλέον συγκρίσιμο κόστος, υπολογιστική ισχύ και ποιότητα υπηρεσιών με τους σταθερούς υπολογιστές. Όλα αυτά έχουν σαν αποτέλεσμα την έρευνα για την ανάπτυξη προτύπων για την υποστήριξη των ασύρματων επικοινωνιών.
Τα τελευταία χρόνια γίνονται σταθερά βήματα προόδου για την βελτίωση της ποιότητας των ασυρμάτων δικτύων με όλο και αυξανόμενες ταχύτητες και νέα πρότυπα από οργανισμούς και συμμαχίες γνωστών εταιρειών. Χαρακτηριστικά είναι τα παραδείγματα του Bluetooth, GPRS (General Packet Radio Service), ενώ σε εξέλιξη βρίσκονται και άλλα δύο πρότυπα. Το ένα αναπτύσσεται στην Ευρώπη από το ETSI (European Telecommunications Standard Institute) και ονομάζεται HIPERLAN (High – Performance European Radio LAN). Το άλλο αναπτύσσεται από την IEEE (Institute of Electrical and Electronics Engineers) και ονομάζεται 802.11 WLAN. Και τα δύο αυτά πρότυπα καλύπτουν τις προδιαγραφές για το φυσικό στρώμα και το υπόστρωμα MAC (Medium Access Control).
Περισσότερες λεπτομέρειες κυρίως για τα πρωτόκολλα και πρότυπα ασύρματων δικτύων θα αναφέρουμε στη συνέχεια.

ΚΑΤΗΓΟΡΙΕΣ ΑΣΥΡΜΑΤΩΝ ΔΙΚΤΥΩΝ

Με μια πρώτη προσέγγιση τα ασύρματα δίκτυα μπορούν να διαιρεθούν σε τρεις κύριες κατηγορίες :

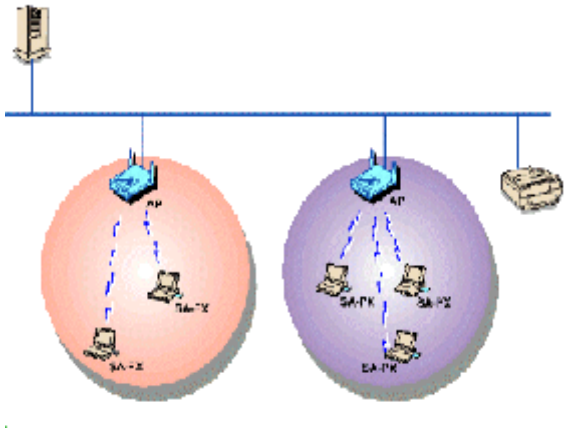
I. Διασύνδεση συστήματος (System interconnection).
II. Ασύρματα LAN.
III. Ασύρματα WAN.

Η διασύνδεση συστήματος αναφέρεται στη διασύνδεση των εξαρτημάτων του υπολογιστή με τη χρήση ραδιοκυμάτων μικρής εμβέλειας. Έτσι ένας χρήστης που δυσκολεύται να συνδέσει καλώδια μπορεί εύκολα να χρησιμοποιήσει ένα ασύρματο ποντίκι ή πληκτρολόγιο κ.α. Κατά συνέπεια μερικές εταιρίες αποφάσισαν να σχεδιάσουν ένα ασύρματο δίκτυο μικρής εμβέλειας το οποίο ονομάζεται *Bluetooth* για την σύνδεση των εξαρτημάτων αυτών χωρίς καλώδια. Να σημειώσουμε εδώ ότι το Bluetooth χρησιμοποιείται ευρέως στην κινητή τηλεφωνία (Σχήμα). Για το Bluetooth θα αναφέρουμε περισσότερα πράγματα στην συνέχεια.

Πριν προχωρήσουμε στα ασύρματα LAN, πρέπει να αναφέρουμε ότι μπορούμε πιθανώς να συναντήσουμε και μία ακόμα κατηγορία ασύρματων δικτύων τα PAN's (Personal area networks). Αυτά είναι δίκτυα που μπορούν να εγκατασταθούν σε κάποιο μικρό γραφείο ή στο σπίτι σε απόσταση 5-15 μέτρων. Μεταξύ των συσκευών του γραφείου πρέπει να υπάρχει οπτική επαφή. Δύο τεχνολογίες που χρησιμοποιούνται σε αυτού του τύπου τα συστήματα είναι η IrDA και το Bluetooth.
Παρεπιπτώντος το Bluetooth δεν απαιτεί οπτική επαφή. Για περισσότερες πληροφορίες για την IrDA επισκεφτείται το site : *www.irda.org*

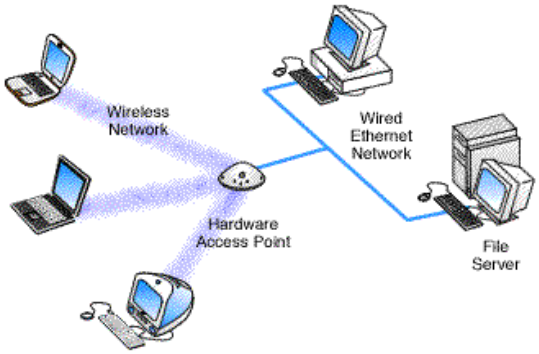
Το επόμενο βήμα προς τα πάνω στην ασύρματη δικτύωση είναι τα ασύρματα LAN's (WLAN's).Αυτά είναι συστήματα στα οποία κάθε

υπολογιστής έχει ένα ασύρματο μόντεμ και μια κεραία μέσω των οποίων μπορεί να επικοινωνεί με άλλα συστήματα.Το ασύρματο LAN με τη σειρά του μπορεί να συνδεθεί σε ένα ενσύρματο LAN ή να αποτελέσει βάση για ένα καινούργιο δίκτυο.Η βασική δομική μονάδα (building block) του WLAN είναι το κελί (cell). Το κελί είναι ουσιαστικά η περιοχή όπου η ασύρματη επικοινωνία λαμβάνει χώρα.Η περιοχή που καλύπτει ένα κελί εξαρτάται από τη ισχύ διάδοσης του ραδιοκύματος και από κάποια φυσικά χαρακτηριστικά (ύπαρξη τοίχου...) που υπάρχουν στην περιοχή του δικτύου. Μπορούμε να φανταστούμε τη περιοχή που καλύπτει το κέλι ως κυκλική. Οι σταθμοι του δικτύου (PC's) μπορούν να μετακινούνται στο κελί χωρίς να χάνουν την επαφή με το δίκτυο. Η επικοινωνία μεταξύ των σταθμών μέσα στο κελί του ασύρματου δικτύου συντονίζονται από ένα σταθμό βάσης που ονομάζεται σημείο πρόσβασης (access point). Το access point μπορεί να συνδέσει πολλά κελιά ενός WLAN μεταξύ τους και μπορεί επίσης να συνδέσει τα cells του WLAN με ένα ενσύρματο Ethernet LAN μέσω καλωδίου σε μια έξοδο του Ethernet LAN. Ένα παράδειγμα μιας τοπολογίας όπου χρησιμοποιείται το πακέτο δικτύωσης BreezeNET PRO.11 φαίνεται στο παρακάτω σχήμα. Να σημειώσουμε εδώ ότι το συγκεκριμμένο πακέτο χρησιμοποιεί το πρότυπο 802.11 το οποίο θα συζητήσουμε παρακάτω

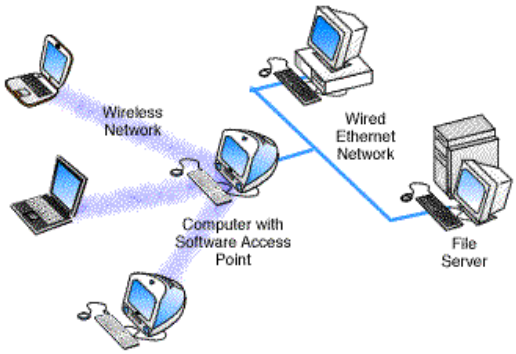


Σχήμα 1. WLAN

Πριν ολοκληρώσουμε την αναφορά μας στα WLAN πρέπει επίσης να σημειώσουμε ότι το access point μπορεί να είναι hardware αλλά και κάποιο PC με κατάλληλο λογισμικό. Χαρακτηριστικές είναι οι εικόνες που ακολουθούν:



Σχήμα 2. Hardware access point.



Σχήμα 3. Software access point

Το τρίτο είδος ασύρματου δικτύου (ασύρματα WAN) χρησιμοποιείται στα συστήματα ευρείας περιοχής. Το δίκτυο ραδιοκυμάτων που χρησιμοποιείται στα κυψελωτά (cellular) κινητά τηλέφωνα είναι παράδειγμα ασύρματου συστήματος με χαμηλό εύρος ζώνης. Αυτό το σύστημα βρίσκεται είδη στη τρίτη γενιά που καλύπτει ψηφιακά φωνή και δεδομένα. Κατά κάποιο τρόπο τα κυψελωτά ασύρματα δίκτυα είναι παρόμοια με τα WLAN's με τη διαφορά ότι οι αποστάσεις είναι πολύ μεγαλύτερες και ο ρυθμός μετάδοσης των bit πολύ χαμηλότερος. Τα WLAN's λειτουργούν σε ταχύτητες μέχρι περίπου 50 Mbps για αποστάσεις μερικών δεκάδων μέτρων. Τα κυψελωτά συστήματα λειτουργούν σε

ταχύτητες κάτω από 1 Mbps αλλά η απόσταση μεταξύ του σταθμού βασης και του υπολογιστή ή του τηλεφώνου μετριέται σε χιλιομετρα αντί σε μέτρα.
Να σημειώσουμε εδώ ότι πολύ συχνα αναφέρεται και μια νέα κατηγορία ασύρματων δικτύων η οποία είναι ενδιάμεση των ασύρματων LAN και ασύρματων WAN. Αυτή η κατηγορία αναφέρεται ως ασύρματα MAN (Wireless Metropolitan Area Networks) και καλύπτει ένα μικρότερο εύρος ασύρματης δικτύωσης. Η σύγκριση του διαφορετικού εύρους των δύο δικτύων ασύρματων WAN και ασύρματων MAN φαίνεται στα δύο παρακάτω σχήματα.

Σχήμα 4. Ασύρματο MAN

Σχήμα 5. Ασύρματο WAN

1.Ασύρματες τεχνολογίες και πρότυπα

Σε αυτή τη παράγραφο θα θέλαμε να κάνουμε μια αναφορά και μια σύντομη αλλά περιεκτική περιγραφή στις πιο δημοφιλείς ασύρματες τεχνολογίες και πρότυπα. Σκοπός μας δεν είναι να αναφέρουμε οτιδήποτε έχει υπάρξει κατά καιρούς αλλά να δώσουμε το παλμό της τεχνολογίας σε αυτό το τομέα. Να τονίσουμε πλέον ότι τα πρότυπα και οι τεχνολογίες στις οποίες θα επικεντρωθούμε αναφέρονται κατά κύριο λόγο σε ασύρματα LAN's.

1.1 Το Πρότυπο IEEE 802.11

Το πρότυπο IEEE 802.11 ή διαφορετικά Wi-Fi εισάγει ένα σύνολο από standards για ασύρματα LAN's (wireless local area networks) από την ομάδα 11 της IEEE 802. Η IEEE 802 είναι η επιτροπή που ασχολείται με LAN, MAN (metropolitan area network) standards. Εδώ πρέπει να αναφέρουμε ότι το Wi-Fi (Wireless Fidelity) είναι ένα εμπορικό όνομα για το πρότυπο 802.11 αλλά τις περισσότερες φορές θα το δούμε να ταυτίζεται με το 802.11b που αναλύεται παρακάτω. Τέλος να αναφέρουμε ότι το WiFi δεν χρησιμοποιείται μόνο για ασύρματα LAN αλλά και για πρόσβαση στο internet.

Η οικογένεια 802.11 περιλαμβάνει καταρχήν τρία βασικά πρωτόκολλα τα οποία έχουν τις κωδικοποιήσεις 802.11a, 802.11b και 802.11g. Η ασφάλεια αρχικά συμπεριλαμβανόταν σε αυτά τα πρότυπα αλλά τώρα είναι κομμάτι άλλων προτύπων της οικογένειας όπως το 802.11i . Άλλα standards της οικογένειας 802.11 (c-f, h-j, n) είναι συμπληρώματα υπηρεσιών ή διορθώσεις σε ήδη υπάρχοντα standards. Παραδόξως σε σχέση με το

802.11a, το 802.11b ήταν το πρώτο ευρέως αποδεκτό πρότυπο στην ασύρματη δικτύωση.
Παρακάτω ακολουθούν κάποιες πολύ βασικές πληροφορίες για τα περισσότερο δημοφιλή standards της οικογένειας 802.11

I. *802.11legacy*
   Η πρώτη εκδοχή του IEEE 802.11 που ανακοινώθηκε το 1997 και καμιά φορά ονομάζεται και "802.1y" , καθορίζει δύο ρυθμούς μετάδοσης δεδομένων, αυτούς των 1 και 2 Mbps (Megabits per second).Αυτά μεταδίδονταν μέσω υπέρυθρων σημάτων σε συχνότητες των 2.4 GHz.Η χρησιμοποίηση υπέρυθρων (infrared) απορρίφθηκε στα πρότυπα που ακολούθησαν γιατί δε μπορούσε να ανταγωνιστεί το ήδη πετυχημένο πρωτόκολλο IrDA και επίσης δεν είχε ουσιαστική εφαρμογή.

II. *802.11b*
   Το 802.11b ήταν αυτό που διαδέχτηκε το 802.11legacy. Το 802.11b έχει περίπου ένα εύρος 50 μέτρων, με μια χαμηλής ισχύος (low gain) omni κεραία η οποία συνήθως χρησιμοποιείται στις 802.11b συσκευές. Αν μιλήσουμε για high gain εξωτερικές κεραίες τότε το πρωτόκολλο μπορεί να χρησιμοποιηθεί σημείο προς σημείο (point to point) επικοινωνία εύρους μεγαλύτερου από 8 χιλιόμετρα. Το πρωτόκολλο 802.11b έχει ρυθμό μετάδοσης δεδομένων 11Mbps αλλά όμως σημαντικό ποσοστό του εύρους ζώνης (bandwidth) χρησιμοποιείται για προετοιμασία της επικοινωνίας (communications overhead). Στη πραγματικότητα ο ρυθμός μετάδοσης δεδομένων που επιτυγχάνεται είναι 5,5Mbps. Δραστικό ρόλο στην εξασθένηση του σήματος παίζουν το νερό το μεγάλος πάχος τοίχων, το μέταλλο και άλλα. Τέλος το 802.11b δουλεύει στο φάσμα συχνοτήτων των 2,4 GHz.
   Διάφορες επεκτάσεις έχουν γίνει στο πρωτόκολλο 802.11b για να αυξηθεί ο ρυθμός μετάδοσης δεδομένων σε 22, 33, και 44 Mbit/s με αποτέλεσμα να μετονομασθεί σε 802.11b+. Αυτό

το πρότυπο υποστηρίχθηκε από εταιρίες αλλά δεν υιοθετήθηκε από την IEEE.

III. *802.11a*

Το 802.11a ανακοινώθηκε το 2001 αν και είχε επικυρωθεί ήδη από το 1999.Το πρωτόκολλο λειτουργεί σε συχνότητα των 5 GHz και με ρυθμό μετάδοσης δεδομένων στα 54 Mbit/s. Στη πραγματικότητα όμως ο ρυθμός μετάδοσης των δεδομένων που επιτυγχάνεται είναι περίπου 20 Mbit/s . Το πρωτόκολλο 802.11a δεν υιοθετήθηκε ευρέως όπως το 802.11b εξαιτίας προβλημάτων που δημιουργούσε η συχνότητα των 5 GHz όπως για παράδειγμα η κατανάλωση ενέργειας.

IV. *802.11g*

Τον Ιούνιο του 2003 ένα άλλο πρότυπο επικυρώθηκε, το 802.11.g . Αυτό το πρωτόκολλο λειτουργεί πάλι σε συχνότητα 2,4 GHz αλλά ο ρυθμός μετάδοσης δεδομένων είναι στα 54 Mbit/s όπως το 802.11.a. Λόγω συχνότητας το 802.11.g είναι απόλυτα συμβατό με το 802.11.b . Όμως κάποιες φορές η χρήση του 802.11.b σε ένα δίκτυο που χρησιμοποιεί το 802.11.g, κάνει το δίκτυο ποιο αργό.

Το πρωτόκολλο 802.11.g κέρδισε το καταναλωτικό κοινό από τον Ιανουάριο του 2003 πριν ακόμα εγκριθεί. Μάλιστα ολοκληρώνοντας αξίζει να αναφέρουμε ότι μία επέκταση του 802.11.g, η Super G έχει ολοκληρωθεί και υπόσχεται ταχύτητες μεγαλύτερες των 108 Mbit/s .

V. *802.11n*

Τον Ιανουάριο του 2004 η IEEE ανακοίνωσε ότι θα δημιουργηθεί ένα νέο πρότυπο το οποίο θα αναφέρεται σε ασύρματα WAN. Η πραγματική του ταχύτητα θα είναι 100 Mbit/s περίπου δηλαδή 4-5 φορές μεγαλύτερη από τη πραγματική ταχύτητα του 802.11g και 50 φορές μεγαλύτερη από τη πραγματική ταχύτητα του 802.11b. Η διαδικασία προτυποποίησης αναμένεται να τελειώσει στα τέλη του 2006.

Το πρότυπο 802.11 θα αναλυθεί σε επόμενο κεφάλαιο. Εκεί θα δοθούν πληροφορίες σχετικά με την αρχιτεκτονική του, την

ασφάλεια για διάφορα εμπορικά ζητήματα και άλλα βεβαίως θέματα. Αυτό επειδή το 802.11 είναι το πιο δημοφιλές αυτή τη στιγμή σε ασύρματα LAN.

1.2 Το πρότυπο 802.16

Το πρότυπο 802.16 ομοίως με το 802.11 αναπτύχθηκε από την ομάδα 16 της IEEE 802.Όπως αναφέραμε και προηγουμένως η IEEE 802 είναι η επιτροπή που ασχολείται με LAN, MAN (metropolitan area network) standards. Το 802.16 ειδικεύεται σε ευρυζωνική σημείου προς σημείο ασύρματη πρόσβαση (point-to-point broadband wireless access). Για να γίνουμε σε αυτό το σημείο περισσότερο κατανοητοί η τεχνολογία broadband wireless access (BWA), έχει ως στόχο να παρέχει ασύρματη πρόσβαση σε δίκτυα δεδομένων, με πολύ υψηλό ρυθμό μετάδοσης δεδομένων. Το πρότυπο 802.16 είναι γνωστό και ως WiMAX που σημαίνει ***W****orldwide* ***I****nteroperability for* ***M****icrowave* ***Access*** . Παρόμοιες τεχνολογίες με το WiMAX είναι η BWA καθώς και η HIPERMAN η οποία είναι και η «Ευρωπαία» ανταγωνίστρια της.
Το WiMAX δεν συγκρούεται με το WiFi αλλά στη πραγματικότητα το συμπληρώνει. Το WiMAX είναι μια ασύρματη WAN (Wide Area Network) τεχνολογία η οποία συνδέει τους σταθμούς βάσης (hotspots) του WiFi με το internet και έτσι αποτελεί μια επέκταση του. Να σημειώσουμε εδώ ότι το hotspot έχει την ίδια έννοια με το access point για το οποίο μιλήσαμε παραπάνω. Βασικό χαρακτηριστικό του 802.16 είναι ότι μπορεί να παρέχει ασύρματη σύνδεση σε ένα εύρος μεγαλύτερο από 50 χιλιόμετρα χωρίς να χρειάζεται άμεση οπτική επαφή με ένα σταθμό βάσης. Επίσης το πρότυπο 802.16 εξασφαλίζει ένα ρυθμό μετάδοσης δεδομένων ίσο με 54 Mbit/s.

Προσδοκίες από το WiMAX:

Το WiMAX στοχεύει στο να δώσει τη δυνατότητα σε εκατομμύρια ανθρώπους να έχουν πρόσβαση στο internet ασύρματα, γρήγορα αλλά και φθηνά. Για να καταλάβουμε καλύτερα ένας σταθμός βάσης WiMAX αναμένεται να παρέχει γρήγορες συνδέσεις στο

internet σε σπίτια και εταιρίες σε ακτίνα μεγαλύτερη των 30 χιλιομέτρων. Ο σταθμοί βάσης αναμένεται να μετατρέψουν μια περιοχή σε WMAN (wireless metropolitan area) και έτσι να επιτρέπουν οποιαδήποτε ασύρματη κίνηση μέσα σε αυτήν όπως επικοινωνία laptops και PDA's.Εδώ όμως πρέπει να πούμε ότι πραγματικό roaming σε ασύρματο ευρυζωνικό δίκτυο βασισμένο σε κελιά αναμένεται να εξυπηρετηθεί από ένα άλλο standard της IEEE το 802.20.

1.3 Bluetooth

Τι είναι το Bluetooth;

Το Bluetooth είναι μια τεχνολογία η οποία καθιστά δυνατή τη μικρού εύρους (short range) ασύρματη σύνδεση μεταξύ desktop PC's και laptops, PDA's, κινητά τηλέφωνα, εκτυπωτές, πληκτρολόγια, ποντίκια καθώς και πολλά άλλα. Η συχνότητα του Bluetooth είναι 2,4GHz καθώς το εύρος ζώνης είναι στο 1 MHz. Τέλος η ταχύτητα μεταφοράς δεδομένων είναι μέχρι 1Mbps ενώ είναι δυνατή και η ταυτόχρονη μεταφορά ήχου.

Ιστορικά στοιχεία.

Το 1994 η εταιρεία Ericsson έδειξε ενδιαφέρον για τη σύνδεση των κινητών τηλεφώνων σε άλλες συσκευές χωρίς καλώδια. Έτσι μαζί με άλλες εταιρίες (IBM Intel, Nokia, Toshiba) σχημάτισε τη SIG (Special Interest Group) που σημαίνει ουσιαστικά κοινοπραξία, για την ανάπτυξη ενός προτύπου ασύρματης διασύνδεσης υπολογιστικών και επικοινωνιακών συσκευών και βοηθημάτων με χρήση ραδιοκυματικών πομποδεκτών μικρής εμβέλειας , χαμηλής ισχύος και χαμηλού κόστους. Το έργο ονομάστηκε Bluetooth, από τον Harald Blaatand το 2° (ή Bluetooth) (940-981), ένα βασιλιά των Βικινγκ που ενοποίησε (κατέκτησε) τη Δανία και τη Νορβηγία χωρίς να χρησιμοποιήσει καλώδια.

Αν και η αρχική ιδέα ήταν να απαλλαγούμε από τα καλώδια ανάμεσα στις συσκευές, το έργο αυτό άρχισε σύντομα να εισβάλλει και στο χώρο των ασύρματων LAN. Αν και αυτή η κίνηση κάνει το πρότυπο ποιο χρήσιμο δημιουργεί κάποιο ανταγωνισμό με το πρότυπο 802.11 .Για να χειροτερέψουν τα πράγματα τα δύο συστήματα παρεμβάλλονται ηλεκτρικά μεταξύ τους. Επίσης να σημειώσουμε εδώ ότι και η Hewlett-Packard παρουσίασε πριν από μερικά χρόνια ένα υπέρυθρο δίκτυο για σύνδεση περιφερειακών υπολογιστών χωρίς καλώδια, αλλά δε γνώρισε επιτυχία.
Η επιτροπή του Bluetooth δε πτοήθηκε από τις εξελίξεις και τον Ιούλιο του 1999 εξέδωσε μια προδιαγραφή 1500 σελίδων για την έκδοση 1.0 του συστήματος. Λίγο αργότερα η ομάδα προτύπων του IEEE που δούλευε πάνω σε WLAN, 802.15 υιοθέτησε ως βάση το έγγραφο του Bluetooth και άρχισε να το τροποποιεί. Αν και μπορεί να φαίνεται περίεργη η τυποποίηση ενός συστήματος που έχει ήδη πολύ λεπτομερείς προδιαγραφές και δεν έχει ασύμβατες υλοποιήσεις που να χρειάζεται να εναρμονιστούν, η ιστορία δείχνει ότι η ύπαρξη ενός ανοικτού προτύπου το οποίο διαχειρίζεται μια ουδέτερη αρχή όπως η IEEE συχνά προάγει τη χρήση μιας τεχνολογίας. Σήμερα αν και οι εκδόσεις της επιτροπής του Bluetooth και του IEEE δεν είναι πανομοιότυπες, υπάρχει ελπίδα ότι θα συγκλίνουν σε ένα μοναδικό πρότυπο.

1.4 Άλλα πρότυπα

Πέρα από τα πρότυπα που αναφέραμε παραπάνω (τα οποία είναι και ιδιαίτερα δημοφιλή) υπάρχουν και πολλά άλλα πρότυπα στα ασύρματα δίκτυα. Αξίζουμε να αναφέρουμε το HIPERLAN, το HomeRF, το UWB (Ultra-wideband) όπως και για τη κινητή τηλεφωνία το GSM,WAP κ.τ.λ. Η λεπτομερής ανάλυση τους είναι έξω από τα πλαίσια αυτής της εργασίας.

2.Δομή του προτύπου 802.11

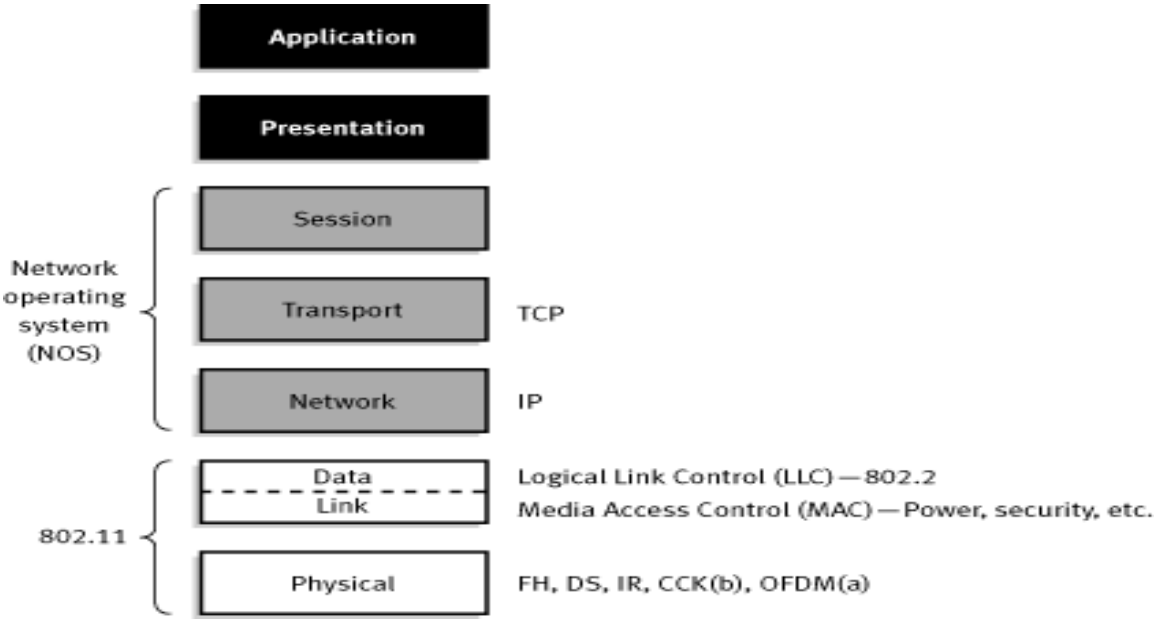
Σχήμα7: IEEE's 802.11 certification.

Τον Ιούνιο του 1997, το Ινστιτούτο των Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών – Institute of Electrical and Electronic Engineers (IEEE) κατέληξε στο αρχικό πρότυπο για ασύρματα δίκτυα WLANs, **IEEE 802.11**. Αυτό το πρότυπο προδιέγραφε ως συχνότητα λειτουργίας τα 2,4 GHz, με ρυθμούς μετάδοσης δεδομένων 1 και 2 Mbps.
Αποτελεί το πρώτο πρότυπο για ασύρματη δικτύωση και ακολουθείται από τα περισσότερα ασύρματα δίκτυα μέχρι και σήμερα.

2.1 Στοίβα πρωτοκόλλων του 802.11

Όπως όλα τα 802.x πρότυπα, έτσι και το 802.11 επικεντρώνεται στα δύο χαμηλότερα στρώματα του μοντέλου OSI (Open System Interconnection), δηλαδή στο φυσικό στρώμα (Physical Layer-PHY) και στο υπόστρωμα MAC (Medium Access Control-Ελέγχου προσπέλασης Μέσων) του στρώματος διασύνδεσης δεδομένων (Data Link Layer) όπως φαίνεται στο σχήμα8 .
Το υπόστρωμα MAC ορίζει πώς γίνεται η εκχώρηση του καναλιού, δηλαδή ποιος θα μεταδώσει στη συνέχεια. Το υπόστρωμα LLC(Logical Link Control-Έλεγχος Λογικού Συνδέσμου) του

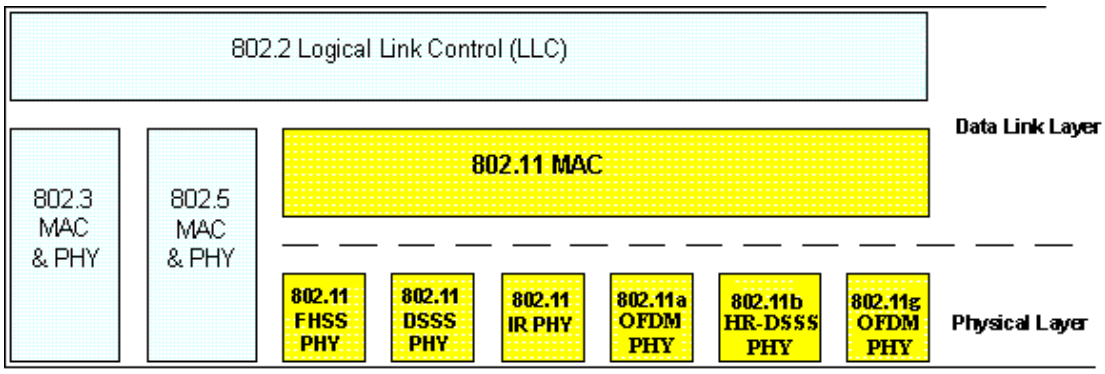
στρώματος Data Link βρίσκεται πάνω από το υπόστρωμα MAC, έχει υλοποιηθεί ως IEEE 802.2 και δουλειά του είναι να κρύβει τις διαφορές ανάμεσα στις διαφορετικές παραλλαγές του 802, έτσι ώστε να κάνει τις παραλλαγές αυτές "αόρατες" όσον αφορά το επίπεδο δικτύου.



Σχήμα8:Μοντέλο αναφοράς OSI

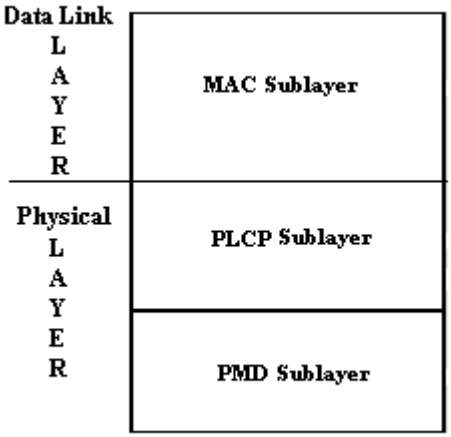
Το πρότυπο του 1997 καθορίζει τρεις επιτρεπόμενες τεχνικές μετάδοσης για το φυσικό στρώμα (PHY). Η μέθοδος των υπερύθρων χρησιμοποιεί σχεδόν την ίδια τεχνολογία με τα τηλεχειριστήρια των τηλεοράσεων. Οι άλλες δύο μέθοδοι χρησιμοποιούν ραδιοκύματα μικρής εμβέλειας χρησιμοποιώντας τεχνικές που ονομάζονται FHSS (Frequency Hopping Spread Spectrum) και DSSS (Direct Sequence Spread Spectrum). Και οι δύο χρησιμοποιούν ένα τμήμα του φάσματος στο οποίο δεν απαιτείται ειδική άδεια (τη ζώνη ISM στα 2,4 GHz). Το 1999 παρουσιάστηκαν δύο νέες τεχνικές για επίτευξη υψηλότερου εύρους ζώνης. Οι τεχνικές αυτές ονομάζονται OFDM (Orthogonal Frequency Division Multiplexing) και HR-DSSS (High Rate DSSS) και λειτουργούν μέχρι τα 54 Mbps και τα 11 Mbps αντίστοιχα. Το 2001 παρουσιάστηκε και μια δεύτερη τεχνική διαμόρφωσης OFDM, αλλά σε διαφορετική ζώνη συχνοτήτων από την πρώτη.

Στο σχήμα 9 φαίνεται η διαστρωμάτωση του προτύπου 802.11.



Σχήμα 9 . Διαστρωμάτωση του προτύπου 802.11

Η φιλοσοφία που ακολουθεί το πρότυπο 802.11 είναι η ύπαρξη ενός μόνο MAC που όμως υποστηρίζει περισσότερα του ενός φυσικά στρώματα. Κάθε φυσικό στρώμα όπως φαίνεται στο σχήμα 10, χωρίζεται σε δύο υποστρώματα.
Το υπόστρωμα PLCP (Physical Layer Convergence Procedure) χρησιμεύει στην προσαρμογή των διαφόρων φυσικών στρωμάτων στο κοινό MAC. Το υπόστρωμα PMD (Physical Medium Dependent) περιέχει όλες τις λειτουργίες που απαιτούνται για τη μετάδοση της πληροφορίας από το εκάστοτε φυσικό στρώμα.



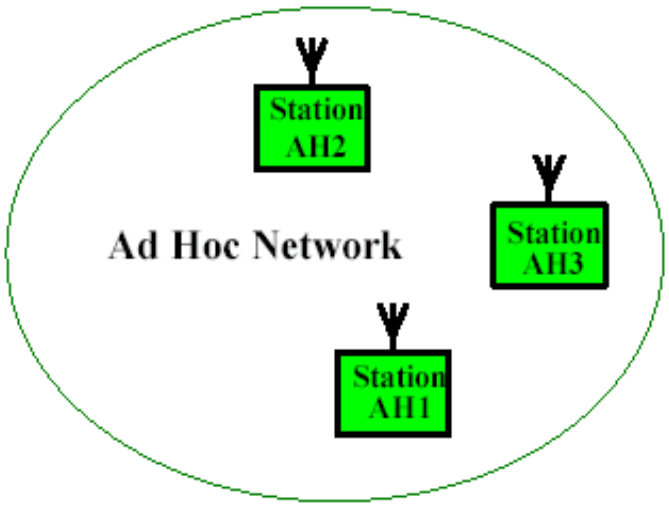
Σχήμα 10. Φυσικό Στρώμα προτύπου 802.11

2.2 Τοπολογία

Υπάρχουν δύο βασικές τοπολογίες, βάσει των οποίων ορίζονται δύο είδη ασύρματων δικτύων. Πρόκειται για τα ανεξάρτητα δίκτυα (independent networks) και τα δίκτυα υποδομής (infrastructure networks).

Ανεξάρτητα Δίκτυα

Το BSS (Basic Service Set - κυψέλη) αποτελείται από δύο ή περισσότερους ασύρματους κόμβους ή σταθμούς (STAs) και κάθε σταθμός επικοινωνεί απευθείας με όλους τους υπόλοιπους εφόσον βρίσκεται στη περιοχή ραδιοκάλυψής τους. Το BSS σε αυτή την περίπτωση αναφέρεται και ως IBSS (Independent Basic Service Set) ή ad-hoc BSS ή ad-hoc δίκτυο και είναι συνήθως προσωρινό, δηλαδή δημιουργείται για κάποιο σκοπό και στη συνέχεια διαλύεται. Πρόκειται για τον απλούστερο τύπο ασύρματου δικτύου. Ένα IBSS φαίνεται στο σχήμα 11.

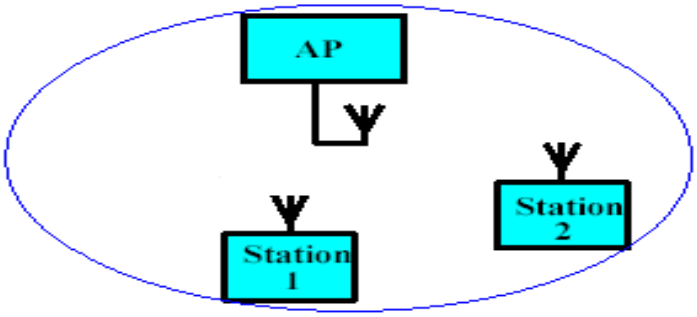


Σχήμα 11. Τοπολογία IBSS

Δίκτυα Υποδομής

Το BSS περιλαμβάνει ένα AP (Access Point-σταθμός βάσης). Το AP είναι υπεύθυνο για τη σύνδεση του BSS με το ενσύρματο δίκτυο, την ανταλλαγή πλαισίων μεταξύ των σταθμών και για τον κεντρικό έλεγχο της λειτουργίας του BSS. Όταν ένας σταθμός

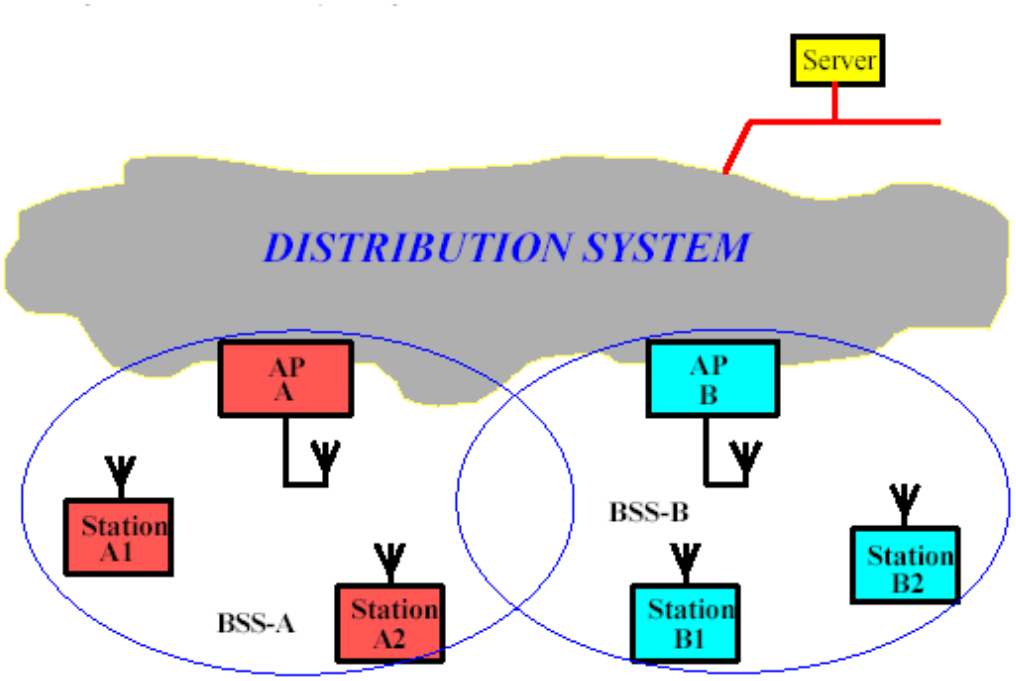
θέλει να στείλει ένα πλαίσιο σε έναν άλλο σταθμό, δεν του το στέλνει απευθείας, αλλά το πλαίσιο αποστέλλεται πρώτα στο AP και αυτό με τη σειρά του το στέλνει στον τελικό προορισμό. Η BSA (Basic Service Area) είναι η περιοχή ραδιοκάλυψης του AP. Δηλαδή οι σταθμοί πρέπει να βρίσκονται στην περιοχή ραδιοκάλυψης του AP για να επικοινωνήσουν μεταξύ τους, χωρίς να παίζει ρόλο η μεταξύ τους απόσταση όπως στην περίπτωση του IBSS. Για να συμμετέχει ένας σταθμός στο BSS θα πρέπει να ακολουθήσει τη διαδικασία association (σύνδεσης) με τον AP. Η διαδικασία αυτή ξεκινάει με πρωτοβουλία του σταθμού και είναι απόφαση του AP αν ο σταθμός θα γίνει δεκτός στο BSS. Ένα infrastructure δίκτυο φαίνεται στο σχήμα 12.



Σχήμα 12. Τοπολογία infrastructure BSS

Ένας αριθμός από BSSs μπορούν να συνδεθούν και να αποτελέσουν ένα ESS (Extended Service Set). Στο ESS τα APs των BSSs συνδέονται μέσω ενός ενσύρματου δικτύου κορμού, που

ονομάζεται σύστημα διανομής (Distribution System-DS). Με αυτόν τον τρόπο είναι εφικτή η επικοινωνία μεταξύ σταθμών που ανήκουν σε διαφορετικά BSSs αλλά στο ίδιο ESS. Σε αυτή την περίπτωση πρέπει τα APs να επικοινωνούν στο στρώμα ζεύξης δεδομένων μέσω του δικτύου κορμού, επιτελώντας τη λειτουργία της γέφυρας για τους σταθμούς διαφορετικών BSSs. Το ESS τελειώνει όταν παρεμβληθεί μεταξύ των APs οντότητα δικτύου που να λειτουργεί σε υψηλότερο στρώμα, όπως είναι ο δρομολογητής (router).Ένα infrastructure δίκτυο δύο BSSs φαίνεται στο σχήμα 13.



Σχήμα 13. Τοπολογία infrastructure δύο BSS

Το 802.11 προσφέρει κινητικότητα σε ένα ESS, αρκεί το δίκτυο κορμού να είναι ένα απλό LAN(Local Area Network) ή και VLAN (Virtual LAN). Σε κάθε άλλη περίπτωση η σύνδεση θα χαθεί εκτός και αν χρησιμοποιείται κάποια άλλη τεχνολογία όπως το Mobile IP.

2.3 Υπηρεσίες ασυρμάτου δικτύου 802.11

Το πρότυπο 802.11 καθορίζει ότι κάθε ασύρματο LAN που ακολουθεί το πρότυπο πρέπει να παρέχει εννέα υπηρεσίες. Οι υπηρεσίες αυτές διαιρούνται σε δύο κατηγορίες: πέντε υπηρεσίες διανομής που σχετίζονται με τη διαχείριση των μελών ενός BSS και την αλληλεπίδραση με σταθμούς εκτός BSS, και τέσσερις υπηρεσίες σταθμών που σχετίζονται με τις δραστηριότητες μέσα σε ένα BSS.

Υπηρεσίες διανομής

- Association (Συσχέτιση): Υπηρεσία συσχέτισης ενός σταθμού με το AP, προκειμένου να είναι σε θέση να δεχθεί και να στείλει πλαίσια μέσω του ασύρματου δικτύου. Τυπικά η υπηρεσία αυτή χρησιμοποιείται μόλις ένας σταθμός μετακινηθεί εντός της BSA του AP, οπότε και του ανακοινώνει την ταυτότητα και τις δυνατότητές του. Το AP μπορεί να δεχθεί ή και να απορρίψει το σταθμό. Αν τον αποδεχθεί θα πρέπει στη συνέχεια να γίνει authentication.
- Disassociation (Αποσυσχέτιση): Υπηρεσία αφαίρεσης ενός σταθμού ή του AP από το δίκτυο. Ένα AP μπορεί να την χρησιμοποιεί πριν απενεργοποιηθεί για λόγους συντήρησης. Το MAC του 802.11 μπορεί να χειριστεί και σταθμούς που εγκαταλείπουν το δίκτυο χωρίς να έχουν κάνει πρώτα χρήση της υπηρεσίας.
- Reassociation (Επανασυσχέτιση): Με τη συγκεκριμένη υπηρεσία ένας σταθμός μπορεί να αλλάξει AP. Είναι πολύ χρήσιμη για κινητούς σταθμούς που μετακινούνται από ένα BSS σε ένα άλλο.

- Distribution (Διανομή): Η υπηρεσία αυτή προσδιορίζει πώς θα δρομολογούνται τα πλαίσια που στέλνονται στο AP. Αν ο σταθμός-παραλήπτης βρίσκεται μέσα στο BSS τότε το πλαίσιο μπορεί να σταλθεί άμεσα από το AP, διαφορετικά θα πρέπει να σταλεί στο DS και από εκεί στο AP που σχετίζεται με τον παραλήπτη.
- Integration (Ενοποίηση): Υπηρεσία που παρέχεται από το DS. Όταν ένα πλαίσιο πρέπει να σταλεί μέσω ενός δικτύου που δεν είναι της μορφής 802.11 και χρησιμοποιεί διαφορετική μέθοδο διευθυνσιοδότησης ή μορφή πλαισίων, η υπηρεσία αυτή διαχειρίζεται τη μετατροπή από τη μορφή του 802.11 στη μορφή που απαιτείται από το δίκτυο προορισμού.

Υπηρεσίες σταθμών

- Authentication (Πιστοποίηση Ταυτότητας): Επειδή οι ασύρματες μεταδόσεις είναι εύκολο να σταλούν ή να ληφθούν από μη εξουσιοδοτημένους σταθμούς, ο σταθμός θα πρέπει να πιστοποιήσει την ταυτότητα του πριν του επιτραπεί να στείλει δεδομένα. Μόλις γίνει το association, το AP στέλνει στον σταθμό ένα ειδικό πλαίσιο "πρόσκλησης" για να δει αν ο σταθμός γνωρίζει το μυστικό κλειδί (συνθηματικό) που του έχει εκχωρηθεί. Ο σταθμός αποδεικνύει ότι γνωρίζει το μυστικό κλειδί κρυπτογραφώντας το πλαίσιο πρόσκλησης και στέλνοντάς το πίσω στο AP. Αν το αποτέλεσμα είναι ορθό, ο σταθμός εγγράφεται πλήρως στην κυψέλη.
- Deauthentication (Ακύρωση πιστοποίησης ταυτότητας): Τερματισμός μίας ισχύουσας κατάστασης authentication. Μετά την ακύρωση της πιστοποίησης, ο σταθμός δεν μπορεί πια να χρησιμοποιήσει το δίκτυο.
- Privacy (Προστασία Απορρήτου): Για να διατηρούνται εμπιστευτικές οι πληροφορίες που στέλνονται μέσω ενός ασύρματου LAN, θα πρέπει να κρυπτογραφούνται. Από το 802.11 έχει ορισθεί μία προαιρετική υπηρεσία κρυπτογράφησης των δεδομένων που ονομάζεται WEP (Wired Equivalent Privacy). Το WEP δεν προσφέρει σε

καμία περίπτωση ασφαλή μεταφορά δεδομένων και ήδη μελετάται η αντικατάστασή του.

MSDU (MAC Service Data Unit) *Delivery* (Παράδοση Πλαισίων MAC): Η υπηρεσία αυτή ασχολείται με την παράδοση πλαισίων MAC στον τελικό προορισμό τους.

2.4 Φυσικό στρώμα του 802.11

Στο φυσικό στρώμα προδιαγράφονται τρεις τεχνικές διαμόρφωσης:

- ***Infrared (Υπέρυθρες Ακτίνες)*** σε μήκη κύματος μεταξύ 850 και 950 nm με ρυθμούς μετάδοσης 1 και 2 Mbps.

- ***Frequency Hopping Spread Spectrum-FHSS (Εξάπλωση Φάσματος με Συνεχή Αλλαγή Συχνότητας)*** στην ISM μπάντα των 2,4 GHz με ρυθμούς μετάδοσης 1 και 2 Mbps.

- ***Direct Sequence Spread Spectrum-DSSS (Εξάπλωση Φάσματος Άμεσης Ακολουθίας)*** στην ISM μπάντα των 2,4 GHz με ρυθμούς μετάδοσης 1 και 2 Mbps.

2.5 Υπόστρωμα MAC του 802.11

Το πρότυπο IEEE 802.11 καθορίζει ένα κοινό medium access control (MAC) υπόστρωμα, το οποίο παρέχει μία ποικιλία υπηρεσιών που υποστηρίζουν τη λειτουργία ασύρματων δικτύων – wireless LANs (WLANS) που βασίζονται στο 802.11. Γενικώς, το υπόστρωμα MAC διαχειρίζεται και διατηρεί επικοινωνίες μεταξύ σταθμών που βασίζονται στο 802.11 με το να συντονίζει την πρόσβαση σε ένα κοινό radio κανάλι και χρησιμοποιώντας πρωτόκολλα που προάγουν τις επικοινωνίες σε ένα ασύρματο μέσον. Συχνά, αν το δούμε σαν τον εγκέφαλο του δικτύου, το υπόστρωμα 802.11 MAC χρησιμοποιεί ένα 802.11 φυσικό στρώμα (PHY), όπως το 802.11b ή το 802.11a, προκειμένου να εκτελέσει τις ενέργειες carrier sensing, μετάδοσης (transmit) και λήψης (receive) πλαισίων του 802.11.

2.5.1 Πρόσβαση στο μέσον

Προτού ξεκινήσει η μετάδοση πλαισίων, ένας σταθμός πρέπει πρώτα να αποκτήσει πρόσβαση στο μέσον, το οποίο είναι ένα κανάλι radio, κοινό για όλους τους σταθμούς. Το πρότυπο 802.11 ορίζει δύο μορφές πρόσβασης στο μέσον :

- Distributed Coordinated Function (DCF)
- Point Coordinated Function (PCF)

Το DCF είναι υποχρεωτικό και βασίζεται στο CSMA/CA (carrier sense multiple access with collision avoidance) πρωτόκολλο. Με το DCF, οι σταθμοί αγωνίζονται να διεκδικήσουν πρόσβαση και επιχειρούν να στείλουν πλαίσια όταν κανένας άλλος σταθμός δεν μεταδίδει. Αν ένας άλλος σταθμός στέλνει πλαίσια εκείνη τη στιγμή, οι σταθμοί διαθέτουν την ευγένεια και αναμένουν έως ότου απελευθερωθεί το κανάλι.
Για την υποστήριξη χρονικά περιορισμένης παράδοσης πλαισίων δεδομένων, το πρότυπο 802.11 ορίζει προαιρετικά τον αλγόριθμο Point Coordination Function (PCF) σύμφωνα με τον οποίο το σημείο πρόσβασης (access point) παραχωρεί την πρόσβαση στο μέσον για ένα σταθμό, σφυγμομετρώντας (polling) το σταθμό κατά τη περίοδο χωρίς ανταγωνισμό (contention free period). Οι σταθμοί δεν μπορούν να μεταδώσουν πλαίσια μέχρις ότου το access point τους σφυγμομετρήσει. Το χρονικό διάστημα για κίνηση δεδομένων που έχουν βάση τον αλγόριθμο PCF (αν είναι ενεργοποιημένος) συμβαίνει εναλλάξ ανάμεσα σε περιόδους ανταγωνισμού DCF.

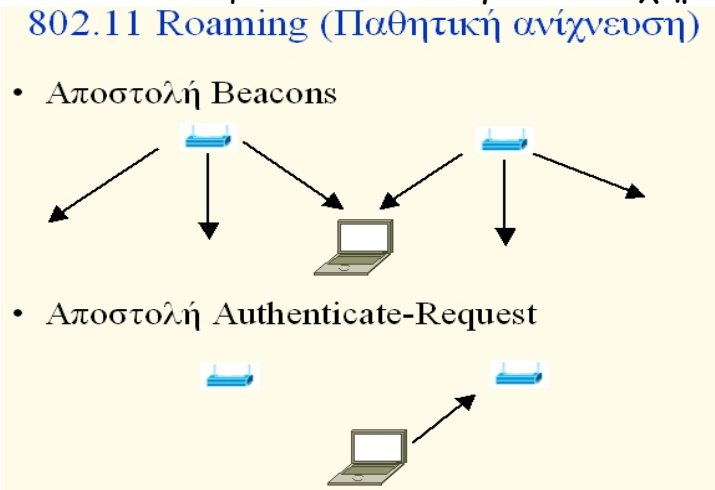
2.5.2 Πρόσβαση στο δίκτυο

Τα βασικά βήματα για να αποκτήσει ένας σταθμός πρόσβαση στο δίκτυο 802.11 είναι τα εξής:

Scanning (Σάρωση)

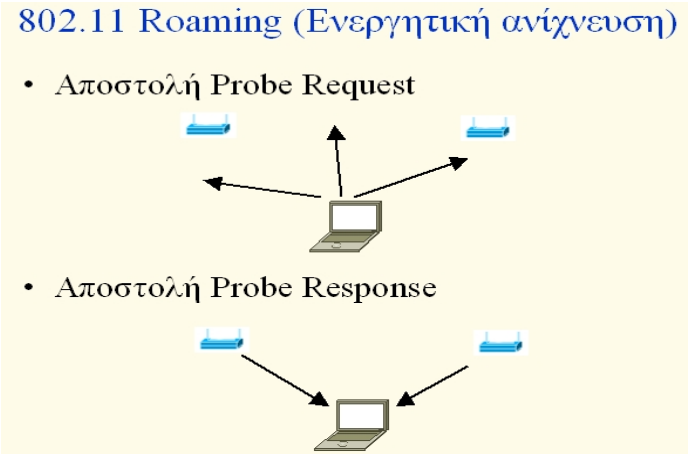
Το πρότυπο 802.11 ορίζει αμφότερα το παθητικό (passive) και ενεργό (active) scanning, όπου μία radio NIC (network interface card) ψάχνει για σημεία πρόσβασης (access points). Το passive

scanning είναι υποχρεωτικό όπου κάθε NIC σαρώνει τα κανάλια για να βρει το καλύτερο σημείο πρόσβασης (Access Point).
Κατά το passive scanning ο σταθμός δεν εκπέμπει τίποτα, εξοικονομώντας έτσι ενέργεια. Παρακολουθεί τα διαθέσιμα κανάλια ψάχνοντας για πλαίσια Beacon που δηλώνουν την ύπαρξη κάποιου δικτύου. Τα πλαίσια Beacon περιέχουν όλες τις απαραίτητες πληροφορίες για το BSS απ' όπου εκπέμπονται ώστε ο σταθμός να μπορεί να προχωρήσει στο επόμενο βήμα, δηλαδή στη διαδικασία του joining.
Η διαδικασία φαίνεται στο παρακάτω σχήμα.



Σχήμα 14. Παθητική ανίχνευση

Προαιρετικά το active scanning είναι παρόμοιο, εκτός του ότι η NIC ξεκινάει τη διαδικασία μεταδίδοντας ένα πλαίσιο ανίχνευσης (probe request frame), και όλα τα σημεία πρόσβασης (access points) εντός του βεληνεκούς απαντούν με απόκριση ανίχνευσης (probe response frame). Το active scanning δίνει τη δυνατότητα σε μία radio NIC να έχει άμεση απάντηση από τα access points, χωρίς να περιμένει τη μετάδοση ενός beacon πλαισίου. Ωστόσο, παραμένει το θέμα ότι το active scanning επιβάλλει πρόσθετο βάρος στο δίκτυο λόγω της μετάδοσης πλαισίων probe request και αντίστοιχων πλαισίων probe response.
Η διαδικασία αυτή φαίνεται στο παρακάτω σχήμα.



Σχήμα 15. Ενεργητική ανίχνευση

Όποιο τρόπο scanning κι αν ακολουθεί ο σταθμός, στο τέλος της διαδικασίας θα έχει αποκτήσει κάποιες βασικές πληροφορίες για τα διαθέσιμα δίκτυα.

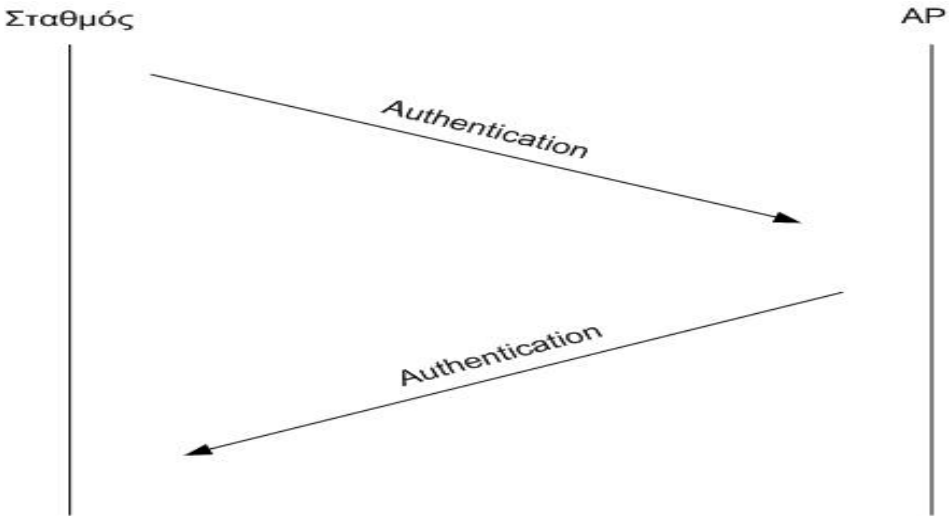
Joining (Σύνδεση)

Όταν εντοπιστεί το δίκτυο ακολουθεί η διαδικασία του joining, χωρίς όμως ο κινητός σταθμός να αποκτήσει ακόμα πρόσβαση στο δίκτυο. Η διαδικασία του joining δεν δίνει σε έναν σταθμό πρόσβαση στο δίκτυο, απλώς είναι ένα απαραίτητο βήμα στη διαδικασία του association. Ο σταθμός, έχοντας τις απαραίτητες πληροφορίες από το scanning, εξετάζει τις παραμέτρους κάθε BSS και αποφασίζει με ποιο από αυτά θα προχωρήσει τη διαδικασία του association.
Για να επιλέξει ο σταθμός ένα BSS πρέπει φυσικά να μπορεί να λειτουργήσει με τις συγκεκριμένες παραμέτρους του BSS. Επιπλέον, κριτήρια όπως το επίπεδο ισχύος ή η ένταση του σήματος από κάθε BSS παίζουν ρόλο. Παρόλα αυτά δεν υπάρχει συγκεκριμένη διαδικασία επιλογής ενός δικτύου έναντι κάποιου άλλου. Η επιλογή γίνεται εσωτερικά στο σταθμό και εξαρτάται από τον εκάστοτε κατασκευαστή.

Authentication (Πιστοποίηση)

Authentication είναι η διαδικασία κατά την οποία αποδεικνύεται και πιστοποιείται η ταυτότητα. Η διαδικασία αυτή είναι εξαιρετικά σημαντική στη διατήρηση της ασφάλειας στα ασύρματα δίκτυα,

εφόσον δεν υπάρχουν ουσιαστικά φυσικοί περιορισμοί για κάποιον που θέλει να αποκτήσει πρόσβαση σε ένα δίκτυο. Το πρότυπο 802.11 προδιαγράφει δύο είδη διαδικασιών πιστοποίησης : Open System Authentication και Shared Key Authentication.Για την πιστοποίηση πρέπει να ανταλλαχθούν οι κατάλληλες πληροφορίες και κλειδιά, όπως φαίνεται στο παρακάτω σχήμα 16.



Σχήμα 16. Διαδικασία Πιστοποίησης

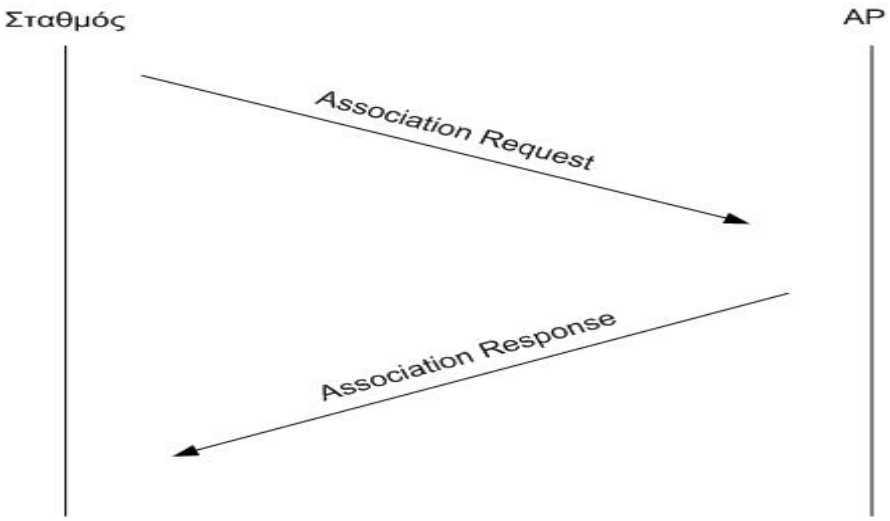
Deauthentication (Ακύρωση Πιστοποίησης)

Προκειμένου ένας σταθμός (που είναι πιστοποιημένος στο δίκτυο) να εγκαταλείψει το δίκτυο, πρέπει να ακυρώσει την πιστοποίησή του. Μετά την ακύρωση της πιστοποίησης, ο σταθμός δεν έχει πλέον τη δυνατότητα να χρησιμοποιήσει το δίκτυο.

Association (Συσχέτιση)

Μόλις γίνει η πιστοποίηση, η radio NIC πρέπει να συσχετιστεί με το access point προτού αρχίσει την αποστολή πλαισίων δεδομένων (data frames). Η Συσχέτιση (Association) είναι αναγκαία προκειμένου να γίνει ο συγχρονισμός σπουδαίων πληροφοριών, όπως ο υποστηριζόμενος ρυθμός δεδομένων,

ανάμεσα στο radio NIC και το access point. Η radio NIC ξεκινάει τη Συσχέτιση (Association) στέλνοντας ένα Association Request Frame που περιέχει στοιχεία ταυτότητας και υποστηριζόμενο ρυθμό δεδομένων. Το access point απαντάει στέλνοντας ένα Association Response Frame που περιέχει ένα Association Identification μαζί με άλλες πληροφορίες που αφορούν το access point. Μόλις η radio NIC και το access point ολοκληρώσουν τη διαδικασία του Association, τότε μπορούν να στείλουν πλαίσια δεδομένων το ένα στο άλλο.
Η όλη διαδικασία φαίνεται στο παρακάτω σχήμα.



Σχήμα 17. Διαδικασία Συσχέτισης

3. Ασύρματος εξοπλισμός


Στη παράγραφο αυτή αναφερόμαστε συνοπτικά σε όλες εκείνες τις μονάδες που συνθέτουν τον απαραίτητο ασύρματο εξοπλισμό, για να μπορεί να γίνει εφικτή η πρόσβαση στο δίκτυο. Οι μονάδες αυτές είναι οι εξής:

1) *Κεραία*

Ένας απλοϊκός ορισμός της κεραίας αναφέρεται σε μια συσκευή που λαμβάνει και εκπέμπει σήματα. Το σχήμα και το μέγεθος της κεραίας έχουν να κάνουν σε μεγάλο ποσοστό, με τη συχνότητα του σήματος που λαμβάνει. Να διασαφηνίσουμε εδώ ότι η κεραία δε δίνει στον εκπομπό μεγαλύτερη ενέργεια. Ουσιαστικά η κεραία είναι μια κατευθυντική συσκευή η οποία δίνει το σχήμα κατεύθυνσης (directional pattern) για το σήμα που παράγει ο εκπομπός. Έτσι γνωρίζοντας αυτό το directional pattern, μπορεί να λάβει και καλύτερο σήμα από κάποιον άλλο εκπομπό.
Ο τύπος της κεραίας καθορίζει την μορφή ακτινοβολίας. Οι κεραίες διακρίνονται σε μη κατευθυντικές που είναι κατάλληλες για την κάλυψη των μεγάλων περιοχών, δικατευθυντικές που είναι κατάλληλες για την κάλυψη των διαδρόμων και μονοκατευθυντικές, που ενδείκνυνται για την σύνδεση μεταξύ κτηρίων (point-to-point). Αξίζει να αναφέρουμε εδώ τους βασικούς τύπους κεραιών :
Dipole: Χρησιμοποιείται για να καλύψει ένα διάδρομο, μία μεγάλη ή και μικρή περιοχή
Vertical: Έχει κέρδος από 3-10 dBi. Είναι μη κατευθυντική σε οριζόντια κατεύθυνση. Είναι μεγαλύτερη από κάθε άλλη κεραία καθώς επίσης και ακριβότερη. Την χρησιμοποιούμε για να καλύψουμε μια περιοχή στην οποία υπάρχουν αρκετά κτίρια που θέλουμε να συνδεθούν ασύρματα.
Yagi: Είναι μια υψηλούς κέρδους (12-18dBi) μονοκατευθυντική κεραία.
Parabolic: Έχει πολύ υψηλό κέρδος μέχρι και 24 dBi (very narrow beam widths). Χρησιμοποιείται στην περίπτωση που θέλουμε να συνδέσουμε δύο κτίρια. Μια τέτοια κεραία έχει εμβέλεια μέχρι και 20 miles. Και οι δύο πλευρές αυτής της ασύρματης σύνδεσης έχουν την ίδια κεραία, οι οποίες πρέπει και να σημαδεύονται σωστά. Παραβολική είναι και η κεραία τύπου grid.

Στο παρακάτω σχήμα φαίνονται παραδείγματα αυτών των τύπων κεραίας.

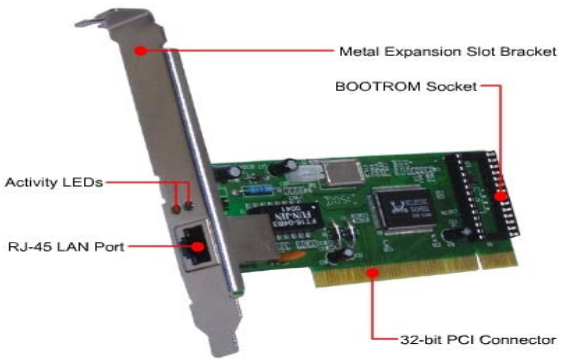
Vertical Grid Parabolic Yagi Dipole

Σχήμα 18. Τύποι κεραιών.

Για να κάνουμε κατανοητή την ορολογία dBi να πούμε ότι όρος dBi υποδηλώνει το υποτιθέμενο κέρδος μίας ισοτροπικής κεραίας (υποθετική κεραία που ακτινοβολεί ενέργεια προς όλες τις κατευθύνσεις). Για παράδειγμα 0dBi είναι το κέρδος μίας υποθετικής κεραίας που ακτινοβολεί όλη την ισχύ της σε μία τέλεια ομοιόμορφη σφαιρική κατανομή. Κεραίες με τέτοια ακτινοβολία δεν υπάρχουν στην πραγματικότητα.

2. *NIC*

NIC ή διαφορετικά Network Interface Card, είναι το υλικό ενσωματώνεται στην κεντρική μητρική κάρτα του υπολογιστή μας (motherboard) ή εισάγεται στο δίαυλο διασύνδεσης (bus) και έχει ως σκοπό τη σύνδεση του υπολογιστή μας με το υποσύστημα επικοινωνίας (καλωδίωση) του δικτύου μας. Κλασσικά παραδείγματα καρτών NIC's είναι αυτές που αποτελούν interface μεταξύ ενός υπολογιστή και ενός Ethernet LAN (Σχήμα 19) ή ενός FDDI δικτύου δακτυλίου.



Σχήμα 19. PCI Ethernet Network Interface Card

3) Καλώδιο RF.

Πρόκειται για το ένα από τα δύο καλώδια που απαιτούνται. Όταν η απόσταση της κεραίας από την κάρτα δικτύου είναι μεγαλύτερη από 50cm χρειάζεται ένα καλώδιο κεραίας που να συνδέει την υποδοχή της κεραίας με το pigtail (αναλύεται παρακάτω).

4) Connectors.

Οι connectors είναι το υλικό που απαιτείται για την διασύνδεση αλλά και την προσαρμογή των επαφών (ακροδεκτών) της κάρτας δικτύου με το σύστημα καλωδίωσης. Στην περίπτωση μάλιστα εξωτερικής χρήσης οι connectors, πρέπει να είναι σωστά τοποθετημένοι, έτσι ώστε τα καλώδια να είναι απόλυτα στεγνά και προστατευμένα. Ένας connector φαίνεται στο παρακάτω σχήμα.

Σχήμα 20. MTRJ fiber optic network connector.

5) UTP καλώδιο.

Το UTP ή διαφορετικά unshielded twisted pair καλώδιο αποτελείται από δύο μη προστατευμένα καλώδια γυρισμένα το ένα γύρω από το άλλο. Αυτά τα καλώδια είναι τα πιο συχνά χρησιμοποιούμενα καλώδια, αφού είναι εύκολα στην

εγκατάσταση και τα πιο οικονομικά. Επίσης χρησιμοποιούνται για την διασύνδεση των συσκευών Wireless to Ethernet Bridge ή USB που τοποθετούνται στην κεραία (όταν το σημείο σύνδεσης με την κεραία μας είναι μακριά από το Η/Υ).

Σχήμα 21. UTP cable.

Το καλώδιο που φαίνεται στο παραπάνω σχήμα είναι UTP 5^{ης} κατηγορίας με λίγο διαφορετική δομή από αυτή που περιγράψαμε και επιτυγχάνει ταχύτητες μεγαλύτερες των 100 million bits per second.

6) <u>Pigtail καλώδιο.</u>

Το καλώδιο Pigtail είναι απλά ένα μικρό κομμάτι καλώδιο με connectors προσαρμογής για την ένωση του αποκλειστικού connector της κάρτας Wi-Fi με το καλώδιο της εξωτερικής κεραίας. Υπάρχουν αρκετοί τύποι αυτού του καλωδίου. ένας από αυτούς φαίνεται στο σχήμα που ακολουθεί.

Σχήμα 22. pigtail cable (type T47)

7) <u>Γέφυρα-Bridge</u>

Μια γέφυρα δικτύου (network bridge), αφηρημένα μπορούμε να πούμε ότι είναι μια συσκευή που συνδέει πολλαπλά τμήματα του δικτύου (network segments) μέσω του επιπέδου

συνδέσμου μετάδοσης δεδομένων (data link layer).Όταν μιλάμε για network segments, μιλάμε για κομμάτια του δικτύου τα οποία χωρίζονται μεταξύ τους από κάποια δικτυακή συσκευή όπως hubs, switches, routers κ.α . Έτσι λοιπόν σε ένα δίκτυο υπολογιστών μια γέφυρα μπορεί να είναι ένας switch.Ο switch να πούμε εδώ ότι συνήθως χρησιμοποιείται για τοπολογία αστέρα.

Σχήμα 23. Linksys 10/100 Etherfast 8 Port Switch – EZXS88W

8) <u>Δρομολογητής (Router).</u>

Router ή δρομολογητή μπορούμε να θεωρήσουμε ένα ειδικού σκοπού υπολογιστή ο οποίος κατευθύνει τα πακέτα δεδομένων στο δίκτυο. Οι δρομολογητές είναι συσκευές που μπορούν να ανιχνεύσουν εάν μέρος του δικτύου δεν λειτουργεί ή βρίσκεται σε συμφόρηση και να επανακατευθύνουν την πληροφορία.

Επίσης οι routers επιτρέπουν την διασύνδεση δικτύων με διαφορετικά πρωτόκολλα επικοινωνίας. Ο router είναι η μόνη συσκευή που ουσιαστικά βλέπει κάθε μήνυμα που αποστέλλεται και από τις δύο πλευρές του δικτύου. Έτσι μπορεί να διασφαλίσει ότι η πληροφορία θα φτάσει στον προορισμό της και απαγορεύει την πρόσβαση από το ένα δίκτυο στο άλλο, απαγορεύοντας μη αναγκαία πληροφορία να μεταφέρεται από δίκτυο σε δίκτυο. Οι routers συνδέουν πολλαπλά δίκτυα LAN και έχει πρόσβαση στις network addresses. Στο παρακάτω σχήμα φαίνεται ένας δρομολογητής της εταιρίας NETGEAR.

Σχήμα 24. NETGEAR RP114 Web Safe 4 Port Cable/DSL Network Route

4.Υποπρότυπα του 802.11

Οι αναθεωρήσεις του Πρότυπου 802.11.

Από τότε που έγινε η επικύρωση του αρχικού προτύπου, η ομάδα εργασίας του IEEE 802.11 έκανε αρκετές αναθεωρήσεις μέσω διαφόρων ομάδων αναθεώρησης.

Η σημασία των γραμμάτων

Οι ομάδες αναθεώρησης εντός της ομάδας εργασίας του 802.11 έχουν ως αποστολή την ενίσχυση – εμπλουτισμό τμημάτων του προτύπου 802.11. Ένα ειδικό γράμμα του αλφαβήτου που αντιστοιχεί σε κάθε αναθεώρηση, όπως π.χ. 802.11a, 802.11b κλπ, αντιπροσωπεύει τις διάφορες ομάδες αναθεώρησης. Ως παράδειγμα μπορούμε να αναφέρουμε την ομάδα αναθεώρησης B (δηλαδή 802.11b) που είναι υπεύθυνη για την αναβάθμιση του αρχικού πρότυπου 802.11 έτσι ώστε να συμπεριλάβει λειτουργία υψηλότερου ρυθμού μετάδοσης δεδομένων χρησιμοποιώντας DSSS στη μπάντα των 2,4 GHz.

4.1 802.11a-OFDM στη μπάντα των 5 GHz

Το 802.11a είναι ένα πρότυπο φυσικού επιπέδου (IEEE Std. 802.11a – 1999) που προδιαγράφει τη λειτουργία στη μπάντα των 5 GHz χρησιμοποιώντας OFDM (Orthogonal Frequency Division Multiplexing / Ορθογωνική Πολυπλεξία Διαίρεσης Συχνότητας). Η βασική ιδέα πίσω από την OFDM είναι η διαίρεση ενός κύριου υψηλού ρυθμού σε πολλούς μικρότερους ρυθμούς και η χρήση αυτών για την αποστολή των δεδομένων ταυτόχρονα. Όλα τα «αργά» κανάλια πολυπλέκονται τελικά σε ένα «γρήγορο» κανάλι και μεταδίδονται. Με την ορθογονοποίηση λύνεται το πρόβλημα της σπατάλης του εύρους ζώνης, προκειμένου να διαχωρίσουμε τα κανάλια μεταξύ τους. Το 802.11a υποστηρίζει ρυθμούς μετάδοσης

δεδομένων που εκτείνονται από 6 έως 54 Mbps. Συσκευές και προϊόντα που στηρίζονται στο πρότυπο 802.11a άρχισαν να γίνονται διαθέσιμα προς το τέλος του έτους 2001.
Επειδή η λειτουργία γίνεται στη μπάντα των 5 GHz, το 802.11a προσφέρει καλύτερη συμπεριφορά στις παρεμβολές ασύρματο συχνοτήτων από ότι άλλα φυσικά πρωτόκολλα (PHY) (π.χ. 802.11b και 802.11g) που χρησιμοποιούν συχνότητες στη μπάντα των 2,4 GHz. Με υψηλούς ρυθμούς μετάδοσης δεδομένων και σχετικά πολύ μικρές παρεμβολές, το 802.11a είναι κατάλληλο για την υποστήριξη εφαρμογών πολυμέσων και πυκνοκατοικημένα περιβάλλοντα χρηστών. Αυτό καθιστά το 802.11a μία εξαιρετική λύση μακράς διαρκείας για να ικανοποιηθούν τρέχουσες και μελλοντικές απαιτήσεις. Συστήνεται να ληφθεί σοβαρά υπόψη η ανάπτυξη του 802.11a, εκτός και αν οι περιστάσεις προτρέπουν τη χρήση ενός διαφορετικού φυσικού πρωτοκόλλου (PHY), όπως το 802.11b.

Οφέλη και επιπτώσεις του 802.11

Τα οφέλη του 802.11a είναι τα εξής:

- **Υψηλότερη απόδοση**. Κατά πολύ ο κυριότερος λόγος για να χρησιμοποιήσουμε το 802.11a είναι η ανάγκη να υποστηριχθούν οι εφαρμογές με υψηλότερες απαιτήσεις όπως αυτές που περιλαμβάνουν βίντεο, φωνή, και τη μετάδοση μεγάλων εικόνων και αρχείων. Επιπλέον, το 802.11a προσφέρει την υποστήριξη των χρηστών σε πυκνοκατοικημένες περιοχές, οι οποίοι έχουν απαιτήσεις χαμηλότερου εύρους συχνοτήτων, όπως το σερφάρισμα στο Διαδίκτυο. Το 802.11a μπορεί να μεταφέρει ρυθμούς δεδομένων μέχρι τα 54Mbps και υπάρχει αρκετός χώρος

στο φάσμα των 5GHz για να υποστηρίξει μέχρι 12 σημεία πρόσβασης που λειτουργούν στην ίδια περιοχή χωρίς να προκαλέσει παρεμβολή μεταξύ των σημείων πρόσβασης. Αυτό σημαίνει 432Mbps (12 X 54Mbps), συνολικός ρυθμός μετάδοσης δεδομένων. Ούτε τα επερχόμενα πρότυπα όπως το 802.11g, που θα προσφέρουν ρυθμό μετάδοσης 54Mbps στη ζώνη των 2.4GHz δεν πλησιάζουν στην απόδοση του 802.11a. Στο 802.11g υπάρχει το ίδιο πρόβλημα όπως με 802.11b: Έχουμε μόνο τρία μη-επικαλυπτόμενα κανάλια για τον καθορισμό σημείων πρόσβασης, το οποίο περιορίζει σοβαρά την χωρητικότητα.

- **Λιγότερη παρεμβολή RF.** Η αυξανόμενη χρήση της συχνότητας των 2.4GHz όπως στα ασύρματα τηλέφωνα και των συσκευών Bluetooth συσσωρεύει το ασύρματο φάσμα μέσα σε πολλές εγκαταστάσεις. Αυτό μειώνει σημαντικά την απόδοση του 802.11a στα ασύρματα LANs.

Τα μειονεκτήματα 802.11a εξής είναι:

- **Μικρή περιοχή κάλυψης**. Η ανώτερη απόδοση του 802.11a προσφέρει την άριστη υποστήριξη για εφαρμογές που δεν απαιτούν μεγάλο εύρος ζώνης, αλλά η υψηλότερη συχνότητα λειτουργίας εξισώνει τη σχετικά μικρή περιοχή κάλυψης. Εντούτοις, ακόμη και με αυτόν τον περιορισμό, το 802.11a μπορεί μερικές φορές να προσφέρει καλύτερη απόδοση από το 802.11b στην ίδια περιοχή κάλυψης από το σημείο πρόσβασης. Για παράδειγμα στην περιοχή των 100 ποδιών, το 802.11a μπορεί να προσφέρει 24Mbps, αλλά οι συσκευές που χρησιμοποιούν το 802.11b στην ίδια περιοχή λειτουργούν στα 5.5Mbps.

- **Περιορισμένη διαλειτουργικότητα**. Το 802.11a δεν μπορεί να επικοινωνήσει με το 802.11b. Για παράδειγμα, ένας τελικός χρήστης που εξοπλίζεται με ένα 802.11a NIC δεν

θα είναι σε θέση να συνδεθεί με ένα σημείο πρόσβασης του 802.11b. Τα τυποποιημένα standard του 802.11 δεν παρέχουν διαλειτουργικότητα μεταξύ των διαφορετικών φυσικών στρωμάτων. Η λύση σε αυτό το πρόβλημα είναι πολλαπλού τύπου κάρτες για ασύρματα δίκτυα που υποστηρίζουν πολλαπλά 802.11 PHYs, όπως τα 802.11a/b, 802.11a/g, κ.λ.π. Αυτές οι κάρτες ξεκίνησαν να διατίθενται στην αγορά στο τέλος του 2002. Κατά συνέπεια, ένα ασύρματο 802.11a/b μέσα σε μια συσκευή τελικού χρήστη αυτόματα θα καταλάβει εάν το σημείο πρόσβασης είναι το 802.11a ή το 802.11b και επικοινωνεί έπειτα αναλόγως.

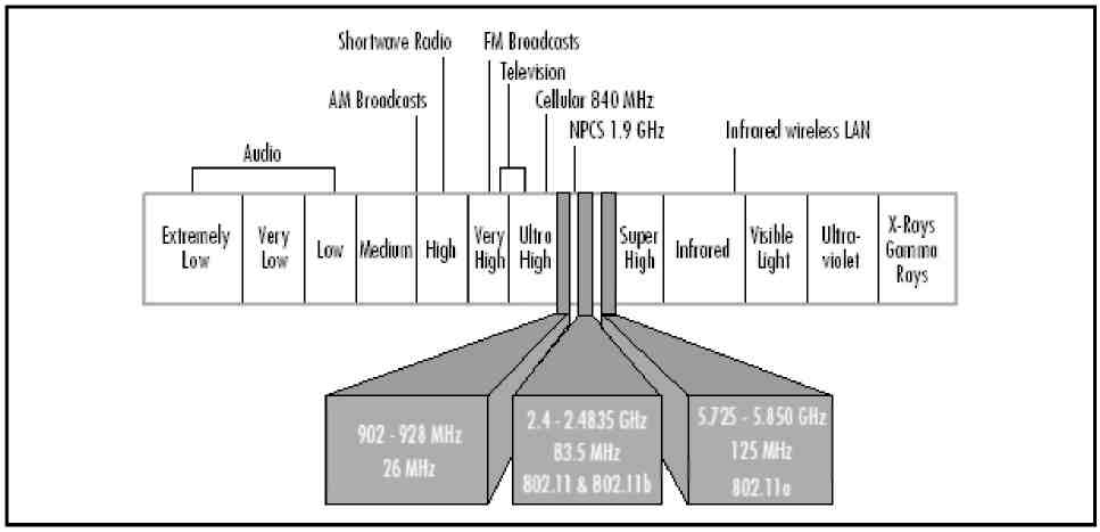
Επιπλέον, ένα σημείο πρόσβασης μπορεί επίσης να προσφέρει μια διπλή λύση όπως το 802.11a/b, επιτρέποντας τη διαλειτουργικότητα με τις συσκευές τελικών χρηστών που εξοπλίζονται με ένα ασύρματο 802.11a ή 802.11b.

- **Υψηλότερο κόστος**. Οι πρόσφατες τιμές των προϊόντων του προτύπου 802.11a είναι περίπου 30 τοις εκατό υψηλότερες από το 802.11b, αλλά το χάσμα αυτό έχει ξεκινήσει και μειώνεται. Εντούτοις η υψηλή τιμή σήμερα, του 802.11 αναγκάζει μερικές επιχειρήσεις να εγκαταστήσουν το 802.11b προκειμένου να μειώσουν τις αρχικές δαπάνες. Το 802.11a είναι διαθέσιμο σήμερα και λειτουργεί σε ένα πολύ μικρό συσσωρευμένο μέρος του φάσματος και έτσι παρέχει μεγαλύτερη χωρητικότητα. Το 802.11a είναι σαφώς μια καλύτερη μακροπρόθεσμη λύση, ειδικά όταν δεν είναι γνωστές οι μελλοντικές ανάγκες απόδοσης . Είναι καλύτερο κάποιος να αυξήσει το κόστος της πρώτης εγκατάστασης και να έχει μια πολύ καλή λύση για το μέλλον παρά να χρειαστεί αργότερα να αντικαταστήσει το υλικό.

4.2 802.11b – Υψηλός ρυθμός μετάδοσης DSSS στη μπάντα των 2,4 GHz

Το 802.11b είναι το πρώτο wireless πρωτόκολλο που κατάφερε να μπει τόσο δυναμικά στο χώρο της δικτύωσης, έναν χώρο που γνωρίζει ελάχιστες επαναστάσεις και αλλαγές. Το πρωτόκολλο 802.11, του οποίου το b αποτελεί επέκταση, και είναι ένας ορισμός του Media Access Control(MAC) καθώς και τριών διαφορετικών και ασύμβατων φυσικών επιπέδων(Physical Layers στο υπάρχον δικτυακό μοντέλο OSI. Το πρωτόκολλο εγκρίθηκε από την ομάδα 802 της IEEE στις 26 Ιουνίου του 1997 και θέτει το πλαίσιο για μια προτυποποιημένη ασύρματη δικτυακή επικοινωνία ευρείας ζώνης. Στις παρακάτω σελίδες δίνουμε μια περιγραφή του 802.11 πρωτοκόλλου, και επεκτείνουμε την έρευνά μας στις επεκτάσεις και τροποποιήσεις που προσέθεσε το 802.11b.

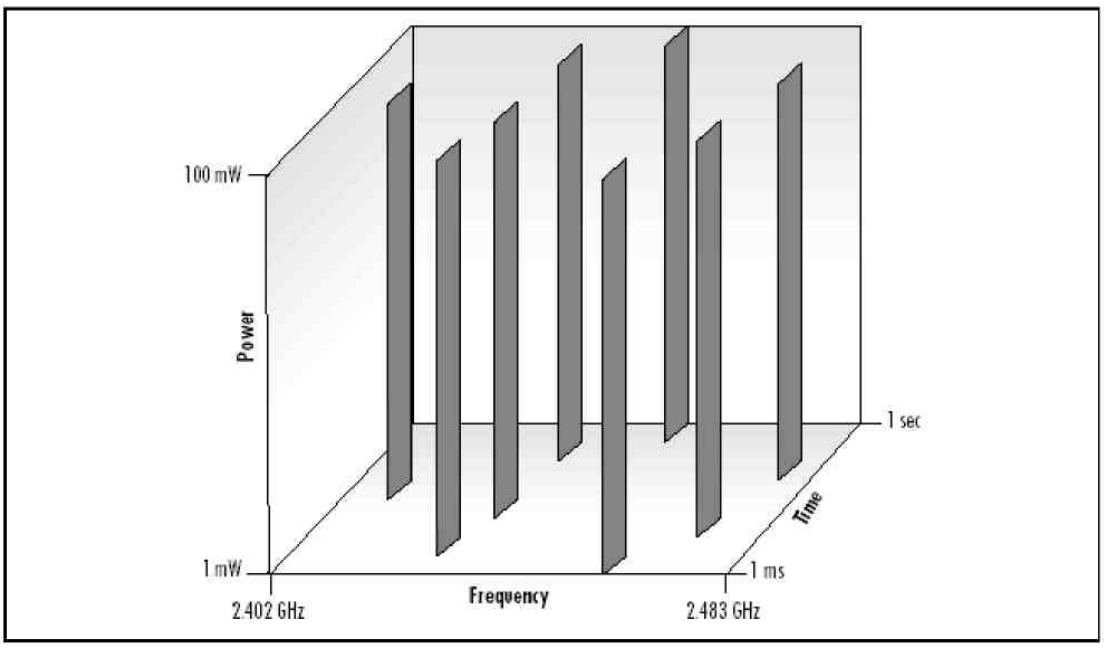
Για τη μετάδοση των δεδομένων το πρωτόκολλο χρησιμοποιεί τη μπάντα των 2.4 GHz. Για να αποφεύγονται παρεμβολές από ραδιοφωνικά σήματα στις ΗΠΑ η Federal Communications Commission(FCC) είναι υπεύθυνη για την εκχώρηση μικρών περιοχών στο φάσμα των ραδιοσυχνοτήτων. Η χρήση οποιασδήποτε από τις ζώνες που ορίζει η FCC, πρέπει να συνοδεύεται από ειδική άδεια. Η FCC παράλληλα χαρακτηρίζει ελεύθερα κάποια τμήματα του ραδιοφωνικού φάσματος. Αυτές οι μπάντες ονομάζονται ISM(Industrial Scientific and Medical) και μπορούν να χρησιμοποιούνται χωρίς άδεια. Στο σχήμα που ακολουθεί μπορούμε να δούμε αναλυτικά το ραδιοφωνικό φάσμα και τις ελεύθερες περιοχές του.



Εικόνα 25 :Οι ελεύθερες περιοχές

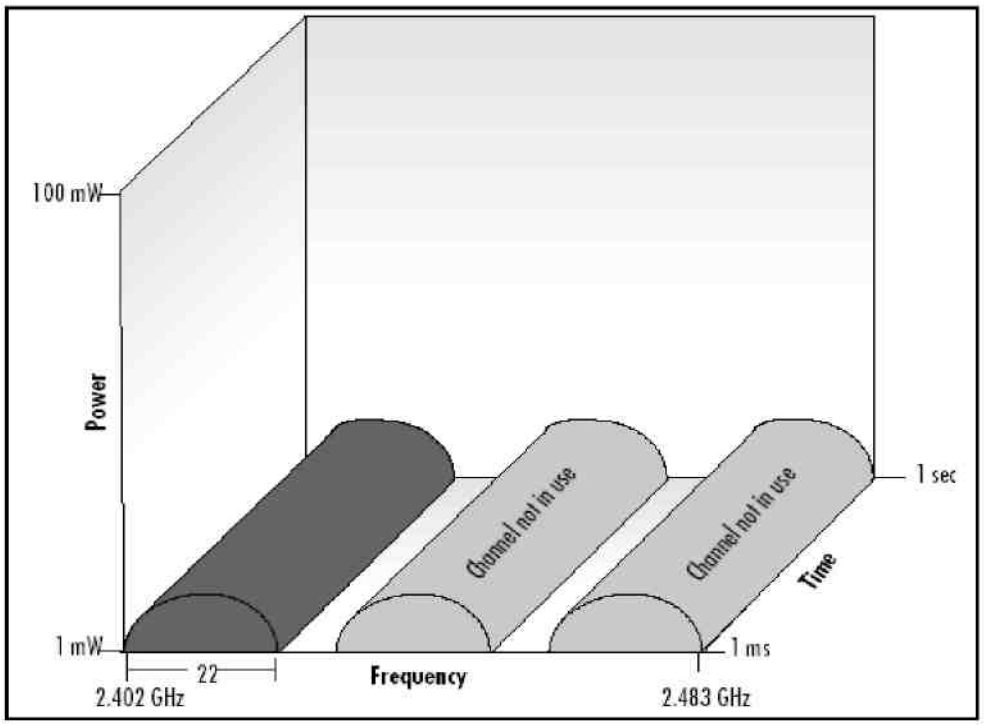
Το 802.11b χρησιμοποιεί όπως βλέπουμε μια ελεύθερη ζώνη η οποία είναι πλήρως ελεύθερη για εκπομπή χαμηλής ισχύος. Όλα τα παραπάνω βέβαια, ισχύουν στις ΗΠΑ. Ευτυχώς και οι υπόλοιπες παρόμοιας ευθύνης οργανώσεις κάθε χώρας συμβαδίζουν, λιγότερο η περισσότερο με αυτά τα πρότυπα της FCC.Δυστυχώς, το νομικό πλαίσιο που διέπει τις λεπτομέρειες χρήσης αυτής της μπάντας, εξαρτάται σε μεγάλο βαθμό από την νομοθεσία κάθε χώρας. Μεγάλα είναι τα νομικά κενά σε πολλές χώρες, όπως και στην Ελλάδα, που αφήνουν πολλά ερωτηματικά ως προς την μέγιστη νόμιμη εκπεμπόμενη ισχύ, την εμπορική ή όχι χρήση του ραδιοφωνικού φάσματος αυτού και πολλά άλλα.
Η ισχύς που ορίζει το στάνταρτ στις εξόδους της κεραίας των εμπορικών συσκευών είναι τα 0.2mw, το οποίο με τις μικρές εργοστασιακές κεραίες που συνοδεύουν τις συσκευές WiFi, δίνει στο 802.11b εμβέλεια της τάξεως των 300μ σε ανοιχτό χώρο. Λόγω της φύσης των μικροκυματικών συχνοτήτων, η εμβέλεια συσκευών WiFi μειώνεται αισθητά όταν μεταξύ τους παρεμβάλλονται τσιμεντένιοι τοίχοι, δέντρα(και γενικώς αντικείμενα που περιέχουν νερό) ή μεταλλικές πόρτες. Μείωση της ποιότητας σύνδεσης, σημαίνει αρχικά μειωμένο throughput του δικτύου με υψηλό ρυθμό σφαλμάτων, και στην χειρότερη περίπτωση αδυναμία σύνδεσης των συσκευών. Για τον ίδιο λόγο,

μακρινές συνδέσεις (>300μ) επιτυγχάνονται μόνο σε καταστάσεις όπου η μία συσκευή έχει οπτική επαφή με την άλλη (Line of Site), ένας κανόνας που ευτυχώς δεν είναι τόσο αυστηρός(καταστάσεις near-LOS). Αντανακλάσεις του σήματος μπορεί να επιτρέψουν σύνδεση χωρίς LOS. Βεβαίως, όπως είναι αναμενόμενο, για την επίτευξη ζεύξεων πολύ μεγάλων αποστάσεων, υπάρχει το φυσικό εμπόδιο της καμπυλότητας της γης. Ακόμη και αν καταφέρουμε δηλαδή να ενισχύσουμε την εκπομπή και την λήψη των 802.11 συσκευών μας, προσπαθώντας να καταστήσουμε δυνατή μια σύνδεση μεγάλης απόστασης, δεν είναι δυνατό να ξεπεράσουμε την δεδομένη μέγιστη απόσταση (~20μίλια), στην οποία η ίδια η γη εμποδίζει την οπτική επαφή.
Στο αρχικό πρωτόκολλο 802.11, καθορίζονται δύο τρόποι κωδικοποίησης, ο FHSS (Frequency Hopping Spread Spectrum) και ο DSSS (Direct Sequence Spread Spectrum). Στον FHSS, η εκπομπή-λήψη μοιράζεται σε 75 κανάλια του ενός MHz και εναλλάσσεται συνεχώς σε ένα από αυτά. Χρησιμοποιώντας αυτή την τεχνική, ο εκπομπός στέλνει τα δεδομένα διαδοχικά σε μια ακολουθία από φαινομενικά τυχαίες συχνότητες(frequency hopping). Ο δέκτης ακολουθεί την ίδια ακολουθία εναλλαγής καναλιών συχνότητας με τον εκπομπό και λαμβάνει το μήνυμα. Το μήνυμα μπορεί να ληφθεί ακέραιο, μόνο όταν είναι γνωστή η ακολουθία της εναλλαγής συχνοτήτων. Καθώς μόνο ο δέκτης γνωρίζει την σωστή ακολουθία, το μήνυμα είναι αναγνώσιμο μόνο από τον πραγματικό του παραλήπτη. Με αυτή την τεχνική, ηλεκτρομαγνητικές παρεμβολές στον χώρο της λήψης θα επηρεάσουν μόνο ένα τμήμα του μηνύματος, έχοντας ως αποτέλεσμα την ανάγκη για επανεκπομπή μόνο μικρού όγκου μηνυμάτων. Ο συγκεκριμένος τρόπος κωδικοποίησης μπορεί να δώσει ταχύτητες μεταφοράς δεδομένων έως και 2mbit. Ακολουθεί γράφημα που δείχνει την τεχνική FHSS συναρτήσει της ισχύος και του χρόνου.



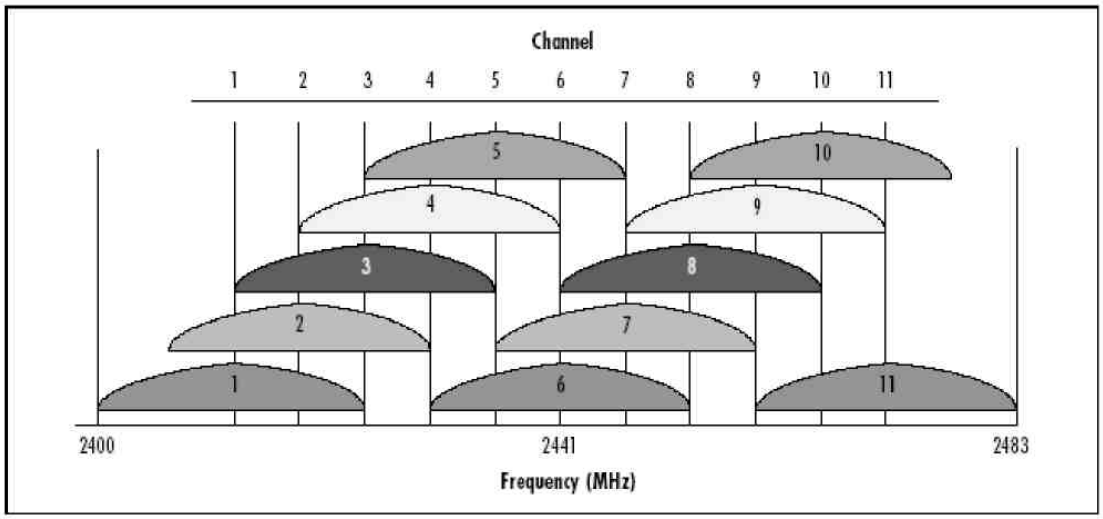
Εικόνα 26: FSSS συναρτήσει ισχύος και χρόνου

Στον DSSS το φάσμα χωρίζεται σε 14 μερικώς (ανά ~4) επικαλυπτόμένα κανάλια πλάτους 22MHz, και χρησιμοποιείται ένα κάθε φορά για επικοινωνία.



Εικόνα 27:DSSS συναρτήσει ισχύος και χρόνου

Ένας εκπομπός direct sequence επικοινωνεί προσθέτοντας bits εφεδρείας που καλούνται chips, στα δεδομένα. Σε κάθε bit πληροφορίας προστίθενται τουλάχιστον 10 chips. Κατόπιν τα τμήματα των δεδομένων στέλνονται σε όσες περισσότερες συχνότητες είναι δυνατόν, εντός του καναλιού λειτουργίας, ταυτόχρονα. Η μέγιστη ταχύτητα φτάνει σε αυτόν τον τρόπο τα 11mbit. Στο ακόλουθο σχήμα βλέπουμε την κατανομή των καναλιών στο φάσμα των 2.4GHz, καθώς και τον τρόπο με τον οποίο επικαλύπτονται.



Εικόνα 28 : BSSS κανάλια

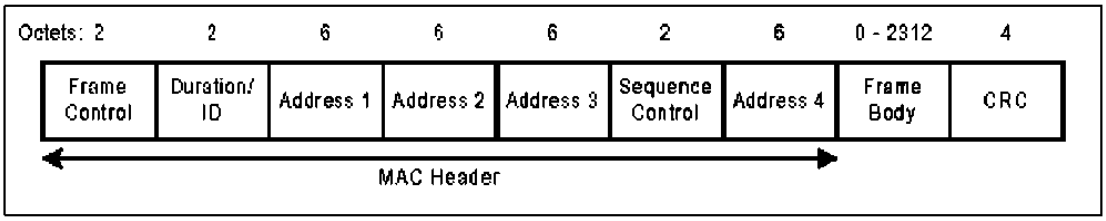
Ας δούμε όμως αναλυτικά ποια κανάλια λειτουργίας του 802.11 είναι ελεύθερα σε μερικές χώρες.

Κανάλι	Συχνότητα	ΗΠΑ	Ευρώπη	Ισπανία	Γαλλία	Ιαπωνία
1	2.412	X	X			
2	2.417	X	X			
3	2.422	X	X			
4	2.427	X	X			
5	2.432	X	X			
6	2.437	X	X			
7	2.442	X	X			
8	2.447	X	X			
9	2.452	X	X			
10	2.457	X	X	X	X	
11	2.462	X	X	X	X	
12	2.467		X		X	
13	2.472		X		X	
14	2.483					X

Εικόνα 29 : Κανάλια σε μερικές χώρες

Τελικά με την έλευση του 802.11b το Σεπτέμβρη του 1999, η επιτροπή αποφάσισε να αφήσει στο πρότυπο μόνο την κωδικοποίηση DSSS, παρόλο που το FHSS αρχικά φαίνονταν σαν ευκολότερο αλλά και φθηνότερο στην υλοποίηση του. Με αυτό τον τρόπο το 802.11b απέκτησε ένα από τα μεγαλύτερά του πλεονεκτήματα, την υψηλή διαμεταγωγή δεδομένων.

Η ταχύτητα σύνδεσης που ορίζει το IEEE802.11b είναι τα 11mbps, και όπως εξηγήσαμε επιβάλλεται από την κωδικοποίηση BSSS που χρησιμοποιεί. Μιας και από την φύση τους οι ασύρματες συνδέσεις είναι επιρρεπής σε σφάλματα μετάδοσης, το overhead μετάδοσης πακέτων ελέγχου και διόρθωσης λαθών(βλ. εικόνα 1), μεταφράζεται σε πραγματική ταχύτητα μεταφοράς δεδομένων πολύ χαμηλότερη της ονομαστικής. Επίσης, λόγω του γεγονότος ότι όλες οι συσκευές WiFi έχουν ένα και μόνο ραδιοφωνικό πομποδέκτη, η λειτουργία τους σαν δικτυακές συσκευές είναι σε half-duplex mode, καθώς ο πομποδέκτης μπορεί να ακούει το δίκτυο ή να στέλνει σε αυτό, αλλά όχι και τα δύο ταυτόχρονα. Έτσι το πραγματικό όριο για το bandwidth μιας 802.11b σύνδεσης είναι διαμορφώνεται στα 5mbps. Πολλές εταιρίες υπόσχονται ονομαστικές διπλάσιες ή και περισσότερο ταχύτητες. Τέτοια χαρακτηριστικά είναι εκτός του στάνταρ, και λειτουργούν μόνο μεταξύ των προϊόντων της ίδιας εταιρίας. Από την στιγμή που επιτευχθεί σύνδεση με μια άλλη συσκευή WiFi, τότε ισχύουν όλοι οι κανόνες ενός κοινού Ethernet δικτύου.



Εικόνα 30 : Μορφή του 802.11 MAC πακέτου

Το εμπόριο έχει κατακλυστεί πλέον από προϊόντα εταιριών που υλοποιούν με κάποιο τρόπο κάποιο μέρος του πρωτοκόλλου 802.11b(Access Points, clients, routers, VoIP terminals, cameras κτλ). Την λύση στην ερώτηση «τι εγγύηση έχει ο καταναλωτής για την συμβατότητα λειτουργίας όλων των 802.11b συσκευών;» έρχεται να δώσει η WECA(Wireless Ethernet Compatibility Alliance). Πρόκειται για μια οργάνωση που εξετάζει και πιστοποιεί την συμβατότητα των 802.11 συσκευών. Πρόκειται για μια πολύ σημαντική πρωτοβουλία, καθώς ένα wireless δίκτυο

μπορεί να αποτελείται από συσκευές διαφορετικών εταιριών. Μια πιστοποιημένη από την weca συσκευή, έχει την εγγύηση ότι θα μπορεί να συνεργαστεί με άλλο ασύρματο ή όχι υλικό, που υποδεικνύεται από το πρωτόκολλο 802.11b για τον συγκεκριμένο τύπο συσκευής(π.χ. ένα Access Point πρέπει να μπορεί να συνδεθεί με οποιονδήποτε client, αλλά και να μπορεί να δεχτεί και μια Ethernet σύνδεση). Η WECA έχει θεσπίσει το Wireless Fidelity πρότυπο, και σε κάθε συσκευή που περνάει επιτυχώς όλες τις δοκιμές συμβατότητας, απονέμεται η «σφραγίδα συμβατότητας».Αυτή η σφραγίδα δίνει στους καταναλωτές την εγγύηση ότι, τα προϊόντα που την φέρουν, θα μπορούν να λειτουργούν μεταξύ τους. Παρόλα αυτά, το wifi δεν είναι ένα τεχνολογικό στάνταρ. Είναι απλά μια εγγύηση συμβατότητας μεταξύ προϊόντων. Βεβαίως τα πράγματα ποτέ δεν είναι τόσο απλά. Πολλές φορές ερχόμαστε αντιμέτωποι με προϊόντα που είτε απλά δεν μπορούν να συνεργαστούν, είτε η συνεργασία τους αυτή είναι προβληματική. Τέτοια προβλήματα τις περισσότερες φορές βρίσκονται στο υλικό των συσκευών, οπότε είναι απίθανο να λυθούν. Έτσι η προσωπική δοκιμή των προϊόντων πριν την αγορά, ή η έρευνα για παραδείγματα αποδεδειγμένης συνεργασίας ενδείκνυται πριν από μια σοβαρή επένδυση σε υλικό διαφορετικών κατασκευαστών.

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 prinvacy), 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 από 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. .υστυχώς, 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

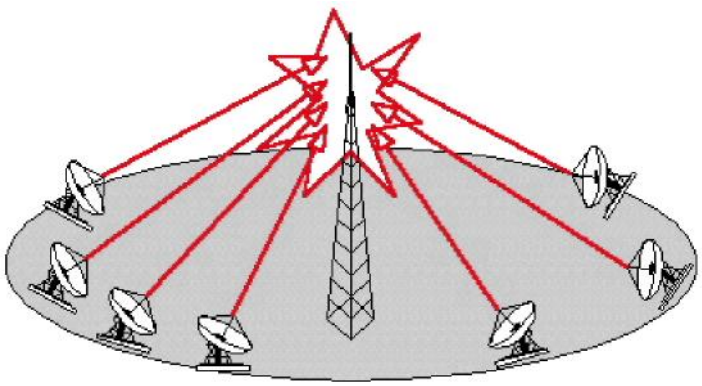
πρότυπο αυτό. Δύο επιστημονικές εργασίες όμως, από ομάδες του πανεπιστημίου του Berkeley και του Maryland, έμελλαν να ταράξουν τα νερά για το πρότυπο, και να καταστήσουν εμφανή τα τρωτά του σημεία. Η εργασία της ομάδας του Berkeley καταδεικνύει τις αδυναμίες του προτύπου λόγω της συνεχούς επαναχρησιμοποίησης 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. .εν δημοσίευσαν ωστόσο κάποια υλοποίηση των ευρημάτων τους. .υστυχώς 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 από 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 802.11i, 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.

Στην παράγραφο αυτή θα ορίσουμε και θα περιγράψουμε ίσως ένα από τα μεγαλύτερα μειονεκτήματα του 802.11b, το πρόβλημα του κρυμμένου κόμβου, το οποίο είναι καθαρά εγγενές στο σχεδιασμό του πρωτοκόλλου και οφείλεται πιθανότατα στους ίδιους τους στόχους τους οποίους έθεσε η ομάδα εργασίας της IEEE για το WiFi σαν εναλλακτικό τρόπο δικτύωσης σε τοπικό επίπεδο. Είναι ένα πρόβλημα που εμφανίζεται μόνο σε infrastructure mode, όπως θα γίνει κατανοητό στις πιο κάτω γραμμές. Ας υποθέσουμε ότι έχουμε ένα κεντρικό Access Point και πολλούς clients σε διαφορετικές τοποθεσίες, έτσι ώστε όλοι οι clients να έχουν οπτική επαφή με το AP, αλλά όχι και καθένας με τον άλλο. Μιλάμε δηλαδή για μια
αρκετά τυπική περίπτωση ενός π.χ., ενδοπανεπιστημιακού δικτύου.
Από τον ορισμό του το 802.11b προοριζονταν για ένα κλειστό περιβάλλον
γραφείου. Σε αυτό το περιβάλλον, η επιτροπή της IEEE θεώρησε λογικό το ότι όλοι οι client κόμβοι που είναι συνδεδεμένοι σε ένα Access Point θα μπορούν «ακούν» το τι στέλνει ο γείτονάς τους. Χωρίς δηλαδή στην πραγματικότητα να λαμβάνουν τα δεδομένα που εκπέμπει ο διπλανός client προς το AP, έχουν την πληροφορία ότι αυτή την στιγμή κάποιος χρησιμοποιεί το κανάλι, στέλνοντας δεδομένα. Η κύρια μέθοδος αποφυγής συγκρούσεων στο 802.11 είναι το CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance). Η λειτουργία Carrier Sense πραγματοποιείται με παρακολούθηση του καναλιού πριν της έναρξη εκπομπής. Αν κάποιος άλλος client εκείνη την ώρα τύχει να εκπέμπει, τότε ο πρώτος περιμένει, έως ότου να βρεθεί στιγμή που το κανάλι να είναι ελεύθερο. Όπως καταλαβαίνουμε, για να

επιτευχθεί ένα καλό ποσοστό συγχρονισμού, που θα εξασφαλίσει την εύρυθμη λειτουργία του δικτύου, πρέπει οι περισσότεροι client να βρίσκονται σε θέση να ακούν τις εκπομπές όλων των άλλων. Όταν δηλαδή ένας σταθμός ελέγχει το μέσο για να δει αν είναι σε χρήση, μπορεί εσφαλμένα να αποφασίσει ότι είναι ελεύθερο, μιας και δεν είναι σε θέση να λαμβάνει τις εκπομπές όλων των άλλων σταθμών του Access Point. Σε αυτήν την περίπτωση, το αποτέλεσμα θα είναι συνεχείς συγκρούσεις. Σε περίπτωση σύγκρουσης, το αποτέλεσμα είναι όμως δεν είναι τυχαίο, κάτι που αν συνέβαινε θα οδηγούσε ίσως σε ισορροπία. Συνήθως το Access Point τείνει να ευνοεί τον εκπομπό με το καλύτερο σήμα, καθώς λαμβάνει το σήμα του ασθενέστερου σαν θόρυβο και απορρίπτοντάς το. Δεδομένων λοιπόν των συνθηκών, μια και μόνο συσκευή μπορεί να μονοπωλήσει ολόκληρο το εύρος ζώνης του AP. Ευνοϊκές συνθήκες για την εμφάνιση προβλήματος κρυμμένου κόμβου δεν είναι όμως μόνο οι περιπτώσεις που υπάρχουν εμπόδια μεταξύ δύο ή περισσότερων σταθμών. Η επικοινωνία τύπου «όλοι ακούν όλους», μπορεί να είναι εφικτή μόνο όταν χρησιμοποιούμε μη κατευθυντικές(omni directional) κεραίες, οι οποίες εκπέμπουν κυκλικά το σήμα τους. Πολλές φορές όμως, η χρήση κατευθυντικών κεραιών(yagi, parabolic grid) υψηλού κέρδους σήματος, είναι μονόδρομος για επιτευχθεί σύνδεσή (βλέπε εικόνα 31). Κάτω από αυτές τις συνθήκες, μια και μόνο client συσκευή είναι δυνατόν να μονοπωλήσει όλο το εύρος ζώνης του Access Point, προκαλώντας έτσι τεράστια συμφόρηση στις διακινήσεις δεδομένων των υπόλοιπων κόμβων.



Εικόνα 31: WLAN με πελάτες κατευθυντικής εκπομπής

Η εισαγωγή του μηχανισμού RTS/CTS έδωσε κάποια ελπιδοφόρα μηνύματα στην κοινότητα χρηστών του 802.11b. Η υλοποίηση βέβαια του μηχανισμού αυτού δεν είναι υποχρεωτική, και υπάρχουν πάρα πολλές συσκευές που δεν το υποστηρίζουν. Τελικά όμως ο μηχανισμός αυτός αποτυγχάνει πλήρως να αμβλύνει το φαινόμενο του Hidden Node, εν μέρει λόγω συγκρούσεων στα ίδια τα πακέτα RTS (περνάνε μόνο τα RTS του δυνατότερου). Παρόλο τον σχεδιασμό του, με πακέτα μικρού μεγέθους και ως εκ τούτου μικρότερη πιθανότητα σύγκρουσης, αλλά και γρηγορότερη διόρθωση των συγκρούσεων, η πραγματική χρήση τους σε δίκτυα εξωτερικού χώρου δεν φαίνεται να έχει αποτέλεσμα. Λύσεις υπάρχουν, και διαφέρουν σε προσέγγιση αλλά και κόστος. Υπάρχουν ειδικές συσκευές (ή firmware για συσκευές) οι οποίες εφαρμόζουν ένα είδος polling στο δίκτυο. Τέτοιες λύσεις έχουν θεωρικά αλλά και πρακτικά μεγάλη επιτυχία στην σωστή χρήση του εύρους ζώνης, αλλά έχουν μεγάλο κόστος, καθώς είναι παντελώς ασύμβατες με τα κλασσικά wifi προϊόντα, μιας και βγαίνουν εκτός του προτύπου. Λύσεις για bandwidth control σε υψηλότερο επίπεδο ερευνούνται, μα και πάλι δεν παρέχουν καμία εγγύηση για την εξάλειψη συγκρούσεων. Ίσως η καλύτερη λύση στο πρόβλημα έχει να προσφέρει η κοινότητα ανοιχτού κώδικα, και για την ακρίβεια, η ομάδα του Patras Wireless.
Η τεχνολογία 802.11b ήταν η πρώτη εδώ και αρκετά χρόνια πρωτοβουλία, για την εισαγωγή ενός πρωτοκόλλου ασύρματης τοπικής δικτύωσης μεγάλου εύρους ζώνης. Τα πλεονεκτήματα που περιγράψαμε ποιο πάνω, σε συνδυασμό με το γεγονός ότι δεν είναι αναγκαία η απόκτηση ειδικής άδειας χρήσης αυτής της ραδιοφωνικής συχνότητας, έκανε την αποδοχή του από τους καταναλωτές και τις εταιρίες ταχύτατη. Μάλιστα οι δυνατότητες της οικογένειας πρωτοκόλλων 802.11,
είναι τέτοιες που το καθιστούν μια καλή λύση του προβλήματος του τελευταίου χιλιομέτρου(last mile problem), δηλαδή την παροχή broadband υπηρεσιών στον τελικό χρήστη από το δίκτυο μεταφοράς δεδομένων του ήδη εγκατεστημένου τηλεφωνικού

δικτύου. Στο εξωτερικό ανθεί η αγορά των wISPs(wireless Internet service provider), που προσφέρουν ευρυζωνικό internet μέσω της ασύρματης υποδομής που κατασκευάζουν οι ίδιοι, και μισθώνοντας γρήγορες συνδέσεις στο διαδίκτυο, τις οποίες και παρέχουν στους τελικούς πελάτες. Στην Ελλάδα κάτι τέτοιο είναι ανέφικτο για την ώρα, λόγω του ασαφούς νομικού πλαισίου περί της εμπορικής χρήσης της συχνότητας των 2,4GHz. Είναι επιτακτική λοιπόν η ανάγκη για νομοθετικές αλλαγές, που θα βοηθήσουν να αρθεί το μονοπώλιο των κρατικών τηλεπικοινωνιακών φορέων, και θα δώσει νέες ανταγωνιστικές δυνατότητες σε μικρότερες επιχειρήσεις.
Παρατηρώντας την μεγάλη αποδοχή του 802.11b, σε σχέση με το πόσο πρόσφατα έγινε η προτυποποίηση, είναι ξεκάθαρη η επιτυχία του σαν standard. Επιπλέον, δεν μπορούμε παρά να αναγνωρίσουμε πως αυτός ο νέος τρόπος ασύρματης επικοινωνίας και ανταλλαγής δεδομένων, είναι μια νέα και σχετικά ανεξερεύνητη περιοχή, που ίσως μας επιφυλάσσει μεγάλες αλλαγές στην ποιότητα, την αποδοτικότητα αλλά και την αντίληψη που έχουμε για τις ψηφιακές τηλεπικοινωνίες.

4.3 802.11c-Bridge Operation Procedures

Το 802.11c παρέχει τις απαραίτητες πληροφορίες προκειμένου να διασφαλιστούν οι κατάλληλες λειτουργίες γεφύρωσης (Bridge). Η μελέτη αυτή έχει ολοκληρωθεί και οι σχετικές διαδικασίες έχουν ενσωματωθεί στο πρότυπο 802.11c. Οι κατασκευαστές προϊόντων χρησιμοποιούν αυτό το πρότυπο όταν αναπτύσσουν σταθμούς πρόσβασης (access points). Δεν υπάρχει σχεδόν τίποτα σε αυτό το πρότυπο που να σχετίζεται με τις εγκαταστάσεις των WLANs.

4.4 802.11-d Global harmonization

Όταν το 802.11 έγινε διαθέσιμο στην αρχή, μόνο μία μικρή μερίδα κανονιστικών πεδίων – περιοχών (USA, Ευρώπη και Ιαπωνία) διέθεταν κανονισμούς για τη λειτουργία των 802.11 WLANs. Για να υπάρξει υποστήριξη και ευρεία υιοθέτηση του 802.11, η ομάδα αναθεώρησης 802.11d είχε μία συνεχώς αυξανόμενη υποχρέωση να καθορίσει απαιτήσεις φυσικού επιπέδου (PHY) που να ικανοποιούν κανονισμούς και σε άλλες τρίτες χώρες.
Αυτό είναι εξαιρετικά σημαντικό για λειτουργία στις μπάντες των 5 Ghz επειδή η χρήση αυτών των συχνοτήτων διαφέρει πολύ από μία χώρα σε μία άλλη. Όπως και με το 802.11c, έτσι και το πρότυπο 802.11d ως επί το πλείστον έχει εφαρμογή σε εταιρείες που αναπτύσσουν προϊόντα με βάση το πρότυπο 802.11.

4.5 802.11e-MAC Enhancements for QoS

Χωρίς ισχυρή ποιότητα υπηρεσιών - QoS (Quality of Service), η υπάρχουσα έκδοση του πρότυπου 802.11 δεν βελτιστοποιεί τη μετάδοση φωνής και εικόνας. Επί του παρόντος δεν υπάρχει κανένας αποτελεσματικός μηχανισμός που να καθορίζει την προτεραιότητα κίνησης εντός του 802.11. Ως εκ τούτου, η εργασία της ομάδας αναθεώρησης 802.11e, είναι να διυλίσει – καθαρίσει το 802.11 MAC (Medium Access Layer) για να βελτιωθεί το Quality of Service (QoS) προκειμένου να υπάρξει καλύτερη υποστήριξη στις εφαρμογές audio και video (όπως οι MPEG-2).

Επειδή το 802.11e είναι εντός των ορίων του MAC υποστρώματος, είναι κοινό και σε όλα τα φυσικά υποστρώματα του 802.11 και επομένως συμβατό προς τα πίσω με όλα τα υπάρχοντα 802.11 WLANs.

4.6 802.11f-Inter Access Point Protocol

Το υπάρχον πρότυπο 802.11 δεν προδιαγράφει τις επικοινωνίες μεταξύ των Access Points και τούτο για να υποστηρίζονται οι χρήστες που περιπλανώνται από το ένα στο άλλο Access Point. Η ομάδα εργασίας του 802.11 εσκεμμένα δεν καθόρισε αυτό το στοιχείο για να υπάρχει ελαστικότητα όταν εργαζόμαστε με διαφορετικά συστήματα διανομής (δηλαδή, ενσύρματα backbones που διασυνδέουν Access Points.
Το πρόβλημα ωστόσο είναι ότι Access Points από διαφορετικούς κατασκευαστές μπορεί να μη έχουν διαλειτουργηκότητα όταν υποστηρίζουν περιπλάνηση (roaming).
Το 802.11f προδιαγράφει ένα Inter Access Point Protocol το οποίο παρέχει τις αναγκαίες πληροφορίες που χρειάζονται να ανταλλάξουν τα Access Points προκειμένου να υποστηριχθούν οι λειτουργίες των συστημάτων διανομής του προτύπου 802.11 (δηλαδή, περιπλάνηση – roaming).
Εν απουσία του προτύπου 802.11f, θα πρέπει να χρησιμοποιείται ο ίδιος κατασκευαστής για τα Access Points έτσι ώστε να διασφαλίζεται η διαλειτουργηκότητα για τους περιπλανώμενους χρήστες. Σε ορισμένες περιπτώσεις μία ανάμιξη από Access Points διαφορετικών κατασκευαστών μπορεί να λειτουργήσει, ειδικά αν τα Access Points έχουν πιστοποίηση Wi – Fi. Η προσμέτρηση του προτύπου 802.11f στο σχεδιασμό των Access Points ενδεχομένων να αυξήσει τις εναλλακτικές λύσεις και να προσθέσει μερικώς ασφάλεια διαλειτουργικότητας όταν πρόκειται να γίνει επιλογή για Access Points διαφορετικών κατασκευαστών.

4.7 802.11g-Υψηλότεροι Ρυθμοί μετάδοσης στη μπάντα των 2,4 GHz

Η αποστολή της ομάδας αναθεώρησης 802.11g ήταν να επεκτείνει το 802.11b και να αναπτύξει μία υψηλότερη ταχύτητα μετάδοσης (μέχρι 54 Mbps), ενώ η λειτουργία θα είναι εντός της μπάντας των 2,4 GHz. Το 802.11g υλοποιεί όλα τα υποχρεωτικά στοιχεία του προτύπου IEEE 802.11b PHY. Παραδείγματος χάριν, ένας

802.11b χρήστης είναι σε θέση να συσχετιστεί με ένα 802.11b access point και να λειτουργεί με ρυθμούς μετάδοσης δεδομένων μέχρι 11 Mbps. Νωρίς το έτος 2002, αποφασίστηκε το 802.11g να χρησιμοποιήσει OFDM αντί για DSSS ως βάση για την παροχή υψηλότερων ρυθμών μετάδοσης.
Ένα ζήτημα είναι ότι η παρουσία ενός 802.11b χρήστη σε ένα 802.11g δίκτυο απαιτεί τη χρήση RTS / CTS (request to send / clear-to-send), το οποίο δημιουργεί ουσιαστικό πρόβλημα και μειώνει σημαντικά την απόδοση για όλους τους 802.11b και 802.11g χρήστες. Το RTS / CTS εξασφαλίζει ότι ο σταθμός που κάνει την αποστολή, να μεταδίδει πρώτα ένα πλαίσιο RTS και να λαμβάνει ένα πλαίσιο CTS από το access point προτού στείλει δεδομένα. Ένας συνδυασμός από 802.11b και 802.11g χρήστες απαιτεί RTS / CTS προκειμένου να αποφευχθούν συγκρούσεις επειδή οι 802.11b σταθμοί δεν μπορούν να ακούσουν τους 802.11g σταθμούς χρησιμοποιώντας OFDM.
Η ομάδα αναθεώρησης IEEE 802.11g, στα μέσα του 2003 ολοκλήρωσε τις εργασίες της και εξέδωσε το πρότυπο 802.11g, το οποίο επεκτείνει το 802.11b, προσφέρει ρυθμούς μετάδοσης μέχρι 54 Mbps αλλά και συμβατότητα με το 802.11b. Χρησιμοποιεί και αυτό τη μπάντα των 2,4 GHz. Σε αντίθεση με το 802.11b χρησιμοποιεί την OFDM για να πετύχει τους επιθυμητούς ρυθμούς μετάδοσης.
Το πιο σημαντικό χαρακτηριστικό του 802.11g είναι η συμβατότητά του με το 802.11b. Το 802.11b ως γνωστό αποτελεί σήμερα το φυσικό στρώμα που υλοποιείται στα περισσότερα προϊόντα ασύρματης δικτύωσης. Το 802.11g λειτουργώντας ταυτόχρονα με το 802.11b μπορεί να το αντικαταστάσει σταδιακά εξολοκλήρου.

4.8 802.11h-Spectrum Managed 802.11a

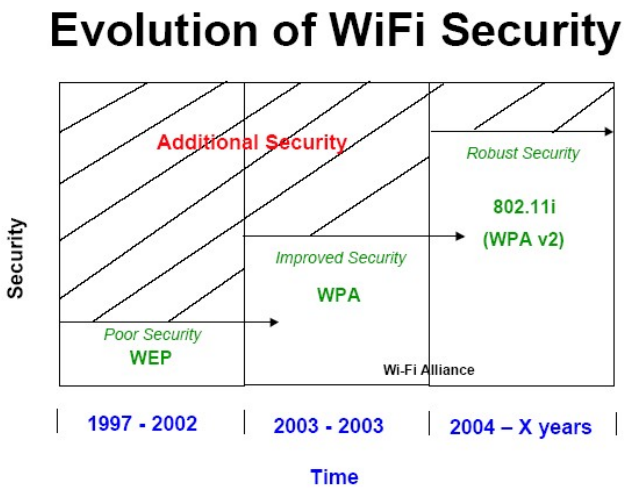
Το 802.11h απευθύνεται και καλύπτει τις απαιτήσεις των Ευρωπαϊκών κανονισμών. Παρέχει Dynamic Channel Selection (DCS) – δυναμική επιλογή καναλιών και Transmit Power Control (TPC) – έλεγχο μετάδοσης ισχύος, για συσκευές που λειτουργούν

στη μπάντα των 5 GHz (802.11a). Στην Ευρώπη υπάρχει εν δυνάμει πιθανότητα το 802.11a να έχει παρεμβολές με τις δορυφορικές επικοινωνίες. Με τη χρήση των DCS και TPC, το 802.11h θα αποφύγει τις παρεμβολές.
Προκειμένου να υλοποιήσει το DCS και TCP, το 802.11h αναπτύσσει πρακτικές που επηρεάζουν αμφότερα τα υποστρώματα MAC και PHY. Με το να συμπεριληφθούν το DCS και το TPC, το 802.11h θα μπορέσει να γίνει ο διάδοχος του 802.11a. Ευτυχώς, δεν υπάρχουν ζητήματα μη καλής διαλειτουργικότητας ανάμεσα σε υπάρχοντα 802.11a και 802.11h χρήστες και access points. Τα καλά νέα είναι ότι το 802.11h ενισχύει τις πωλήσεις των 802.11a δικτύων στην Ευρώπη, πράγμα που ενδεχομένως να έχει ως αποτέλεσμα υψηλότερους όγκους πωλήσεων και χαμηλότερες τιμές.

4.9 802.11i-Ενίσχυση των χαρακτηριστικών του MAC για ενισχυμένη ασφάλεια

Το 802.11i εμπλουτίζει το υπόστρωμα MAC προκειμένου να αντιμετωπίσει τα ζητήματα ασφαλείας που σχετίζονται με το Wired Equivalent Privacy (WEP).
Οι αλγόριθμοι κρυπτογράφησης που χρησιμοποιούνται σήμερα, όπως ο WEP (Wired Equivalent Privacy), ο WPA (Wi-Fi Protected Access) και IP SEC παρουσιάζουν κάποια προβλήματα. Για παράδειγμα ο πρώτος εμφανίζει σημαντικά κενά ασφαλείας, ο WPA ενώ έρχεται να καλύψει τα κενά του WEP, στην πραγματικότητα δεν καλύπτει την ουσιαστική ασφάλεια στα ασύρματα τοπικά δίκτυα. Τέλος ο IP SEC εφαρμόζεται τοπικά σε κάθε χρήστη και καλύπτει Point-to-Point συνδέσεις.
Το υπάρχον πρότυπο 802.11 προδιαγράφει τη χρήση σχετικά αδύναμων, στατικών κρυπτογραφικών κλειδιών χωρίς καμία μορφή διαχείρισης της κατανομής των κλειδιών. Αυτό δίνει τη δυνατότητα σε hackers να αποκτήσουν πρόσβαση και να αποκρυπτογραφήσουν δεδομένα του ασύρματου δικτύου (WLAN)

που έχουν κρυπτογραφηθεί με τον αλγόριθμο WEP. Η ομάδα αναθεώρησης του 802.11i θα προσπαθήσει να αντικαταστήσει το WEP και την υποστήριξή του σε συσκευές, αρχικά με την δημιουργία ανώτερου πρωτοκόλλου ασφαλείας προς τα πίσω συμβατό με το WEP, και τελικά με την πλήρη κατάργησή του.
Το 802.11i θα ενσωματώσει το 802.1x και μεταγενέστερες ισχυρότερες τεχνικές κρυπτογράφησης, όπως το AES (Advanced Encryption Standard). Η υλοποίηση του AES, ωστόσο, μπορεί να απαιτήσει νέο εξοπλισμό.
Στο παρακάτω σχήμα γίνεται μια αναδρομή στους διάφορους αλγορίθμους κρυπτογράφησης.



Σχήμα 32:Αλγόριθμοι κρυπτογράφησης

4.10-802.11j

Το 802.11j είναι πολύ σημαντικό υποπρότυπο μόνο για την Ιαπωνία. Για άλλες περιοχές είναι τελείως άσχετο. Επειδή το υποπρότυπο αυτό είναι σχετικά νέο και δεν χρησιμοποιείται ευρέως, παρά μόνο από την Ιαπωνία, δεν έχει δημοσιευθεί το σχέδιο του.

Η Ιαπωνία έχει εγκρίνει μια ελαφρώς διαφορετική ζώνη συχνότητας (4,9 GHz - 5 GHz) και το οποίο έχει περίπου την ίδια λειτουργία με το 802.11a. Το 802.11j επιτυγχάνει τις ταχύτητες OFDM PHY στην εξουσιοδοτημένη ιαπωνική ζώνη.

4.11-802.11k

Το υποπρότυπο αυτό είναι πρόσφατα διαμορφωμένο και πολύ σημαντικό για το μέλλον των ασυρμάτων δικτύων. Μέχρι την στιγμή αυτή που κάνουμε την εργασία δεν έχει δημοσιευθεί κανένα πρόγραμμα διαθέσιμο για το κοινό.
Ο εξοπλισμός του 802.11 δεν αναφέρει πολλά για την υγεία και τη θέση της ραδιοσύνδεσης, και οι διαχειριστές των δικτύων έχουν ελάχιστη επίγνωση για την απόδοσή του. Αυτό το πρόγραμμα θα καταστήσει διαθέσιμο το χαμηλού επιπέδου στοιχείο στη διαχείριση των διαφόρων συστημάτων έτσι ώστε ο εξοπλισμός μπορεί δυναμικά να αλλάξει στα ασύρματα κανάλια, τα επίπεδα δύναμης, και της ισορροπίας των φορτίων στους πελάτες απέναντι στα APs.

4.12-802.11m

Είναι υποπρότυπο μικρότερης σημασίας, μέχρι την στιγμή αυτή δεν έχουμε κάποιο έγγραφο που να το ορίζει επίσημα, όπως και το πρόγραμμα του άγνωστο. Με το πρότυπο αυτό έχουμε συντήρηση της αναβάθμισης του 802.11 που θα ενσωματωθεί επάνω στις αλλαγές που έγιναν στο 802,11 έως το 1999 και των 802.11a, 802.11b, και 802.11d στην αναθεώρηση του 2003.

4.13-802.11n

Το 802.11n είναι το τελευταίο υποπρότυπο του αρχικού 802.11 που ξεκίνησε να λειτουργεί λίγους μήνες πριν. Στη συνέχεια θα γίνει μια επισκόπηση της τεχνολογίας αυτής, θα περιγράψουμε τις τεχνικές που χρησιμοποιούνται για να επιτύχουν μεγαλύτερες ταχύτητες και εύρους ζώνης, και θα προσδιορίσουμε τις εφαρμογές, τα προϊόντα και τα περιβάλλοντα που θα ωφεληθούν από αυτήν την τεχνολογία. Μιας και τα ασύρματα δίκτυα βρίσκονται αυτή τη στιγμή σε μεγάλη άνθιση, καθώς αυξάνονται συνεχώς οι νέοι χρήστες, οι οποίοι είτε δημιουργούν δικό τους μητροπολιτικό δίκτυο(μια ομάδα χρηστών) είτε ενσωματώνονται στα είδη υπάρχοντα αυξάνοντας έτσι το κάθε δίκτυο. Βλέποντας αυτή την ανάπτυξη η βιομηχανία έχει έρθει σε συμφωνία για τα συστατικά που θα αποτελέσουν το υποπρότυπο αυτό. Αν και οι προδιαγραφές δεν αναμένεται να έχουν οριστικοποιηθεί πριν από το 2007, έχουν ξεκινήσει και διατίθενται στην αγορά τα προϊόντα που θα πλαισιώσουν το 802.11n, έτσι οι καταναλωτές μπορούν να ξεκινήσουν να σχεδιάζουν τα νέα ασύρματα δίκτυα που θα βασίζονται σε αυτήν την τεχνολογία, εξασφαλίζοντας διαλειτουργικότητα, ταχύτητα, μεγάλο εύρος ζώνης, απόδοση, αξιοπιστία.
Το αναδυόμενο αυτό υποπρότυπο διαφέρει από τους προκατόχους του δεδομένου ότι επιτρέπει ποικίλους τρόπους και διαμορφώσεις καθώς και δυνατότητα εναλλαγής του μέγιστου εύρους ζώνης ροής δεδομένων. Αυτό επιτρέπει στο πρότυπο να παρέχει τις βασικές παραμέτρους ώστε να μπορούν να ρυθμιστούν κατάλληλα οι νέες συσκευές και εφαρμογές που θα δημιουργηθούν για να λειτουργούν στα πλαίσια του 802.11n. εφαρμόζοντας κάθε δυνατή επιλογή το 802.11n θα μπορούσε να προσφέρει ταχύτητα μεταφοράς δεδομένων πάνω από 600 Mbps, το πρόβλημα είναι ότι δεν το επιτρέπουν το υπάρχον υλικό για τα WLANs. Μέχρι το τέλος του 2006 τα περισσότερα WLANs που θα είναι σχεδιασμένα με το πρότυπο 802.11n, αναμένεται να μπορούν να λειτουργήσουν σε ταχύτητες μεταφοράς δεδομένων που θα φθάνουν τα 300 Mbps. Στο σχέδιο του 802.11n η πρώτη απαίτηση είναι να υποστηριχθεί

μια εφαρμογή OFDM, η οποία θα είναι περισσότερο βελτιωμένη από τα υπάρχοντα πρότυπα 802.11a/b/g, χρησιμοποιώντας μεγαλύτερο ρυθμό μετάδοσης δεδομένων και ένα ελαφρώς μεγαλύτερο εύρος ζώνης. Ένα από τα ευρύτατα γνωστά συστατικά των διαφόρων υποπροτύπων του 802.11 είναι γνωστό ως MIMO-Maximum Input -Maximum Output(μέγιστη είσοδος-μέγιστη έξοδος). Το MIMO εκμεταλλεύεται ένα φαινόμενο ραδιο-κύματος γνωστό ως multipath: οι μεταφερόμενες πληροφορίες περνούν ανάμεσα από τοίχους, πόρτες, παράθυρα καθώς και άλλα αντικείμενα, ώστε να φθάσουν στις επιθυμητές κεραίες μέσα από διαφορετικές διαδρομές και σε ελαφρώς διαφορετικούς χρόνους. Οι ανεξέλεγκτες πολλαπλές διαδρομές διαστρεβλώνουν το αρχικό σήμα, πράγμα που καθιστά δύσκολη την αποκρυπτογράφηση και με άμεσο αποτέλεσμα την μείωση της απόδοσης του 802.11. Η τεχνική multipath του MIMO ανέπτυξε μια νέα τεχνολογία γνωστή ως space-division multiplexing. Η συσκευή του WLAN που μεταδίδει το σήμα χωρίζει από μόνη της τα δεδομένα σε πολλαπλές διαδρομές το οποίο ονομάζεται spatial stream και μεταδίδει κάθε spatial stream σε ξεχωριστές κεραίες, το ίδιο γίνεται και στην πλευρά του παραλήπτη έτσι ώστε να μην υπάρχει σύγχυση στον παραλήπτη. Το παρόν σχέδιο για το 802.11n προωθεί μόνο 4 spatial streams, και αυτό γιατί το υπάρχον υλικό των WLANs δεν επιτρέπει παραπάνω spatial streams. Ο διπλασιασμός των spatial streams από 1 σε 2, διπλασιάζει και την ταχύτητα των δεδομένων, θα έχουμε όμως και μεγαλύτερη κατανάλωση ισχύος και σε μικρότερο βαθμό αύξηση του κόστους. Υπάρχουν δυο χαρακτηριστικά του σχεδίου του 802.11n που εστιάζονται στη βελτίωση της απόδοσης του MIMO που ονομάζονται beam-forming και diversity. Το beam-forming είναι μια τεχνική που στρέφει τα ραδιοσήματα ευθεία στην κεραία λήψης βελτιώνοντας έτσι την απόδοση και το εύρος, μειώνοντας την παρεμβολή. Η diversity εκμεταλλεύεται τις πολλαπλές κεραίες με το συνδυασμό των διαφόρων εξόδων ή επιλέγοντας την καλύτερη διαδρομή μεταξύ των πολλών ενδιάμεσων κεραιών ώστε ο παραλήπτης να παραλάβει μεγάλο αριθμό spacial stream.

Βασικά στοιχεία του 802.11n

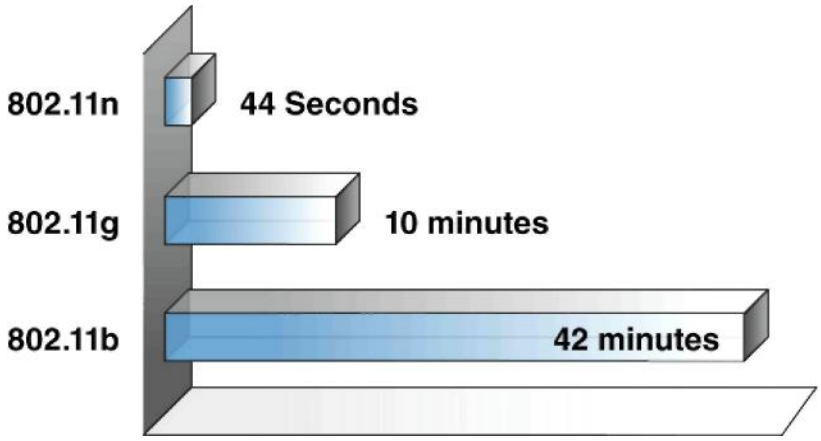
Χαρακτηριστικό	***Επεξήγηση***	***Προδιαγραφές***
Καλύτερο OFDM	Υποστηρίζει μεγαλύτερο εύρος& υψηλότερο ρυθμό κωδικοποίησης για να επιτρέψει μέγιστο ρυθμό μετάδοσης στα 65 Mbps	Υποχρεωτικό
Space-Division Multiplexing	Χωρίζει τα προς μετάδοση δεδομένα σε multiple streams που φθάνουν σε πολλαπλές κεραίες	Προαιρετικό για πάνω από 4spatial streams
Diversity	Χωρίζει τα μεταδιδόμενα δεδομένα σε πολλαπλά streams έτσι ώστε να φθάνουν στις διάφορες κεραίες που διαθέτει ο παραλήπτης	Προαιρετικό για πάνω από 4spatial streams
MIMO-Εξοικονόμηση ενέργειας	Το MIMO εξοικονομεί ενέργεια με το να χρησιμοποιεί ακριβώς τον αριθμό κεραιών που χρειάζεται κάθε φορά	Απαιτείται
Κανάλια 40 MHz	Διπλασιάζει το ρυθμό μετάδοσης δεδομένων, διπλασιάζοντας το εύρος των καναλιών από 20 σε 40 MHz	Προαιρετικό
Συγκέντρωση	Επιτυγχάνει απόδοση με το πακετάρισμα των δεδομένων σε κάθε επικοινωνία	Απαιτείται
Μείωση των κενών ανάμεσα στα εσωτερικά frames (RIFS)	Ένα από τα πολλά χαρακτηρ. Του 802.11n για την αύξηση της απόδοσης. Παρέχει μικρότερη καθυστέρηση μεταξύ των OFDM μεταδόσεων από τα 802.11a,g	Απαιτείται
Greenfield Mode	Επιτυγχάνει απόδοση με το να παραλείπει την υποστήριξη για 802.11a,b,g συσκευές σ' ένα 802.11n δίκτυο	Προσωρινά απαιτητικό

Σύγκριση των βασικών υποπροτύπων 802.11a,b,g,n

	802.11a	802.11b	802.11g	802.11n
Δημιουργία προτύπου	Ιούλιος 1999	Ιούλιος 1999	Ιούλιος 2003	Δεν έχει επικυρωθεί ακόμη
Μέγιστος ρυθμός μετάδοσης	54 Mbps	11 Mbps	54 Mbps	600 Mbps
Διαμόρφωση	OFDM	DSSS ή CCK	DSSS ή CCK ή OFDM	DSSS ή CCK ή OFDM
RF Band	5 GHz	2.4 GHz	2.4 GHz	2.4 GHz ή 5 GHz
Αριθμός των Spatial Streams	1	1	1	1, 2, 3, ή 4
Εύρος καναλιού	20 MHz	20 MHz	20 MHz	20 MHz ή 40

Επειδή το 802.11n υπόσχεται μεγαλύτερο εύρος ζώνης, μεγαλύτερο ρυθμό μεταφοράς δεδομένων, μεγαλύτερη αξιοπιστία και λιγότερο κόστος στο μέλλον, οι διαμορφώσεις των δικτύων θα γίνονται με βάση το υποπρότυπο αυτό. Επειδή οι εφαρμογές του 802.11n φθάνουν μέχρι το σπίτι των διαφόρων χρηστών, οι περισσότεροι θα το προτιμήσουν. Άλλοι λόγοι που οι διάφοροι χρήστες θα επιλέξουν το υποπρότυπο αυτό είναι οι ανάγκες για μετάδοση φωνής(VoIP), video, γρήγορο δικτυακό παιχνίδι και γρήγορο download. Πιο αναλυτικά οι επιχειρήσεις αρχίζουν να συνειδητοποιούν ότι με αυτό το υποπρότυπο μπορούν να μειώσουν το κόστος των υπεραστικών κλήσεων με την χρησιμοποίηση του VoIP. Τη στιγμή αυτή για τους μικρής ηλικίας χρήστες αλλά και για τους μεγάλους έχει παραγκωνισθεί το απλό παιχνίδι σε κάθε υπολογιστή και έχει αναπτυχθεί το δικτυακό παιχνίδι με πλήθος διαφόρων χρηστών, έτσι αυτοί οι χρήστες απαιτούν από τις διάφορες τεχνολογίες γρήγορο δικτυακό παιχνίδι.

Όμως ίσως το πιο βασικό πλεονέκτημα είναι το γρήγορο download. Μιας και η τεχνολογία προχωράει με ανεξέλεγκτους ρυθμούς όπως πολλοί αναφέρουν καθημερινά, και εμείς ως χρήστες απαιτούμε να 'κατεβάσουμε' ,από το Internet ή από το εκάστοτε δίκτυο στο οποίο βρισκόμαστε, μεγαλύτερα σε μέγεθος αρχεία και σε όσο το δυνατόν μικρότερο χρόνο λόγω μερικές φορές φόρτου εργασίας στο γραφείο όπου βρισκόμαστε. Το παρακάτω σχήμα συγκρίνει το χρόνο που θα έπαιρνε για να κατεβάσει κάποιος ένα video 30 λεπτών, σε κάθε πρότυπο ξεχωριστά.



Όπως είναι προφανές και από τις προηγούμενες σελίδες, ουσιαστικά όλες οι επιχειρήσεις θα μπορούν να ωφεληθούν σημαντικά από το μεγάλο εύρος ζώνης των WLANs. Εντούτοις πολλές μεγάλες επιχειρήσεις περιμένουν μέχρι να επικυρωθεί το 802.11n.

4.14-802.11p

Ασύρματη πρόσβαση σε περιβάλλοντα με ειδική γλώσσα επικοινωνίας(WAVE-Wireless Access in Vehicular Enviroments). Τα 5.9 GHz DSRC είναι μια μικρή περιοχή στις μεσαίου εύρους υπηρεσίες επικοινωνιών, οι οποίες υποστηρίζουν μαζί δημόσια ασφάλεια και ιδιωτικές διαδικασίες στα μέσα επικοινωνίας. Το DSRC προορίζεται να συμπληρώσει τις κυψελοειδείς επικοινωνίες με την παροχή υψηλών ρυθμών μεταφοράς δεδομένων στις περιοχές όπου η ελαχιστοποίηση της λανθάνουσας κατάστασης στη σύνδεση επικοινωνίας και η απομόνωση των σχετικά μικρών ζωνών επικοινωνίας είναι σημαντικές.

4.15-802.11r

Γρήγορα σημείο πρόσβασης για τις εφαρμογές φωνής. Τα νέα πρωτόκολλα, όπως η προ-επικύρωση, υπόσχονται να πετύχουν τον επιθυμητό χαμηλό χρόνο περιπλάνησης ακόμα και όταν απαιτείται η επικύρωση μήκους στο 802.11i.

4.16-802.11s

Σκοπός του υποπροτύπου αυτού είναι να καθοριστεί η MAC και το PHY για τα εμπλεκόμενα δίκτυα. Σε τέτοια δίκτυα, τα σημεία πρόσβασης αναμεταδίδουν τις πληροφορίες από το ένα στο άλλο, βήμα-βήμα, όπως στη μέθοδο με τον δρομολογητή. Όσο προσθέτουμε χρήστες και σημεία πρόσβασης, αυξάνουμε την ικανότητα - και προσθέτοντας κόμβους γίνεται μια εξελικτική και περιττή προσπάθεια.

4.17-802.11t

Το υποπρότυπο αυτό είναι προτεινόμενο για τη δοκιμή απόδοσης

Συμπερασματικά

Εκτός από τις παραπάνω αναφερθείσες ομάδες αναθεώρησης, η ομάδα εργασίας του 802.11 μελετάει και νέες μεθόδους για να αυξηθεί η απόδοση και να γίνει καλύτερη χρήση του ράδιο φάσματος. Παραδείγματος χάριν, η ομάδα εργασίας σκέφτεται σοβαρά τη χρήση διαμόρφωσης ultrawideband ως ένα νέο μηχανισμό για την υποστήριξη εφαρμογών υψηλότερων ταχυτήτων και για τη μείωση της εν δυνάμει πιθανότητας RF παρεμβολών. Ωστόσο, θα περάσουν αρκετά χρόνια μέχρι να δούμε αυτά τα νεότερα και ταχύτερα πρότυπα.
Η ασύρματη τεχνολογία internet με τη χρήση του 802.11 είναι μία φυσική επιλογή για απομακρυσμένες, αραιοκατοικημένες περιοχές. Σε αυτή τη κατεύθυνση έχουν αρχίσει να δουλεύουν πολλές κυβερνήσεις σε συνεργασία με WISP. Σύμφωνα με πρόσφατα στατιστικά περισσότεροι από 2.500 WISPs που εκμεταλλεύονται το χωρίς άδεια φάσμα (exempt-licensed spectrum) έχουν ανοιχτεί σε περισσότερες από 6.000 αγορές στης ΗΠΑ. Γενικά όμως σε διεθνές επίπεδο οι περισσότερες επεκτάσεις γίνονται στο νόμιμο φάσμα συχνοτήτων σε πελάτες που απαιτούν καλή ποιότητα μεταφοράς φωνής παρά δεδομένων. Αυτό συμβαίνει κυρίως συμβαίνει σε κάποιες περιοχές που δεν υπάρχει ενσύρματο δίκτυο. Υπάρχει η ορολογία "Wireless Local Loop" που χρησιμοποιείται για να περιγράψει όλες αυτές τις εφαρμογές που αναφέρονται στην αντικατάσταση του ενσύρματου δικτύου από το ασύρματο.

Κεφάλαιο 5

ΟΔΗΓΙΕΣ ΔΗΜΙΟΥΡΓΙΑΣ ΑΣΥΡΜΑΤΟΥ ΔΙΚΤΥΟΥ ΣΤΗΝ Α.Δ.ΑΡΤΑΣ

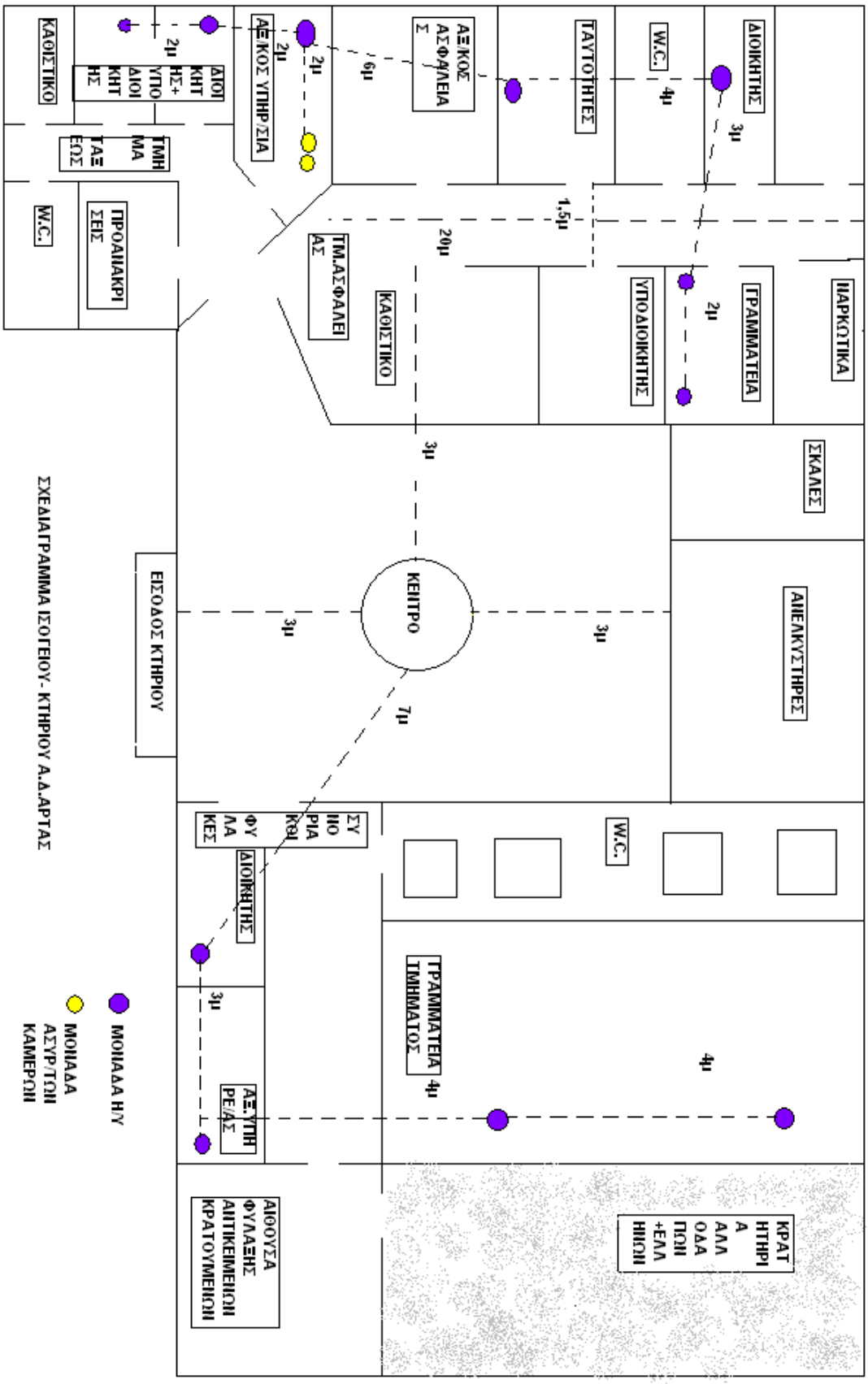
Στην συνέχεια της εργασίας μας θα περιγράψουμε αναλυτικά την δημιουργία ενός ασυρμάτου τοπικού δικτύου στο κτήριο της Α.Δ.Άρτας που βρίσκεται στην περιφερειακή οδό Άρτας.Το κτήριο

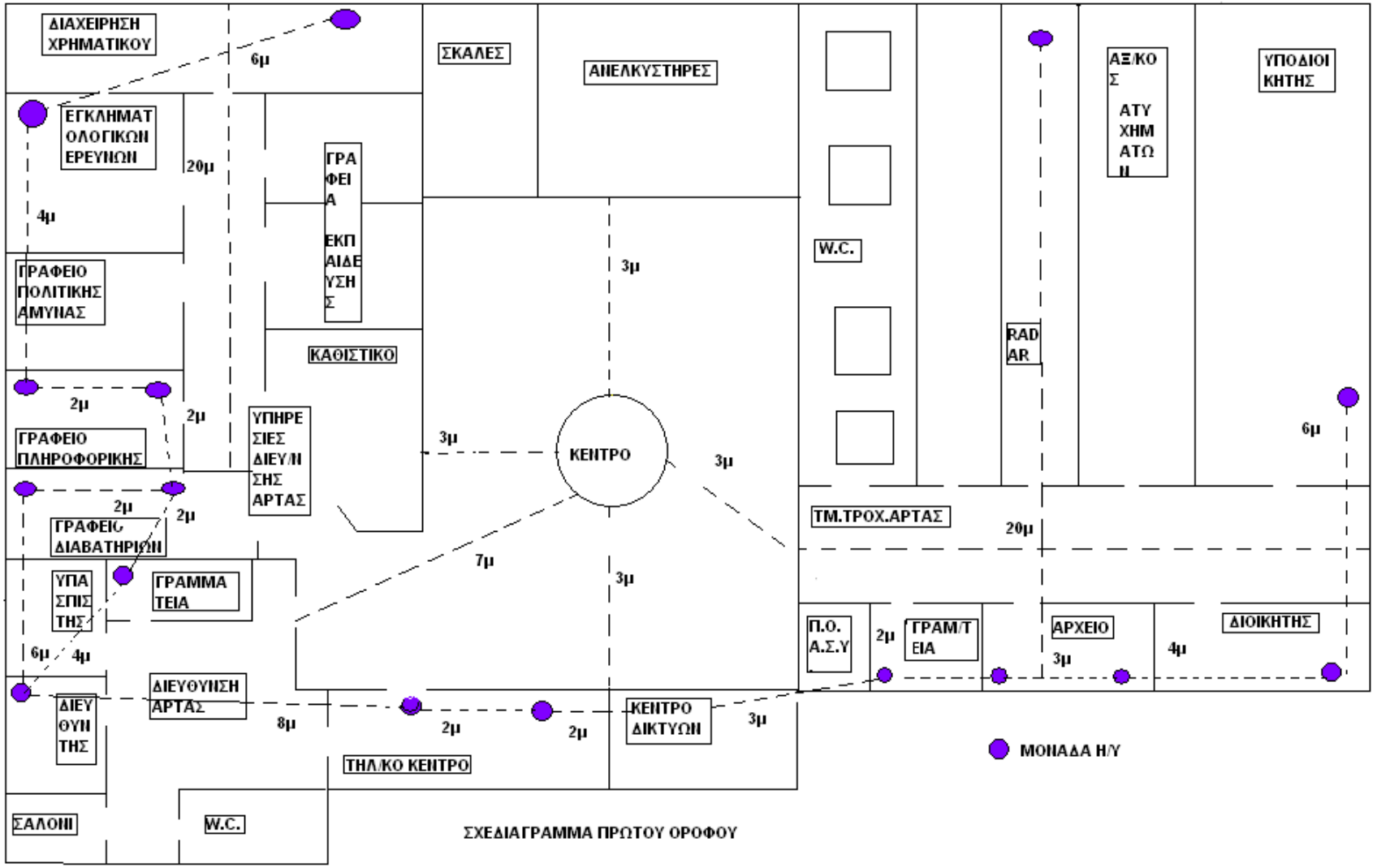
αποτελείται από 3 ορόφους και κάθε όροφος απεικονίζεται αναλυτικά στα παρακάτω σχέδια.

ΣΧΕΔΙΟ 1:ΙΣΟΓΕΙΟ ΚΤΗΡΙΟΥ

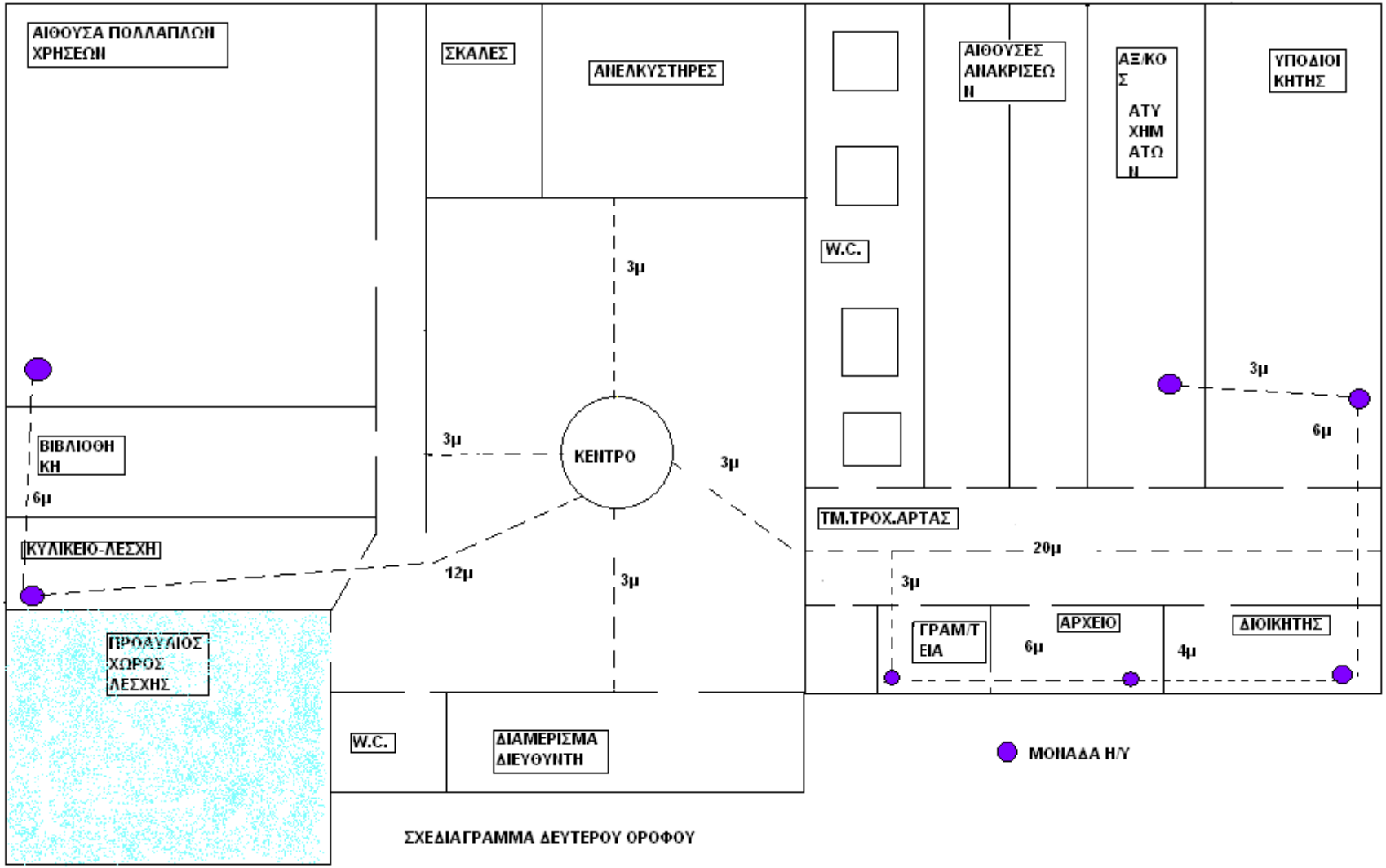
ΣΧΕΔΙΟ 2:ΠΡΩΤΟΣ ΟΡΟΦΟΣ

ΣΧΕΔΙΟ 3:ΔΕΥΤΕΡΟΣ ΟΡΟΦΟΣ


ΣΧΕΔΙΑΓΡΑΜΜΑ ΙΣΟΓΕΙΟΥ - ΚΤΗΡΙΟΥ Α.Δ.ΑΡΤΑΣ
ΜΟΝΑΔΑ Η/Υ
ΜΟΝΑΔΑ ΑΣΥΡ/ΤΩΝ ΚΑΜΕΡΩΝ
ΔΙΟΙΚΗΤΗΣ
W.C.
ΤΑΥΤΟΤΗΤΕΣ
ΑΞ/ΚΟΣ ΑΣΦΑΛΕΙΑΣ
ΑΞ/ΚΟΣ ΥΠΗΡ/ΣΙΑ
ΚΑΘΙΣΤΙΚΟ
ΠΡΟΑΝΑΚΡΙΣΕΙΣ
ΤΑΞΕΩΣ
ΤΜΗΜΑ
ΔΙΟΙΚΗΤΗΣ ΥΠΟΔΙΟΙΚΗΤΗΣ
ΓΡΑΜΜΑΤΕΙΑ
ΤΜ.ΑΣΦΑΛΕΙΑΣ
ΚΑΘΙΣΤΙΚΟ
ΠΑΡΚΩΤΙΚΑ
ΣΚΑΛΕΣ
ΑΙΘΕΛΚΥΣΤΗΡΕΣ
ΚΕΝΤΡΟ
ΕΙΣΟΔΟΣ ΚΤΗΡΙΟΥ
ΣΥΝΟΔΙΑ ΚΑΙ ΦΥΛΛΑΚΕΣ
ΔΙΟΙΚΗΤΗΣ
ΑΞ.ΥΠΗΡΕΣΙΑΣ
ΓΡΑΜΜΑΤΕΙΑ ΤΜΗΜΑΤΟΣ
ΚΡΑΤΗΤΗΡΙΑ ΑΛΛΟΔΑΠΩΝ +ΕΛΛΗΝΩΝ
ΑΙΘΟΥΣΑ ΦΥΛΑΞΗΣ ΔΙΚΤΥΟΜΕΝΩΝ ΚΡΑΤΟΥΜΕΝΩΝ
1,5μ
20μ
3μ
2μ
4μ
6μ
7μ



ΣΧΕΔΙΑΓΡΑΜΜΑ ΠΡΩΤΟΥ ΟΡΟΦΟΥ



ΣΧΕΔΙΑΓΡΑΜΜΑ ΔΕΥΤΕΡΟΥ ΟΡΟΦΟΥ

Το κεντρικό ασύρματο δίκτυο της Α.Δ. Άρτας (A.D.ARTAS Wireless Network) έχει αναπτυχθεί θεωρητικά στα πλαίσια της παρούσας πτυχιακής εργασίας. Το ασύρματο δίκτυο προσφέρει τη δυνατότητα σύνδεσης στο Internet και στις εφαρμογές του τοπικού δικτύου της Α.Δ Άρτας φορητών υπολογιστών και σταθερών υπολογιστών χωρίς τη χρήση καλωδίου δικτύου. Απαραίτητες προϋποθέσεις είναι να διαθέτει ο υπολογιστής κάρτα ασύρματης δικτύωσης, και να βρίσκεται εντός της εμβέλειας ενός από τα σημεία πρόσβασης (Access Points) του δικτύου.

Οι τοποθεσίες στις οποίες έχουν τοποθετηθεί σημεία πρόσβασης προς το δίκτυο (Access Points) είναι οι ακόλουθες:

- Καθιστικό(Ισόγειο)
- Γραμματεία τμήματος Συνοριοφυλάκων(Ισόγειο)
- Καθιστικό(1^{ου} Ορόφου)
- Γραφείο Αξιωματικού Ατυχημάτων(1^{ου} ορόφου)
- Αίθουσα ανακρίσεων(2^{ου} ορόφου)
- Αίθουσα πολλαπλών χρήσεων(2^{ου} ορόφου)

Σε κάθε όροφο και σε απόσταση 3 μέτρων από το κέντρο με κατεύθυνση προς την είσοδο-κέντρο δικτύου-διαμέρισμα διευθυντή, αντίστοιχα για κάθε όροφο θα τοποθετηθούν επιπλέον ένας κατανεμητής σε κάθε όροφο. Επιπλέον ο κατανεμητής του 1^{ου} ορόφου, θα λειτουργεί σαν κεντρικός κατανεμητής ο οποίος θα συνδέεται με έναν router, ώστε οι τελικοί χρήστες να έχουν πρόσβαση στο διαδίκτυο. Τέλος στο κέντρο δικτύου θα υπάρχει ο κατάλληλος εξοπλισμός ώστε μελλοντικά το ασύρματο τοπικό δίκτυο της Α.Δ Άρτας να συνδεθεί ασύρματα και με το Ασύρματο Μητροπολιτικό δίκτυο της Άρτας(εφόσον δημιουργηθεί).
Πρέπει να αναφερθεί ότι η πρόσβαση στο ασύρματο δίκτυο θα είναι πιθανά δυνατή και σε χώρους οι οποίοι βρίσκονται πλησίον των χώρων όπου έχουν τοποθετηθεί τα σημεία πρόσβασης.

Όλα τα σημεία πρόσβασης παρέχουν υποστήριξη σύνδεσης με τη βοήθεια του πρωτοκόλλου 802.11b/g (μέγιστη ταχύτητα 54Mbps). Στο ασύρματο δίκτυο έχουν δυνατότητα πρόσβασης όλοι οι Αστυνομικοί της Α.Δ Άρτας, και συγκεκριμένα όλοι όσοι διαθέτουν λογαριασμό e-mail/dial-up στην Α.Δ άρτας.
Στον τομέα της ασφάλειας χρησιμοποιούνται σύγχρονα πρωτόκολλα κρυπτογράφησης και αυθεντικοποίησης (authentication). Συγκεκριμένα, χρησιμοποιείται το πρωτόκολλο WPA σε συνδυασμό είτε με το πρωτόκολλο αυθεντικοποίησης PEAP (MS-CHAPv2), είτε με το πρωτόκολλο αυθεντικοποίησης EAP-TLS. Βέβαια, πρέπει να τονιστεί ότι το πρωτόκολλο WPA χρησιμοποιείται αποκλειστικά και μόνο για την κρυπτογράφηση που παρέχει στην ασύρματη επικοινωνία (έτσι ώστε να μην υποκλέπτονται τα δεδομένα της επικοινωνίας), και όχι για την αυθεντικοποίηση των χρηστών (user authentication). Λόγω όμως του ότι το WPA προϋποθέτει απαραίτητα αυθεντικοποίηση χρηστών, χρησιμοποιούνται τα πρωτόκολλα PEAP και EAP-TLS για να παρέχουν μια υποτυπώδη αρχική αυθεντικοποίηση. Τα PEAP και EAP-TLS είναι μέρος ενός ευρύτερου standard που ονομάζεται 802.1X, το οποίο έχει σαν σκοπό να παρέχει ασφάλεια στις ασύρματες δικτυώσεις.

Η πραγματική αυθεντικοποίηση χρηστών γίνεται σε επόμενο επίπεδο (μετά την αρχική σύνδεση) με τη χρήση του ανοιχτού λογισμικού NoCat, το οποίο έχει προσαρμοστεί στις ανάγκες του A.D.ARTAS Wireless Network. Με τη χρήση του NoCat καθίσταται δυνατή η χρήση για αυθεντικοποίηση του ήδη υπάρχοντος συστήματος που χρησιμοποιείται για το ηλεκτρονικό ταχυδρομείο και το dial-up, και μάλιστα με τις ίδιες προδιαγραφές ασφάλειας (π.χ., passwords αποθηκευμένα σε κρυπτογραφημένη μορφή, την ώρα που το PEAP προϋποθέτει passwords μη κρυπτογραφημένα). Οι χρήστες μπορούν, συνεπώς, να μπαίνουν με το συνδυασμό username/password που έχουν για το e-mail/dial-up (κάτι που, από την άλλη, δεν θα επέτρεπε η χρήση του EAP-

TLS, το οποίο χρησιμοποιεί πιστοποιητικά και όχι συνδυασμό username/password).

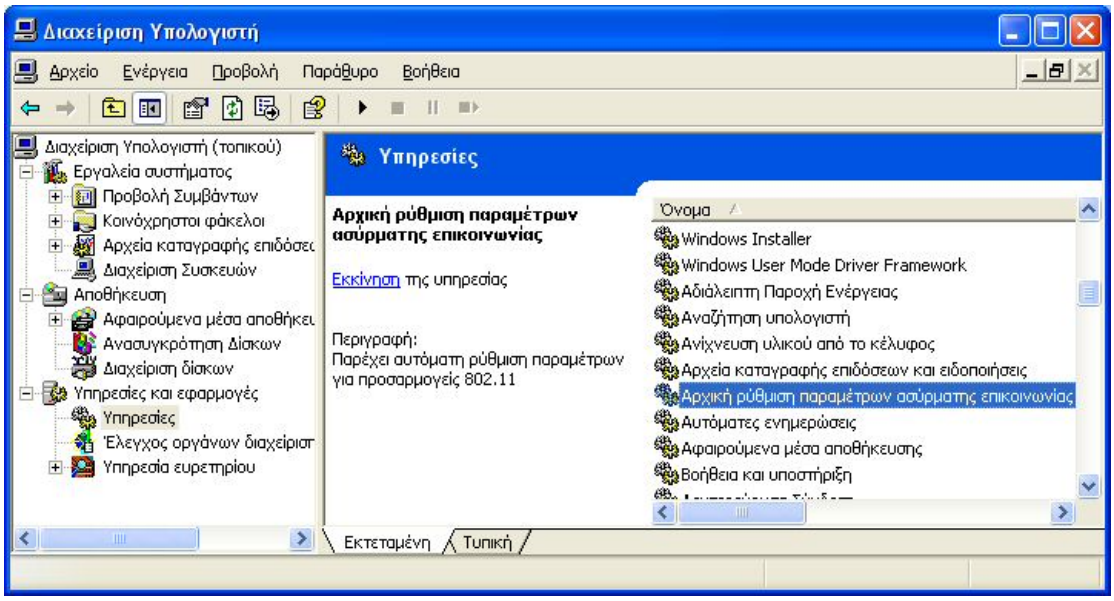
Το πρωτόκολλο WPA χρησιμοποιεί σημαντικά ισχυρότερες τεχνικές κρυπτογράφησης των δεδομένων της επικοινωνίας (κρυπτογράφηση TKIP) σε σχέση με το πιο ευρέως χρησιμοποιούμενο και γνωστό πρωτόκολλο WEP. Για το μέλλον υπάρχει η πρόβλεψη για χρήση του ακόμα ισχυρότερου πρωτοκόλλου WPA2, για το οποίο η υποστήριξη στα Windows XP είναι ακόμα πρόσφατη (και μάλιστα απαιτεί την εγκατάσταση ενός "update"), ενώ πολλές από τις ασύρματες κάρτες δικτύου δεν το υποστηρίζουν ακόμη. Σαν αποτέλεσμα, η χρήση του WPA2 στο A.D.ARTAS Wireless Network από τώρα θα εγκυμονούσε σοβαρούς κινδύνους συμβατότητας.

Ακολούθως αναφέρονται οι ρυθμίσεις με τη χρήση του βοηθήματος (utility) που παρέχουν τα Windows για τα ασύρματα δίκτυα. Αν ο φορητός σας υπολογιστής δεν διαθέτει ενσωματωμένη κάρτα ασύρματου δικτύου αλλά επιπρόσθετη (PCMCIA ή USB) και επιθυμείτε να χρησιμοποιήσετε το λογισμικό της κάρτας, προβείτε στις αντίστοιχες ρυθμίσεις, ανάλογα με το λογισμικό. Υπάρχει επίσης πιθανότητα οι ρυθμίσεις για την PCMCIA ή USB κάρτα ασύρματου δικτύου να μη μπορούν με το βοήθημα των Windows να γίνουν σύμφωνα με τις οδηγίες που ακολουθούν. Στην περίπτωση αυτή πρέπει να δοκιμάσετε να χρησιμοποιήσετε το λογισμικό της κάρτας.
Για τη χρήση του πρωτοκόλλου WPA (το οποίο χρησιμοποιείται από το AUEB-Wireless) απαιτούνται Windows XP SP2 . Ακόμη, αν ο υπολογιστής σας είναι κάπως παλιότερος, υπάρχει περίπτωση ο οδηγός (driver) της κάρτας ασύρματης δικτύωσης να μην υποστηρίζει το WPA. Σε αυτήν την περίπτωση πρέπει να «κατεβάσετε» από την ιστοσελίδα του κατασκευαστή της κάρτας τον ενημερωμένο οδηγό. Σαν παράδειγμα, για τις κάρτες της εταιρείας Intel μπορείτε να βρείτε τους οδηγούς στο

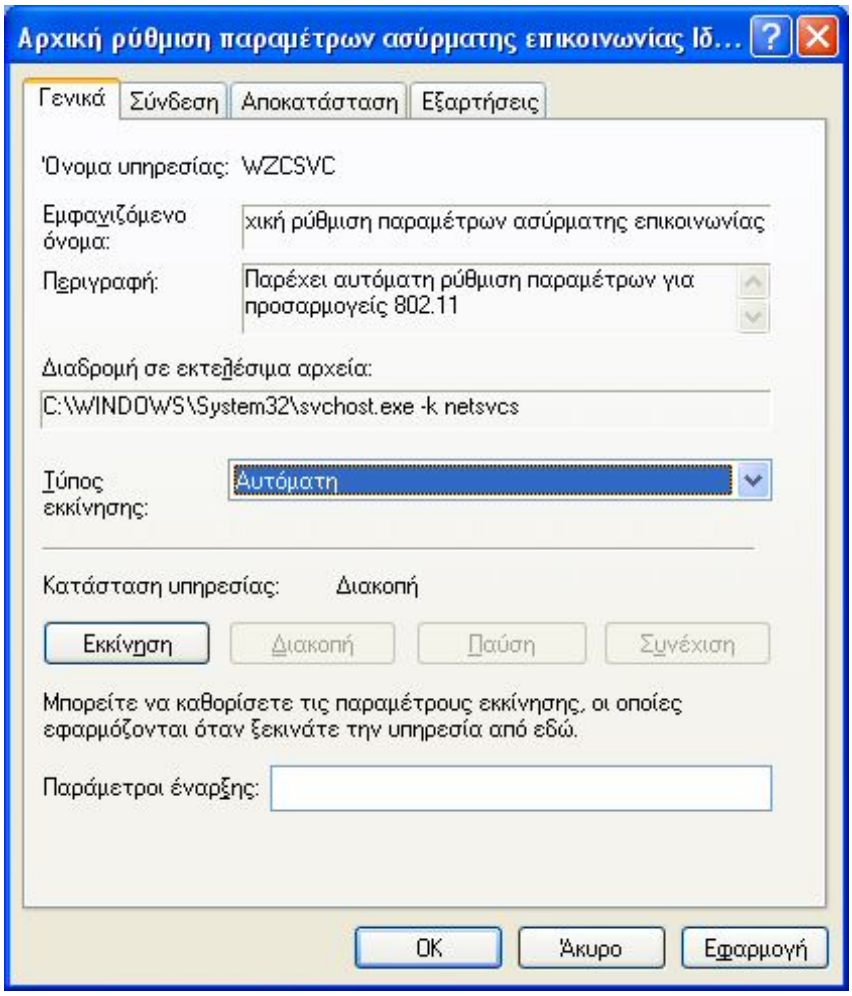
http://support.intel.com/support/wireless/wlan/sb/cs-010623.htm

1. Ενεργοποιείστε την ασύρματη κάρτα δικτύου του φορητού υπολογιστή σας (οι ενσωματωμένες κάρτες συνήθως ενεργοποιούνται από κάποιο κουμπί που διαθέτει ο φορητός).

2. Ενεργοποιείστε την **Αρχική Ρύθμιση Παραμέτρων Ασύρματης Επικοινωνίας** των Windows (αν δεν είναι ήδη ενεργοποιημένη): Κάντε δεξί κλικ στο **Ο Υπολογιστής μου**, και επιλέξτε **Διαχείριση**. Στο παράθυρο που ανοίγει κάντε διπλό κλικ στο **Υπηρεσίες και Εφαρμογές**, και κλικ στο **Υπηρεσίες**. Στο δεξί τμήμα του παραθύρου κάντε διπλό κλκ στην **Αρχική ρύθμιση παραμέτρων ασύρματης επικοινωνίας**.



Στο παράθυρο που ανοίγει αλλάξτε τον **Τύπο εκκίνησης** σε **Αυτόματη**, πατήστε το κουμπί **Εκκίνηση**, και στη συνέχεια το **OK**.

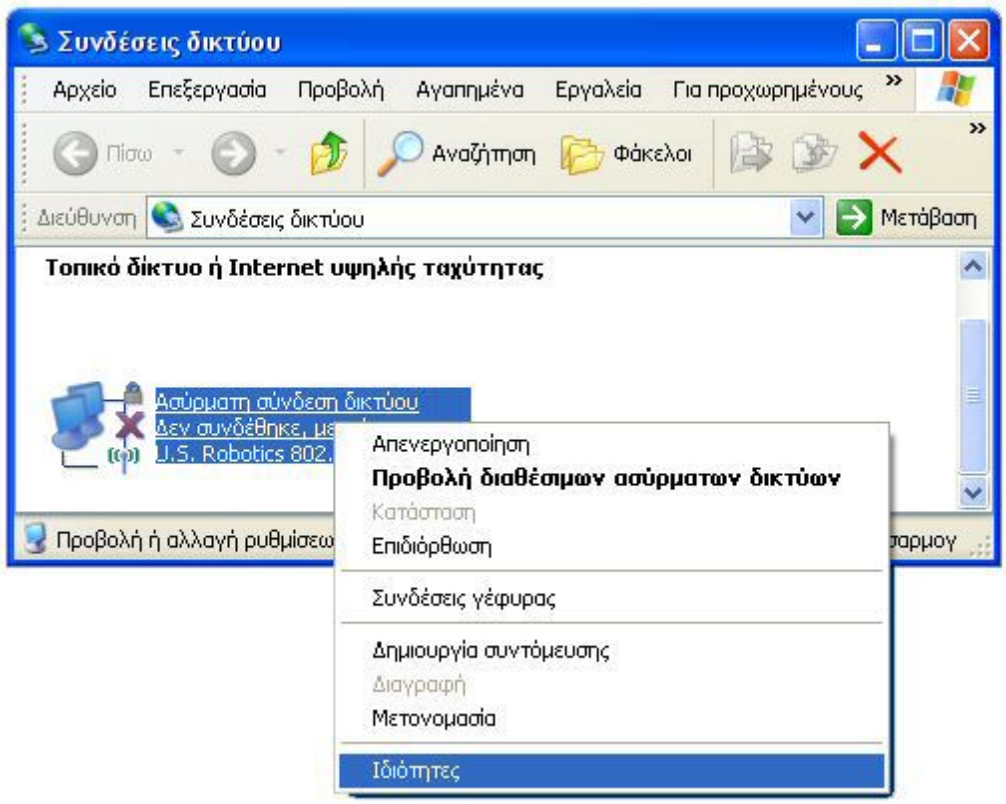


3. Ρυθμίστε το πρωτόκολλο TCP/IP της ασύρματης κάρτας δικτύου (αν οι ρυθμίσεις της δεν είχαν πειραχτεί άλλη φορά, είναι ήδη ρυθμισμένο, οπότε με το βήμα αυτό απλώς το επιβεβαιώνετε):

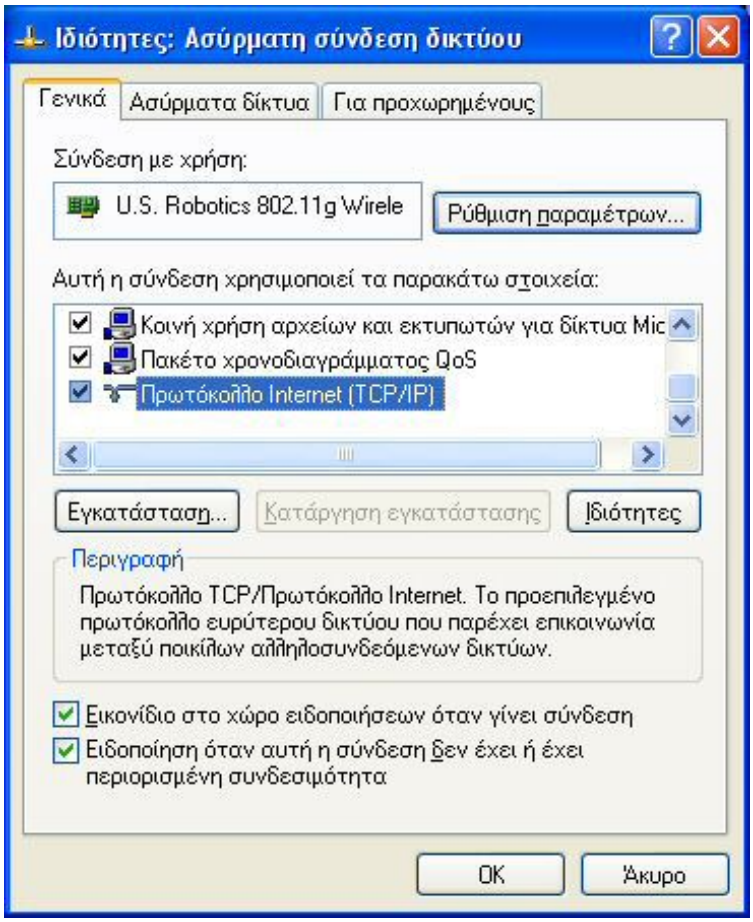
Στην επιφάνεια εργασίας των Windows κάντε δεξί κλικ πάνω από το εικονίδιο **Θέσεις Δικτύου**, επιλέξτε **Ιδιότητες**, κάντε δεξί κλικ πάνω από το εικονίδιο **Ασύρματη Σύνδεση Δικτύου**, και επιλέξτε **Ιδιότητες**.

ΣΗΜΕΙΩΣΗ: Σε περίπτωση που το εικονίδιο **Θέσεις Δικτύου** δεν εμφανίζεται στην επιφάνεια εργασίας, πατήστε το κουμπί **Έναρξη** (κάτω αριστερή γωνία της οθόνης), επιλέξτε τον **Πίνακα Ελέγχου**, και ανοίξτε (διπλό κλικ) το **Συνδέσεις δικτύου**. Στη

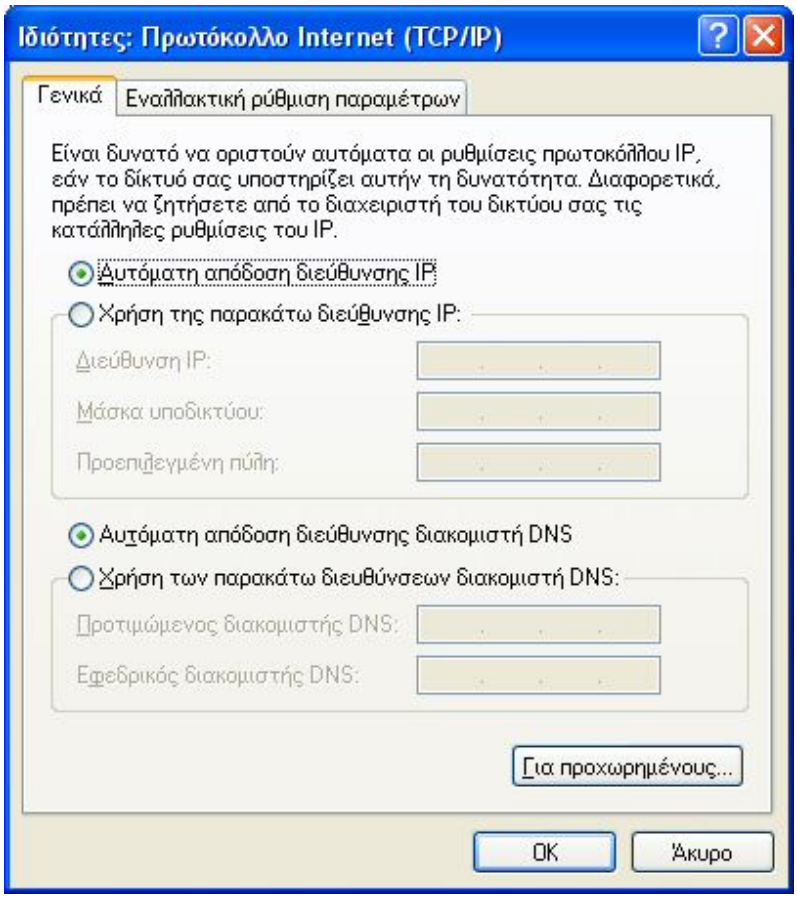
συνέχεια κάντε δεξί κλικ πάνω από το εικονίδιο **Ασύρματη Σύνδεση Δικτύου**, και επιλέξτε **Ιδιότητες**.



Στο παράθυρο που ανοίγει κάντε διπλό κλικ στο **Πρωτόκολλο Internet (TCP/IP)**.

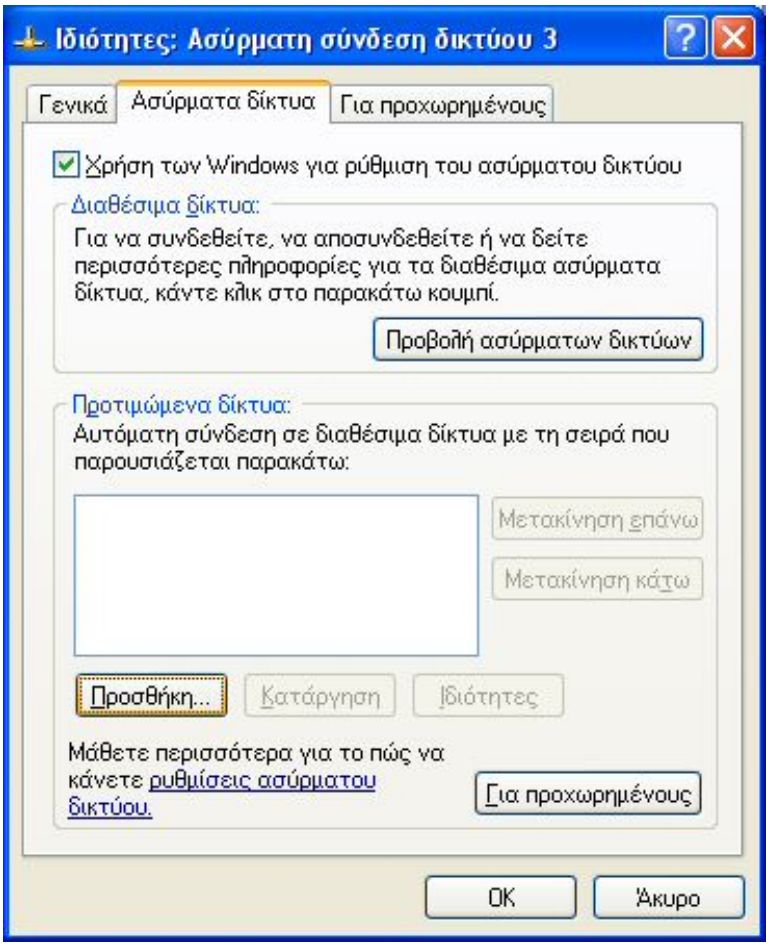


Επιλέξτε το **Αυτόματη απόδοση διεύθυνσης IP** και το **Αυτόματη απόδοση διεύθυνσης διακομιστή DNS**. Στη συνέχεια πατήστε το **OK** (μία μόνο φορά ώστε να μην κλείσει το παράθυρο **Ιδιότητες: Ασύρματη σύνδεση δικτύου**).

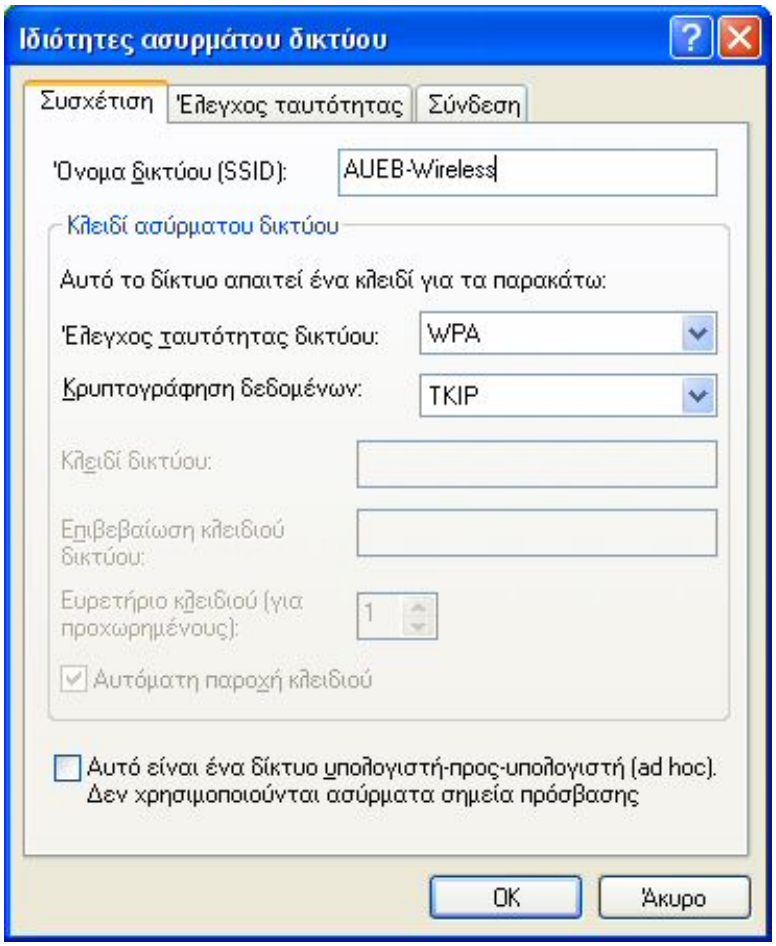


4. Ρυθμίσετε το ασύρματο δίκτυο.

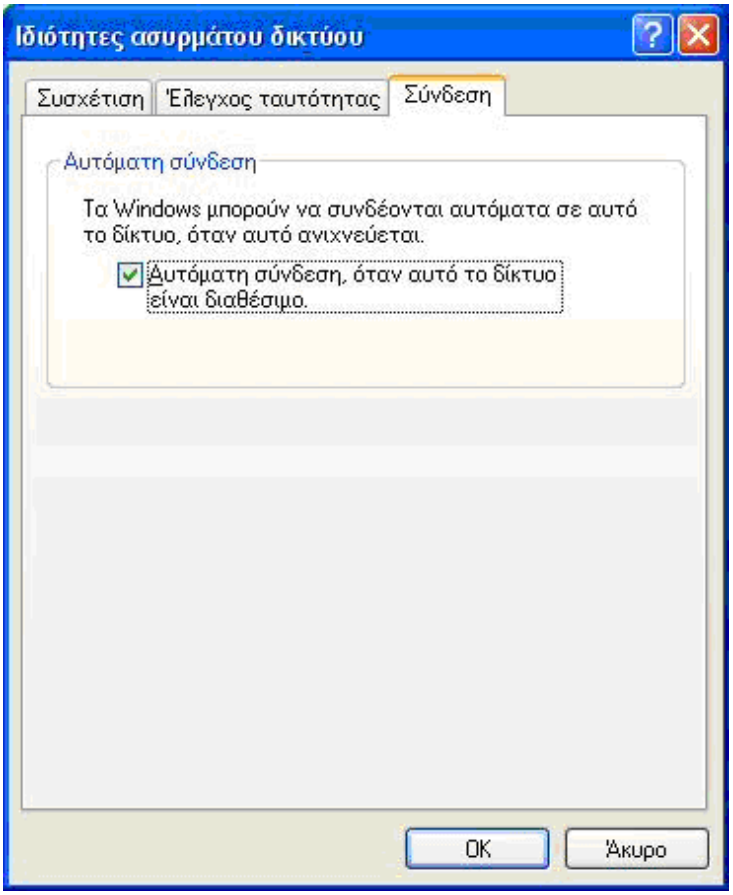
Στο παράθυρο **Ιδιότητες: Ασύρματη σύνδεση δικτύου** στο οποίο βρίσκεστε από το προηγούμενο βήμα επιλέξτε την καρτέλα **Ασύρματα δίκτυα**. Τσεκάρετε το **Χρήση των Windows για ρύθμιση του ασύρματου δικτύου** και κάντε κλικ στο κουμπί **Προσθήκη** (αν στα **Προτιμώμενα δίκτυα** υπάρχει ήδη το **AUEB-Wireless**, απλώς κάντε διπλό κλικ επάνω του, αντί για κλικ στο **Προσθήκη**).



Στο **Όνομα δικτύου (SSID)** πληκτρολογείστε **AUEB-Wireless**, στο **Έλεγχος ταυτότητας δικτύου** επιλέξτε **WPA**, και στο **Κρυπτογράφηση δεδομένων** επιλέξτε **TKIP**.

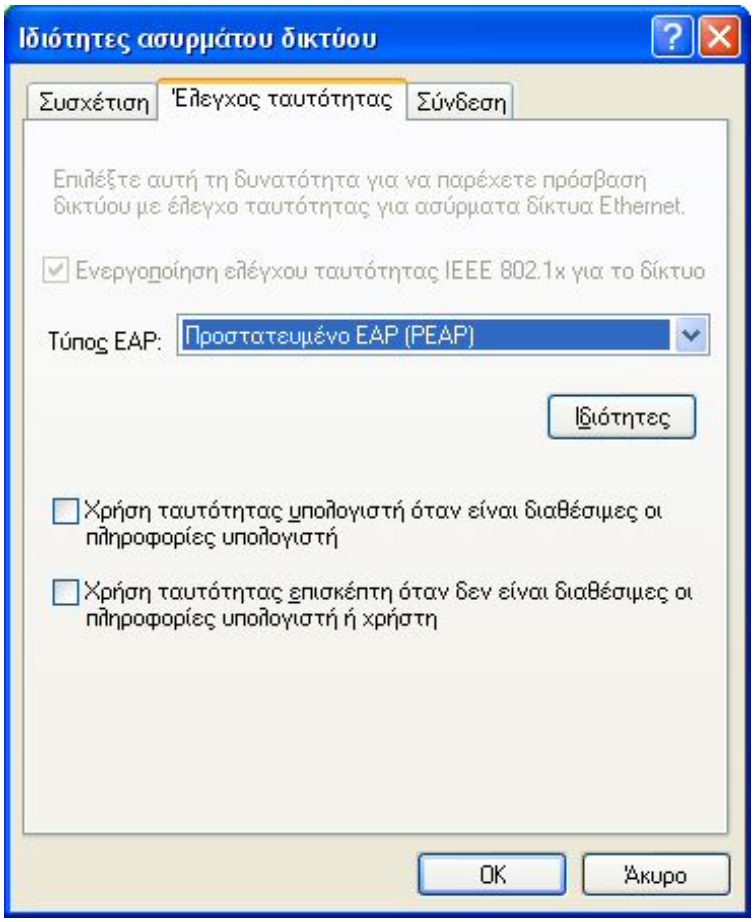


Στο ίδιο παράθυρο επιλέξτε την καρτέλα **Σύνδεση**, όπου τσεκάρετε το **Αυτόματη σύνδεση, όταν αυτό το δίκτυο είναι διαθέσιμο**, αν θέλετε ο υπολογιστής σας να συνδέεται αυτόματα («από μόνος του») στο AUEB-Wireless κάθε φορά που βρίσκεται μέσα στην εμβέλεια ενός σημείου πρόσβασης του AUEB-Wireless (και εφόσον έχουν ολοκληρωθεί σωστά όλες οι ρυθμίσεις που αναφέρονται στο παρόν κείμενο).

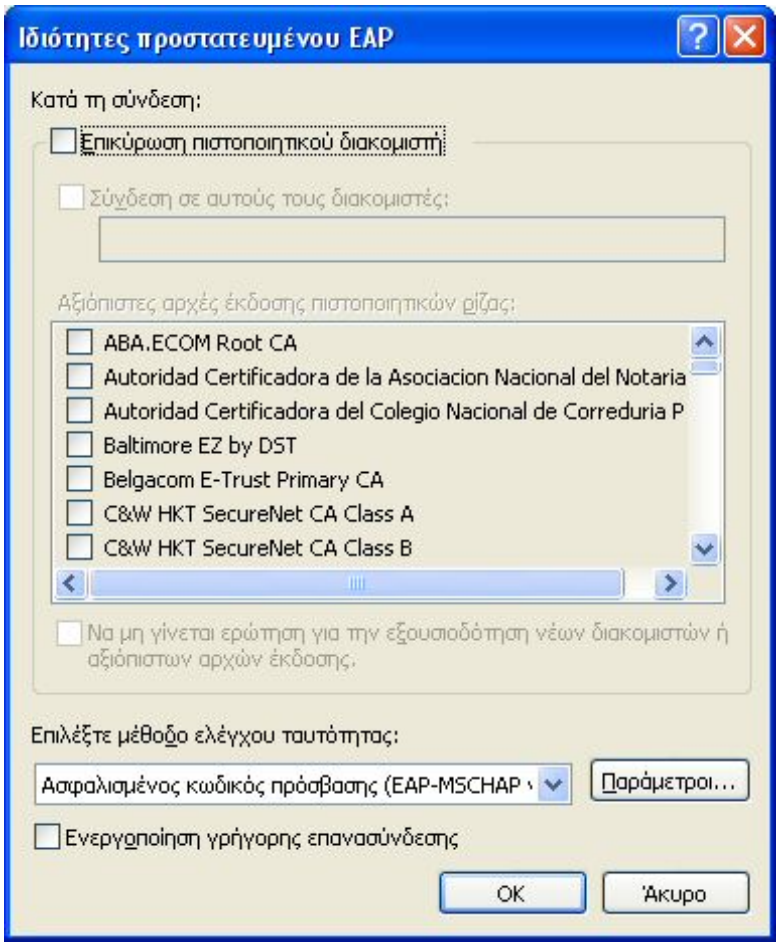


Στο ίδιο παράθυρο και πάλι επιλέξτε την καρτέλα **Έλεγχος ταυτότητας**, όπου στο **Τύπος EAP** επιλέξτε το **Προστατευμένο EAP (PEAP)**, και ξετσεκάρετε τα δύο **Χρήση ταυτότητας**... που ακολουθούν.

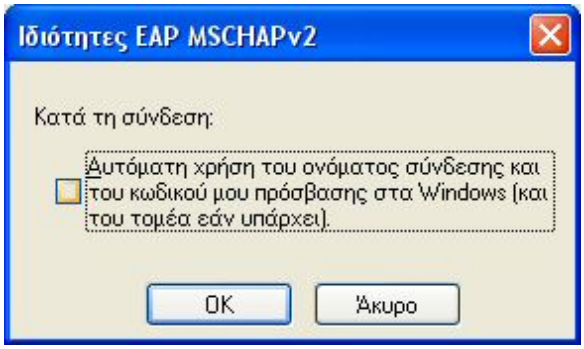
<u>ΣΗΜΕΙΩΣΗ</u>: Σε περίπτωση που χρησιμοποιείτε το λογισμικό της ασύρματης κάρτας δικτύου (και όχι το βοήθημα των Windows) για να ρυθμίσετε τη σύνδεση σας στο AUEB-Wireless, και το λογισμικό αυτό δεν παρέχει δυνατότητα χρήσης του PEAP, αλλά μόνο του EAP-TLS, τότε διαβάστε το ΠΑΡΑΡΤΗΜΑ του παρόντος κειμένου, ή επικοινωνήστε με το Κέντρο Διαχείρισης Δικτύων για να σας δοθούν οδηγίες ρύθμισης και χρήσης του EAP-TLS.



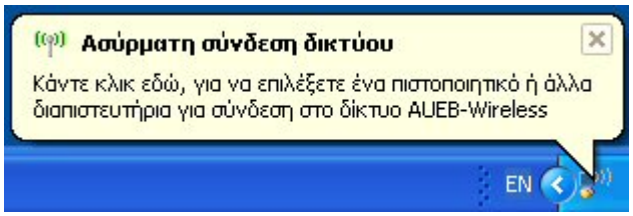
Στη συνέχεια πατήστε το κουμπί **Ιδιότητες** του **Τύπος EAP**, και ξε-τσεκάρετε το **Επικύρωση πιστοποιητικού διακομιστή**.



Βεβαιωθείτε ότι στο **Επιλέξτε μέθοδο ελέγχου ταυτότητας** είναι επιλεγμένο το ***Ασφαλισμένος κωδικός πρόσβασης (EAP-MSCHAP v2)***, και πατήστε το κουμπί **Παράμετροι**. Ξε-τσεκάρετε το ***Αυτόματη χρήση του ονόματος σύνδεσης***....

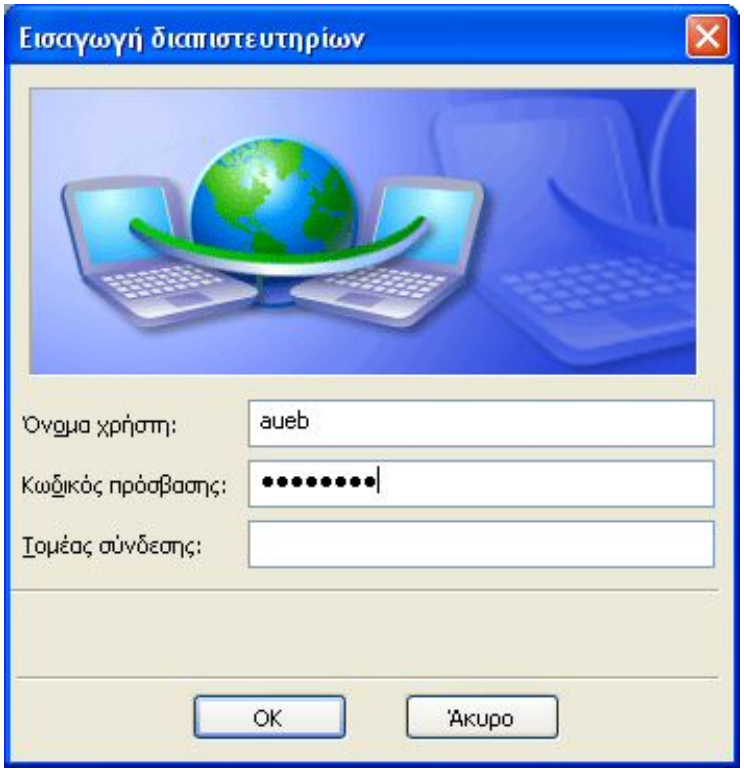


Πατήστε το ***OK*** σε όλα τα ανοιχτά παράθυρα ρυθμίσεων. Μετά από λίγα δευτερόλεπτα εμφανίζεται κάτω δεξιά στην οθόνη των Windows το ακόλουθο μήνυμα:



Κάνοντας με το ποντίκι κλικ επάνω του εμφανίζεται το παράθυρο στο οποίο δίνουμε το username και το password που απαιτούνται για να συνδεθεί ο υπολογιστής μας στο AUEB Wireless με τη χρήση του πρωτοκόλλου WPA. Δίνετε:
Όνομα χρήστη: aueb
Κωδικός πρόσβασης: wireless
Ο **Τομέας σύνδεσης** μένει κενός.

Μετά τη συμπλήρωση του Ονόματος χρήστη και του Κωδικού πρόσβασης, πατήστε το **OK**.



Πρέπει να ξανατονιστεί ότι το συγκεκριμένο username και password χρησιμοποιούνται απλώς και μόνο για να είναι δυνατή η χρήση του πρωτοκόλλου WPA, η οποία παρέχει ικανοποιητική

κρυπτογράφηση στην ασύρματη επικοινωνία. Η πραγματική αυθεντικοποίηση του χρήστη (ώστε να μην μπορεί να συνδεθεί στο δίκτυο οποιοδήποτε μη-μέλος της ακαδημαϊκής κοινότητας) γίνεται αργότερα. Επίσης να τονιστεί ότι η γνώση του συγκεκριμένου username και password από κάποιον εξωτερικό «παρείσακτο» δεν του δίνει κανένα πλεονέκτημα σε πιθανή του προσπάθεια να παραβιάσει την ασφάλεια της ασύρματης επικοινωνίας.

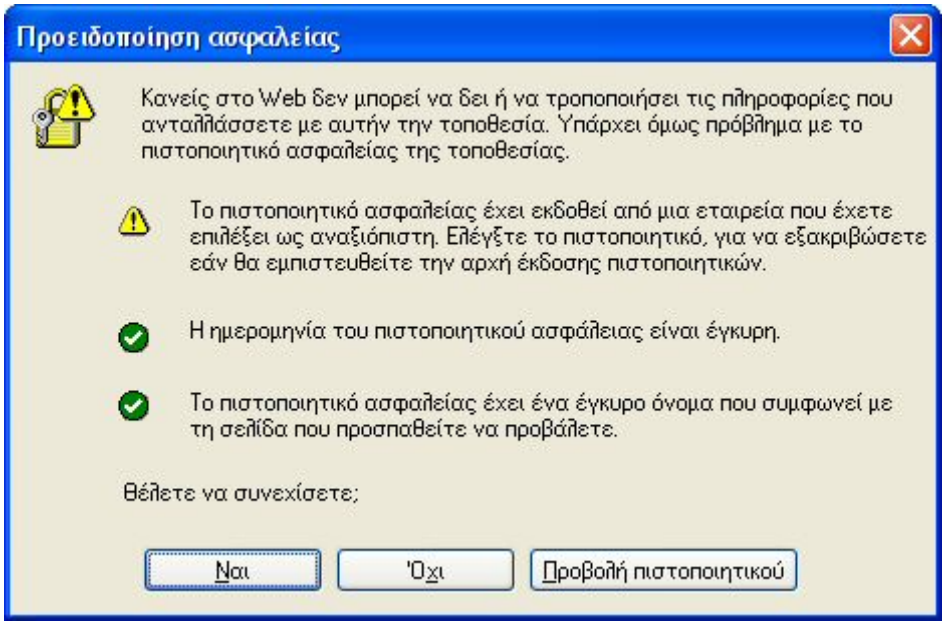
Αν στη πληκτρολόγηση των aueb/wireless γίνει κάποιο λάθος επανεμφανίζεται μετά από κάποια δευτερόλεπτα στην κάτω δεξιά γωνία των Windows το μήνυμα της προ-προηγούμενης εικόνας (**Κάντε κλικ εδώ, για να επιλέξετε ένα πιστοποιητικό**…). Αν τα aueb/wireless πληκτρολογηθούν σωστά εμφανίζεται κάτω δεξιά στην οθόνη των Windows το ακόλουθο μήνυμα, το οποίο δηλώνει ότι ο υπολογιστής μας έχει συνδεθεί στο AUEB Wireless (αυτό βέβαια δεν σημαίνει ότι μπορείτε ακόμη να συνδεθείτε στο Internet, διότι δεν έχει γίνει ακόμη η πραγματική αυθεντικοποίηση χρήστη):

Το **Ισχύς σήματος** μας δείχνει την ποιότητα του σήματος της ασύρματης σύνδεσης. Το εικονίδιο δηλώνει ότι υπάρχει ασύρματη σύνδεση, και το ότι υπάρχει ασύρματη σύνδεση πάνω από την οποία περνούν αυτή τη στιγμή δεδομένα. Σε αντίθεση, το εικονίδιο δηλώνει ότι δεν υπάρχει αυτή τη στιγμή ενεργή ασύρματη σύνδεση του υπολογιστή μας με κάποιο δίκτυο.

Οι ρυθμίσεις που αναφέρθηκαν έως εδώ για το AUEB-Wireless γίνονται μόνο μία αρχική φορά, και δεν χρειάζεται να

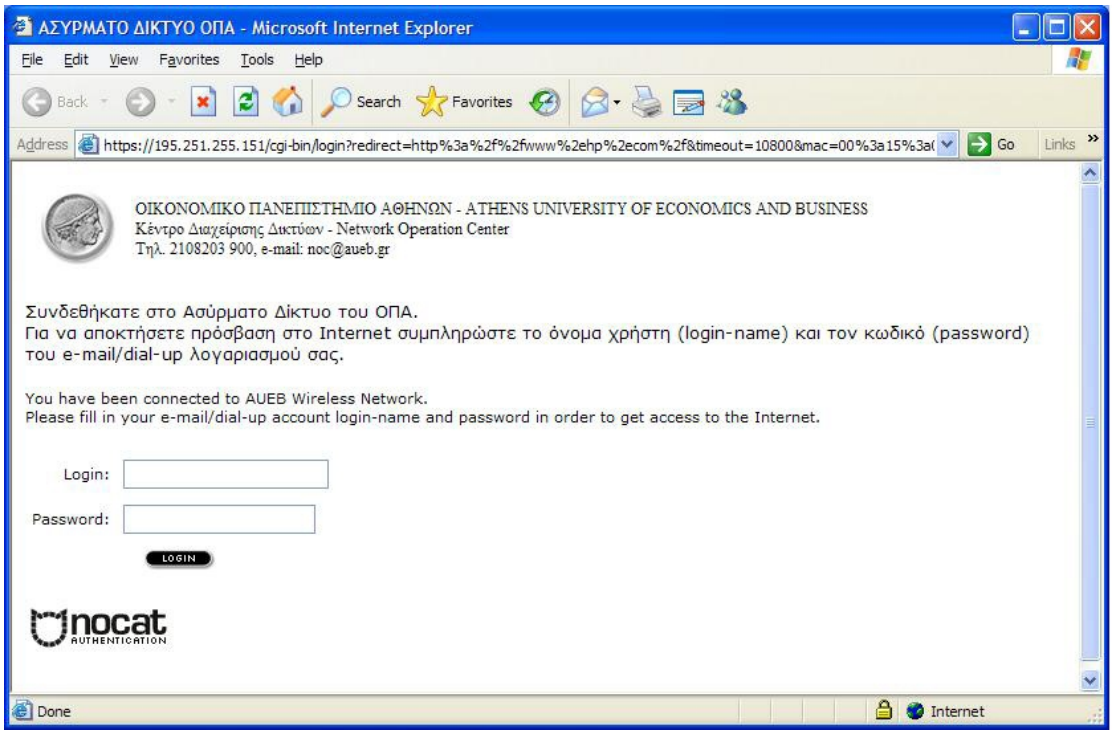
ξαναεπαναλαμβάνονται κάθε φορά που θέλουμε να συνδεθούμε σε αυτό.

Από εδώ και πέρα, για να αποκτήσει ο υπολογιστής σας πρόσβαση σε οποιαδήποτε υπηρεσία του Internet θα πρέπει <u>οπωσδήποτε</u> να ανοίξετε πρώτα έναν Web browser, όπως π.χ. τον Internet Explorer. Όποια σελίδα και να έχετε δηλώσει σαν αρχική (Home page), ή όποια σελίδα και να πληκτρολογήσετε στη Διεύθυνση (Address), θα εμφανιστεί το ακόλουθο μήνυμα, στο οποίο κάνετε κλικ το **Ναι**.



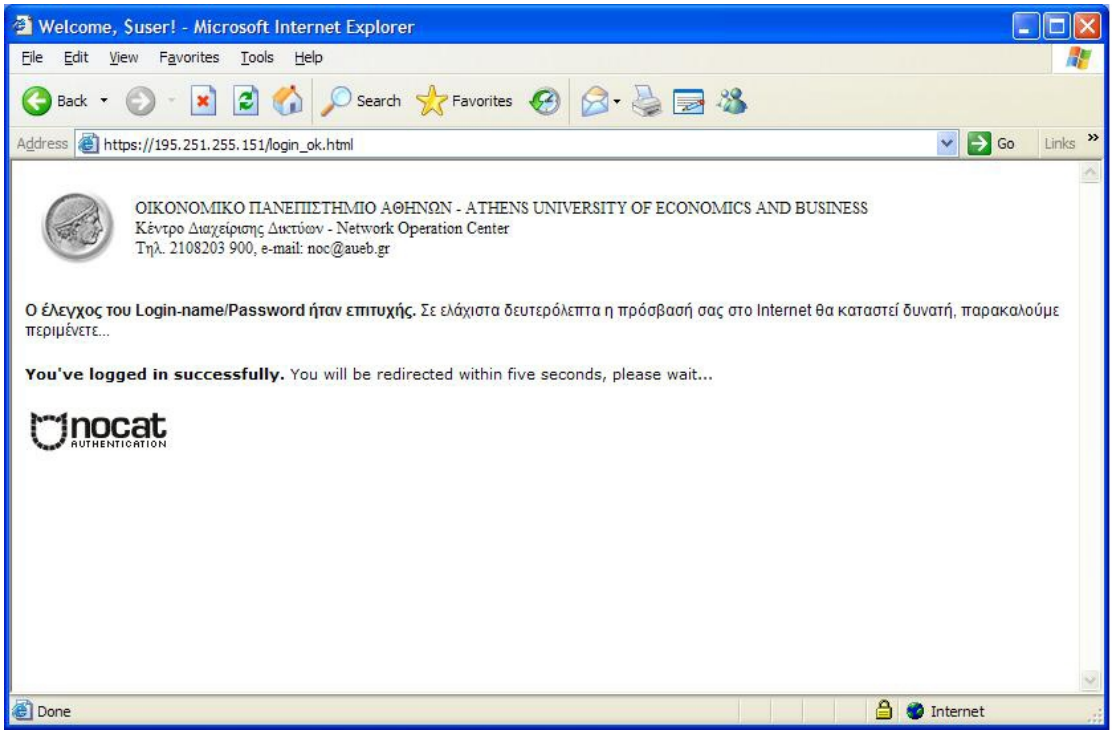
ΣΗΜΕΙΩΣΗ: αν δεν θέλετε να εμφανίζεται το ανωτέρω μήνυμα κάθε φορά που αρχικοποιείται η πρόσβαση του υπολογιστή σας στο Internet, πρέπει να εγκαταστήσετε (εισάγετε) στον υπολογιστή το πιστοποιητικό ασφαλείας (security certificate) του διακομιστή ασύρματης πρόσβασης (wireless server) από το http://www.aueb.gr/help/certificates/ .

Στη συνέχεια εμφανίζεται η φόρμα που ακολουθεί. Με τη φόρμα αυτή γίνεται η πραγματική αυθεντικοποίηση του χρήστη. Στη φόρμα αυτή συμπληρώστε το Όνομα χρήστη (Login-name ή Username) και τον κωδικό (Password) που χρησιμοποιείτε για τις υπηρεσίες ηλεκτρονικού ταχυδρομείου και dial-up του Πανεπιστημίου, και κάντε κλικ στο **LOGIN**.



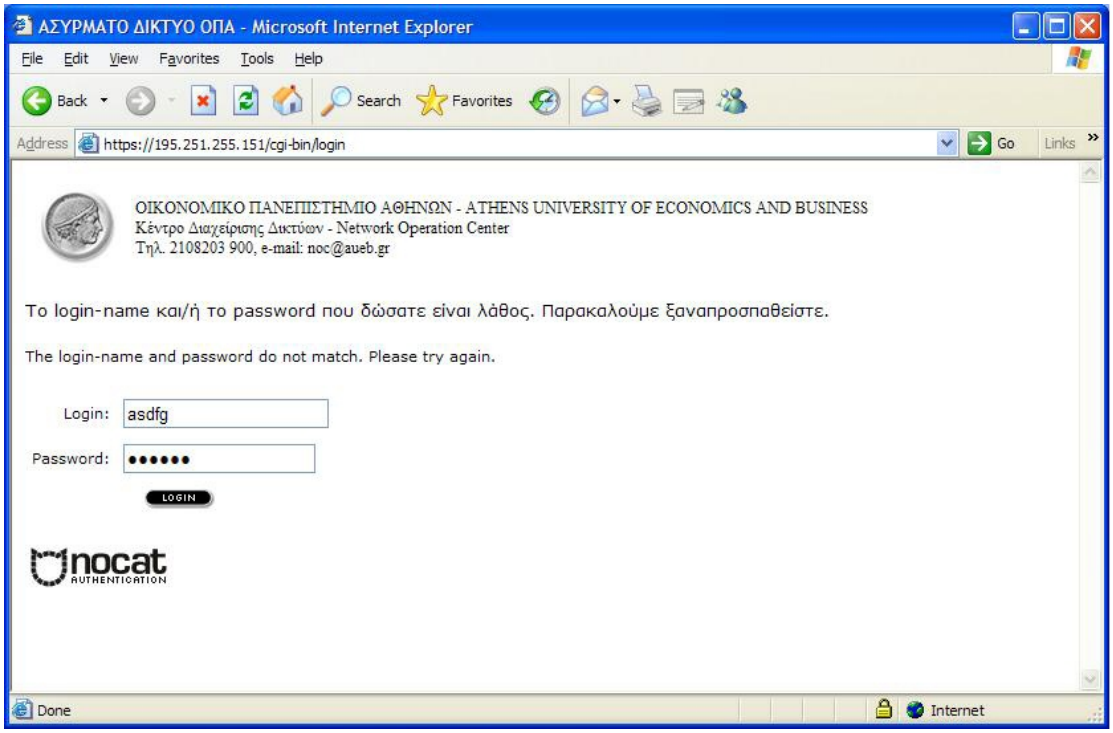
Η αποστολή των Login-name/Password γίνεται με τη χρήση του ασφαλούς πρωτοκόλλου http (https), το οποίο προσθέτει ένα επιπλέον επίπεδο ισχυρής ασφάλειας πάνω από την ασφάλεια που παρέχει το πρωτόκολλο ασύρματης σύνδεσης WPA.

Αν τα Login-name/Password εισαχθούν σωστά, εμφανίζεται η παρακάτω σελίδα, και μετά από λίγα δευτερόλεπτα εμφανίζεται η αρχική σελίδα του browser (ή η σελίδα την οποία πληκτρολογήσατε όταν ανοίξατε τον browser). *Ο υπολογιστής σας πλέον έχει σύνδεση (πρόσβαση) στο Internet για οποιαδήποτε υπηρεσία (Web, mail, ftp, κτλ.).*



Η διάρκεια της παροχής πρόσβασης στο Internet είναι επί του παρόντος 3 ώρες, μετά το πέρας των οποίων θα σας ζητηθεί από τον Internet Browser (π.χ., τον Internet Explorer) να ξανα-εισάγετε τα Login-name/Password σας και πάλι για να ανανεωθεί η πρόσβαση στο Internet. Αν, όμως, δεν έχετε στον Internet Browser ενεργοποιημένο τον αποκλεισμό αναδυόμενων παραθύρων (pop-up blocker), τότε εμφανίζεται το ακόλουθο παράθυρο, το οποίο, κρατώντας το ανοιχτό, επιτρέπει την ανανέωση της πρόσβασής μας στο Internet και πέρα των 3 ωρών (=8100 seconds), χωρίς να χρειαστεί να ξαναδώσουμε το Login-name και το Password.

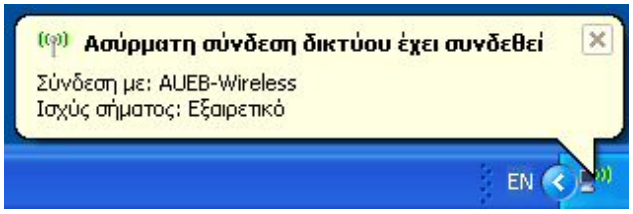
Αν παραπάνω κάναμε λάθος στην πληκτρολόγηση του Login-name ή του Password, εμφανίζεται η ακόλουθη σελίδα, και πρέπει να τα ξαναεισάγουμε.



3. Επόμενες συνδέσεις

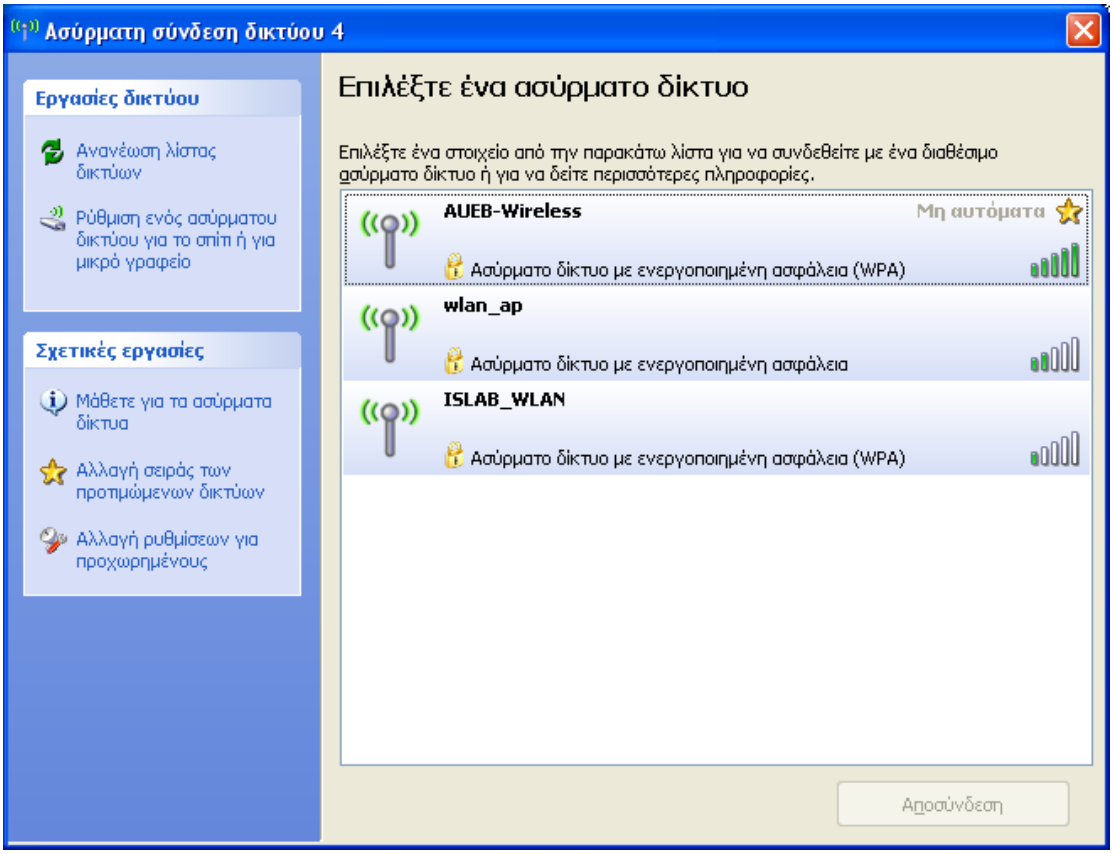
Αν δεν έχετε αλλάξει την προεπιλεγμένη ρύθμιση για αυτόματη σύνδεση στο AUEB-Wireless, τότε, με το που ανοίγετε τον

φορητό σας υπολογιστή σε σημείο το οποίο βρίσκεται στη εμβέλεια ενός σημείου πρόσβασης του AUEB-Wireless, αυτός θα συνδέεται αυτόματα σε αυτό, και στη κάτω δεξιά γωνία θα εμφανίζεται μετά από μερικά δευτερόλεπτα το ακόλουθο μήνυμα.

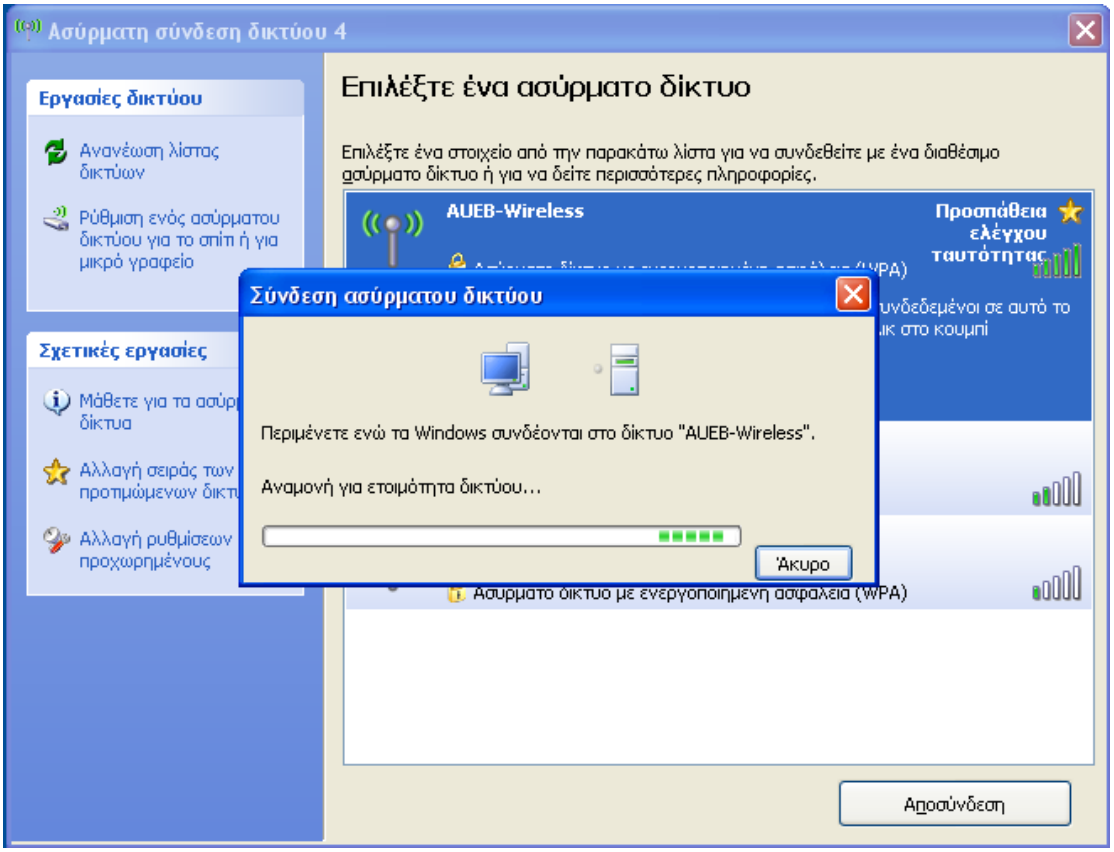


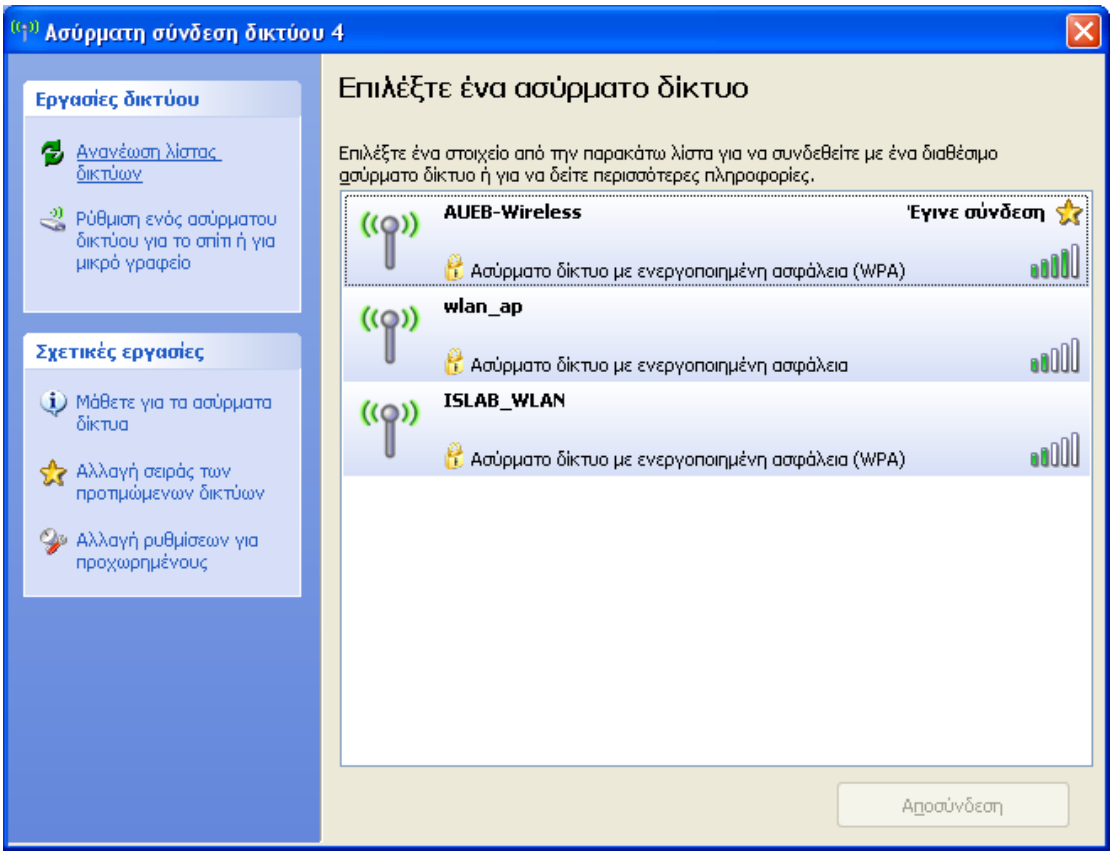
Ας μη ξεχνάτε ότι πρέπει απαραίτητα στη συνέχεια να ανοίγετε τον Web browser (π.χ., τον Internet Explorer) για να εισάγετε το Login-name/Password, ώστε να αποκτήσετε πρόσβαση στο Internet.

Αν έχετε ρυθμίσει τον υπολογιστή σας να μη συνδέεται αυτόματα στο AUEB-Wireless, με αποτέλεσμα ο υπολογιστής σας να μη συνδέεται σε κανένα ασύρματο δίκτυο (εικονίδιο κάτω δεξιά), ή να συνδεθεί σε άλλο ασύρματο δίκτυο (εικονίδιο κάτω δεξιά), τότε, για να συνδεθείτε στο AUEB-Wireless, κάντε διπλό κλικ στο ή στο αντίστοιχα, οπότε εμφανίζεται το ακόλουθο παράθυρο.



Κάνοντας διπλό κλικ στο AUEB-Wireless, η σύνδεση επιτυγχάνεται σε ελάχιστα δευτερόλεπτα (υπό την προϋπόθεση, βέβαια, ότι έχουν γίνει σωστά όλες οι αρχικές ρυθμίσεις που αναφέρθηκαν στο παρόν κείμενο).


Ασύρματη σύνδεση δικτύου 4
Εργασίες δικτύου
Ανανέωση λίστας δικτύων
Ρύθμιση ενός ασύρματου δικτύου για το σπίτι ή για μικρό γραφείο
Σχετικές εργασίες
Μάθετε για τα ασύρ δίκτυα
Αλλαγή σειράς των προτιμώμενων δικτ
Αλλαγή ρυθμίσεων προχωρημένους
Επιλέξτε ένα ασύρματο δίκτυο
Επιλέξτε ένα στοιχείο από την παρακάτω λίστα για να συνδεθείτε με ένα διαθέσιμο ασύρματο δίκτυο ή για να δείτε περισσότερες πληροφορίες.
AUEB-Wireless
Προσπάθεια ελέγχου ταυτότητας
Σύνδεση ασύρματου δικτύου
Περιμένετε ενώ τα Windows συνδέονται στο δίκτυο "AUEB-Wireless".
Αναμονή για ετοιμότητα δικτύου...
Άκυρο
Ασύρματο δίκτυο με ενεργοποιημένη ασφάλεια (WPA)
Αποσύνδεση


Ασύρματη σύνδεση δικτύου 4
Εργασίες δικτύου
Ανανέωση λίστας δικτύων
Ρύθμιση ενός ασύρματου δικτύου για το σπίτι ή για μικρό γραφείο
Σχετικές εργασίες
Μάθετε για τα ασύρματα δίκτυα
Αλλαγή σειράς των προτιμώμενων δικτύων
Αλλαγή ρυθμίσεων για προχωρημένους
Επιλέξτε ένα ασύρματο δίκτυο
Επιλέξτε ένα στοιχείο από την παρακάτω λίστα για να συνδεθείτε με ένα διαθέσιμο ασύρματο δίκτυο ή για να δείτε περισσότερες πληροφορίες.
AUEB-Wireless
Έγινε σύνδεση
Ασύρματο δίκτυο με ενεργοποιημένη ασφάλεια (WPA)
wlan_ap
Ασύρματο δίκτυο με ενεργοποιημένη ασφάλεια
ISLAB_WLAN
Ασύρματο δίκτυο με ενεργοποιημένη ασφάλεια (WPA)
Αποσύνδεση

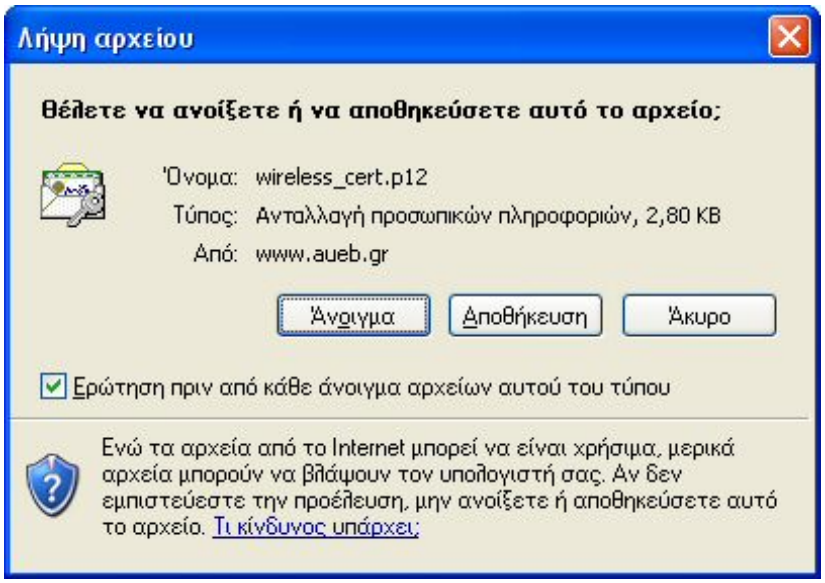
Οι κάθετες πράσινες γραμμές δεξιά του ονόματος του δικτύου δείχνουν το πόσο ισχυρό είναι το σήμα της ασύρματης σύνδεσης.

ΠΑΡΑΡΤΗΜΑ: Σύνδεση WPA με χρήση του πρωτοκόλλου EAP-TLS

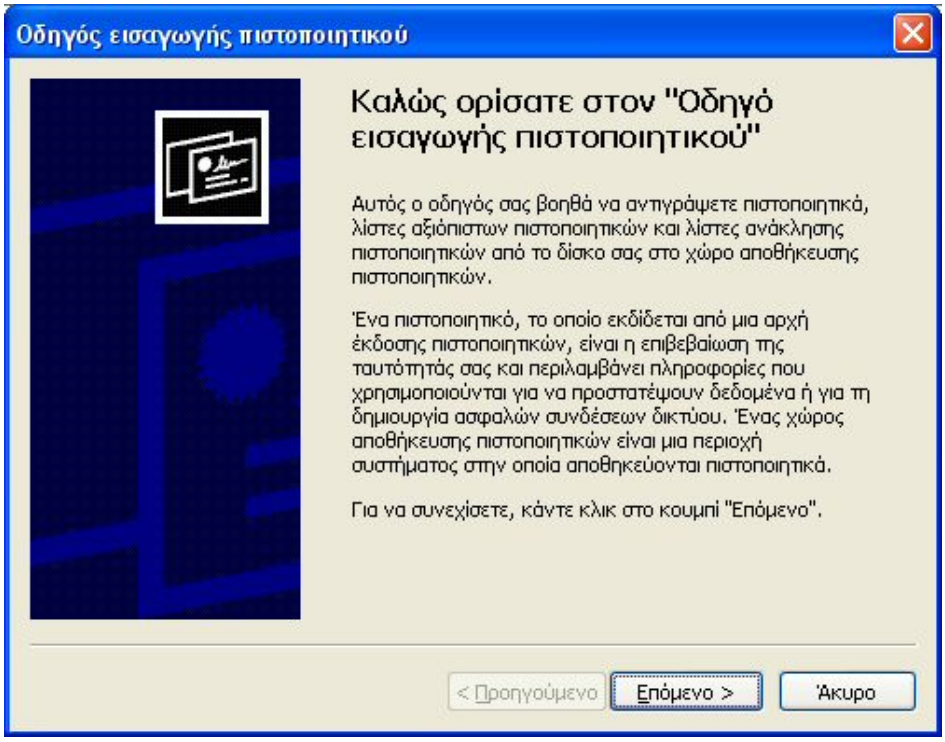
Για να γίνει δυνατή η σύνδεση στο AUEB Wireless με χρήση του EAP-TLS, πρέπει αρχικά να εγκατασταθεί στον υπολογιστή μας το πιστοποιητικό ασφάλειας (certificate) χρήστη, το οποίο είναι κοινό για όλους τους χρήστες του AUEB Wireless. Όπως και στη περίπτωση του πρωτοκόλλου PEAP (όπου έχουμε έναν κοινό χρήστη για όλους, τον **aueb** με password το **wireless**), έτσι κι εδώ δεν μας ενδιαφέρει η αυθεντικοποίηση χρηστών (user authentication), άλλα η έναρξη του πρωτοκόλλου WPA για την ύπαρξη ικανοποιητικής ασφάλειας στην ασύρματη επικοινωνία. Η κατοχή του συγκεκριμένου πιστοποιητικού από κάποιον εξωτερικό «παρείσακτο» δεν του δίνει κανένα πλεονέκτημα σε πιθανή του προσπάθεια να παραβιάσει την ασφάλεια της ασύρματης επικοινωνίας.

Αν ο φορητός υπολογιστής μας έχει δυνατότητα ενσύρματης δικτύωσης, δίνουμε στον Internet Explorer τη διεύθυνση http://www.aueb.gr/certificates/wireless_cert.p12 . Αλλιώς, σε κάποιον άλλο υπολογιστή αποθηκεύουμε το αρχείο από αυτή τη διεύθυνση σε δισκέττα, CD-RW, USB flash disk, κτλ., το μεταφέρουμε στον φορητό υπολογιστή, και κάνουμε διπλό κλικ επάνω του. Σε αυτή περίπτωση προχωράμε στο μεθεπόμενο σχήμα.

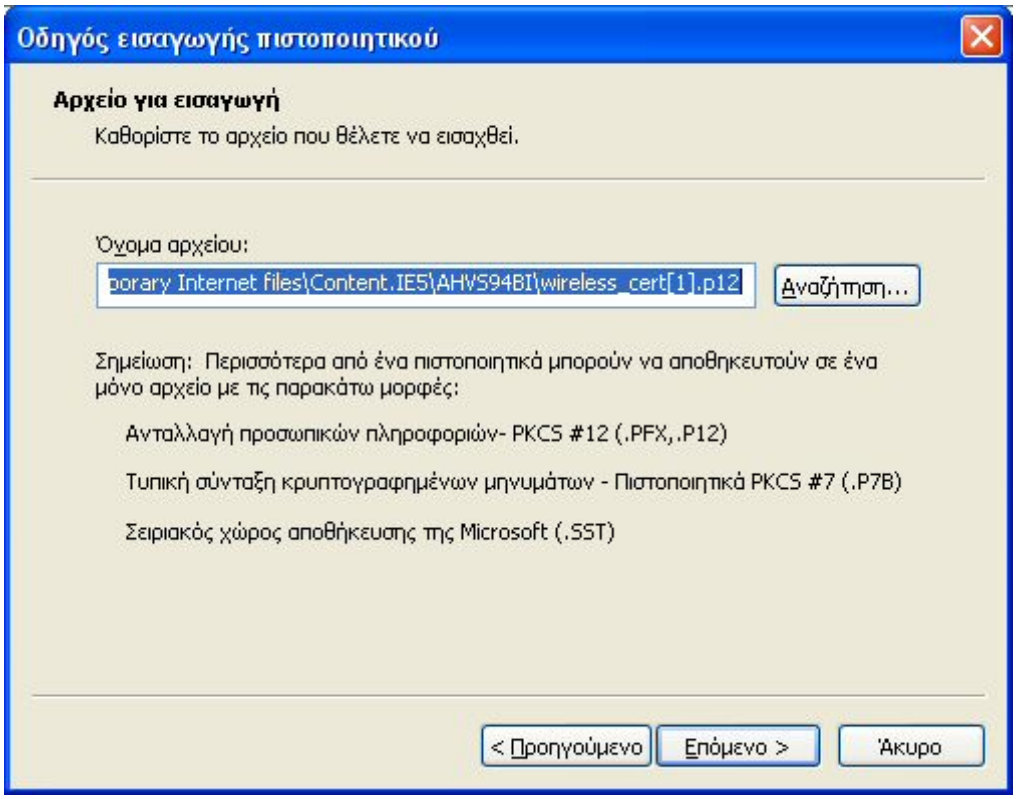
Εμφανίζεται το ακόλουθο παράθυρο.



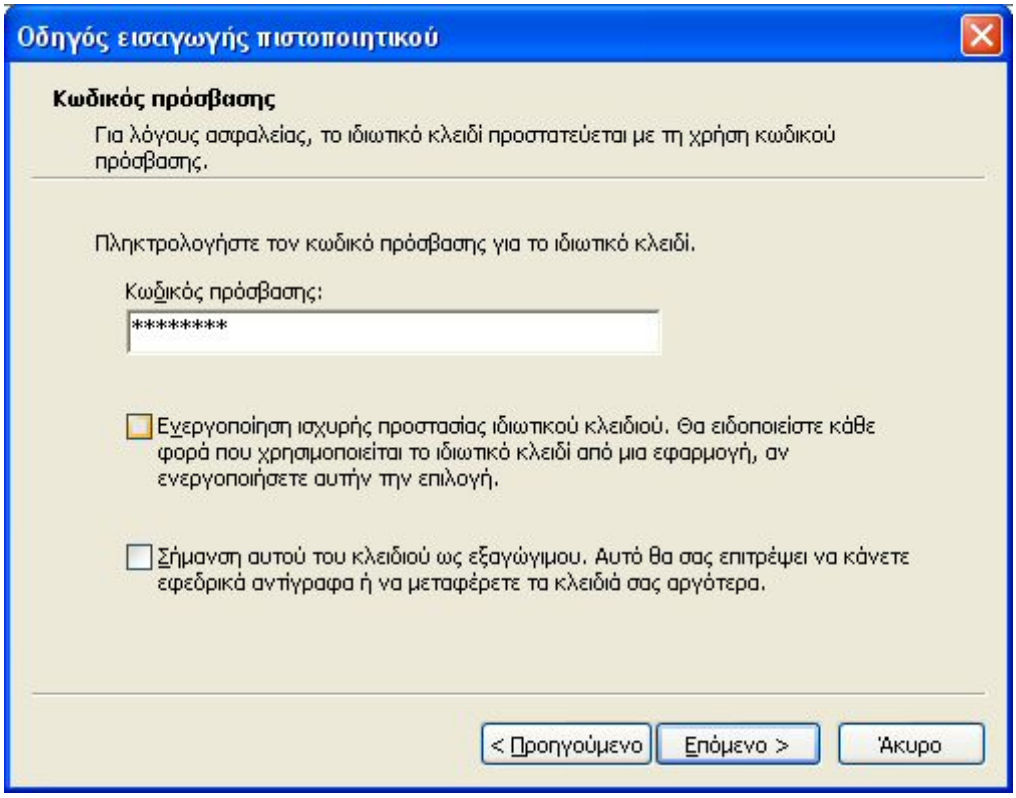
Κάνουμε κλικ στο κουμπί **Άνοιγμα**.



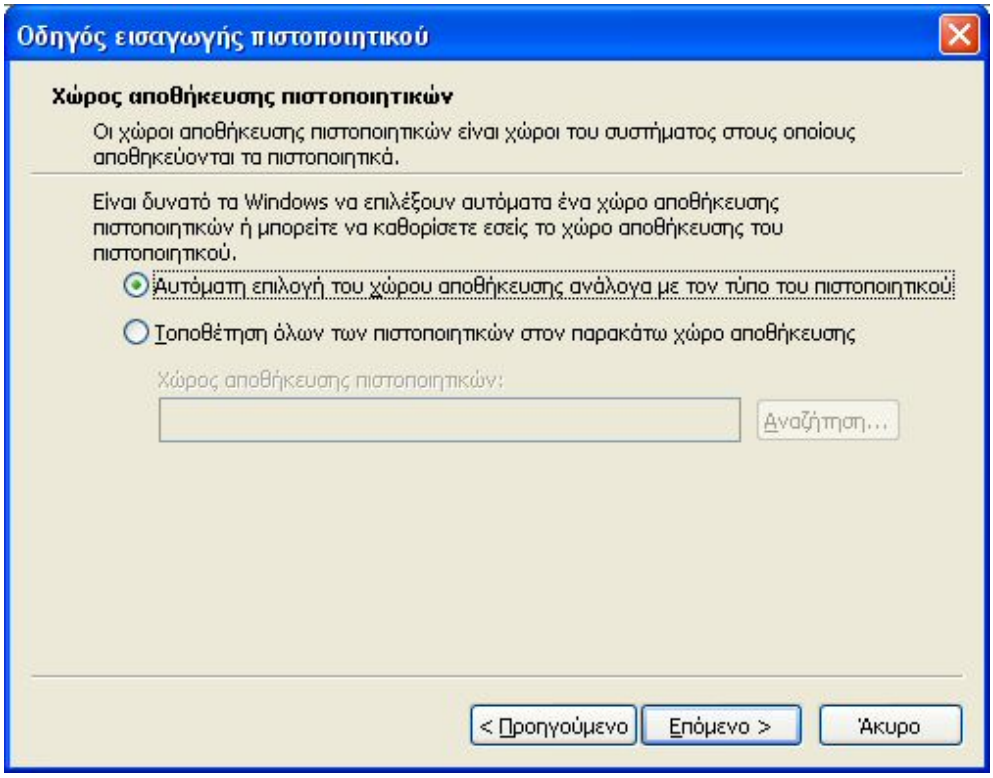
Πατάμε στο **Επόμενο**.



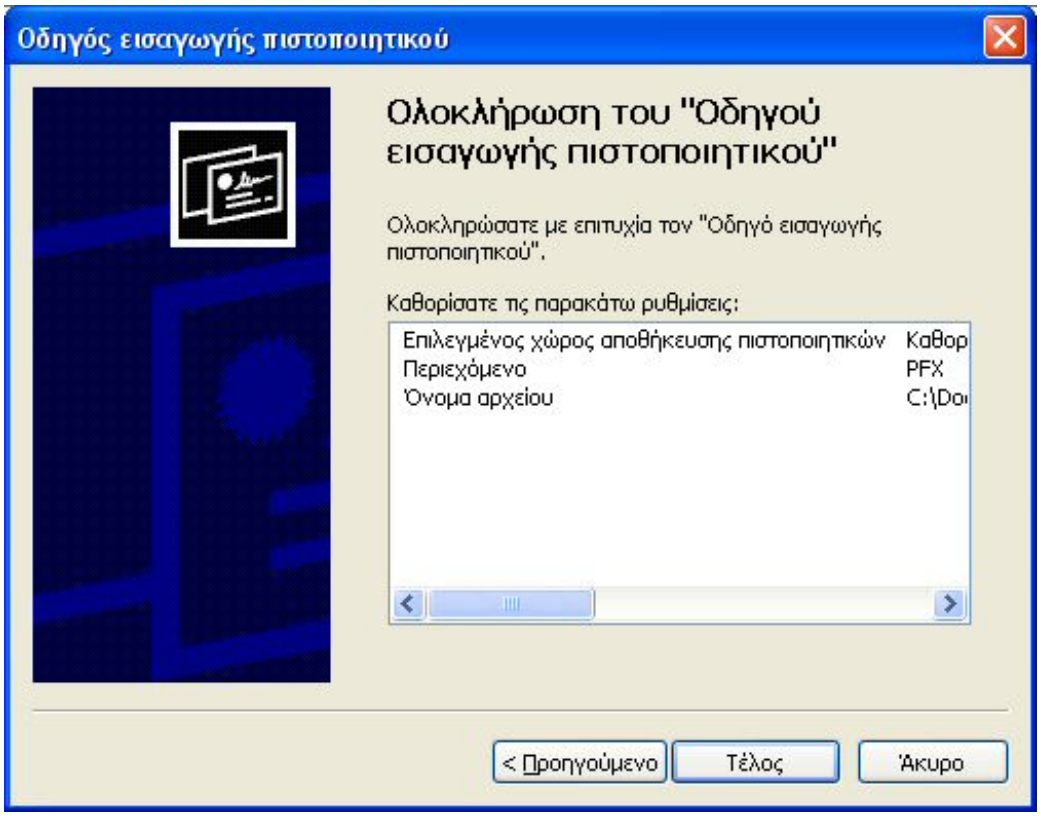
Ξανά **Επόμενο**.



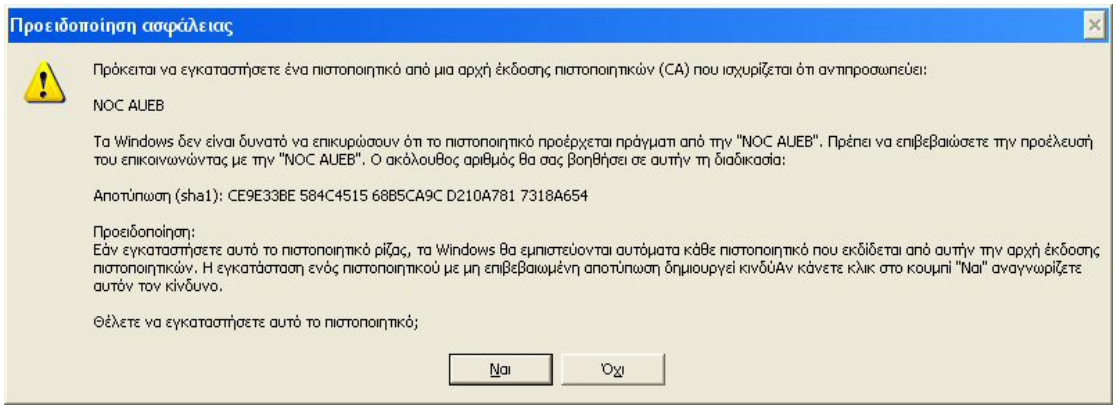
Συμπληρώνουμε σαν **Κωδικό πρόσβασης** το **wireless** και κάνουμε κλικ στο **Επόμενο**.



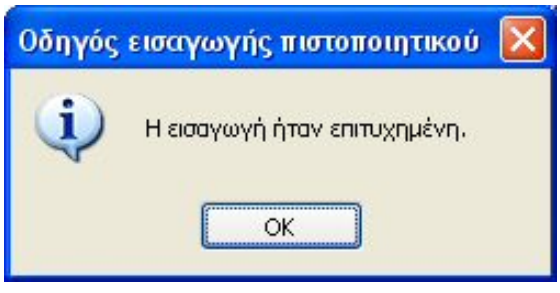
Αφήνουμε το **Αυτόματη επιλογή του χώρου αποθήκευσης ανάλογα με τον τύπο πιστοποιητικού** και πατάμε το **Επόμενο**.



Πατάμε το κουμπί **Τέλος**. Εμφανίζεται το ακόλουθο μήνυμα.



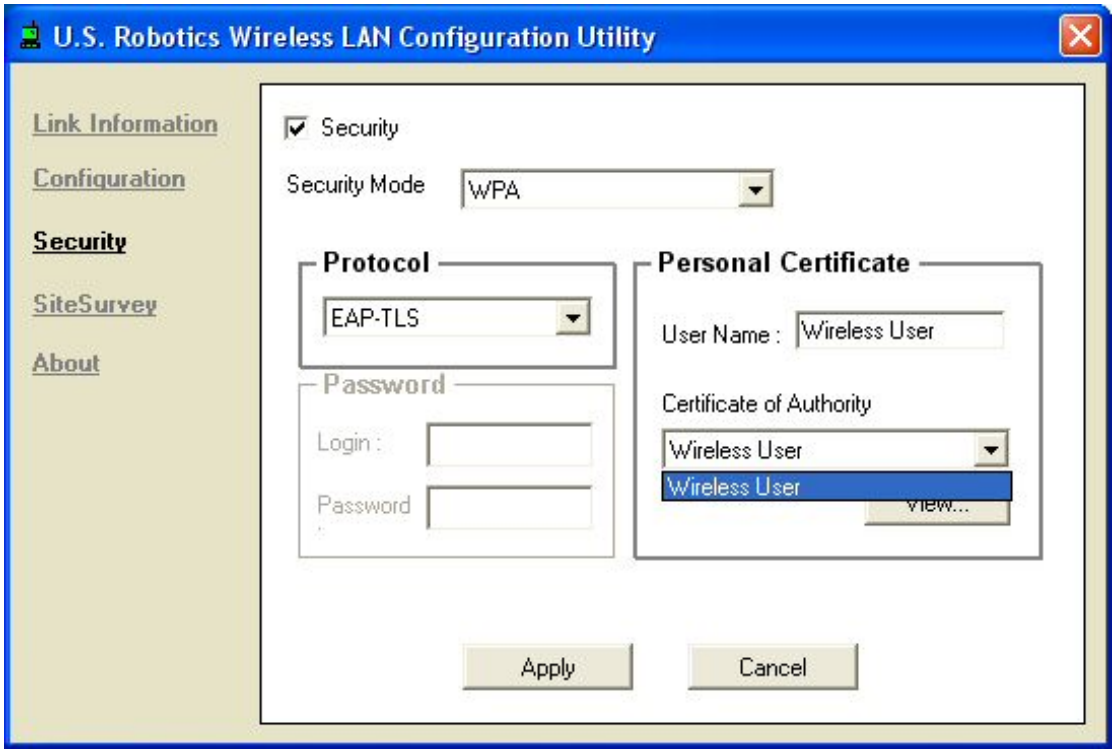
Πατάμε στο **Ναι**.



Η εισαγωγή του πιστοποιητικού ολοκληρώθηκε. Ο χρήστης του οποίου το πιστοποιητικό εισήχθη ονομάζεται **Wireless User**.

Στη συνέχεια, στο λογισμικό της ασύρματης κάρτας δικτύου μας ρυθμίζουμε το AUEB-Wireless με WPA/802.1X σε συνδυασμό με EAP-TLS, και στα certificates επιλέγουμε τον χρήστη **Wireless User** (του οποίου το πιστοποιητικό το βρίσκει το λογισμικό λόγω του ότι το έχουμε εισάγει στα Windows).

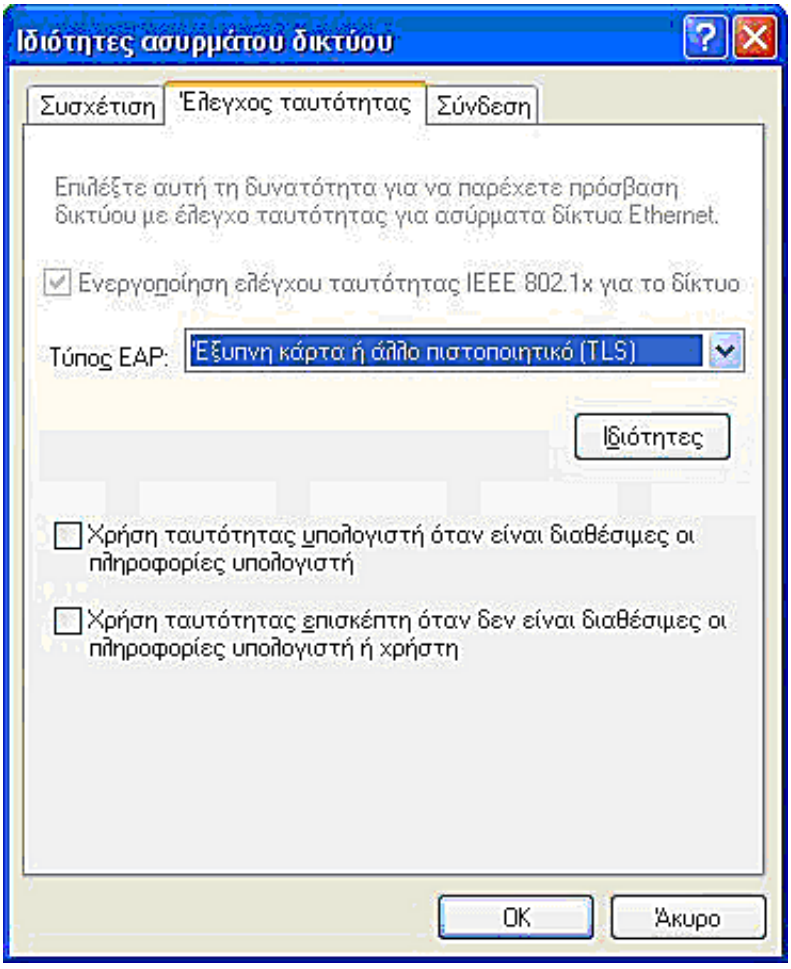
Σαν παράδειγμα, ακολουθεί το στιγμιότυπο από το λογισμικό της κάρτας ***U.S. Robotics Wireless Turbo PC Card***.



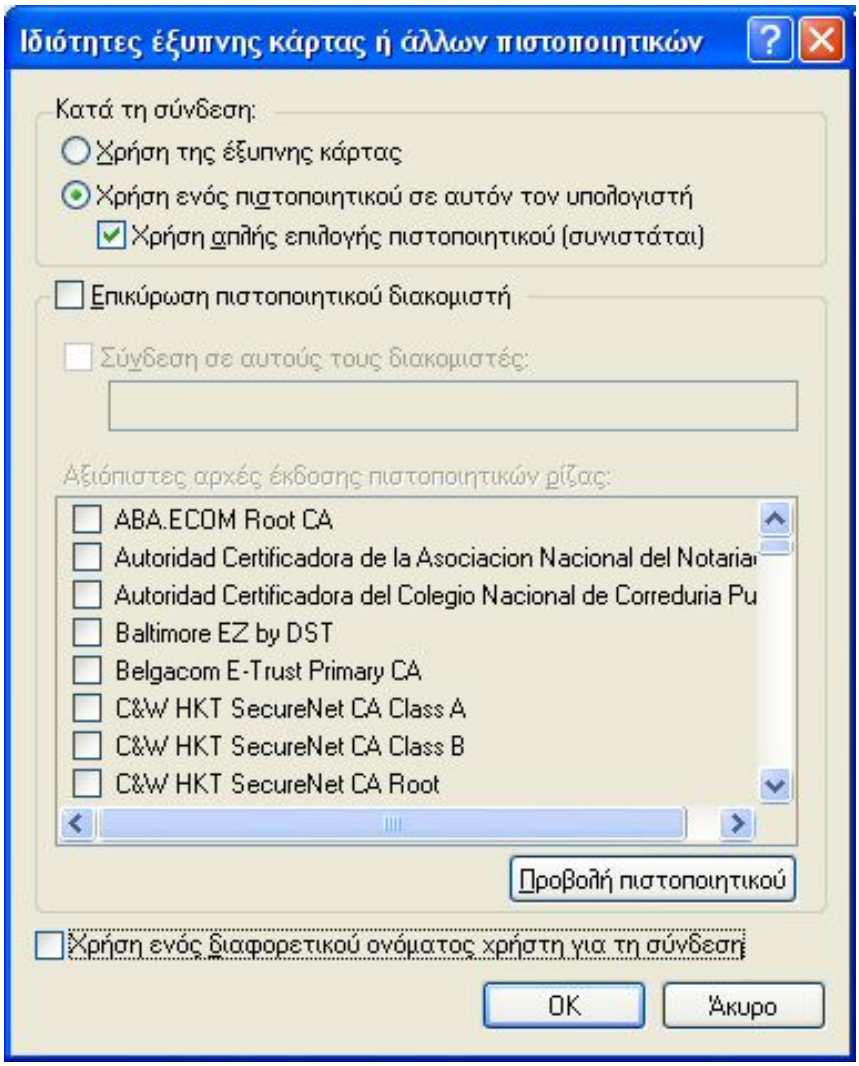
Αν χρησιμοποιείτε το βοήθημα (utility) των Windows και θέλετε να ρυθμίσετε το AUEB-Wireless με EAP-TLS (κάτι το οποίο δεν συνιστούμε, γιατί το βοήθημα των Windows υποστηρίζει το PEAP, οπότε δεν υπάρχει λόγος χρήσης του EAP-TLS), οι ρυθμίσεις που αναφέρθηκαν παραπάνω τροποποιούνται μόνο στα ακόλουθα (με

την προϋπόθεση, βέβαια, να έχει εγκατασταθεί το πιστοποιητικό του χρήστη **Wireless User** στον υπολογιστή σας):

Στον **Έλεγχο ταυτότητας** του παραθύρου **Ιδιότητες ασύρματου δικτύου**, στον **Τύπο EAP** επιλέξτε **Έξυπνη κάρτα ή άλλο πιστοποιητικό (TLS)** (αντί για το **Προστατευμένο EAP (PEAP)**).



Στη συνέχεια, κάνοντας κλικ στο κουμπί **Ιδιότητες**, ρυθμίζουμε τις ιδιότητες του TLS ως ακολούθως:



Σημείωση: αν στον υπολογιστή σας έχετε εγκαταστήσει και άλλα πιστοποιητικά χρηστών (user certificates), τότε στο προηγούμενο παράθυρο τσεκάρετε το **Χρήση ενός διαφορετικού ονόματος χρήστη για τη σύνδεση**, ώστε τα Windows να σας δώσουν τη δυνατότητα επιλογής του χρήστη κατά τη διάρκεια αρχικοποίησης της σύνδεσης (με μήνυμα που εμφανίζεται στην κάτω δεξιά γωνία των Windows).

Όλες οι υπόλοιπες ρυθμίσεις είναι ίδιες.

ΠΗΓΕΣ…

- http://ru6.cti.gr/broadband/el/evrizonikotita.php
- http://www.noc.ntua.gr/index.php?name=FAQ&id_cat=33
- http://www.unipi.gr
- http://www.upatras.gr
- www.zdnet.co.uk
- http://www.ibm.com
- http://www.awmn.gr
- http://ieee802.org/11
- http://www.ja.net/services/publications
- http://grouper.ieee.org/groups/802.11/
- http://www.tropos.com
- http://www.hswn.gr
- http://www.2-tee-n-smyrn.gr

- Douglas E. Comer(2004) Δίκτυα και διαδίκτυα υπολογιστών
- Abramson, N. (1970), the aloha system, another alternative for computer communications
- Postel, J. B(1980), internetwork protocol approaches
- Pelton,J(1995), wireless and satellite telecommunications
- Kaufman,C.,Perlman,R. and speciner, m.(1995) network security: private communication in a public world
- Denning P.J.(1989) the science of computing:the ARPAnet after 20 years
- Boggs,D.,J.Shoch,E.Taft and R. Metcalfe(1980),pup:an internet work architecture,IEEE transactions of communication