

ΕΠΙΣΕΥ
ΕΡΕΥΝΗΤΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΑΚΟ
ΙΝΣΤΙΤΟΥΤΟ ΣΥΣΤΗΜΑΤΩΝ
ΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ
ΥΠΟΛΟΓΙΣΤΩΝ



(ΝΠΙΔ : ΠΔ 271/89 • Ν2083/92 • ΠΔ 13/98)

ICCS
INSTITUTE OF COMMUNICATION
AND COMPUTER SYSTEMS

(P.L.L.E.: Decrees 271/89 & 13/98 • Law 2083/92)

Διεύθυνση Αλληλογραφίας
ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ
ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
Ηρώων Πολυτεχνείου 9
15773 Ζωγράφου
Αθήνα Tel.: +30 210-772 1531, 2279, 1449

Address for Correspondence
NATIONAL TECHNICAL UNIVERSITY
OF ATHENS
DEPARTMENT OF ELECTRICAL AND
COMPUTER ENGINEERING
9, Iroon Polytechniou Str.
15773 Zografou
Athens , Greece



ΤΟ ΠΑΡΟΝ ΕΡΓΟ ΕΧΕΙ ΧΡΗΜΑΤΟΔΟΤΗΘΕΙ ΚΑΤΑ 75% ΑΠΟ ΤΟ
ΕΥΡΩΠΑΪΚΟ ΤΑΜΕΙΟ ΠΕΡΙΦΕΡΕΙΑΚΗΣ ΑΝΑΠΤΥΞΗΣ (ΕΤΠΑ)

**Έργο: «Ανάπτυξη Ασύρματων Ευρυζωνικών Υποδομών και Προώθηση
Ζήτησης Ασύρματων Υπηρεσιών Διαδικτύου σε Πολυσύχναστους
Εξωτερικούς Χώρους»**

**2ο Υποέργο: «Τεχνική Μελέτη του Έργου, Διαχείριση και Παρακολούθηση του
Έργου, Επιχειρησιακή (κανονική) Λειτουργία με ίδια μέσα»**

Αποφάσεις Ένταξης: 151.369/ΚτΠ9371-B3 24/2/2004 και 152.679/ΚτΠ7356-B3 23/7/2004,
Κωδικός ΟΠΣ: 91016

Τεχνική Μελέτη Ασύρματου Δικτύου

ΟΔΗΓΟΣ ΓΙΑ ΤΟΥΣ ΑΝΑΔΟΧΟΥΣ ΤΗΣ ΠΡΟΣΚΛΗΣΗΣ 84 του ΕΠ ΚτΠ
ΓΙΑ ΤΗΝ ΕΠΙΔΕΙΚΤΙΚΗ ΠΑΡΟΧΗ ΥΠΗΡΕΣΙΩΝ ΑΣΥΡΜΑΤΗΣ ΠΡΟΣΒΑΣΗΣ
ΣΤΟ ΔΙΑΔΙΚΤΥΟ

Απρίλιος 2005

Περιεχόμενα

1 ΕΙΣΑΓΩΓΗ	5
1.1 Σκοπός του Έργου	5
2 ΠΕΡΙΒΑΛΛΟΝ ΕΓΚΑΤΑΣΤΑΣΗΣ, ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΑΙ ΛΕΙΤΟΥΡΓΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ ΤΟΥ ΑΣΥΡΜΑΤΟΥ ΔΙΚΤΥΟΥ.....	7
2.1 Περιγραφή Λειτουργίας ενός Δημόσιου Ασύρματου Δικτύου Ανοικτού Χώρου	9
2.1.1 Από την πλευρά του χρήστη	9
2.1.2 Δίκτυο Δεδομένων	9
2.2 Διευθυνσιοδότηση	11
2.3 Captive Portal	11
2.4 Περιοχή Κάλυψης Ασύρματου Δικτύου Wi-Fi	13
2.4.1 Επικάλυψη Καναλιών	14
2.5 Αρχιτεκτονική ενός Δημόσιου Ασύρματου Δικτύου Ανοικτού Χώρου	15
2.5.1 Υποσύστημα Ασύρματης Πρόσβασης Χρηστών	16
2.5.2 Υποσύστημα Backhaul.....	17
2.5.3 Υποσύστημα Κεντρικού Σημείου Διασύνδεσης.....	18
2.6 Λειτουργικές Απαιτήσεις	20
2.7 Πολιτική Ασφάλειας	20
2.8 Υψηλή Διαθεσιμότητα	21

2.9 Ρυθμός Μετάδοσης Δεδομένων	22
2.10 Πλήθος Εξυπηρετούμενων Χρηστών	23
2.11 Τεκμηρίωση	24
3 ΔΙΚΤΥΟ ATHENSWIFI: “ΔΗΜΟΣΙΟ ΔΙΚΤΥΟ ΑΣΥΡΜΑΤΗΣ ΠΡΟΣΒΑΣΗΣ ΣΤΟ ΔΙΑΔΙΚΤΥΟ ΣΤΗΝ ΠΛΑΤΕΙΑ ΣΥΝΤΑΓΜΑΤΟΣ” (<i>WWW.ATHENSWIFI.GR</i>)	26
3.1 Περιγραφή Λειτουργίας του Ασύρματου Δικτύου AthensWiFi	27
3.2 Περιοχή Κάλυψης Δικτύου AthensWiFi	28
3.3 Αρχιτεκτονική Ασύρματου Δικτύου AthensWiFi	35
3.3.1 Υποσύστημα Ασύρματης Πρόσβασης Χρηστών (hotspot)	36
3.3.2 Υποσύστημα Backhaul.....	36
3.3.3 Υποσύστημα Κεντρικού Σημείου Διασύνδεσης.....	37
4 ΔΙΑΔΙΚΑΣΙΑ ΕΛΕΓΧΟΥ ΑΣΥΡΜΑΤΗΣ ΔΙΚΤΥΑΚΗΣ ΥΠΟΔΟΜΗΣ ΚΑΙ ΥΠΗΡΕΣΙΩΝ	38
4.1 Διαδικασία ελέγχου.....	38
4.2 Έλεγχος με Περιπλάνηση (Walkabout Test)	38
4.3 Έλεγχος Λειτουργίας με διαφορετικού είδους συσκευές	39
4.4 Συμβατότητα με Πρωτόκολλο IEEE 802.11g.....	39
4.5 Έλεγχος Μέγιστου Χώρου Κάλυψης.....	40
4.6 Έλεγχος της Διαδικασίας Περιαγωγής (roaming).....	40
4.7 Έλεγχος εμφάνισης Συμφωνητικού Χρήσης του δικτύου και Προειδοποίησης Ασφαλείας	40

4.8 Έλεγχος Υπηρεσίας Firewall	41
4.9 Έλεγχος Συστημάτων Αδιάλειπτης Παροχής Ρεύματος.....	41
4.10 Έλεγχος Υψηλής Διαθεσιμότητας δικτύου	41
4.11 Έλεγχος Υπηρεσίας Διαπίστευσης	41
4.12 Έλεγχος Τήρησης Στατιστικών Χρήσης.....	42
5 ΒΙΒΛΙΟΓΡΑΦΙΑ.....	43

1 Εισαγωγή

Η μελέτη αυτή αποτελεί μέρος του έργου με τίτλο «Ανάπτυξη Ασύρματων Ευρυζωνικών Υποδομών και Προώθηση Ζήτησης Ασύρματων Υπηρεσιών Διαδικτύου σε πολυσύχναστους εξωτερικούς χώρους», αποφάσεις ένταξης: 151.369/ΚτΠ9371-B3 24/2/2004 και 152.679/ΚτΠ7356-B3 23/7/2004, κωδικός ΟΠΣ: 91016. Συγκεκριμένα η παρούσα μελέτη είναι παραδοτέο του 2^{ου} υποέργου με τίτλο «Τεχνική Μελέτη του Έργου, Διαχείριση και Παρακολούθηση του Έργου, Επιχειρησιακή (κανονική) Λειτουργία με ίδια μέσα» και έχει στόχο την υποστήριξη του 1^{ου} υποέργου με τίτλο «Προμήθεια, Εγκατάσταση & Δοκιμαστική Λειτουργία Εξοπλισμού και Ευρυζωνικής Πρόσβασης». Παρακάτω καταγράφονται και αναλύονται οι πληροφορίες που απαιτούνται για τη δημιουργία ενός δημόσιου ασύρματου δικτύου ανοιχτού χώρου.

1.1 Σκοπός του Έργου

Σκοπός του έργου είναι η πιλοτική παροχή ασύρματης πρόσβασης σε όλους τους χρήστες του εξωτερικού χώρου με στόχο την προώθηση της ιδέας της ευρυζωνικότητας και των σχετικών τεχνολογιών. Πρόκειται για μια καθαρά επιδεικτική δράση η οποία ως στόχο έχει να διαδώσει την έννοια της ευρυζωνικότητας και των σχετικών υπηρεσιών, με τελικό αποτέλεσμα την τόνωση της ζήτησης για τις υπηρεσίες αυτές. Το έργο προωθεί την ασύρματη ευρυζωνική πρόσβαση, μέσα από την, μικρής διάρκειας, επιδεικτική λειτουργία του δικτύου και με μικρό συνολικά διαθέσιμο εύρος ζώνης προς το διαδίκτυο. Αυτός είναι συνολικά και ο στόχος της πρόσκλησης 84 συνεπώς και των υπολοίπων έργων που υλοποιούνται σε όλη τη χώρα στο πλαίσιο αυτής.

Συνολικά οι δράσεις που προωθούνται στο πλαίσιο της πρόσκλησης 84 στοχεύουν στην προώθηση της ευρυζωνικότητας μέσα από την επίδειξη δράσεων και υπηρεσιών καθώς και μέσα από την παροχή της δυνατότητας στους τελικούς χρήστες να έρθουν σε επαφή με υπηρεσίες οι οποίες βασίζονται σε ευρυζωνικές υποδομές κάνοντας χρήση των δικών τους συσκευών και για προσωπική τους ουσιαστικά χρήση. Η σύντομη επαφή των τελικών χρηστών με τέτοιες υπηρεσίες, στο πλαίσιο μιας ημερίδας ή διημερίδας, δεν μπορεί να υποκαταστήσει μια σχετικά μακροχρόνια χρήση των υπηρεσιών αυτών, η οποία μπορεί να κάνει σαφές στον τελικό χρήστη τα οφέλη της ευρυζωνικότητας στην καθημερινότητά του.

Για το λόγο αυτό και με στόχο την ευρύτερη προώθηση των ευρυζωνικών τεχνολογιών και υπηρεσιών, η παροχή στην περιοχή της πλατείας Συντάγματος θεωρείται και είναι εξαιρετικά σημαντική. Η υποδομή που θα αναπτυχθεί μπορεί να αποτελέσει τη βάση για τη διάδοση των

υπηρεσιών από τους εμπορικούς φορείς, καθώς οι χρήστες θα έρχονται σε επαφή με τις ευρυζωνικές υπηρεσίες.

Επιπλέον η παροχή ασυρματικών υπηρεσιών πρόσβασης στο διαδίκτυο στην περιοχή του Συντάγματος λαμβάνει και συμβολική σημασία καθώς τονίζει τη βούληση της κοινωνίας μας να προχωρήσει στην κοινωνία της πληροφορίας ακολουθώντας τις υπόλοιπες ευρωπαϊκές χώρες.

2 Περιβάλλον Εγκατάστασης, Χαρακτηριστικά και Λειτουργικές Απαιτήσεις του Ασύρματου Δικτύου

Τα ασύρματα δίκτυα υπάρχουν εδώ και μια δεκαετία, αλλά μόλις τα τελευταία χρόνια πραγματοποιήθηκε μια έκρηξη στη χρήση τους, εξαιτίας κυρίως της τεχνολογικής εξέλιξης στις ασύρματες δικτυακές φορητές συσκευές (φορητοί υπολογιστές, PDA, κλπ.) καθώς και της πτώσης της τιμής των τελευταίων. Τα ασύρματα δίκτυα μπορούν να αναπτυχθούν και να παρέχουν δικτυακές υπηρεσίες σε πολλούς διαφορετικούς χώρους και περιβάλλοντα. Τα ιδιαίτερα χαρακτηριστικά του κάθε χώρου καθώς και οι ανάγκες των χρηστών υποδεικνύουν μια σειρά από λειτουργικές απαιτήσεις οι οποίες πρέπει να ληφθούν υπόψη κατά το σχεδιασμό του ασύρματου δικτύου.

Στη μελέτη αυτή μας απασχολεί το θέμα του σχεδιασμού ενός δημοσίου ασύρματου δικτύου το οποίο μπορεί να χρησιμοποιηθεί από όλους του χρήστες χωρίς κανένα περιορισμό. Ο χώρος στον οποίο θα παρέχεται ασύρματη δικτυακή κάλυψη είναι του τύπου μιας πλατείας ή ενός πάρκου. Η σχεδίαση αφορά ιδιαίτερα φορείς που έχουν αναλάβει την υποχρέωση να πραγματοποιήσουν επιδεικτικές δράσεις της ευρυζωνικότητας στο πλαίσιο της πρόσκλησης 84 του προγράμματος της Κοινωνίας της Πληροφορίας.

Γενικά, τέτοιου είδους συστήματα χρησιμοποιούνται κυρίως για την προσβασιμότητα στο Διαδίκτυο, χωρίς εγγυήσεις όσον αφορά στο ρυθμό μετάδοσης δεδομένων (π.χ. 50 - 100kbrps ανά χρήστη). Ο συνολικός αριθμός των χρηστών ενός τέτοιου δικτύου, αν και μεγαλώνει σχετικά γρήγορα, είναι μικρός σε σχέση με το συνολικό πλήθος ατόμων που επισκέπτεται τις συγκεκριμένες περιοχές.

Τέτοιου είδους συστήματα που απευθύνονται στο ευρύ κοινό πρέπει να σχεδιάζονται χωρίς να θέτονται προϋποθέσεις για το είδος και την ποιότητα των συσκευών που θα χρησιμοποιήσουν οι χρήστες. Θα πρέπει δηλαδή να επιτρέπεται η σύνδεση μιας οποιασδήποτε συσκευής ασύρματης δικτυακής πρόσβασης και αυτό επιτυγχάνεται με την υιοθέτηση τεχνολογιών οι οποίες ακολουθούν πρότυπα είτε αυτά είναι θεσμοθετημένα είτε έχουν εδραιωθεί εκ των πραγμάτων. Τέτοια πρότυπα είναι τα 802.11a, 802.11b και 802.11g τα οποία υποστηρίζονται από το σύνολο σχεδόν των σύγχρονων φορητών υπολογιστών.

Τέτοιου είδους συστήματα χρειάζονται και κάποιου είδους έλεγχο της πρόσβασης σε αυτό. Συνήθως, ο έλεγχος αυτός δεν πραγματοποιείται στο ασύρματο τμήμα του δικτύου, αλλά μέσω ενός

εξυπηρετητή AAA (Authentication - Authorization - Accounting) στο υπόλοιπο τμήμα του δικτύου. Ένας τέτοιου είδους εξυπηρετητής ανακατευθύνει τη σύνδεση ενός νέου χρήστη σε μια σελίδα όπου ακολουθεί μια διαδικασία εγγραφής και αποδοχής ή όχι ενός συμφωνητικού για τη χρήση του συγκεκριμένου δικτύου. Οι συγκεκριμένες διαδικασίες ελέγχουν την προσβασιμότητα, παρέχουν πληροφορίες στους χρήστες και κρατάνε στατιστικά στοιχεία για τη χρήση του δικτύου.

Συνοψίζοντας, για ένα τυπικό δημόσιο ασύρματο δίκτυο ανοικτού χώρου, τα χαρακτηριστικά που θα πρέπει να ληφθούν υπόψη κατά το σχεδιασμό του είναι τα ακόλουθα:

- **Ελάχιστος Ρυθμός Μετάδοσης Χρηστών:** Της τάξης των 50-100Kbps ανά χρήστη. Ο μέγιστος ρυθμός μπορεί να φτάσει στο όριο της χρησιμοποιούμενης ασύρματης τεχνολογίας (π.χ. 802.11b, 802.11g) σε συνδυασμό με το μέγιστο ρυθμό παροχής της σύνδεσης με το Διαδίκτυο.
- **Πυκνότητα Χρηστών:** Μικρή, με δυνατότητα επέκτασης
- **Υπηρεσίες:** Πρόσβαση στο Διαδίκτυο, μέσω της οποίας παρέχονται όλες οι αντίστοιχες υπηρεσίες όπως: Παγκόσμιος Ιστός (www), Ηλεκτρονική Αλληλλογραφία (e-mail), Σύγχρονη Γραπτή Επικοινωνία (chat), Μεταφορά Αρχείων (ftp), κ.α.
- **Περιοχή:** Λόγω της έκτασης ενός τέτοιου δικτύου, υπάρχει απαίτηση για δυνατότητα περιοχής (roaming). Με αυτό τον τρόπο θα είναι εφικτό για κάθε χρήστη να μετακινείται μεταξύ των διαφορετικών σημείων πρόσβασης κρατώντας τα ίδια συνθηματικά και όνομα.
- **Ασφάλεια:** Συνήθως δεν παρέχεται ασφάλεια στο επίπεδο του ασύρματου δικτύου. Ο χρήστης προειδοποιείται για το συγκεκριμένο χαρακτηριστικό του δικτύου και του προτείνεται η λήψη κατάλληλων μέτρων (κυρίως η επίτευξη ασφάλειας με τη χρήση κατάλληλων εφαρμογών). Ασφάλεια μπορεί να επιτευχθεί μέσω της τεχνικής Μετάφρασης Διευθύνσεων (Network Address Translation), ενώ για την περαιτέρω προστασία των χρηστών προτείνεται η χρήση προσωπικού firewall από τους ίδιους.
- **Διαθεσιμότητα:** Παρέχεται συνήθως υψηλή διαθεσιμότητα όσον αφορά την καλυπτόμενη περιοχή (αλληλοεπικάλυψη με πολλαπλά hotspot) και όσον αφορά την προσβασιμότητα στο Διαδίκτυο με συνδεσιμότητα ανάνηψης από σφάλματα (fail-over) και κατανομής φορτίου (load-balancing).

Οι παραπάνω επιλογές ουσιαστικά περιορίζουν και αποκλείουν κάποιες υπηρεσίες και χαρακτηριστικά, όπως π.χ. αποδοτική μετάδοση ζωντανού video σε υψηλή ανάλυση λόγω σχετικά χαμηλού ρυθμού μετάδοσης, αποδοτική απομακρυσμένη εργασία μέσω δικτύου (NFS, κλπ.) λόγω ενδεχομένων διακοπών στη σύνδεση, μαζική λήψη μεγάλων αρχείων μέσω συστημάτων Peer-to-Peer λόγω σχετικά χαμηλού ρυθμού μετάδοσης, ασφαλή μετάδοση ευαίσθητων πληροφοριών (π.χ. ιατρικών) λόγω μη παροχής ασφάλειας στο επίπεδο του δικτύου, κλπ.

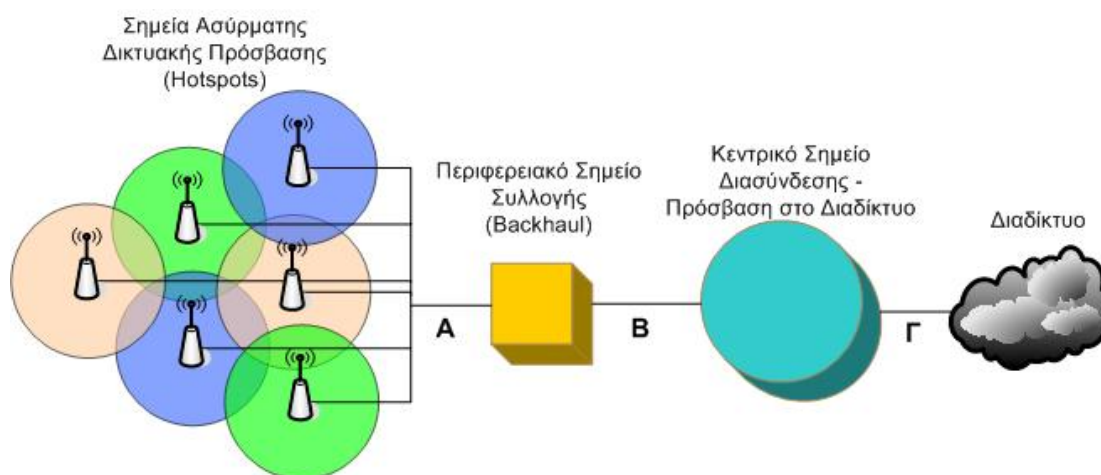
2.1 Περιγραφή Λειτουργίας ενός Δημόσιου Ασύρματου Δικτύου Ανοιχτού Χώρου

2.1.1 Από την πλευρά του χρήστη

Ο πελάτης-χρήστης, χρησιμοποιώντας μια ασύρματη δικτυακή συσκευή, συνδέεται σε κάποιο από τα εγκατεστημένα Σημεία Πρόσβασης (Access Points), χωρίς να γνωρίζει ή να τον ενδιαφέρει ποιο είναι αυτό. Όταν προσπαθήσει να προσπελάσει κάποια σελίδα του Παγκόσμιου Ιστού (www), η σύνδεσή του ανακατευθύνεται σε μια ειδική ιστοσελίδα-συμφωνητικό, η οποία τον ενημερώνει για τους όρους χρήσης του δικτύου, τη μη ύπαρξη ασφάλειας στο επίπεδο του δικτύου και την προτροπή για χρήση εφαρμογών ασφαλούς μετάδοσης πληροφορίας (όπως τα πρωτόκολλα HTTPS, SIMAP, SPOR, κλπ). Ο χρήστης πρέπει να αποδεχθεί το συμφωνητικό χρήσης και να παρέχει έναν ειδικό κωδικό πρόσβασης ώστε να μπορέσει να αποκτήσει πρόσβαση στο δίκτυο. Αν ο κωδικός είναι σωστός, στη συνέχεια μπορεί να κάνει χρήση των υπηρεσιών του ασύρματου δικτύου.

2.1.2 Δίκτυο Δεδομένων

Ο πελάτης-χρήστης αφού έχει συνδεθεί στο Ασύρματο Δίκτυο μπορεί πλέον να χρησιμοποιεί τις υπηρεσίες του. Τα δεδομένα (πακέτα πληροφορίας) μεταφέρονται από την ασύρματη δικτυακή συσκευή στο Σημείο Ασύρματης Πρόσβασης. Το πρωτόκολλο στο επίπεδο δικτύου είναι το IEEE 802.11b ή 802.11g. Τα Σημεία Ασύρματης Πρόσβασης ομαδοποιούνται σύμφωνα με την μεταξύ τους απόσταση και οι ομάδες που σχηματίζονται αποτελούν σύνολα από κοντινά μεταξύ τους Σημεία Πρόσβασης. Τα δεδομένα από τα πακέτα των δικτυακών συνδέσεων μιας ομάδας συγκεντρώνονται σε περιφερειακά σημεία συλλογής και από τα συγκεκριμένα σημεία συλλογής τα δικτυακά πακέτα προωθούνται προς και από ένα κεντρικό σημείο. Στο κεντρικό σημείο υπάρχει μια ευρυζωνική σύνδεση με το Διαδίκτυο, μέσω της οποίας τα πακέτα προωθούνται προς και από το Διαδίκτυο. Όλα αυτά απεικονίζονται σχηματικά στην Εικόνα 1.



Εικόνα 1: Διαδρομή Δεδομένων

Χαρακτηριστικά ενός συγκεκριμένου τρόπου υλοποίησης είναι το είδος των συνδέσεων Α, Β και Γ. Η σύνδεση Γ είναι συνήθως ενσύρματη, μιας και η ευρυζωνική πρόσβαση στο Διαδίκτυο πρόκειται συνήθως για μία ή περισσότερες γραμμές ADSL. Η σύνδεση Β για ανοιχτού χώρου δίκτυα είναι συνήθως ασύρματη, ενώ η διασύνδεση των σημείων ασύρματης πρόσβασης γίνεται ενσύρματα. Η συνηθέστερη μορφή ανάπτυξης ενός τέτοιου δικτύου γίνεται με ενσύρματη δικτύωση τύπου Ethernet (IEEE 802.3) για την διασύνδεση των σημείων ασύρματης πρόσβασης με το Περιφερειακό Σημείο Συλλογής, ασύρματη σύνδεση (IEEE 802.11b ή IEEE 802.11g) του Περιφερειακού Σημείου Συλλογής με το Κεντρικό Σημείο Διασύνδεσης και ενσύρματα η Διαδικτυακή Πρόσβαση (ADSL).

Αυτή είναι η συνηθέστερη μέθοδος υλοποίησης ενός Δημόσιου Ασύρματου Δικτύου Ανοιχτού Χώρου. Ωστόσο, υπάρχουν και λιγότερο δημοφιλείς τρόποι. Για παράδειγμα, σε κάθε περιφερειακό σημείο συλλογής θα μπορούσε να υπάρχει ευρυζωνική πρόσβαση στο Διαδίκτυο και τα δικτυακά πακέτα να προωθούνται απευθείας στο Διαδίκτυο, χωρίς να απαιτείται η κεντρική συλλογή τους σε ένα σημείο ευρυζωνικής Διαδικτυακής πρόσβασης. Δηλ. στην Εικόνα 1 να λείπει το Κεντρικό Σημείο Διασύνδεσης και όλη η λειτουργικότητα του να παρέχεται από το Περιφερειακό Σημείο Συλλογής. Η συγκεκριμένη λύση αυξάνει το συνολικό κόστος, μιας και θα απαιτούνταν αρκετές ευρυζωνικές γραμμές πρόσβασης στο Διαδίκτυο καθώς και ειδικοί εξυπηρετητές σε κάθε τέτοιο περιφερειακό σημείο. Επίσης, θα ήταν δυνατή η ενσύρματη διασύνδεση των Περιφερειακών Σημείων Συλλογής με το Κεντρικό Σημείο Συλλογής, αλλά αυτή η λύση εξαρτάται από το είδος της συγκεκριμένης περιοχής (κτίρια, πλατεία, κλπ.), την έκτασή της (οι κόμβοι σε ένα δίκτυο Ethernet πρέπει να απέχουν το πολύ 100μ, ειδάλλως απαιτούνται ειδικές συσκευές, repeater), κλπ.

2.2 Διευθυνσιοδότηση

Η κύρια υπηρεσία που παρέχεται μέσω του ασύρματου δικτύου είναι η πρόσβαση στο Διαδίκτυο. Το Διαδίκτυο είναι βασισμένο στη στοίβα πρωτοκόλλων TCP/IP. Βασική προϋπόθεση για να συνδεθεί ένα υπολογιστής στο Διαδίκτυο είναι να έχει μία διεύθυνση IP. Επειδή είναι τεχνικά αδύνατο με βάση τη σημερινή δομή (4 bytes) των IP διευθύνσεων κάθε συσκευή που συνδέεται στο δίκτυο να έχει τη δική της διεύθυνση IP, υιοθετείται η τεχνική Network Address Translation (NAT) μέσω της οποίας οι διευθύνσεις IP του ασύρματου δικτύου είναι εσωτερικές/ιδιωτικές, ενώ όλες οι συσκευές προσπελαίνουν το Διαδίκτυο μέσω μιας ή περισσότερων εξωτερικών διευθύνσεων IP. Εξαιτίας των χαρακτηριστικών της σύνδεσης μέσω NAT, παρέχεται σχετική προστασία στους χρήστες από δικτυακές επιθέσεις.

Για να λάβει κάθε ασύρματη συσκευή των χρηστών τη δική της εσωτερική διεύθυνση IP, υιοθετείται το πρωτόκολλο Dynamic Host Configuration Protocol (DHCP). Η λειτουργία απόδοσης της διεύθυνσης IP γίνεται κατά την σύνδεση της ασύρματης συσκευής στο ασύρματο δίκτυο. Το σύνολο των συσκευών που κυκλοφορούν σήμερα στο εμπόριο υποστηρίζουν το συγκεκριμένο πρωτόκολλο. Κατά τη διάρκεια της σύνδεσης της συσκευής στο ασύρματο δίκτυο, η συσκευή στέλνει ειδικά πακέτα, μέσω των οποίων ρωτάει να μάθει ποια είναι η δική της διεύθυνση IP. Ο εξυπηρετητής DHCP απαντάει στη συγκεκριμένη συσκευή με μια διεύθυνση IP από ένα κατάλογο διαθέσιμων διευθύνσεων καθώς και με ότι άλλο είναι απαραίτητο για τη σύνδεση της συσκευής στο δίκτυο (DNS server, Default Gateway κ.λπ.). Επειδή οι συγκεκριμένες διευθύνσεις είναι εσωτερικές/ιδιωτικές και ανήκουν ουσιαστικά μόνο στο ασύρματο δίκτυο πρόσβασης στη συγκεκριμένη περιοχή, ο εξυπηρετητής μπορεί να παρέχει τις κατάλληλες πληροφορίες σε ένα πολύ μεγάλο πλήθος συσκευών.

2.3 Captive Portal

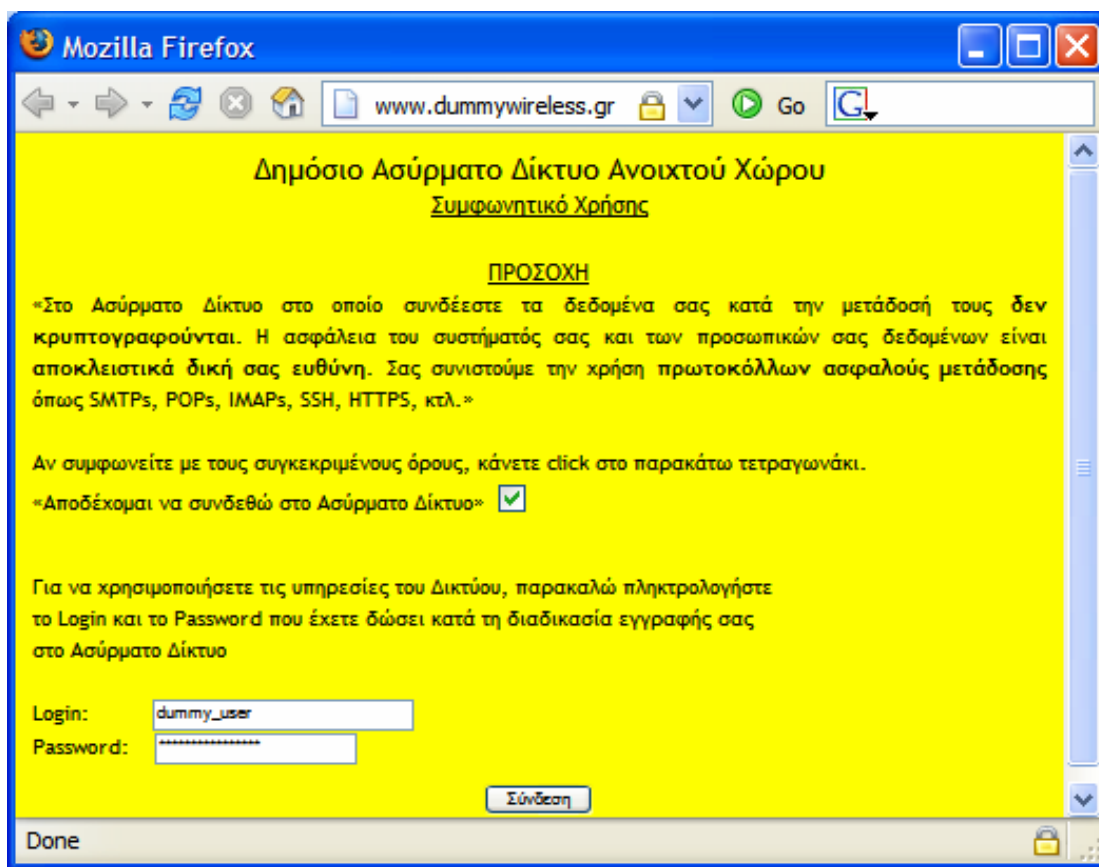
Για να γίνει η σύνδεση ενός χρήστη στο ασύρματο δίκτυο, θα πρέπει ο χρήστης να απαντήσει θετικά σε ένα συμφωνητικό χρήσης του δικτύου. Ανάλογα με τον σκοπό και το είδος του δικτύου, κάθε φορέας λειτουργίας μπορεί να έχει το δικό του συμφωνητικό. Πέρα από τις ιδιαίτερες απαιτήσεις που μπορεί να έχει κάθε φορέας λειτουργίας, υπάρχουν κάποιες ενέργειες οι οποίες καλό είναι να υιοθετούνται από όλες τις ασύρματες δικτυακές εγκαταστάσεις.

Συγκεκριμένα, στο χρήστη πρέπει να καταστεί σαφές ότι το ασύρματο δίκτυο δεν διαθέτει χαρακτηριστικά ασφάλειας στο επίπεδο του δικτύου. Οι περισσότεροι χρήστες δεν λαμβάνουν

υπόψη τους τον παράγοντα της ασφάλειας στις ηλεκτρονικές τους επικοινωνίες. Στις περισσότερες περιπτώσεις είναι δύσκολο να παραβιαστεί η ιδιωτικότητα των ηλεκτρονικών συνδιαλέξεων μιας και αυτές πραγματοποιούνται με ενσύρματα μέσα. Στην περίπτωση όμως του ασύρματου δικτύου οι πληροφορίες διαδίδονται μέσω από ραδιοσυχνότητες οι οποίες είναι προσβάσιμες σε όλους (όπως όλοι μπορούν και ακούνε τον ίδιο σταθμό στα ραδιόφωνο). Συνεπώς είναι αναγκαίο να γνωστοποιηθεί από την αρχή στους χρήστες ότι για το θέμα της ασφάλειας πρέπει να μεριμνήσουν οι ίδιοι χρησιμοποιώντας ασφαλείς εφαρμογές και πρωτόκολλα.

Επίσης της χρήσης των υπηρεσιών που παρέχει το ασύρματο δίκτυο θα πρέπει να προηγείται μια διαδικασία πιστοποίησης. Ο λόγος ύπαρξης της διαδικασίας πιστοποίησης είναι η καλύτερη και ευκολότερη διαχείριση του δικτύου, ο έλεγχος της προσβασιμότητας και η δημιουργία στατιστικών. Η πιστοποίηση πραγματοποιείται μέσω της παροχής από πλευράς του χρήστη ενός ονόματος και ενός κωδικού.

Η πιστοποίηση και η παρουσίαση των πληροφοριών για την ασφάλεια των επικοινωνιών λαμβάνουν χώρα κατά τη σύνδεση του χρήστη στο ασύρματο δίκτυο ως εξής: Όταν ο χρήστης προσπαθήσει να προσπελάσει μια οποιαδήποτε σελίδα του Παγκόσμιου Ιστού (www) τότε η αίτησή του ανακατευθύνεται σε μια ειδική ιστοσελίδα (Captive Portal). Η συγκεκριμένη σελίδα (βλ. Εικόνα 2) περιέχει τις παραπάνω πληροφορίες και ζητάει από την χρήστη να τις διαβάσει και να απαντήσει θετικά. Αν ο χρήστης δεν δώσει σωστά στοιχεία ή δεν συμφωνήσει με το συμφωνητικό τότε δεν του παρέχεται πρόσβαση στις υπηρεσίες. Στην περίπτωση θετικής απάντησης ο εξυπηρετητής Captive Portal επικοινωνεί με το Firewall του ασύρματου δικτύου και του μεταφέρει την πληροφορία ότι ο συγκεκριμένος χρήστης μπορεί να χρησιμοποιεί τις υπηρεσίες που παρέχονται από το ασύρματο δίκτυο.



Εικόνα 2: Παράδειγμα ενός Captive Portal

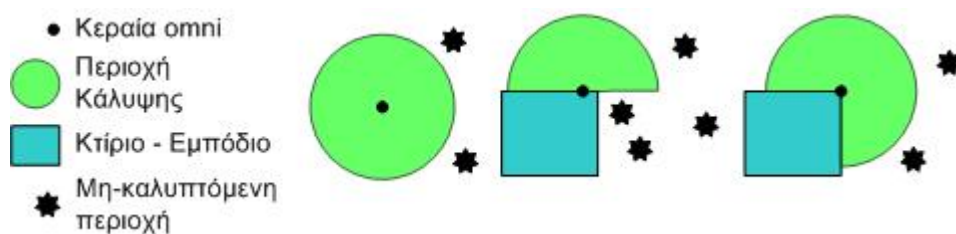
Η ύπαρξη των συγκεκριμένων ενεργειών γίνονται επ' ωφελεία των χρηστών και σε καμία περίπτωση δεν μειώνουν την προσβασιμότητα στο δίκτυο. Η μικρή ενόχληση που ενδεχομένως να προκαλούν είναι απολύτως αναγκαία για τη σωστή λειτουργία και διαχείριση του δικτύου, καθώς και για την προστασία και ενημέρωση των χρηστών. Στην περίπτωση ενός Δημόσιου Ασύρματου Δικτύου, η εγγραφή για τη λήψη κωδικού πρόσβασης θα είναι δωρεάν και θα μπορεί να γίνει από το Διαδίκτυο, καθώς και κατά τη διάρκεια επιδεικτικών δράσεων προώθησης του έργου.

2.4 Περιοχή Κάλυψης Ασύρματου Δικτύου Wi-Fi

Προκειμένου να επιτύχει ένα έργο παροχής ασύρματων δικτυακών υπηρεσιών, θα πρέπει η καλυπτόμενη από το ασύρματο δίκτυο περιοχή να είναι όσο το δυνατόν μεγαλύτερη και με όσο το δυνατόν καλύτερη κάλυψη σε κάθε σημείο. Επίσης, είναι προφανές ότι οι καλυπτόμενες περιοχές θα πρέπει να είναι πολυσύχναστες, έτσι ώστε οι παρεχόμενες υπηρεσίες να είναι διαθέσιμες σε γίνεται περισσότερο κόσμο.

Για να επιτευχθεί τέτοιου είδους κάλυψη, πρέπει να τοποθετηθεί ικανός αριθμός από hotspot, ένα ανά υπο-περιοχή του συνολικού χώρου κάλυψης. Όμως τα σημεία στα οποία μπορεί να τοποθετηθεί ο δικτυακός εξοπλισμός ασύρματης πρόσβασης ενδεχομένως να είναι περιορισμένα τόσο στον αριθμό όσο και στην διασπορά τους στην δεδομένη περιοχή κάλυψης. Συνεπώς πρέπει να επιτευχθεί η μέγιστη δυνατή κάλυψη τοποθετώντας hotspot μόνο στα συγκεκριμένα επιτρεπόμενα σημεία.

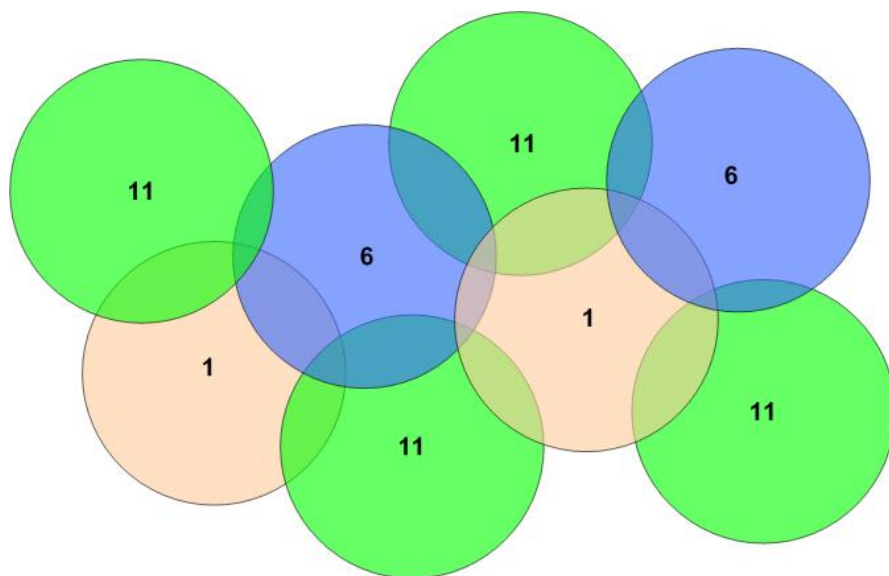
Οι κεραίες που χρησιμοποιούνται στο κομμάτι της ασύρματης πρόσβασης των χρηστών είναι πολυκατευθυντικές (οmni) και εκπέμπουν σε 360° στο οριζόντιο επίπεδο. Παρατηρώντας από πάνω, η κάλυψη που επιτυγχάνεται φαίνεται στην Εικόνα 3.



Εικόνα 3: Περιοχή κάλυψης κεραίας τύπου omni.

2.4.1 Επικάλυψη Καναλιών

Τα κανάλια (συνολικά 11 στις Η.Π.Α. και 13 στην Ε.Ε.) στα οποία λειτουργεί το πρωτόκολλο 802.11b, παρουσιάζουν επικαλύψεις μεταξύ τους. Δηλ. ενώ η κεντρική συχνότητα κάθε καναλιού απέχει από αυτή του διπλανού καναλιού 5MHz, το εύρος κάθε καναλιού είναι 22MHz, παρουσιάζοντας επικάλυψη εύρους 17MHz. Προκειμένου να αποφευχθεί το φαινόμενο των παρεμβολών λόγω της συγκεκριμένης επικάλυψης, ακολουθείται η πολιτική χρήσης μόνο των καναλιών 1, 6 και 11, τα οποία δεν παρουσιάζουν καμία επικάλυψη συχνοτήτων. Με την χρήση αυτών των καναλιών δημιουργείται μια περιοχή κάλυψης της μορφής που φαίνεται στην Εικόνα 4.



Εικόνα 4: Επαναχρησιμοποίηση Καναλιών 802.11 2.4GHz

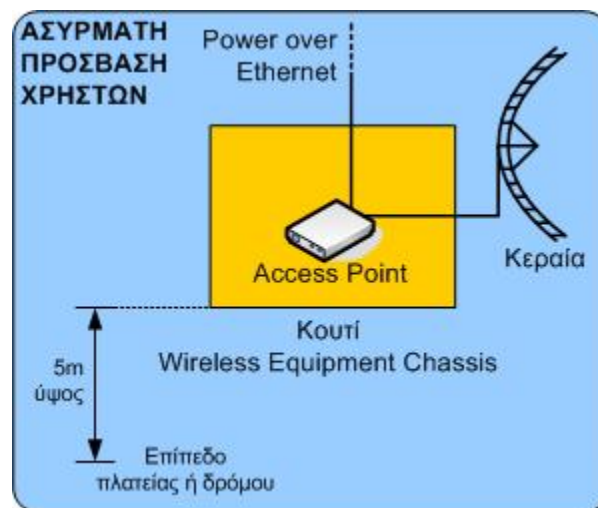
Τα κανάλια 12 και 13, αν και προβλέπονται από τον ευρωπαϊκό οργανισμό ETSI, καλό είναι να μην χρησιμοποιούνται για την πρόσβαση των χρηστών προκειμένου να διατηρηθεί η συμβατότητα με τα προϊόντα που είναι κατασκευασμένα από εταιρίες των Η.Π.Α. και δεν λειτουργούν στα κανάλια 12 και 13. Σε κάθε περίπτωση, με τη συγκεκριμένη επιλογή δεν έχουμε αύξηση παρεμβολών, αφού με την επαναχρησιμοποίηση των συγκεκριμένων καναλιών και μόνο επιτυγχάνεται κάλυψη μιας περιοχής με οποιοδήποτε μέγεθος. Τα κανάλια 12 και 13 μπορούν να χρησιμοποιηθούν σε άλλες περιπτώσεις επικοινωνίας στις οποίες δεν συμμετέχουν οι τελικοί χρήστες, όπως για παράδειγμα, στη διασύνδεση επιμέρους συστημάτων του ασύρματου δικτύου.

2.5 Αρχιτεκτονική ενός Δημόσιου Ασύρματου Δικτύου Ανοικτού Χώρου

Το Δημόσιο Ασύρματο Δίκτυο Ανοικτού Χώρου σχεδιάζεται ως ένα ολοκληρωμένο πληροφοριακό σύστημα, το οποίο προσφέρει ασύρματη πρόσβαση στο Διαδίκτυο. Το συνολικό σύστημα χωρίζεται σε επιμέρους υποσυστήματα, καθένα από τα οποία εξυπηρετεί κάποια ξεχωριστή λειτουργία που είναι απαραίτητη για την ολοκλήρωση των υπηρεσιών που παρέχονται στους τελικούς χρήστες. Η μεταφορά των δεδομένων από τα Σημεία Ασύρματης Πρόσβασης Χρηστών στα Περιφερειακά Σημεία Συλλογής γίνεται ενσύρματα (Ethernet), ενώ από τα Περιφερειακά Σημεία Συλλογής προς το Κεντρικό Σημείο Διασύνδεσης ασύρματα (IEEE 802.11b).

2.5.1 Υποσύστημα Ασύρματης Πρόσβασης Χρηστών

Η παροχή τελικών ασύρματων δικτυακών υπηρεσιών προς το χρήστη επιτυγχάνεται με τη χρήση των Hotspot. Κάθε Hotspot, αποτελείται ουσιαστικά από μία συσκευή Access Point, ένα κουτί (wireless equipment chassis) μέσα στο οποίο τοποθετείται το Access Point και μία κεραία (βλ. Εικόνα 5). Σκοπός των κουτιών είναι η προστασία των Access Point από τις καιρικές συνθήκες, αλλά και η κατάλληλη εμφάνιση προκειμένου να μην έρχονται σε αντίθεση με τη αισθητική του χώρου εγκατάστασης. Η κατάλληλη εμφάνιση μπορεί να επιτευχθεί με κατάλληλη διακόσμηση ή χρωματισμό.



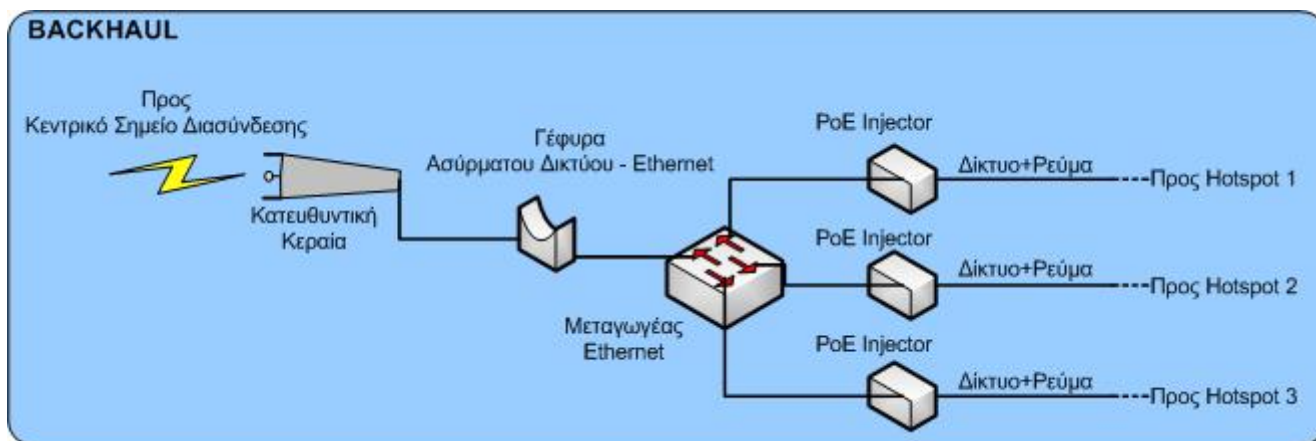
Εικόνα 5: Wireless Hotspot

Τα κουτιά που θα φιλοξενούν τα Hotspot εγκαθίστανται σε ύψος το πολύ 5 μέτρων από το επίπεδο των χρηστών στο συγκεκριμένο σημείο. Σε κάθε κουτί καταλήγει ένα καλώδιο δικτύου (cat. 5e). Μέσα από το καλώδιο αυτό θα μεταφέρονται και τα δικτυακά δεδομένα, αλλά και η απαραίτητη ισχύς για την λειτουργία του hotspot. Η τεχνολογία που επιτρέπει την μεταφορά ηλεκτρικής ισχύς μέσα από τυπικά καλώδια δικτύου ονομάζεται Power Over Ethernet (PoE) και είναι ιδιαίτερα διαδεδομένη σε τέτοιου είδους εφαρμογές. Το καλώδιο αυτό ξεκινά από το σημείο όπου έχει εγκατασταθεί ένα Περιφερειακό Σημείο Συλλογής (Υποσύστημα Backhaul).

Η λειτουργία που επιτελεί κάθε ένα από τα ασύρματα hotspot είναι να συλλέγει την ασύρματη κίνηση που βρίσκεται στην ακτίνα κάλυψής του, να την μετατρέπει σε ενσύρματη κίνηση τύπου Ethernet και να την προωθεί προς το Υποσύστημα Backhaul.

2.5.2 Υποσύστημα Backhaul

Το Υποσύστημα Backhaul (βλ. Εικόνα 6) περιλαμβάνει μία ασύρματη γέφυρα (wireless bridge), μια κατευθυντική κεραία, ένα μικρό μεταγωγέα (switch) και συσκευές power-over-ethernet injectors. Η ασύρματη γέφυρα είναι μια δικτυακή συσκευή η οποία ενσωματώνει το κατάλληλο λογισμικό για την υλοποίηση ασύρματων πρωτοκόλλων, προκειμένου να ενώσει το τοπικό δίκτυο που δημιουργείται από τα Hotspot με το κεντρικό δίκτυο. Ο μεταγωγέας χρησιμεύει για την διασύνδεση των δικτύων των Hotspot, ενώ οι συσκευές power-over-ethernet injectors αναλαμβάνουν να πολυπλέξουν το σήμα του δικτύου και την παροχή ρεύματος για κάθε Hotspot σε ένα μόνο καλώδιο (cat 5e).



Εικόνα 6: Υποσύστημα Backhaul

Το Υποσύστημα Backhaul είναι τοποθετημένο σε σχετικά μεγάλο ύψος (π.χ. στην ταράτσα ενός κτιρίου) όσο το δυνατόν πιο κοντά σε μία ομάδα Σημείων Ασύρματης Πρόσβασης (hotspot). Χρησιμοποιώντας την κατευθυντική κεραία, το Υποσύστημα Backhaul συνδέεται με το Υποσύστημα Κεντρικού Σημείου Διασύνδεσης.

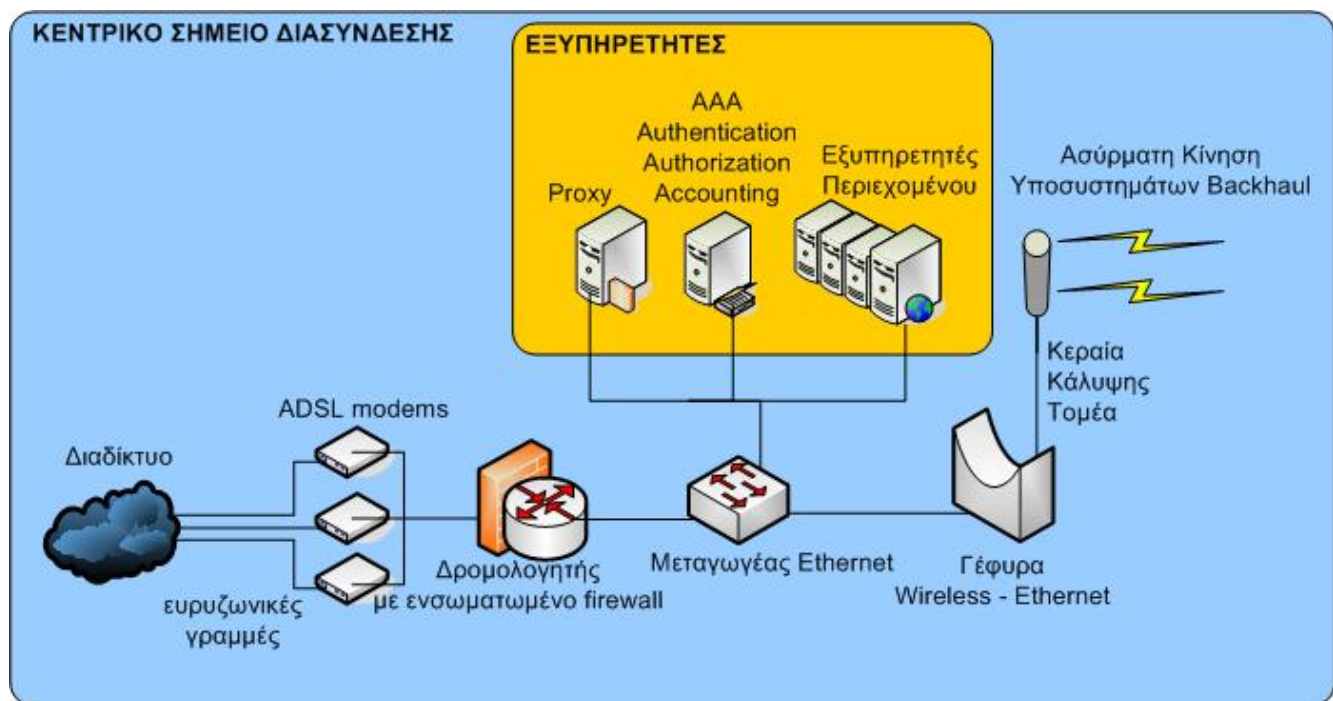
Η λειτουργία που επιτελεί κάθε ένα από τα υποσυστήματα Backhaul είναι να συλλέγει τη κίνηση από το επιμέρους hotspot που είναι τοποθετημένα στο επίπεδο των χρηστών (π.χ. επίπεδο κάποιας πλατείας), να την μετατρέπουν σε ασύρματη μορφή τύπου 802.11b και να την προωθούν προς το Κεντρικό Σημείο Διασύνδεσης.

Για να μην υπάρχουν παρεμβολές ανάμεσα στις συχνότητες των Σημείων Ασύρματης Πρόσβασης με τις συχνότητες επικοινωνίας των συστημάτων Backhaul με το Κεντρικό Σημείο Διασύνδεσης, καλό είναι να χρησιμοποιηθεί το κανάλι 13. Λαμβάνοντας υπόψη ότι τα κανάλια που έχουν χρησιμοποιηθεί για τα Σημεία Ασύρματης Πρόσβασης είναι τα 1, 6 και 11, η χρήση του καναλιού 13 είναι η καλύτερη επιλογή. Στην περίπτωση που παρατηρηθούν παρεμβολές από τη χρήση των

συγκεκριμένων καναλιών, μπορεί να γίνει χρήση διαφορετικών καναλιών για την κάθε περίπτωση. Συγκεκριμένα μπορούν να χρησιμοποιηθούν τα κανάλια 1, 5 και 9 για τα Σημεία Ασύρματης Πρόσβασης και το 13 για την επικοινωνία των συστημάτων Backhaul με το Κεντρικό Σημείο Διασύνδεσης.

2.5.3 Υποσύστημα Κεντρικού Σημείου Διασύνδεσης

Το Κεντρικό Σημείο Διασύνδεσης (βλ. Εικόνα 7) είναι το υποσύστημα που συνδέει όλη την δικτυακή υποδομή με το δίκτυο κορμού (Διαδίκτυο). Εκεί γίνεται η εγκατάσταση των ευρυζωνικών γραμμών πρόσβασης στο Διαδίκτυο (ευρυζωνικές υπηρεσίες σταθερής πρόσβασης μεσαίας ταχύτητας - xDSL). Επίσης, εκεί εγκαθίστανται ένας κεντρικός εξυπηρετητής, που αναλαμβάνει να ενοποιεί τις ευρυζωνικές γραμμές σε μία εικονική πύλη στο Διαδίκτυο - Internet gateway, ο εξυπηρετητής AAA που αναλαμβάνει την πιστοποίηση της ταυτότητας των χρηστών του δικτύου, οι εξυπηρετητές περιεχομένου που φιλοξενούν διάφορες ηλεκτρονικές υπηρεσίες για τους χρήστες και ο κεντρικός μεταγωγέας.



Εικόνα 7: Κεντρικό Σημείο Διασύνδεσης

Ο παραπάνω εξοπλισμός συνδέεται σε κάποιο σημείο σε μεγάλο ύψος (π.χ. τάρτσα κτιρίου) όπου εγκαθίσταται και η κεντρική ασύρματη γέφυρα, η οποία μέσω μιας κεραίας κάλυψης τομέα (sector antenna) θα επικοινωνεί με τις αντίστοιχες γέφυρες στις οροφές των διάφορων περιφερειακών

κτιρίων (point-to-multipoint communication). Λόγω των κατευθυντικών κεραιών που χρησιμοποιούν τα Υποσυστήματα Backhaul, η επικοινωνία με την κεντρική Κεραία Κάλυψης Τομέα πραγματοποιείται χωρίς ιδιαίτερες παρεμβολές.

2.5.3.1 Γραμμές Ευρυζωνικής Πρόσβασης

Ο κεντρικός εξυπηρετητής διαμοιράζει τον φόρτο των εξερχόμενων πακέτων δικτύου στις ευρυζωνικές γραμμές - τύπου ADSL, μέσω των αντίστοιχων, ανεξάρτητων συνδέσεων που θα έχει με κάθε μια από τις συσκευές ADSL modem/router (modem/δρομολογητές ADSL). Σε κάθε μια από τις συσκευές αυτές θα καταλήγει και από μία γραμμή ευρυζωνικής πρόσβασης.

2.5.3.2 Λογισμικό Εξυπηρετητών

Εκτός από τη ρύθμιση των ασύρματων συσκευών, ώστε αυτές να λειτουργούν όπως περιγράφεται παραπάνω, θα πρέπει να γίνει εγκατάσταση και ρύθμιση του λογισμικού των εξυπηρετητών του Κ.Σ.Δ. Συνοπτικά σε κάθε έναν από τους εξυπηρετητές θα πρέπει εκτός από το λειτουργικό σύστημα, να είναι εγκατεστημένες και να λειτουργούν απρόσκοπτα οι παρακάτω εφαρμογές:

2.5.3.2.1 Λογισμικό Κεντρικού Εξυπηρετητή

Εφαρμογή διαμοιρασμού του φόρτου εξερχόμενης κίνησης στους τρεις από τους προσαρμογείς δικτύου που θα είναι συνδεδεμένοι οι ADSL modem/δρομολογητές (load-balancing). Σε περίπτωση που οποιαδήποτε γραμμή σταματήσει να λειτουργεί για οποιαδήποτε λόγο, θα πρέπει ο εξυπηρετητής να την παρακάμπτει και να χρησιμοποιεί όσες λειτουργούν (fail-over).

2.5.3.2.2 Λογισμικό Εξυπηρετητή AAA

Εφαρμογή ελέγχου της ταυτότητας των χρηστών μέσω ζευγαριών ονόματος και κωδικού πρόσβασης (username/password pair). Η εφαρμογή αυτή θα πρέπει να επικοινωνεί με κάποιου είδους τοπικό Firewall σε επίπεδο λογισμικού, το οποίο δεν θα επιτρέπει στους μη διαπιστευμένους χρήστες να χρησιμοποιούν το ασύρματο δίκτυο για να προσπελαίνουν το Διαδίκτυο (captive portal). Επίσης, θα πρέπει η εφαρμογή να αποθηκεύει όλες τις πληροφορίες των χρηστών σε κάποιο τρίτο ανεξάρτητο σύστημα, όπως για παράδειγμα μια σχεσιακή βάση δεδομένων ή έναν εξυπηρετητή LDAP.

2.5.3.2.3 Λογισμικό Εξυπηρετητών Περιεχομένου

Πρόκειται για λογισμικό τύπου Εξυπηρετητή Ιστοσελίδων (web server) καθώς και λογισμικό προσωρινής αποθήκευσης ιστοσελίδων (web proxy). Οι Εξυπηρετητές ιστοσελίδων περιέχουν το σύνολο των ιστοσελίδων που είναι αναγκαίες για την παροχή των υπηρεσιών στους χρήστες. Ανάλογα με το είδος του περιεχομένου (δυναμικό, στατικό, κλπ.) ενδέχεται να είναι απαραίτητοι και Εξυπηρετητές Εφαρμογών (Application server) ή/και Εξυπηρετητής Βάσης Δεδομένων (Database Server) προκειμένου να υλοποιηθούν οι διάφορες δικτυακές υπηρεσίες. Θεωρούμε ότι ένα σύνολο τεσσάρων εξυπηρετητών περιεχομένου καλύπτει το σύνολο των υπηρεσιών που θα ήταν χρήσιμες για ένα περιβάλλον δημόσιας ασύρματης δικτυακής πρόσβασης.

2.5.3.2.4 Λογισμικό Ανοιχτού Κώδικα

Όσον αφορά στο είδος του λογισμικού που θα χρησιμοποιηθεί, προτείνεται η χρήση Ελεύθερου Λογισμικού / Λογισμικού Ανοιχτού Κώδικα (ΕΛ/ΛΑΚ) καθώς οι λύσεις αυτές αποτελούν παγκόσμια το εκ των πραγμάτων πρότυπο για αντίστοιχες εγκαταστάσεις. Στο Διαδίκτυο υπάρχει διαθέσιμο λογισμικό ικανό να παρέχει όλες τις υπηρεσίες που χρειάζεται ένα τέτοιο δίκτυο. Προφανώς, απαιτείται η κατάλληλη παραμετροποίηση, εγκατάσταση και ρύθμιση προκειμένου το λογισμικό να καταστεί λειτουργικό για ένα συγκεκριμένο περιβάλλον ασύρματου δικτύου.

2.6 Λειτουργικές Απαιτήσεις

Το δίκτυο θα πρέπει να είναι πλήρως συμβατό με το πρότυπο WiFi (IEEE 802.11b). Οι ασύρματες συνδέσεις και οι ασύρματες γέφυρες στις οροφές των κτιρίων θα πρέπει να λειτουργούν σύμφωνα με το πρότυπο αυτό. Τα Wireless Hotspot θα πρέπει να απαγορεύουν συνδέσεις στο πρότυπο IEEE 802.11g, και να ενημερώνουν τις συσκευές πελάτη να χρησιμοποιήσουν το πρότυπο IEEE 802.11b (όλες οι συσκευές που είναι συμβατές με το πρότυπο IEEE 802.11g έχουν τη δυνατότητα επικοινωνίας και με το πρότυπο IEEE 802.11b). Όλος ο ασύρματος τηλεπικοινωνιακός εξοπλισμός θα πρέπει να είναι συμβατός με το πρότυπο IEEE 802.11g, ώστε να είναι δυνατή η μελλοντική επέκταση της χωρητικότητας του δικτύου χωρίς την ανάγκη προμήθειας επιπλέον εξοπλισμού ή λογισμικού. (Αρχικά προτιμάται το πρότυπο IEEE 802.11b επειδή έχει μεγαλύτερη εμβέλεια λειτουργίας και προκαλεί λιγότερες παρεμβολές στα γειτονικά κανάλια του).

2.7 Πολιτική Ασφάλειας

Στο υπο δημιουργία δίκτυο δεν θα υποστηρίζονται ασφαλείς συνδέσεις στο επίπεδο του ασύρματου δικτύου. Τα συστήματα που υλοποιούν πραγματική ασφάλεια σε ασύρματα δίκτυα, έχουν υψηλό

κόστος και απαιτούν αντίστοιχη υποστήριξη και από τις συσκευές των χρηστών. Από την άλλη, ο χρήστης μπορεί εύκολα να χρησιμοποιεί τεχνικές κρυπτογραφίας και κωδικοποίησης δεδομένων στο επίπεδο των εφαρμογών (π.χ. συνδέσεις με secure sockets, εξυπηρετητές που υποστηρίζουν HTTPS, SFTP αντί για FTP, κ.λπ.) καθώς το σύνολο των τερματικών συσκευών υποστηρίζει πλέον αντίστοιχες τεχνικές. Οι χρήστες θα ενημερώνονται για αυτό με την είσοδό τους στο δίκτυο, μέσω ειδικής ιστοσελίδας που θα τους παρουσιάζει ένα συμφωνητικό χρήσης του δικτύου και μια προειδοποίηση ότι το ίδιο το δίκτυο δεν είναι ασφαλές (welcome screen από το σύστημα captive portal).

Για παράδειγμα, η σχετική προειδοποίηση μπορεί να αναφέρει:

"Στο Ασύρματο Δίκτυο στο οποίο θα συνδεθείτε δεν κρυπτογραφούνται τα δεδομένα σας κατά την μετάδοσή τους. Η ασφάλεια του συστήματός σας και των προσωπικών σας δεδομένων είναι αποκλειστικά δική σας ευθύνη. Σας συνιστούμε την χρήση πρωτοκόλλων ασφαλούς μετάδοσης όπως SMTPs, POPs, IMAPs, SSH, HTTPS, κτλ."

2.8 Υψηλή Διαθεσιμότητα

Για τις ανάγκες ενός Δημόσιου Ασύρματου Δικτύου Ανοιχτού Χώρου, υψηλή διαθεσιμότητα παρέχεται σε 3 διακριτά σημεία του συνολικού συστήματος:

- Ασύρματη Πρόσβαση Χρηστών
- Πρόσβαση στο Διαδίκτυο
- Σύστημα Εξυπηρετητών

Υψηλή διαθεσιμότητα παρέχεται στο κομμάτι της ασύρματης πρόσβασης χρηστών μέσω της ύπαρξης πολλαπλών hotspot. Στην περίπτωση που κάποιο hotspot παρουσιάσει βλάβη, τότε ο χρήστης συνεχίζει να εξυπηρετείται από κάποιο άλλο hotspot. Αν εκείνη η περιοχή δεν καλύπτεται από δεύτερο hotspot, τότε ο χρήστης θα πρέπει να μετακινηθεί σε κάποιο άλλο σημείο της περιοχής όπου συνεχίζει να υπάρχει ασύρματη δικτυακή κάλυψη.

Στο κομμάτι που αφορά στην σύνδεση με το Διαδίκτυο πρέπει να έχει προβλεφθεί η ύπαρξη διαφορετικών ευρυζωνικών γραμμών xDSL. Αν κάποια από τις γραμμές αστοχήσει, τότε η συνολική

κίνηση δρομολογείται μέσω των υπολοίπων γραμμών, επιτυγχάνοντας έτσι την συνέχιση της παροχής υπηρεσιών, έστω και με μικρότερο συνολικό ρυθμό μετάδοσης.

Οι κεντρικοί εξυπηρετητές, βρίσκονται μέσα σε ειδικά διαμορφωμένα χώρο και υποστηρίζονται από μηχανήμα αδιάλειπτης παροχής ηλεκτρικού ρεύματος (UPS). Με τον τρόπο αυτό εξασφαλίζεται ότι δεν θα πάψουν να λειτουργούν εξαιτίας σύντομων διακοπών ρεύματος. Σε περίπτωση διακοπής ρεύματος μεγάλης διάρκειας, δεν προβλέπεται η συνέχιση της παροχής υπηρεσιών. Ο εξοπλισμός των εξυπηρετητών προστατεύεται μέσω της ομαλής τους απενεργοποίησης, μετά από εντολή του συστήματος αδιάλειπτης παροχής ρεύματος. Ειδικά στο θέμα των εξυπηρετητών, υψηλή διαθεσιμότητα μπορεί να επιτευχθεί μέσω χρήσης επιπλέον εφεδρικών μηχανημάτων (σε διατάξεις active-active ή active-passive). Αν και τέτοιες διατάξεις χρησιμοποιούνται ευρέως σε άλλου είδους εφαρμογές, έχουν υψηλό κόστος και εφαρμόζονται κυρίως σε συστήματα mission critical. Δεν προτείνονται λοιπόν για έργα με τις συγκεκριμένες λειτουργικές προδιαγραφές.

Τέλος, η σύνδεση με το Διαδίκτυο ενέχει και κινδύνους όσον αφορά την διαθεσιμότητα των υπηρεσιών, εξαιτίας των δικτυακών επιθέσεων από κακόβουλους τρίτους. Στην περίπτωση αυτή, υψηλή διαθεσιμότητα παρέχεται μέσω συστήματος firewall, το οποίο πρέπει να είναι προγραμματισμένο να αποτρέπει το σύνολο των γνωστών Διαδικτυακών επιθέσεων και να παρέχει τη δυνατότητα για την προσθήκη επιπλέον κανόνων για την αντιμετώπιση μελλοντικών τύπων επιθέσεων. Εντούτοις δεν είναι δυνατό να προστατευθεί ένα τέτοιο σύστημα από επιθέσεις τύπου DoS (Denial of Service) καθώς και DDoS (Distributed Denial of Service). Συστήματα τα οποία να προστατεύουν από τέτοιες επιθέσεις είναι σαφώς εκτός των στόχων των συγκεκριμένων έργων και αφορούν κυρίως ιδιαίτερα κρίσιμες υποδομές παροχής υπηρεσιών. Τέτοιες υποδομές είναι για παράδειγμα Web εξυπηρετητές εμπορικών επιχειρήσεων οι οποίες πραγματοποιούν μεγάλο όγκο πωλήσεων μέσω διαδικτύου, επιχειρήσεων και εταιριών ενημέρωσης - ειδήσεων και ψυχαγωγίας καθώς και κρατικών φορέων οι οποίοι παρέχουν υπηρεσίες προς τους πολίτες ή/και τις επιχειρήσεις κ.λπ.

2.9 Ρυθμός Μετάδοσης Δεδομένων

Το πρωτόκολλο IEEE 802.11b είναι σχεδιασμένο για ταχύτητες 11 Mbit/sec. Η ταχύτητα αυτή είναι ονομαστική. Η πραγματική ταχύτητα είναι περίπου η μισή. Όταν η απόσταση είναι μεγάλη ή υπάρχει θόρυβος και παρεμβολές, η ονομαστική ταχύτητα μπορεί να πέσει στα 5.5, 2 και 1 Mbit/sec.

Το πρωτόκολλο IEEE 802.11g είναι σχεδιασμένο για ταχύτητες 54 Mbit/sec. Η ταχύτητα αυτή είναι ονομαστική και η πραγματική είναι πολύ μικρότερη. Όμως παρότι το 802.11g είναι πιο ελκυστικό πρωτόκολλο εξαιτίας του μεγαλύτερου ρυθμού παροχής δεδομένων που επιτυγχάνει, έχει μικρότερη ακτίνα κάλυψης. Συνεπώς για την κάλυψη της ίδιας περιοχής απαιτείται η χρήση περισσότερων hotspot 802.11g από ότι 802.11b.

Οι ευρυζωνικές γραμμές που επιτρέπουν την πρόσβαση στο Διαδίκτυο συνδυάζονται προσφέροντας κάποια συνολική χωρητικότητα και κατ' επέκταση δυνατότητα μετάδοσης δεδομένων. Το σύνολο της συγκεκριμένης χωρητικότητας θα πρέπει να μοιράζεται στο σύνολο των χρηστών του ασύρματου δικτύου Wi-Fi. Αυτό σημαίνει ότι κανένας χρήστης δεν θα έχει προτεραιότητα έναντι κάποιου άλλου. Αν όλοι οι χρήστες μεταφέρουν δεδομένα με τον μέγιστο ρυθμό, τότε κάθε χρήστης θα πάει το ίδιο ποσοστό του συνολικού ρυθμού μετάδοσης.

Παράδειγμα: Αν η συνολικός ρυθμός μετάδοσης (download) που προσφέρει το σύνολο των ευρυζωνικών γραμμών είναι 3Mbps, τότε σε ένα σύνολο 30 χρηστών κάθε χρήστης μπορεί να κατεβάζει δεδομένα με ρυθμό 102Kbps. Όμως, στην περίπτωση όπου μόνο ένας χρήστης χρησιμοποιεί την πρόσβαση στο Διαδίκτυο, τότε θα μπορεί να αξιοποιήσει το σύνολο του εύρους, δηλ. και τα 3Mbps.

2.10 Πλήθος Εξυπηρετούμενων Χρηστών

Σύμφωνα με τα χαρακτηριστικά ενός Δημόσιου Ασύρματου Δικτύου Ανοικτού Χώρου, η πολιτική που ακολουθείται όσον αφορά την πρόσβαση είναι η ελεύθερη χρήση του από το σύνολο των χρηστών. Παρ' όλα αυτά, ενδεχομένως να υπάρχουν κάποια σημεία τα οποία περιορίζουν τον συνολικό αριθμό χρηστών που είναι ταυτόχρονα συνδεδεμένοι στο δίκτυο. Συγκεκριμένα τα σημεία στα οποία μπορεί να παρουσιαστεί το φαινόμενο της στενωπού (bottleneck) είναι δύο (2):

- Τα Σημεία Πρόσβασης (Access Points) στο υποσύστημα ασύρματης πρόσβασης χρηστών.
- Οι ασύρματες συνδέσεις μεταξύ των Υποσυστημάτων Backhaul με το Κεντρικό Σημείο Διανομής (Κ.Σ.Δ.).

Κάθε Υποσύστημα Ασύρματης Πρόσβασης Χρηστών περιέχει ένα Access Point για την ασύρματη επικοινωνία με τους χρήστες. Κάθε Access Point μπορεί να υποστηρίξει συνολικό ονομαστικό ρυθμό μετάδοσης 11Mbps, ενώ λόγω την πλεονάζουσας πληροφορίας για την σωστή αποστολή των

δικτυακών πακέτων ο πραγματικός ρυθμός μετάδοσης είναι μισός, δηλ. περίπου 5.5Mbps. Αυτός ο ρυθμός μετάδοσης μοιράζεται στους χρήστες που είναι συνδεδεμένοι σε κάθε Access Point, πράγμα που σημαίνει ότι σε σύνολο 20 συνδεδεμένων «ενεργών» χρηστών (στο ίδιο Access Point), κάθε χρήστες θα λαμβάνει δεδομένα με 275Kbps ή 34KBps. Αυτή η ταχύτητα είναι η μέγιστη στην περίπτωση που όλοι οι χρήστες κατεβάζουν δεδομένα την ίδια χρονική στιγμή. Συνήθως οι περισσότεροι χρήστες περιηγούνται στον Παγκόσμιο Ιστό ή διαβάζουν την Ηλεκτρονική Αλληλογραφία τους. Αυτό σημαίνει ότι για ένα μικρό χρονικό διάστημα κατεβάζουν πληροφορίες στην συσκευή τους και στη συνέχεια τις επεξεργάζονται. Εκείνη τη στιγμή δεν χρησιμοποιούν το δίκτυο, πράγμα που σημαίνει ότι κάποιοι άλλοι χρήστες, που κατεβάζουν δεδομένα, μπορούν να απολαμβάνουν καλύτερη δικτυακή εμπειρία. Δεδομένου ότι κάθε χρονική στιγμή, κατά μέσο όρο 5 χρήστες χρησιμοποιούν το δίκτυο για το κατέβασμα πληροφοριών, τότε κάθε χρήστης μπορεί θεωρητικά να λάβει πληροφορίες με ρυθμό μεγαλύτερο από 1Mbps.

Όσον αφορά στην ασύρματη σύνδεση μεταξύ του Υποσυστήματος Backhaul με το Κ.Σ.Δ. αναφέρεται ότι ο συνολικός ρυθμός μετάδοσης πληροφορίας είναι αυτός του 802.11b, δηλ. 11Mbps ονομαστικά και περίπου 5.5Mbps πρακτικά. Στην περίπτωση που στο Σύστημα Backhaul υπάρχει συνδεδεμένο μόνο ένα Υποσύστημα Ασύρματης Πρόσβασης Χρηστών, δεν παρουσιάζεται πρόβλημα. Πρόβλημα ενδεχομένως να παρουσιαστεί στην περίπτωση που 2 hotspot είναι συνδεδεμένα στο ίδιο Υποσύστημα Backhaul. Τότε ο μέγιστος συνολικός ρυθμός μετάδοσης μειώνεται στο μισό.

Εξετάζοντας συνολικά τα παραπάνω σημεία, γίνεται σαφές ότι ο συνολικός αριθμός των χρηστών που μπορούν να «συνδεθούν» στο σύστημα δεν περιορίζεται, χωρίς να εγγυάται κάποια συγκεκριμένη ποιότητα υπηρεσίας. Όμως, εκ των πραγμάτων, ο αριθμός περιορίζεται λόγω του πιλοτικού χαρακτήρα του έργου. Ένας αριθμός 75 ταυτόχρονα «πολύ ενεργών» χρηστών θα απολαμβάνει εμπειρία δικτυακής πρόσβασης με ταχύτητες όμοιες με εκείνες των συσκευών modem. Στην τυπική περίπτωση που οι χρήστες έχουν τα προαναφερθέντα χαρακτηριστικά (www, e-mail, chat, μικρά αρχεία), τότε ο συνολικός αριθμός των χρηστών μπορεί να διπλασιαστεί.

2.11 Τεκμηρίωση

Κατά την παραλαβή ενός τέτοιου συστήματος, πρέπει να υπάρχει ένα πλήρως λειτουργικό ασύρματο δίκτυο και ένα Κεντρικό Σημείο Διασύνδεσης (όπως αυτά περιγράφονται παραπάνω). Επίσης, είναι πολύ σημαντικό να υπάρχει και η κατάλληλη τεκμηρίωση, στην οποία θα υπάρχουν όλες οι πληροφορίες σχετικά με την κάλυψη του δικτύου, την αρχιτεκτονική, τη λειτουργικότητα του, τα σημεία που έχουν τοποθετηθεί τα hotspot και τα συστήματα backhaul, καθώς και όλες οι

παράμετροι του λογισμικού που χρησιμοποιείται για τη λειτουργία του δικτύου. Με τον τρόπο αυτό διασφαλίζεται η ομαλή μετάβαση από πειραματική σε επιχειρησιακή (κανονική) λειτουργία.

3 Δίκτυο AthensWiFi: “Δημόσιο Δίκτυο Ασύρματης Πρόσβασης στο Διαδίκτυο στην πλατεία Συντάγματος” (www.athenswifi.gr)

Στη συνέχεια παρουσιάζουμε ένα συγκεκριμένο παράδειγμα υλοποίησης ενός Δημόσιου Ασύρματου Δικτύου Ανοιχτού Χώρου το θα αναπτυχθεί στην περιοχή της Πλατείας Συντάγματος στην Αθήνα, στο πλαίσιο του έργου «**Ανάπτυξη Ασύρματων Ευρυζωνικών Υποδομών και Προώθηση Ζήτησης Ασύρματων Υπηρεσιών Διαδικτύου σε Πολυσύχναστους Εξωτερικούς Χώρους**», του ΕΠ ΚτΠ, αποφάσεις ένταξης: 151.369/ΚτΠ9371-B3 24/2/2004 και 152.679/ΚτΠ7356-B3 23/7/2004, κωδικός ΟΠΣ: 91016. Σκοπός του δικτύου είναι η πιλοτική παροχή ασύρματης πρόσβασης στο διαδίκτυο σε όλους τους χρήστες του εξωτερικού χώρου, με στόχο την προώθηση της ιδέας της ευρυζωνικότητας. Η επιτυχία του έργου βασίζεται στην μεγάλη αποδοχή που θα έχει από τους πολίτες. Για το λόγο αυτό έπρεπε να επιλεγεί ανοικτός χώρος μεταξύ δημόσιων χώρων συνάθροισης, όπως είναι πλατείες, σταθμοί μητροπολιτικού σιδηροδρόμου, μεγάλοι εμπορικοί πεζόδρομοι, σταθμοί λεωφορείων, εμπορικά κέντρα, χώροι αναψυχής, κ.λπ. Η Πλατεία Συντάγματος καλύπτει πλήρως την απαίτηση για πολυσύχναστο δημόσιο χώρο, καθημερινά επισκέψιμο από μεγάλο αριθμό πολιτών όλων των ηλικιών, ώστε να γνωρίσουν από κοντά τις δυνατότητες της ασύρματης ευρυζωνικότητας.

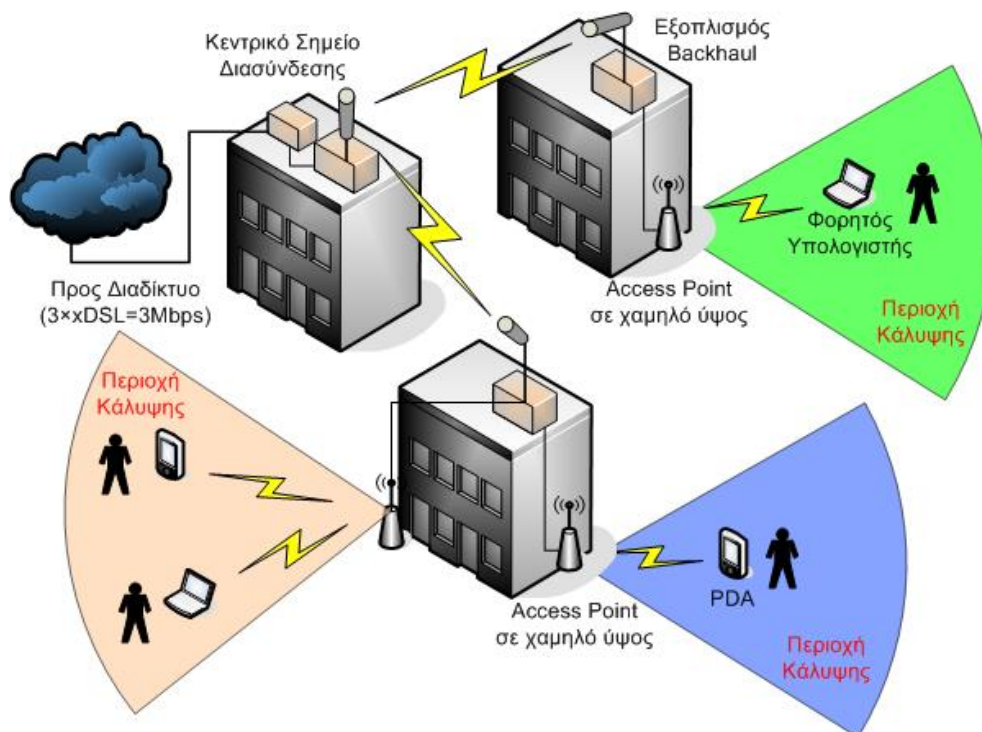
Επομένως, στο πλαίσιο της προώθησης ζήτησης ασύρματων ευρυζωνικών υποδομών για μεγάλο αριθμό πολιτών, θα πραγματοποιηθεί, η προμήθεια, εγκατάσταση και δοκιμαστική λειτουργία εξοπλισμού για τη δημιουργία ασύρματων τοπικών δικτύων (Wireless Hotspots) στην Πλατεία Συντάγματος της Αθήνας, εγκαθιστώντας το πρώτο «**Δημόσιο Δίκτυο Ασύρματης Πρόσβασης στο Διαδίκτυο στην πλατεία Συντάγματος (www.athenswifi.gr)**». Μέσω των Wireless Hotspots θα παρέχονται, σε δοκιμαστική - πιλοτική βάση, ευρυζωνικές υπηρεσίες Internet στους πολίτες, καθώς και στους επισκέπτες της Πλατείας.

Κάθε Wireless Hotspot θα επικοινωνεί ασύρματα με τις συσκευές των χρηστών του δικτύου (φορητοί υπολογιστές, υπολογιστές παλάμης, κτλ.), εφόσον αυτές διαθέτουν τον κατάλληλο εξοπλισμό (ενσωματωμένους προσαρμογείς, ειδικές κάρτες επέκτασης κτλ.) που να είναι συμβατός με το πρότυπο WiFi (ειδικότερα IEEE 802.11b και IEEE 802.11g). Ένα Wireless Hotspot θα επικοινωνεί με πολλαπλές συσκευές χρηστών, ενώ κρίνεται απαραίτητο να εγκατασταθούν πολλά Hotspot (περί τα δέκα), περιμετρικά ή και στο κέντρο της πλατείας, ώστε αφενός να καλύπτεται ομοιόμορφα όλος ο χώρος της πλατείας και αφετέρου να μην απαιτείται αυξημένη ένταση εκπομπής από κάθε Wireless Hotspot χωριστά.

Επιπρόσθετα, θα πρέπει να ληφθεί υπόψη ότι η εγκατάσταση των Wireless Hotspot θα πρέπει να γίνει με τέτοιο τρόπο ώστε να μειωθούν όσο το δυνατόν περισσότερο οι παρεμβολές μεταξύ τους. Επίσης οι χρήστες του δικτύου θα πρέπει να μπορούν να περιφέρονται στην Πλατεία, αλλάζοντας ανάλογα με τη θέση τους σημείο εξυπηρέτησης, χωρίς να αποσυνδέονται και να επανασυνδέονται στο ασύρματο δίκτυο (roaming).

3.1 Περιγραφή Λειτουργίας του Ασύρματου Δικτύου AthensWiFi

Η λειτουργία του Ασύρματου Δικτύου AthensWiFi είναι όμοια με εκείνη του γενικού Δημόσιου Ασύρματου Δικτύου Ανοικτού Χώρου που περιγράφηκε παραπάνω. Οι χρήστες που βρίσκονται στην Πλατεία Συντάγματος μπορούν μέσω μιας ασύρματης δικτυακής συσκευής (π.χ. φορητού υπολογιστή, PDA, κλπ.) να χρησιμοποιήσουν τις υπηρεσίες του δικτύου. Οι φορητές συσκευές συνδέονται με τα Σημεία Πρόσβασης (hotspot) που βρίσκονται στο επίπεδο της Πλατείας. Η κίνηση από τα hotspot μεταφέρεται ενσύρματα (Ethernet) στην οροφή ενός κτιρίου όπου υπάρχει ένα υποσύστημα Backhaul. Το υποσύστημα Backhaul συγκεντρώνει την κίνηση από όλα τα hotspot που είναι συνδεδεμένα με αυτό. Στη συνέχεια προωθεί όλη την κίνηση με ασύρματο τρόπο (IEEE 802.11b) προς το Κεντρικό Σημείο Διασύνδεσης, όπου υπάρχουν τρεις (3) ευρυζωνικές γραμμές τύπου ADSL (1Mbps), μέσω των οποίων όλη η κίνηση του ασύρματου δικτύου προωθείται στο Διαδίκτυο. Όλα αυτά φαίνονται σχηματικά στην Εικόνα 8.



Εικόνα 8: Λειτουργία Ασύρματου Δικτύου AthensWiFi

3.2 Περιοχή Κάλυψης Δικτύου AthensWiFi

Προκειμένου να επιτύχει το συγκεκριμένο έργο παροχής ασύρματων δικτυακών υπηρεσιών, θα πρέπει η καλυπτόμενη από το ασύρματο δίκτυο περιοχή να είναι όσο γίνεται μεγαλύτερη και με όσο το δυνατόν ισχυρότερο σήμα σε κάθε σημείο. Οι πλέον πολυσύχναστες περιοχές, οι οποίες θα πρέπει να καλύπτονται, είναι οι ακόλουθες:

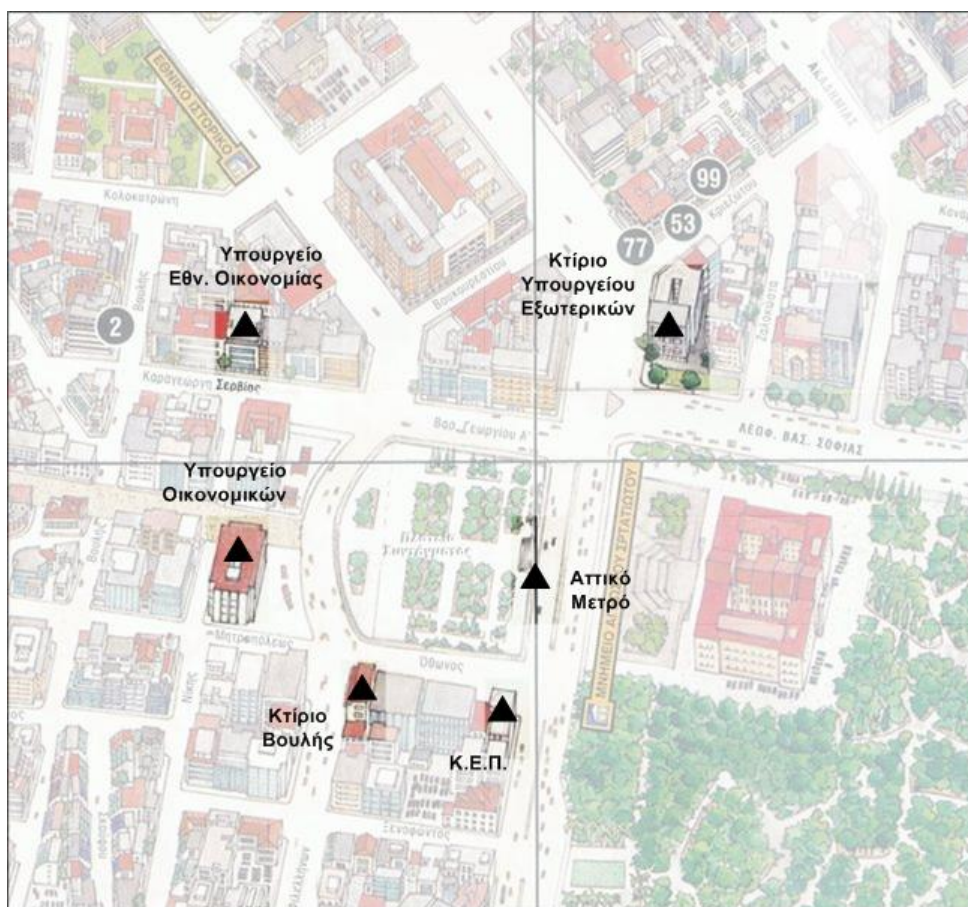
1. Η Πλατεία Συντάγματος
2. Τα πεζοδρόμια μπροστά από τον χώρο του Υπουργείου Οικονομικών
3. Το πάνω τμήμα της οδού Ερμού που καταλήγει στην Πλατεία
4. Το πεζοδρόμιο μπροστά από την Εθνική Τράπεζα και η κατάληξη της οδού Σταδίου στην Πλατεία
5. Το πάνω τμήμα της οδού Μητροπόλεως που καταλήγει στην Πλατεία

6. Ο επίπεδος χώρος μπροστά από το Μνημείο του Άγνωστου Στρατιώτη
7. Το τμήμα της Λεωφόρου Βασιλίσσης Αμαλίας που περνάει από την πλατεία
8. Η αρχή της οδού Ελευθερίου Βενιζέλου (Πανεπιστημίου)
9. Ένα τμήμα της Λεωφόρου Βασιλίσσης Σοφίας που ξεκινάει από την Πλατεία

Για να επιτευχθεί η προτεινόμενη κάλυψη, θα πρέπει να τοποθετηθούν αρκετά hotspot, ένα ανά υπο-περιοχή του συνολικού χώρου κάλυψης. Τα σημεία αυτά αντιστοιχίζονται σε κτίρια, στο κάτω μέρος των οποίων τοποθετούνται τα hotspot και στην ταράτσα κάθε κτιρίου τοποθετείται από ένα υποσύστημα Backhaul. Τα κτίρια αυτά θα πρέπει να βρίσκονται περιμετρικά της Πλατείας προκειμένου να επιτευχθεί η κάλυψη που περιγράφηκε παραπάνω.

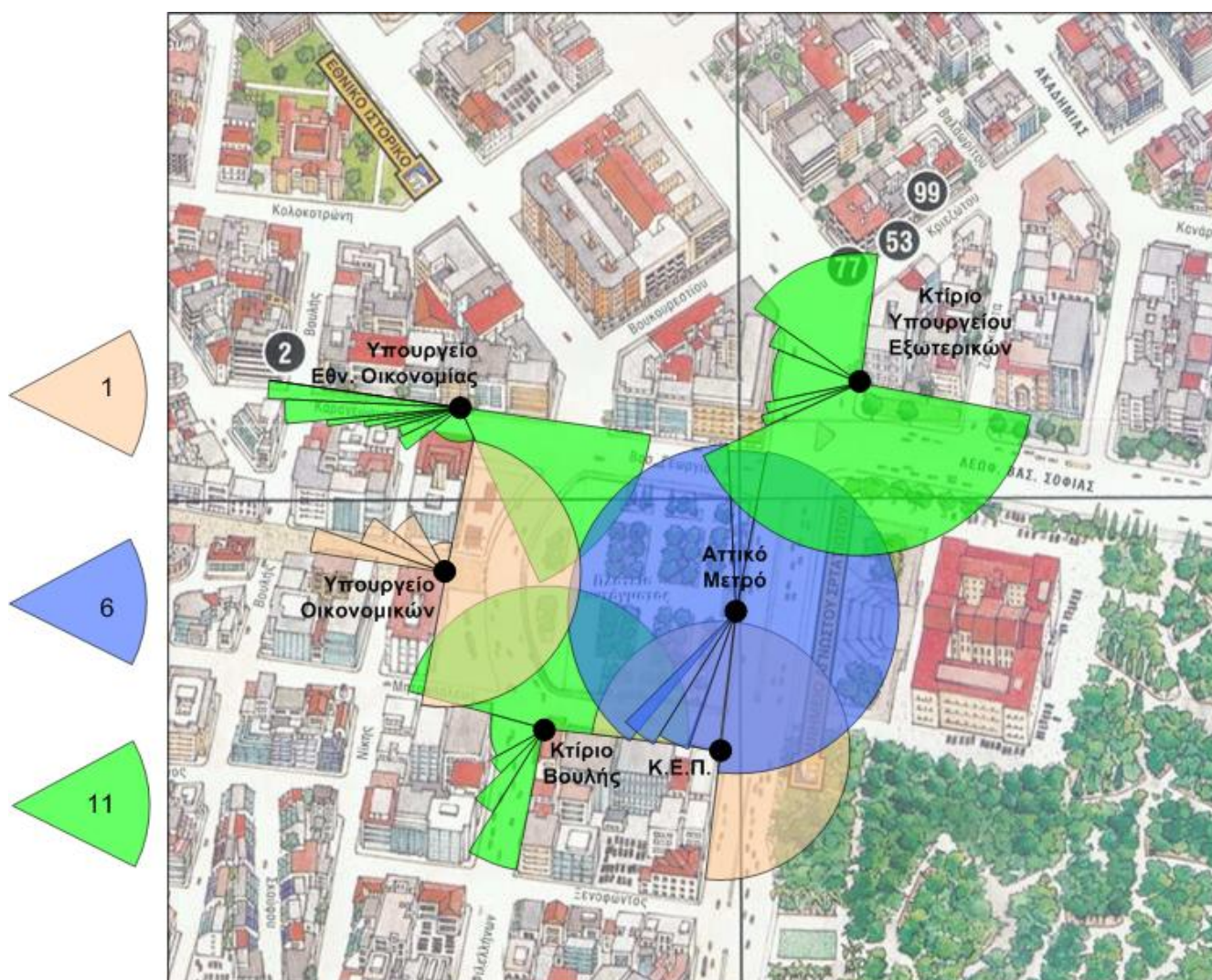
Είναι προφανές ότι υπάρχουν περισσότεροι από ένας διαφορετικοί συνδυασμοί κτιρίων και σημείων τοποθέτησης hotspot μέσω των οποίων μπορεί να καλυφθεί ο χώρος της Πλατείας. Ένας πιθανός συνδυασμός αποτελείται από το σύνολο των κτιρίων που απεικονίζεται στην Εικόνα 9. Τα κτίρια που φαίνονται είναι τα ακόλουθα:

1. Κτίριο Υπουργείου Οικονομικών
2. Κτίριο Κέντρου Εξυπηρέτησης Πολιτών επί των Λεωφόρου Βασιλίσσης Αμαλίας και οδού Όθωνος
3. Κτίριο που ανήκει στη Βουλή επί των οδών Φιλελλήνων και Όθωνος
4. Κτίριο Υπουργείου Εθνικής Οικονομίας επί της οδού Καραγεώργη Σερβίας
5. Κτίριο που ανήκει στο Υπουργείο Εξωτερικών επί της λεωφόρου Βασιλίσσης Σοφίας και της οδού Ελευθερίου Βενιζέλου (Πανεπιστημίου)



**Εικόνα 9: Ένα σύνολο κτιρίων που μπορούν να επιτύχουν κάλυψη της
ζητούμενης περιοχής.**

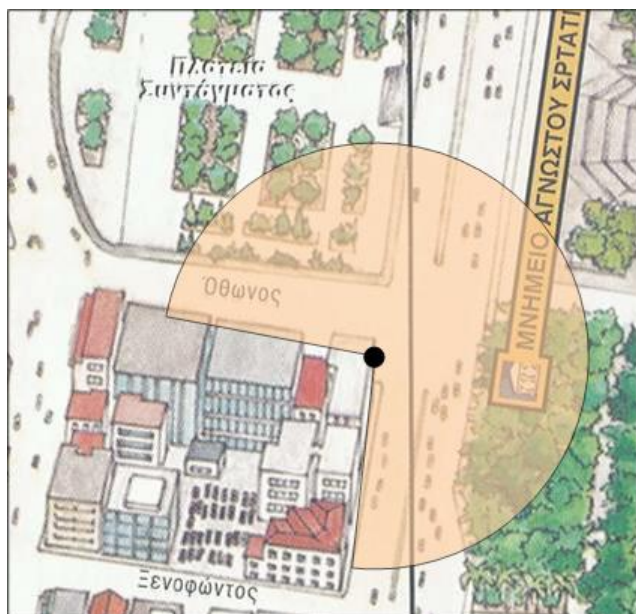
Η περιοχή κάλυψης του ασύρματου δικτύου φαίνεται στην Εικόνα 10. Αυτή η κάλυψη επιτυγχάνεται με τον συνδυασμό σημείων πρόσβασης στα κτίρια που προαναφέρθηκαν. Τα σημεία είναι τοποθετημένα με τέτοιο τρόπο ώστε να καλύπτουν τη μέγιστη δυνατή έκταση στην Πλατεία Συντάγματος και γύρω από αυτή. Οι κεραιές που χρησιμοποιούνται στο κομμάτι της ασύρματης πρόσβασης των χρηστών είναι πολυκατευθυντικές (οmnι) και ακτινοβολούν σε 360° στο οριζόντιο επίπεδο.



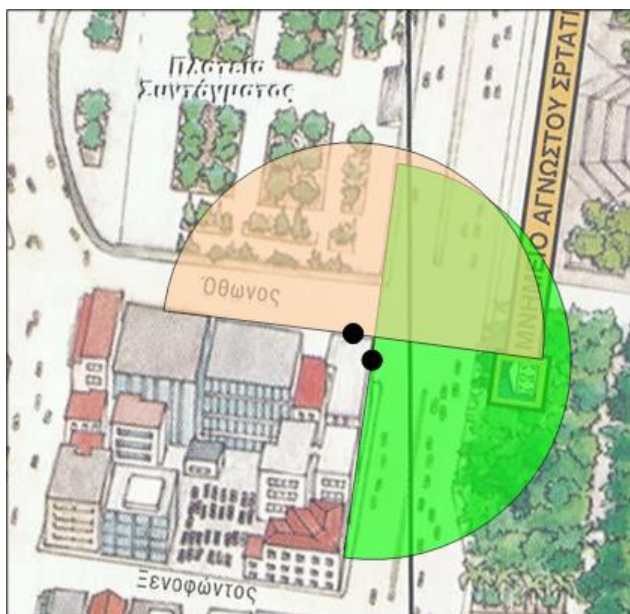
Εικόνα 10: Συνολική Περιοχή Κάλυψης

Η Εικόνα 10 παρουσιάζει την τοποθέτηση των hotspot στα προαναφερθέντα κτίρια περιμετρικά της Πλατείας. Τα διαφορετικά κανάλια (1, 6 και 11) που χρησιμοποιούνται για τις περιπτώσεις επικάλυψης φαίνονται με το αντίστοιχα χρώμα. Τα σημεία στα οποία τοποθετούνται τα hotspot (φαίνονται με ένα μαύρο κύκλο στην Εικόνα 10) είναι τα εξής:

1. Κτίριο Κέντρου Εξυπηρέτησης Πολιτών επί της λεωφόρου Βασιλίσσης Αμαλίας και της οδού Όθωνος. Το hotspot τοποθετείται ακριβώς στη γωνία, προκειμένου να καλύψει τμήματα της Πλατείας και της λεωφόρου Βασιλίσσης Αμαλίας. Στην περίπτωση που δεν είναι δυνατόν να τοποθετηθεί ακριβώς στη γωνία (βλ. Εικόνα 11), τότε μπορεί να δημιουργηθεί η ίδια κάλυψη με τη χρήση 2 hotspot (βλ. Εικόνα 12).

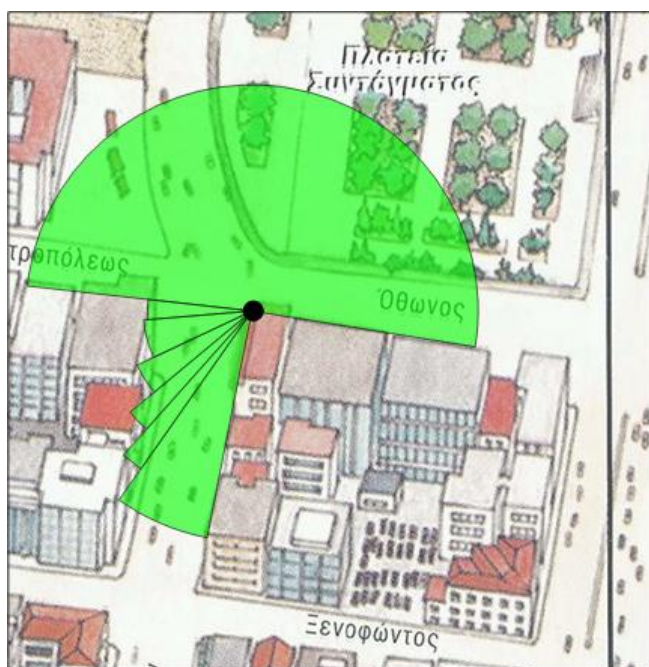


Εικόνα 11: Κάλυψη από Κ.Ε.Π. με ένα hotspot ακριβώς στη γωνία.

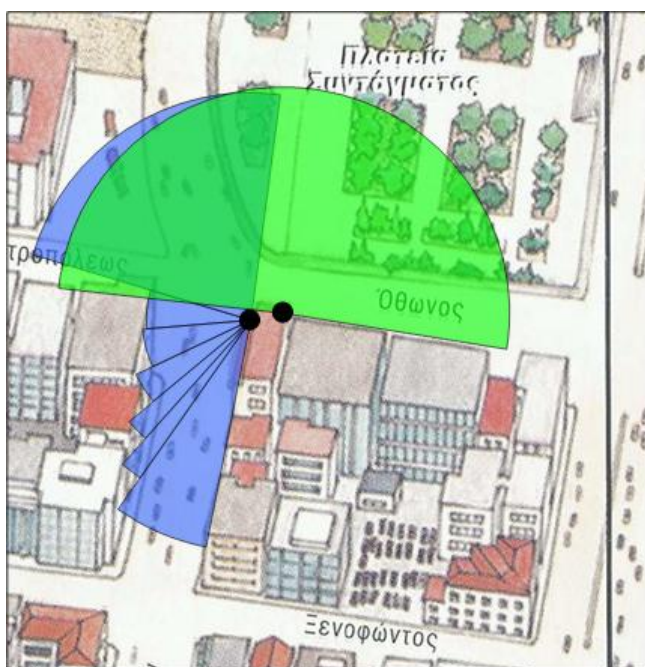


Εικόνα 12: Κάλυψη από Κ.Ε.Π. με δύο hotspot.

2. Κτίριο της Βουλής επί των οδών Όθωνος και Φιλελλήνων. Το hotspot τοποθετείται ακριβώς στη γωνία του κτιρίου, προκειμένου να καλύψει τμήματα τόσο της Πλατείας όσο και της οδού Όθωνος, καθώς και ένα μικρό κομμάτι στην αρχή της οδού Μητροπόλεως (βλ. Εικόνα 13). Στην περίπτωση που αυτό δεν καταστεί εφικτό, τοποθετούνται δύο hotspot, το ένα επί της οδού Όθωνος και το δεύτερο επί της οδού Φιλελλήνων, πετυχαίνοντας την ίδια κάλυψη (βλ. Εικόνα 14).

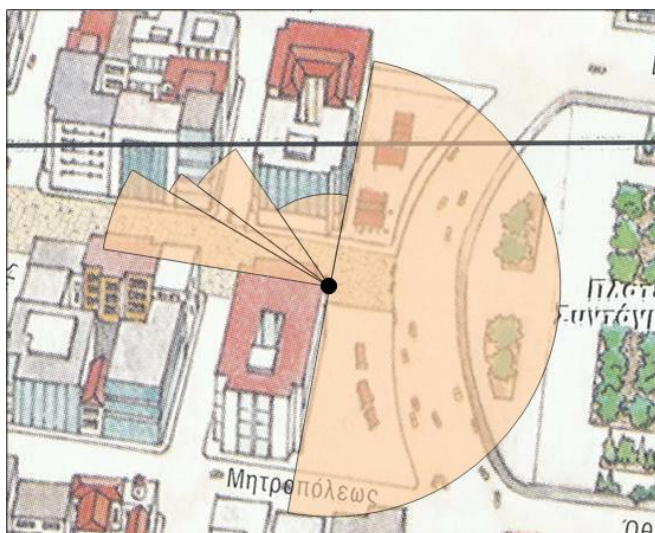


Εικόνα 13: Κάλυψη από κτίριο Βουλής με ένα hotspot ακριβώς στη γωνία.

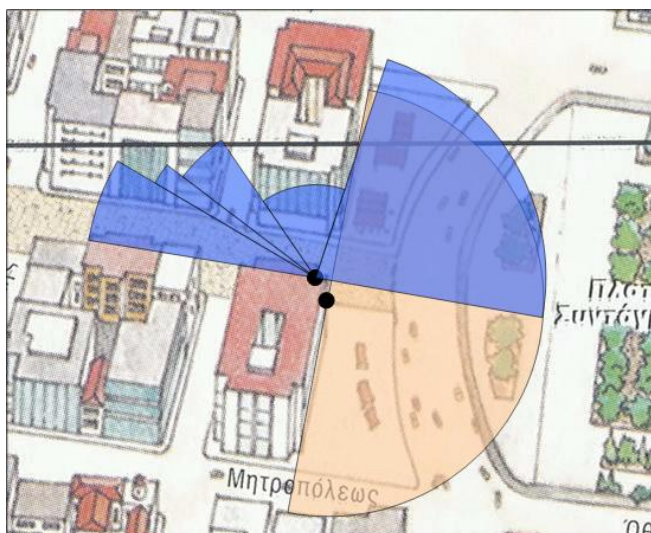


Εικόνα 14: Κάλυψη από κτίριο Βουλής με δύο hotspot.

3. Κτίριο Υπουργείου Οικονομικών. Το hotspot τοποθετείται ακριβώς στη γωνία επί της οδού Ερμού, προκειμένου να καλύψει τόσο τμήμα της Πλατείας όσο και ένα τμήμα στην αρχή της οδού Ερμού (βλ. Εικόνα 15). Στην περίπτωση που δεν επιτευχθεί η τοποθέτηση ακριβώς στη γωνία, τότε μπορούν να τοποθετηθούν δύο hotspot, το ένα επί της πλευράς που κτιρίου προς την μεριά της Πλατείας και το άλλο επί της οδού Ερμού, δημιουργώντας την ίδια κάλυψη (βλ. Εικόνα 16).

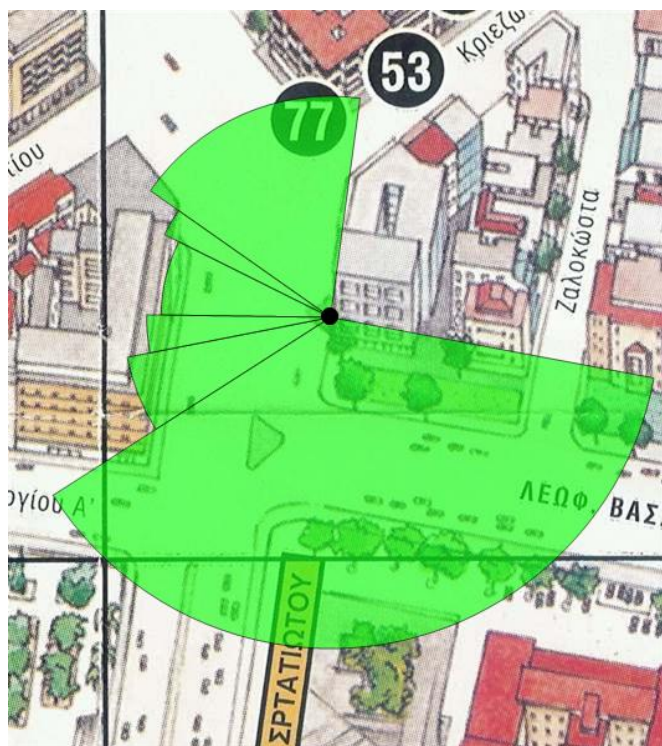


Εικόνα 15: Κάλυψη από κτίριο Υπ. Οικονομικών με ένα hotspot ακριβώς στη γωνία.

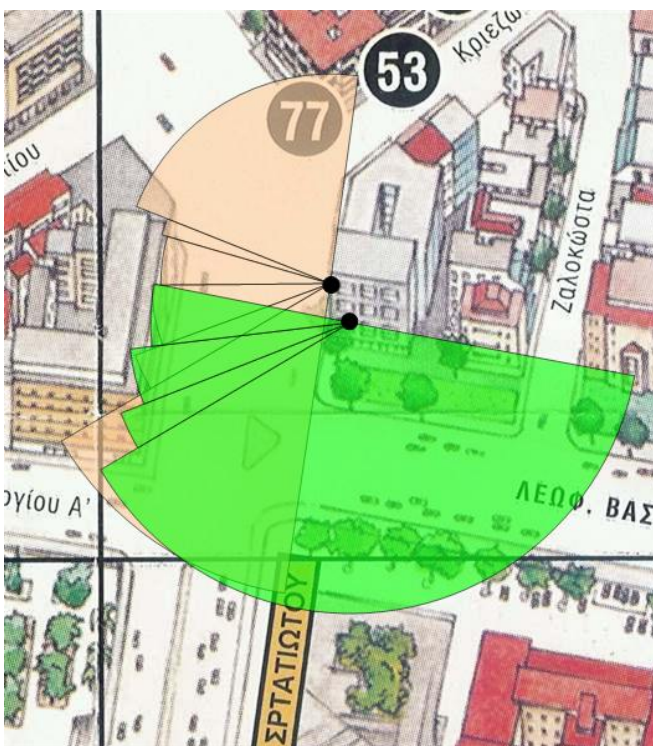


Εικόνα 16: Κάλυψη από κτίριο Υπ. Οικονομικών με δύο hotspot.

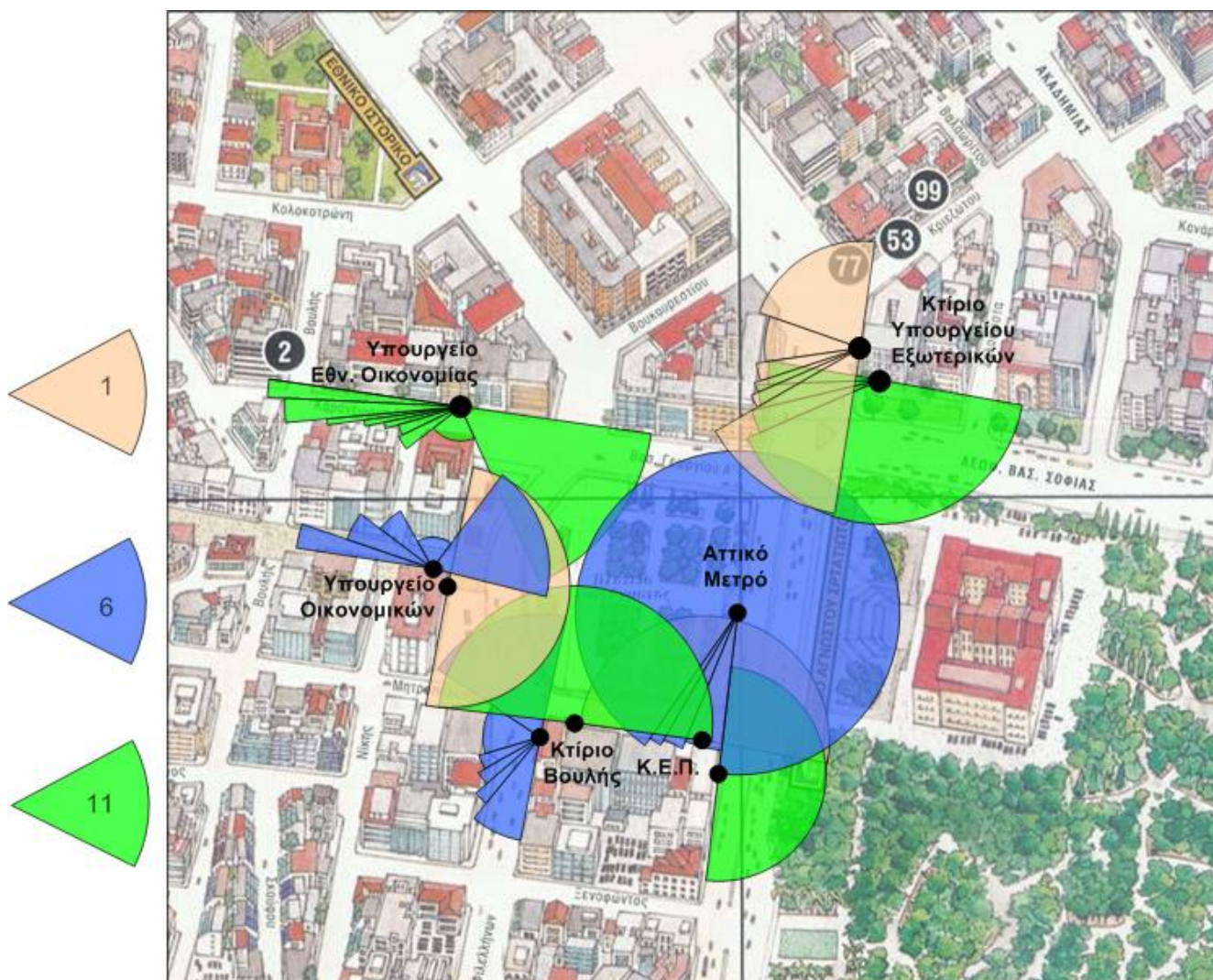
4. Κτίριο Υπουργείου Εθνικής Οικονομίας επί της οδού Καραγεώργη Σερβίας. Στη συγκεκριμένη περίπτωση δεν υπάρχει η δυνατότητα κάλυψης μεγάλης περιοχής. Η περιοχή που καλύπτεται είναι ένα τμήμα της Πλατείας, καθώς και το αρχικό τμήμα της οδού Καραγεώργη Σερβίας περίπου μέχρι το ύψος της οδού Βουλής.
5. Σημείο της «Αττικό Μετρό» επί της Λεωφόρου Βασιλίσσης Αμαλίας. Το συγκεκριμένο hotspot επιτυγχάνει κάλυψη στο κύριο κομμάτι της Πλατείας.
6. Σημείο του Υπουργείου Εξωτερικών επί της Λεωφόρου Βασιλίσσης Σοφίας και της οδού Ελευθερίου Βενιζέλου (Πανεπιστημίου). Η περιοχή που καλύπτεται είναι (βλ. Εικόνα 17) ένα τμήμα της Πλατείας, ένα τμήμα στην αρχή της οδού Βασιλίσσης Σοφίας και ένα τμήμα στην αρχή της οδού Ελευθερίου Βενιζέλου (Πανεπιστημίου). Στην περίπτωση αυτή τοποθετείται ένα hotspot ακριβώς στη γωνία επί της λεωφόρου Βασιλίσσης Σοφίας και Ελευθερίου Βενιζέλου. Στην περίπτωση που αυτό δεν καταστεί δυνατό, τότε μπορούν να τοποθετηθούν δύο hotspot, ένα επί της Λεωφόρου Βασιλίσσης Σοφίας και ένα επί της οδού Ελευθερίου Βενιζέλου (βλ. Εικόνα 18).



Εικόνα 17: Κάλυψη από κτίριο Υπ. Εξωτερικών με ένα hotspot ακριβώς στη γωνία.



Εικόνα 18: Κάλυψη από κτίριο Υπ. Εξωτερικών με δύο hotspot.



Εικόνα 19: Περιοχή Συνολικής Κάλυψης χρησιμοποιώντας 2 hotspot στα κτίρια Κ.Ε.Π., Υπ. Οικονομικών, Βουλής και Υπ. Εξωτερικών.

Στην Εικόνα 19 φαίνεται η συνολική περιοχή κάλυψης χρησιμοποιώντας το μέγιστο αριθμό hotspot, δηλ. 2 hotspot σε κάθε γωνιακό σημείο εξυπηρέτησης. Παρατηρούμε ότι στην περίπτωση αυτή απαιτούνται 10 hotspot προκειμένου να καλυφθεί η περιοχή που μας ενδιαφέρει. Από την εικόνα γίνεται εμφανές ότι η καλυπτόμενη περιοχή είναι η πλέον πολυσύχναστη, γεγονός που αυξάνει την αξία του συγκεκριμένου έργου, προωθώντας σημαντικά τη χρήση ασύρματων δικτυακών τεχνολογιών στους πολίτες.

3.3 Αρχιτεκτονική Ασύρματου Δικτύου AthensWiFi

Η αρχιτεκτονική του Ασύρματου Δικτύου AthensWiFi είναι όμοια με εκείνη του γενικού Δημόσιου Ασύρματου Δικτύου Ανοικτού Χώρου που περιγράφηκε παραπάνω. Το συνολικό δίκτυο χωρίζεται σε

επιμέρους υποσυστήματα, καθένα από τα οποία πραγματοποιεί και μια ιδιαίτερη λειτουργία. Τα υποσυστήματα αυτά είναι τα εξής:

- Υποσύστημα Ασύρματης Πρόσβασης Χρηστών (hotspot)
- Υποσύστημα Περιφερειακού Σημείου Συλλογής κίνησης (Backhaul)
- Υποσύστημα Κεντρικού Σημείου Διασύνδεσης

Τα συστήματα αυτά έχουν περιγραφεί αναλυτικά προηγουμένως. Παρακάτω περιγράφουμε τα ιδιαίτερα χαρακτηριστικά που έχουν τα υποσυστήματα του συγκεκριμένου δικτύου.

3.3.1 Υποσύστημα Ασύρματης Πρόσβασης Χρηστών (hotspot)

Στην περίπτωση του Ασύρματου Δικτύου AthensWiFi τα σημεία ασύρματης πρόσβασης βρίσκονται κοντά στο επίπεδο της Πλατείας. Επειδή τα hotspot δεν πρέπει να είναι φυσικώς προσβάσιμα από τον κόσμο που βρίσκεται στην Πλατεία (για λόγους προστασίας του εξοπλισμού), τοποθετούνται σε ένα ύψος 5μ από το επίπεδο της Πλατείας. Κάθε hotspot περιέχει ένα κουτί μέσα στο οποίο βρίσκεται κλειδωμένο το Access Point. Εκτός του κουτιού υπάρχει μια πολυκατευθυντική κεραία (omni) και ένα καλώδιο ethernet (cat 5e) που μεταφέρει και το ρεύμα (power-over-ethernet). Το καλώδιο συνδέεται με ένα υποσύστημα backhaul που βρίσκεται στην ταράτσα του κτιρίου στο οποίο είναι τοποθετημένο το hotspot.

3.3.2 Υποσύστημα Backhaul

Κάθε υποσύστημα Backhaul είναι τοποθετημένο στην ταράτσα του κτιρίου στο οποίο είναι τοποθετημένα 1-2 hotspot. Χρησιμοποιώντας την κατευθυντική κεραία, το Υποσύστημα Backhaul συνδέεται με το Υποσύστημα Κεντρικού Σημείου Διασύνδεσης.

Η λειτουργία που επιτελεί κάθε ένα από τα υποσυστήματα Backhaul είναι να συλλέγουν τη κίνηση από τα επιμέρους hotspot που είναι τοποθετημένα στο επίπεδο των χρηστών (π.χ. επίπεδο κάποιας πλατείας), να τη μετατρέπουν σε ασύρματη μορφή τύπου 802.11b και να την προωθούν προς το Κεντρικό Σημείο Διασύνδεσης.

3.3.3 Υποσύστημα Κεντρικού Σημείου Διασύνδεσης

Το Κεντρικό Σημείο Διασύνδεσης (βλ. Εικόνα 7) είναι το υποσύστημα που συνδέει όλη τη δικτυακή υποδομή με το δίκτυο κορμού (Διαδίκτυο). Στην περίπτωση του ασύρματου Δικτύου AthensWiFi, το Κ.Σ.Δ. είναι τοποθετημένο σε ειδικά εξοπλισμένο χώρο στο **Υπουργείο Οικονομικών** (βλ. Εικόνα 15).

Στο σημείο του Κεντρικού Σημείου Διασύνδεσης, εκτός από τον δικτυακό εξοπλισμό για την συγκέντρωση της κίνησης από τα επιμέρους Υποσυστήματα Backhaul, τοποθετείται εξοπλισμός Backhaul προκειμένου να καταστεί εφικτή η τοποθέτηση hotspot (ενός ή δύο), κοντά στο επίπεδο της Πλατείας. Στην περίπτωση αυτή δεν απαιτείται η προμήθεια κατευθυντικής κεραίας.

4 Διαδικασία Ελέγχου Ασύρματης Δικτυακής Υποδομής και Υπηρεσιών

Στόχος αυτού του κεφαλαίου είναι να δοθεί και να περιγραφεί η διαδικασία ελέγχου μιας ασύρματης δικτυακής εγκατάστασης τύπου Wi-Fi.

4.1 Διαδικασία ελέγχου

Διαδικασία ελέγχου είναι ένα σύνολο βημάτων μέσω των οποίων θα ελεγχθεί το σύνολο της δικτυακής υποδομής, υλικού και λογισμικού. Κάθε βήμα έχει στόχο να επιβεβαιώσει την λειτουργία ενός επιμέρους τμήματος της υποδομής. Κάποια τμήματα της υποδομής είναι πιο σημαντικά από κάποια άλλα σε σχέση με την συνολική υπηρεσία που προσφέρεται στην τελικό χρήστη, και σε αυτά δίδεται ιδιαίτερη βαρύτητα. Παρακάτω ακολουθούν τα βήματα που αποτελούν τη διαδικασία ελέγχου. Τα βήματα δεν είναι ανάγκη να εκτελεστούν με τη σειρά με την οποία είναι καταγεγραμμένα.

4.2 Έλεγχος με Περιπλάνηση (Walkabout Test)

Ο έλεγχος με περιπλάνηση (walkabout test) είναι ένα βασικό βήμα για την επιθεώρηση μιας τοποθεσίας και της ολοκλήρωσης της ανάπτυξης ενός ασύρματου δικτύου. Η διαδικασία συνίσταται στην περιπλάνηση στην περιοχή αυτή, κατά την οποία λαμβάνονται μετρήσεις και εξακριβώνεται ότι υπάρχει επαρκής κάλυψη σε όλα τα σημεία αυτής. Αν και η διαδικασία είναι αρκετά απλή και εύκολη δεν θα πρέπει να παραληφθεί. Κατά την διάρκεια της περιπλάνησης πιστοποιείται η εξασθένιση του σήματος, ορίζονται τα όρια των κυψελών (cells), αναγνωρίζονται προβλήματα noise-floor και εξακριβώνεται ότι η σύνδεση μεταξύ ενός πελάτη και του AP διατηρεί τον απαραίτητο ρυθμό μετάδοσης δεδομένων που απαιτείται από τις προδιαγραφές του ασύρματου δικτύου. Η διαδικασία βοηθάει στην αποδοτικότερη τοποθέτηση των APs και στην επιλογή του κατάλληλου τύπου της κεραίας που θα χρησιμοποιηθεί.

Η παράλειψη του ελέγχου με περιπλάνηση οδηγεί, στην συντριπτική πλειοψηφία των περιπτώσεων, σε δύο αντιδιαμετρικά προβλήματα. Στο ένα παρουσιάζονται πολλά “νεκρά” σημεία, όπου δεν υπάρχει κάλυψη, ενώ στο άλλο οδηγούμαστε στην ανάπτυξη ενός υπερκοστολογημένου ασύρματου δικτύου. Μια κατάλληλη περιπλάνηση συνδυασμένη με μια ολοκληρωμένη μελέτη του χώρου

ανάπτυξης του δικτύου είναι ο μόνος τρόπος για να επιτευχθεί η όσο το δυνατόν αποδοτικότερη σχεδίαση, όσο αφορά την επίδοση, το κόστος και την αποτελεσματικότητα του.

4.3 Έλεγχος Λειτουργίας με διαφορετικού είδους συσκευές

Πραγματοποιείται έλεγχος της λειτουργίας όλων των παρεχόμενων υπηρεσιών χρησιμοποιώντας διαφορετικού τύπου φορητές συσκευές. Οι φορητές συσκευές που χρησιμοποιούνται είναι:

- φορητοί υπολογιστές (laptops), με διαφορετικές συνθέσεις όσον αφορά την αρχιτεκτονική του υλικού τους (hardware) και το λειτουργικό σύστημα (operating system) που εκτελούν. Οι συνθέσεις που χρησιμοποιούνται είναι από τις πλέον γνωστές και αναγνωρισμένες στην αγορά.
- υπολογιστές παλάμης (PDAs)

Με το τρόπο αυτό διασφαλίζεται η πλειονότητα των συσκευών που θα βρεθούν στον χώρο κάλυψης το ασύρματου δικτύου Wi-Fi θα έχουν τη δυνατότητα να συνδεθούν και να χρησιμοποιήσουν τις υπηρεσίες του. Έτσι, διασφαλίζεται επίσης και ένα σημαντικό κομμάτι της επιτυχίας του συγκεκριμένου έργου.

4.4 Συμβατότητα με Πρωτόκολλο IEEE 802.11g

Πραγματοποιείται έλεγχος συμβατότητας με το πρωτόκολλο IEEE 802.11g. Αν και οι περισσότερες φορητές ασύρματες συσκευές χρησιμοποιούν το πρωτόκολλο IEEE 802.11b, ένα σημαντικό ποσοστό αυτών χρησιμοποιεί το νεότερο πρωτόκολλο IEEE 802.11g, το οποίο επιτυγχάνει μεγαλύτερη ταχύτητα μετάδοσης δεδομένων. Επειδή τα δύο συγκεκριμένα πρωτόκολλα είναι συμβατά μεταξύ τους, θα γίνει έλεγχος χρήσης της ασύρματης δικτυακής υποδομής χρησιμοποιώντας συσκευές IEEE 802.11g. Οι συγκεκριμένες συσκευές θα πρέπει να λειτουργούν κανονικά στο χώρο κάλυψης, χωρίς να απαιτείται η επίτευξη των ρυθμών μετάδοσης που υποστηρίζονται από το συγκεκριμένο πρωτόκολλο. Η συγκεκριμένη δυνατότητα θεωρείται εξαιρετικά σημαντική, μιας και αυξάνει το δυνητικό πλήθος των τελικών χρηστών που μπορούν να χρησιμοποιήσουν τις παρεχόμενες υπηρεσίες.

4.5 Έλεγχος Μέγιστου Χώρου Κάλυψης

Πραγματοποιείται έλεγχος στην προβλεπόμενη περιοχή κάλυψης του δικτύου. Θα πρέπει η περιοχή κάλυψης να είναι η μέγιστη δυνατή, ώστε οι παρεχόμενες υπηρεσίες να μπορούν να προσπελαστούν αποδοτικότερα. Ο συγκεκριμένος έλεγχος πραγματοποιείται με την Διαδικασία της Περιπλάνησης που περιγράφηκε προηγουμένως.

4.6 Έλεγχος της Διαδικασίας Περιαγωγής (roaming)

Πραγματοποιείται έλεγχος της διαδικασίας περιαγωγής (roaming) για να εξασφαλιστεί ότι οι χρήστες του δικτύου θα μπορούν να περιφέρονται στην περιοχή κάλυψης, αλλάζοντας ανάλογα με τη θέση τους το σημείο ασύρματης πρόσβασης με διαφανή τρόπο και χωρίς να αποσυνδέονται και να επανασυνδέονται στο ασύρματο δίκτυο. Ο συγκεκριμένος έλεγχος πραγματοποιείται με την Διαδικασία της Περιπλάνησης που περιγράφηκε αναλυτικά παραπάνω.

4.7 Έλεγχος εμφάνισης Συμφωνητικού Χρήσης του δικτύου και Προειδοποίησης Ασφαλείας

Πραγματοποιείται έλεγχος εμφάνισης του συμφωνητικού χρήσης του δικτύου και της σχετικής προειδοποίησης ότι το δίκτυο δεν είναι ασφαλές. Δεδομένου ότι δεν υποστηρίζονται ασφαλείς συνδέσεις στο επίπεδο του ασύρματου δικτύου, είναι σημαντικό ο χρήστης να ενημερωθεί πριν αρχίσει να χρησιμοποιεί τις υπόλοιπες δικτυακές υπηρεσίες. Θα πρέπει να εμφανίζεται σχετική προειδοποίηση της μορφής:

«Στο **«Δημόσιο Δίκτυο Ασύρματης Πρόσβασης στο Διαδίκτυο στην πλατεία Συντάγματος (www.athenswifi.gr)**» στο οποίο θα συνδεθείτε δεν κρυπτογραφούνται τα δεδομένα σας κατά την μετάδοσή τους. Η ασφάλεια του συστήματός σας και των προσωπικών σας δεδομένων είναι αποκλειστικά δική σας ευθύνη. Σας συνιστούμε την χρήση πρωτοκόλλων ασφαλούς μετάδοσης όπως SMTPs, POPs, IMAPs, SSH, HTTPS, κτλ.»

Ο έλεγχος πραγματοποιείται με την σύνδεση στο ασύρματο χρησιμοποιώντας διαφορετικού είδους συσκευές, όπως αναφέρεται στην παράγραφο 4.3

4.8 Έλεγχος Υπηρεσίας Firewall

Πραγματοποιείται έλεγχος της υπηρεσίας firewall προσομοιώνοντας δικτυακές επιθέσεις στο σύνολο των εξυπηρετητών του δικτύου. Επειδή τα τελευταία χρόνια, οι δικτυακές επιθέσεις που έχουν ως αποτέλεσμα την άρνηση υπηρεσιών (Denial of Service attacks) γίνονται όλο και πιο συχνές, είναι αναγκαίο να εξασφαλιστεί η σωστή και αποτελεσματική λειτουργία της υπηρεσίας firewall.

4.9 Έλεγχος Συστημάτων Αδιάλειπτης Παροχής Ρεύματος

Πραγματοποιείται έλεγχος υψηλής διαθεσιμότητας στο τμήμα των εξυπηρετητών. Το φαινόμενο της πτώσης τάσης ή της διακοπής παροχής ηλεκτρικού ρεύματος δεν είναι ασύνηθες στην Ελλάδα, ιδίως τους καλοκαιρινούς μήνες. Δεδομένου ότι η ασύρματη πρόσβαση δεν πρέπει να διακόπτεται για τέτοιου είδους φαινόμενα, θα ελεγχθεί η υποδομή αδιάλειπτης παροχής ρεύματος σε όλους τους εξυπηρετητές. Επιπλέον, θα ελεγχθεί η ομαλή απενεργοποίηση των εξυπηρετητών σε περίπτωση μεγάλης διακοπής ηλεκτρικού ρεύματος. Οι συγκεκριμένοι έλεγχοι πραγματοποιούνται με την διακοπή παροχής ηλεκτρικού ρεύματος για μικρά και μεγάλα χρονικά διαστήματα αντίστοιχα.

4.10 Έλεγχος Υψηλής Διαθεσιμότητας δικτύου

Πραγματοποιείται έλεγχος υψηλής διαθεσιμότητας στην παροχή δικτυακών υπηρεσιών. Κάποιες από τις ευρυζωνικές γραμμές που χρησιμοποιούνται για την σύνδεση του δικτύου Wi-Fi με το Διαδίκτυο μπορεί να παρουσιάσουν βλάβη. Στις περιπτώσεις αυτές, δεν πρέπει να σταματάει η παροχή υπηρεσιών Διαδικτύου στους τελικούς χρήστες, αλλά η πρόσβαση στο Διαδίκτυο θα πρέπει να πραγματοποιείται μέσω των υπόλοιπων ευρυζωνικών γραμμών που συνεχίζουν να λειτουργούν. Προκειμένου να ελεγχθεί η υψηλή διαθεσιμότητα πρόσβασης στο Διαδίκτυο, πραγματοποιούνται προσομοιώσεις διακοπής λειτουργίας κάποιων ευρυζωνικών γραμμών (ADSL), έτσι ώστε να διασφαλιστεί η ενεργοποίηση και η αποδοτικότητα της διαδικασίας fail-over και η κίνηση από και προς το Διαδίκτυο να πραγματοποιηθεί από τις εναπομείνουσες γραμμές. Στη συνέχεια οι γραμμές θα επανέλθουν στη σωστή λειτουργία για να διασφαλιστεί ότι συμμετέχουν κανονικά και σύμφωνα με τις διαδικασίες διαμοιρασμού φόρτου (load balancing) στην προσπέλαση του Διαδικτύου.

4.11 Έλεγχος Υπηρεσίας Διαπίστευσης

Πραγματοποιείται έλεγχος της υπηρεσίας διαπίστευσης (authentication) των χρηστών προκειμένου να διασφαλιστεί ότι μόνο διαπιστευμένοι χρήστες μπορούν να κάνουν χρήση των διαδικτυακών

υπηρεσιών. Ο έλεγχος αυτός είναι αναγκαίος για λόγους ασφάλειας των χρηστών και του ίδιου του συστήματος. Επίσης, μέρος της υπηρεσίας διαπίστευσης είναι και η παρουσίαση του συμφωνητικού χρήσης και της προειδοποίησης για τη μη υποστήριξη ασφαλών συνδέσεων στο επίπεδο ασύρματου δικτύου. Ο έλεγχος πραγματοποιείται με την προσπάθεια σύνδεσης στο ασύρματο δίκτυο μη διαπιστευμένων χρηστών.

4.12 Έλεγχος Τήρησης Στατιστικών Χρήσης

Πραγματοποιείται έλεγχος της Τήρησης Στατιστικών (accounting) στοιχείων της χρήσης του δικτύου. Τα στατιστικά στοιχεία χρησιμεύουν στην εξαγωγή συμπερασμάτων για τη χρήση των παρεχομένων υπηρεσιών και την μελλοντική τους βελτίωση, ενώ βοηθούν στην επίλυση τυχόν προβλημάτων ασφαλείας. Ο έλεγχος πραγματοποιείται με σύνδεση στον εξυπηρετητή AAA (Authentication - Authorization - Accounting) και παρατήρηση των εκτελούμενων ενεργειών στις περιπτώσεις σύνδεσης και αποσύνδεσης χρηστών στο/από το ασύρματο δίκτυο.

5 Βιβλιογραφία

- [1] «**Ασύρματο Μητροπολιτικό Δίκτυο Αθηνών**», <http://wiki.awmn.org/>, ημερομηνία ανάκτησης ιστοσελίδας 02-2005
- [2] «**Ασύρματο Δίκτυο Θεσσαλονίκης**», <http://www.salonicawireless.net/>, ημερομηνία ανάκτησης ιστοσελίδας 02-2005
- [3] «**Κανονισμός Εκχώρησης Μεμονωμένων Ραδιοσυχνοτήτων σε Σταθμούς Ραδιοεπικοινωνιών για Ιδία Χρήση**» (ΦΕΚ/895/Β/16-7-2002), http://www.eett.gr/gr_pages/telec/kanonistika_keimena/APOF2002/APOF254-72FEK.pdf
- [4] «**Εθνικός Κανονισμός Κατανομής Ζωνών Συχνοτήτων (ΕΚΚΖΣ)**», <http://www.yme.gov.gr/pressdetail.php?section=167&pressid=134&sessdata=62a9ceb5914db138cf1d8e80bc7a06c5>
- [5] «**Πίνακας Κατανομής Ζωνών Συχνοτήτων**», http://www.yme.gov.gr/imagebank/articles/rctl134_8_1099052244.zip
- [6] «**Τροποποίηση "Κύρωσης Ελληνικού Κανονισμού Κατανομής Ζωνών Συχνοτήτων (ΕΚΚΖΣ)"**» Αριθ. 39085/1586, ΦΕΚ 979/Β/03, http://www.eett.gr/gr_pages/telec/RadioEquip/FEK979.pdf
- [7] «**Exploiting and Protecting 802.11b Wireless Networks**», <http://www.extremetech.com/article2/0,1558,11388,00.asp>, ημερομηνία ανάκτησης ιστοσελίδας 02-2005
- [8] Alexander, Bruce «**802.11 Wireless Network Site Surveying and Installation**», Cisco Press, 2004, ISBN 1-58705-164-8
- [9] «**Deploying WLAN in outdoor networks**», http://www.radionet.com/_FileRoot/318025.pdf, ημερομηνία ανάκτησης ιστοσελίδας 02-2005

Επιστημονικός υπεύθυνος έργου

Κοζύρης Νεκτάριος, Επ. Καθ. ΕΜΠ (nkoziris@cslab.ece.ntua.gr)

Ομάδα Υλοποίησης ΕΠΙΣΕΥ

Μερεκούλιας Βασίλης (merek@netmode.ece.ntua.gr)

Σωτηρόπουλος Αριστείδης, Δρ. (sotirop@cslab.ece.ntua.gr)

Χαζάπης Αντώνης (chazapis@cslab.ece.ntua.gr)

Τηλ: +30 210 772 2279, 772 1531

Fax: +30 210 772 1292