Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακή Διατριβή
στα Πληροφοριακά Συστήματα

Διερεύνηση Λειτουργίας Ασύρματων Τοπικών Δικτύων (WLAN)

Γεώργιος Ιωάννου

Επιβλέπων Καθηγητής
Σταύρος Σταύρου

Φεβρουάριος 2012

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Διερεύνηση Λειτουργίας Ασύρματων Τοπικών Δικτύων (WLAN)

Γεώργιος Ιωάννου

Επιβλέπων Καθηγητής
Σταύρος Σταύρου

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε
προς μερική εκπλήρωση των απαιτήσεων για απόκτηση

μεταπτυχιακού τίτλου σπουδών
στα Πληροφοριακά Συστήματα

από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών
του Ανοικτού Πανεπιστημίου Κύπρου

Φεβρουάριος 2012

Περίληψη

Η ασύρματη σύνδεση με ένα δίκτυο και η ταυτόχρονη επικοινωνία με απομακρυσμένους κόμβους χωρίς προβλήματα, είναι άμεση ανάγκη για τα σημερινά ασύρματα δίκτυα. Τα προβλήματα αυτά έχουν διάφορες αιτίες. Μπορεί να παρουσιαστούν λόγω υπερφόρτωσης ενός δικτύου λόγω μεγάλης διακίνησης πληροφοριών (υψηλό Bandwidth), ή λόγω παρεμβολών που μπορούν να υπάρξουν σε ένα ασύρματο δίκτυο, ή λόγω μεγάλης απόστασης ενός κόμβου από το Access Point (AP) κλπ. Οι συνέπειες αυτών των προβλημάτων είναι η κακή ποιότητα του σήματος (QoS) μεταξύ των χρηστών του ασύρματου δικτύου και του απομακρυσμένου κόμβου.

Η διατριβή αποσκοπεί στην διερεύνηση της λειτουργίας (χαρακτηριστικών) ασύρματων τοπικών δικτύων (WLAN) και τον έλεγχο των προϋποθέσεων (packet loss) που πρέπει να υπάρχουν, για μεταφορά ενός ασύρματου χρήστη σε ένα άλλο ασύρματο δίκτυο.

Σκοπός αυτής της διατριβής είναι η δημιουργία ενός συστήματος που θα συλλέγει και θα αποθηκεύει την καταγραμμένη απόδοση (QoS), μεταξύ ασύρματων χρηστών και του Router (AP-Network link) ενός WLAN. Η απόδοση αυτή καταγράφεται σε μια Βάση Δεδομένων (ΒΔ). Βάσει αυτής της απόδοσης θα διερευνούνται τα χαρακτηριστικά των ασύρματων τοπικών δικτύων (WLAN). Επίσης θα ελέγχεται αν υπάρχουν οι προϋποθέσεις (μεγάλο packet loss), για μεταφορά κάποιου χρήστη σε άλλο ασύρματο δίκτυο.

Η μεθοδολογία που ακολουθήθηκε είναι η ακόλουθη:

1. Διεξαγωγή μετρήσεων με το πρόγραμμα iperf, για την αξιολόγηση της απόδοσης του δικτύου.

2. Υλοποίηση λογισμικού για την καταγραφή της απόδοσης του δικτύου και της λήψης απόφασης για Handover.

3. Βιβλιογραφική μελέτη για τα ασύρματα δίκτυα 2ης και 3ης γενιάς (GSM,GPRS,,UMTS), την IP-Κινητικότητα (IPv4 & IPv6) , για τα ασύρματα τοπικά δίκτυα (WLAN) καθώς και για το Handover.

Τα αποτελέσματα έδειξαν ότι οι βασικοί παράγοντες που επηρεάζουν την ποιότητα επικοινωνίας (QoS) σε ένα ασύρματο δίκτυο (WLAN) είναι τρείς:

1. Το traffic intensity (αL/R<=1)

2. η ένταση του σήματος (signal strength) μεταξύ του Access Point του δικτύου και του ασύρματου χρήστη.

3. Το μέγεθος του Buffer του Router. Όσο πιο μεγάλο Buffer, τόσο λιγότερο packet loss έχουμε.

Summary

The wireless connection to a network and simultaneous communication with remote nodes without problems is a necessity need for today's wireless networks. These problems derive from several causes. They may occur due to an overload, due to heavy network traffic information (High Bandwidth), due to interference that can occur in a wireless network, or even because of a long distance of the node from the Access Point (AP), etc. The consequences of these problems is poor signal quality (QoS), between users of the wireless network and the remote node.

The thesis aims to study the operation (features) of wireless local area networks (WLAN) and control conditions (packet loss) to be there, in order to transfer a wireless user to another wireless network.

The aim of this thesis is to create a system that will collect and store the recorded performance (QoS), between wireless users and the Router (AP-Network link) of a WLAN. This performance is stored in a database (DB). Taking into consideration this performance, the characteristics of wireless local area networks (WLAN) will be explored and checked, if there are the necessary conditions (large packet loss), to transfer a wireless user to another wireless network.

The methodology used is the following:

1. Perform measurements with the program iperf, to evaluate network performance.

2. Implementation of software for recording network performance and decision for Handover.

3. Literature study for wireless networks second and third generation (GSM, GPRS, UMTS), the IP-Mobility (IPv4 & IPv6), for wireless local area networks (WLAN) and the Handover as well.

The results showed that key factors affecting communication quality (QoS) in a wireless network (WLAN) are three:

1. the traffic intensity (aL / R <= 1),

2. the signal strength (signal strength) between the Network Access Point and the wireless user

3. The significant third key factor is the size of the Buffer of the Router. The larger Buffer, the less packet loss.

Ευχαριστίες

Καταρχήν, θα ήθελα να ευχαριστήσω τον επιβλέπων καθηγητή μου, Δρ. Σταύρο Σταύρου, ο οποίος μου παρείχε την άρτια επιστημονική καθοδήγηση για την ολοκλήρωση της παρούσας μεταπτυχιακής εργασίας.

Επίσης θα ήθελα να ευχαριστήσω τον υποψήφιο διδάκτορα Ευαγόρα Χαραλάμπους για την άρτια συνεργασία που είχαμε, για την επιτυχή κατάληξη αυτής της εργασίας.

Θα ήθελα επίσης να ευχαριστήσω την καθηγήτριά μου στο μεταπτυχιακό πρόγραμμα του τμήματος Πληροφοριακά Συστήματα του Ανοικτού Πανεπιστημίου Κύπρου Δρ. Ιωσηφίνα Αντωνίου για τις χρήσιμες συμβουλές της.

Τέλος, θα ήθελα να ευχαριστήσω την Οικογένειά μου για την υπομονή που έδειξε όλο αυτόν τον καιρό.

Περιεχόμενα

Κεφάλαιο 1
Εισαγωγή

Η ραγδαία ανάπτυξη της τεχνολογίας έχει επιφέρει και την ανάπτυξη των δικτύων Η.Υ. ούτως ώστε το Internet να έχει διαδοθεί και εξαπλωθεί σε όλες τις ηπείρους, από τη μια γωνιά του πλανήτη μέχρι την άλλη (Εικόνες 1.1- 1.4).

1.1 Ορισμός του Προβλήματος

Τα τοπικά δίκτυα (WLAN) μιας γεωγραφικής περιοχής, τα οποία μπορεί να υπάρχουν στα σπίτια μας ή να ανήκουν σε εταιρίες, πανεπιστήμια, οργανισμούς, κρατικές υπηρεσίες, καφετέριες, έχουν τη δυνατότητα να παρέχουν ασύρματη σύνδεση με το διαδίκτυο. Ένα αρκετά σοβαρό πρόβλημα που προκύπτει είναι η κακή ποιότητα του σήματος (QoS), μεταξύ ενός ή πολλών χρηστών που ανήκουν σε ένα ασύρματο τοπικό δίκτυο (WLAN) και ενός κινητού IP Server (MIPS) στο διαδίκτυο, με αποτέλεσμα την διακοπή της σύνδεσης.

1.2 Σκοπός της Μεταπτυχιακής Διατριβής

Σκοπός αυτής της μεταπτυχιακής διατριβής είναι η δημιουργία ενός συστήματος που θα συλλέγει και θα αποθηκεύει την καταγραμμένη απόδοση (QoS), μεταξύ των ασύρματων χρηστών και του Router (AP-Network link) ενός WLAN, σε μια Βάση Δεδομένων (ΒΔ). Βάσει αυτής της απόδοσης θα διερευνά τα χαρακτηριστικά ενός ασύρματου δικτύου (WLAN). Θα ελέγχεται επίσης αν υπάρχουν οι προϋποθέσεις (packet loss), για μεταφορά κάποιου χρήστη σε άλλο ασύρματο δίκτυο.

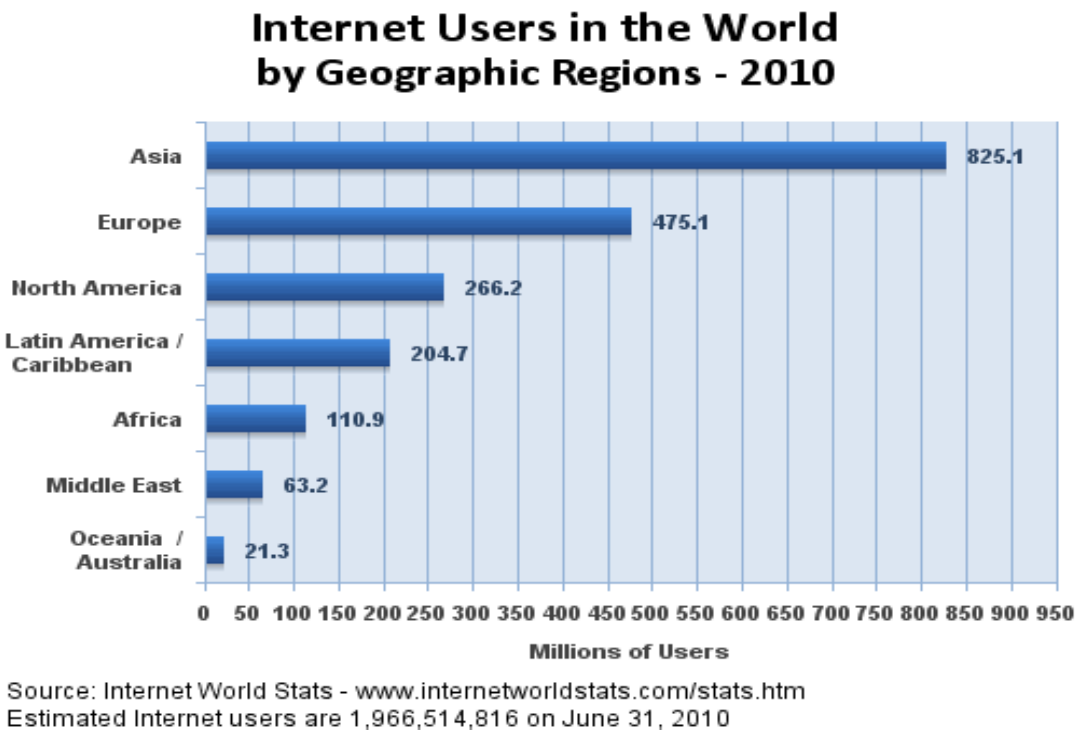
Στα πλαίσια αυτής της μεταπτυχιακής διατριβής, εκτός από την διερεύνηση των χαρακτηριστικών των τοπικών ασύρματων δικτύων (WLAN) και των συνθηκών που πρέπει να υπάρχουν για ποιοτικό σήμα (QoS), θα ελέγχεται επίσης αν υπάρχουν οι προϋποθέσεις (packet loss) για μεταφορά κάποιου χρήστη σε άλλο ασύρματο δίκτυο..

1.3 Η χρήση του Internet

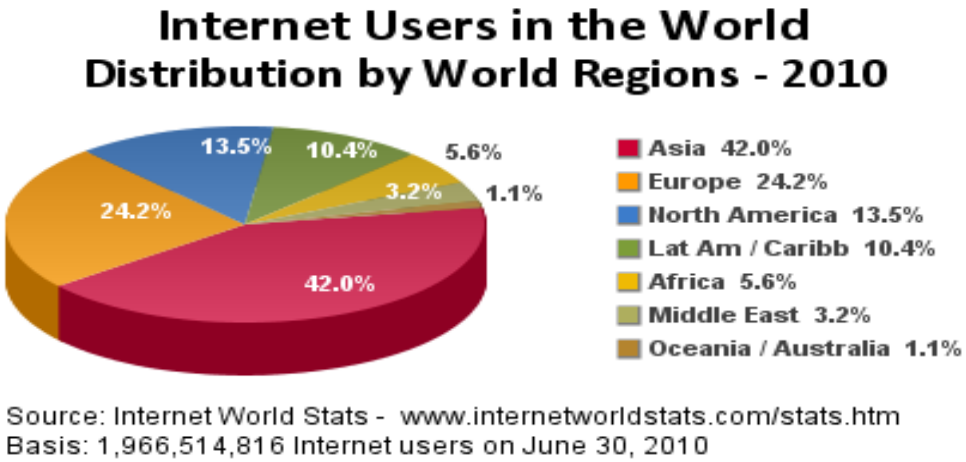
Η ανάπτυξη του Διαδικτύου έχει επιφέρει τεράστιες αλλαγές στον κόσμο των υπολογιστών και των επικοινωνιών. Την τελευταία πενταετία έχει παρατηρηθεί μια σημαντική ανάπτυξη στην ευρυζωνική κάλυψη (ευρυζωνικές συνδέσεις) στη ευρωπαϊκή ένωση λόγω της μεγάλης αύξησης του πληθυσμού (αριθμού των πολιτών) με πρόσβαση στο διαδίκτυο και γενικότερα της αύξησης στη διείσδυση και χρήση online υπηρεσιών μέσω διαδικτύου, τόσο στην Ευρωπαϊκή Ένωση (Ε27) όσο και στην Κύπρο. Στην ΕΕ, στα νοικοκυριά με σύνδεση στο διαδίκτυο, το ποσοστό των νοικοκυριών με ευρυζωνική σύνδεση έφτασε στο 80% το 2008 (από 48% το 2005) και το ποσοστό των πολιτών που χρησιμοποίει συχνά το διαδίκτυο (σχεδόν κάθε μέρα) αυξήθηκε από 29% στο 43% την ίδια περίοδο [01]. Στατιστικά στοιχεία [02] δείχνουν πως σχεδόν 2 δισεκατομμύρια άνθρωποι χρησιμοποιούν αυτή τη στιγμή το Internet, αριθμός που αντιπροσωπεύει το 28% του παγκόσμιου πληθυσμού.

WORLD INTERNET USAGE AND POPULATION STATISTICS						
World Regions	Population (2010 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Growth 2000-2010	Users % of Table
Africa	1,013,779,050	4,514,400	110,931,700	10.9 %	2,357.3 %	5.6 %
Asia	3,834,792,852	114,304,000	825,094,396	21.5 %	621.8 %	42.0 %
Europe	813,319,511	105,096,093	475,069,448	58.4 %	352.0 %	24.2 %
Middle East	212,336,924	3,284,800	63,240,946	29.8 %	1,825.3 %	3.2 %
North America	344,124,450	108,096,800	266,224,500	77.4 %	146.3 %	13.5 %
Latin America/Caribbean	592,556,972	18,068,919	204,689,836	34.5 %	1,032.8 %	10.4 %
Oceania / Australia	34,700,201	7,620,480	21,263,990	61.3 %	179.0 %	1.1 %
WORLD TOTAL	6,845,609,960	360,985,492	1,966,514,816	28.7 %	444.8 %	100.0 %

Εικόνα 1.1: Στατιστική χρήσης του Internet και του πληθυσμού της Γης. 30 Ιουνίου 2010 [02]



Εικόνα 1.2 : Η χρήση του Internet ανά γεωγραφική περιοχή [02]



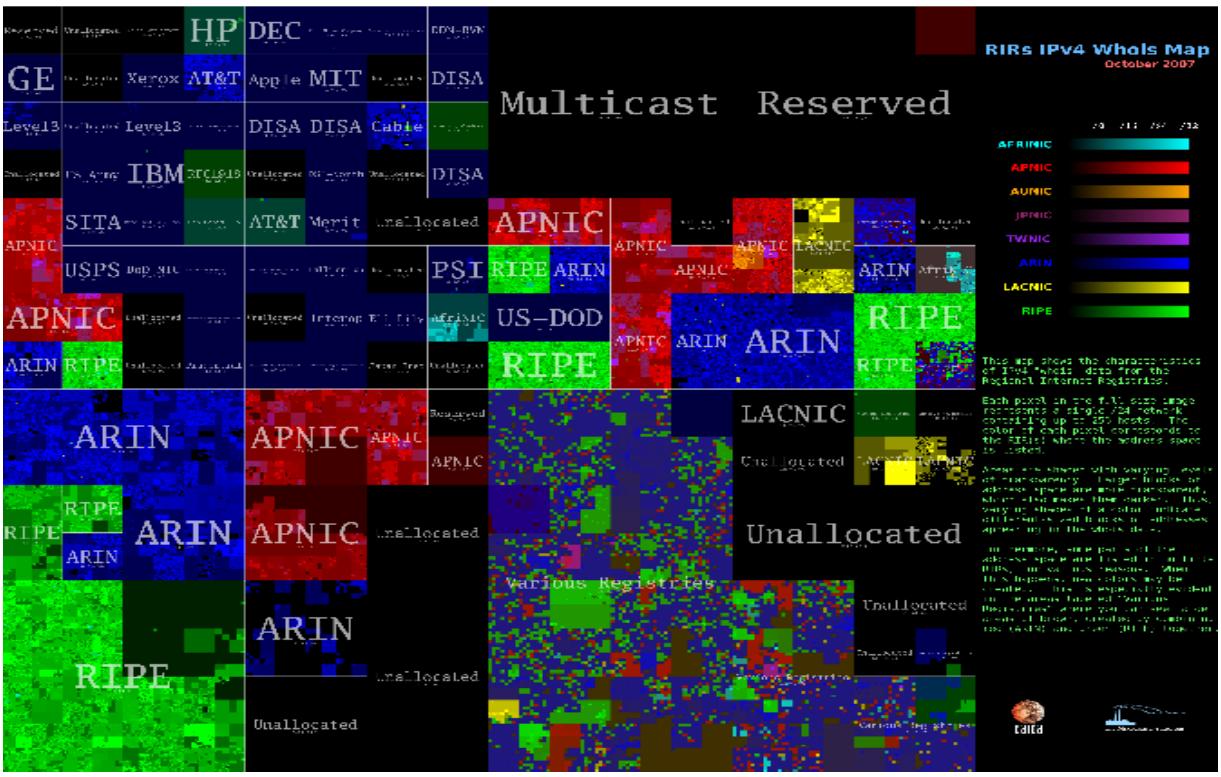
Εικόνα 1.3 : Χρήση του Internet παγκοσμίως χωρισμένη ανά περιοχές [02]

Στην Εικόνα 1.3 παρατηρούμε την ραγδαία αύξηση των χρηστών στο διαδίκτυο. Μόνο η Ασία έχει το 42% των χρηστών παγκοσμίως λόγω του ότι είναι και η πολυπληθέστερη ήπειρος. Δεύτερη ήπειρος στη σειρά έρχεται η Ευρώπη με 24%. Αρκετά χαμηλά ποσοστά έχει η Μέση Ανατολή με 3.2% και η Αφρική με μόνο 5.6% που αναλόγως του πληθυσμού της διαθέτει ένα πολύ χαμηλό ποσοστών χρηστών του διαδικτύου. Το συμπέρασμα που εξάγεται από αυτά τα στοιχεία είναι ότι το Internet έχει πλέον καθιερωθεί ως το δημοφιλέστερο μέσο επικοινωνίας , άντλησης πληροφοριών και ενημέρωσης όλων των ανθρώπων παγκοσμίως. Μόνο η Αφρική υστερεί συγκριτικά. Όσο αυξάνεται η χρήση του internet τόσο αυξάνονται και οι απαιτήσεις των χρηστών**.** Η ραγδαία ανάπτυξη της τεχνολογίας στις επικοινωνίες έχει δημιουργήσει και διάφορα νέα είδη δικτύων. Π.χ WiFi/WiMAX/GSM/UMTS.

Το πρωτόκολλο IP χρησιμοποιείται σε όλα αυτά τα δίκτυα και αποτελεί μαζί με το TCP την καρδιά της οικογένειας των internet πρωτοκόλλων. Το πρωτόκολλο IP είναι τυποποιημένο από την Internet Engineering Task Force (IETF). Το IP χρησιμοποιείται σε ετερογενείς συσκευές δικτύων τρίτης γενιάς 3G για πρόσβαση στο internet [03]. Το IPv4 χρησιμοποιείται σήμερα στο internet σαν το κύριο πρωτόκολλο χρήσης διευθύνσεων. Εντούτοις όμως άρχισε να χρησιμοποιείται και το IPv6 το οποίο θα λύσει πολλά προβλήματα που υπάρχουν σήμερα με τη χρήση του IPv4. Ένα σοβαρό πρόβλημα που υπάρχει είναι η έλλειψη διευθύνσεων. Με το IPv4 μπορούμε θεωρητικά να έχουμε 2^{32} IPv4 διευθύνσεις. Με τον αυξανόμενο όμως αριθμό των users στο internet και με την προκλητική παρακράτηση διευθύνσεων από διάφορα πανεπιστήμια και εταιρίες της Αμερικής χωρίς να τις χρησιμοποιούν (εικόνα 1.5) , οι διευθύνσεις αυτές

έχουν μειωθεί στο ελάχιστο [21]. Έτσι η χρήση του IPv6 που αυξάνει το εύρος των διευθύνσεων σε 2^{128} έρχεται να λύσει αυτό το πρόβλημα.

Εικόνα 1.4: Πίνακας κατανομής IPv4 2009-01-01 to 2009-11-09. [02]



Εικόνα 1.5: Address blocks are labeled based on IANA's list of IPv4 allocations [06]

Regional Internet Registries: RIPE, APNIC, ARIN, LACNIC, and AfriNIC.

Με τον αυξανόμενο όμως αριθμό των users στο internet και με την προκλητική παρακράτηση διευθύνσεων από διάφορα πανεπιστήμια και εταιρίες της Αμερικής χωρίς να τις χρησιμοποιούν (εικόνα 1.5) , οι διευθύνσεις αυτές έχουν μειωθεί στο ελάχιστο (εικόνα 1.6). Παρατηρούμε ότι το χρώμα μπλε (ARIN) στην εικόνα 1.5 είναι το κυρίαρχο.

RIPE : Network Coordination Center

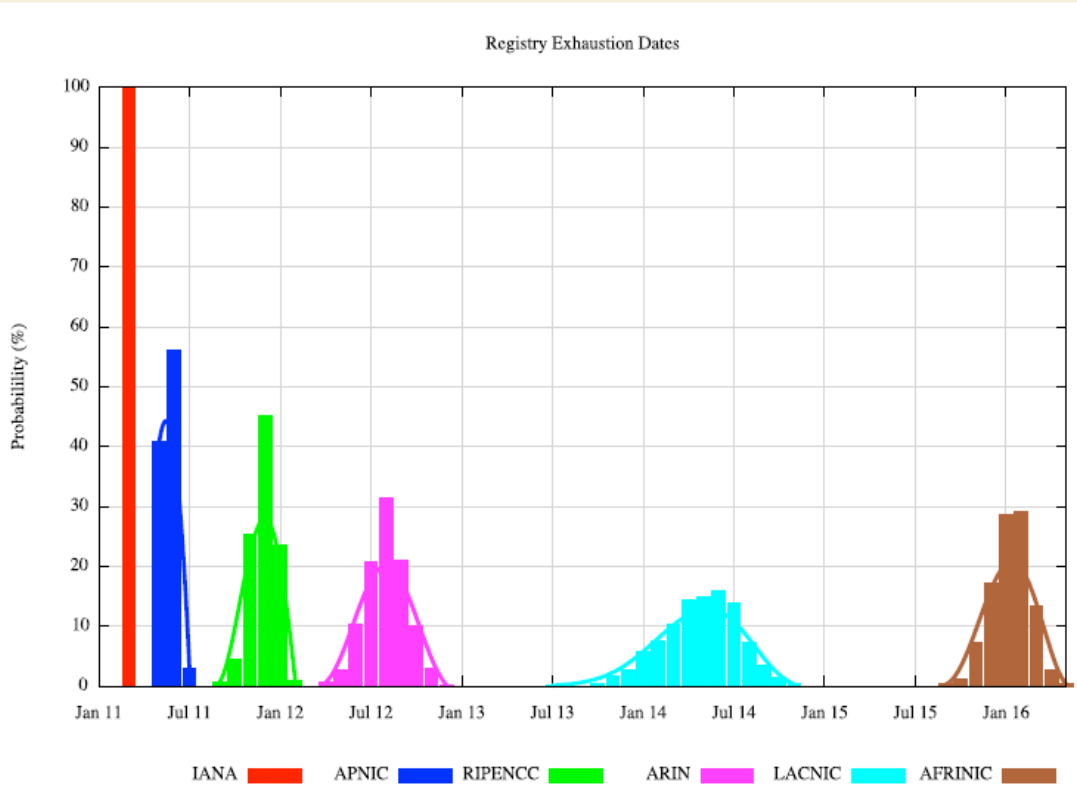
AfriNIC: African Network Information Center

APNIC: Asia Pacific Information Center

ARIN : American Registry for Internet Numbers

LACNIC: Latin American and Caribbean Internet Addresses Registry

for each RIR and the associated variance of these so-called "exhaustion times" is shown in the figure below.

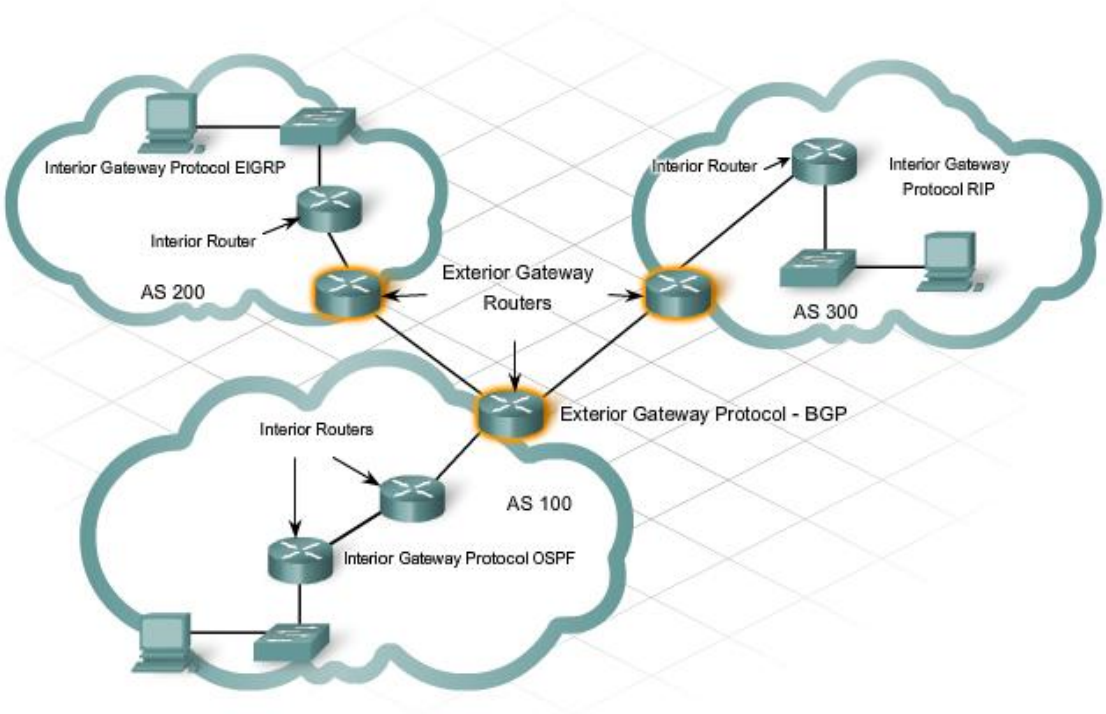


Εικόνα 1.6: The remaining pools of IPv4 address space [23]

Στην εικόνα 1.6 παρατηρούμε ότι στο Regional Internet Registries APNIC, οι IPv4 διευθύνσεις μέχρι τον Απρίλη ή Μάιο του 2011 θα εξαντληθούν. Ακολούθως υπολογίζεται ότι και για τον ARIN οι IPv4 διευθύνσεις θα εξαντληθούν μέχρι το τέλος του 2011.

Η μεγάλη αύξηση των portable computers σε συνδυασμό με την ολοένα αυξανόμενη παροχή wireless υπηρεσιών έχει κάνει τη χρήση πρωτοκόλλων MIPv4, MIPv6 απαραίτητη. Αυτά τα πρωτόκολλα επιτρέπουν σε κινητούς κόμβους να διατηρούν την ίδια IP διεύθυνσή τους ανεξάρτητα από την θέση τους [02].

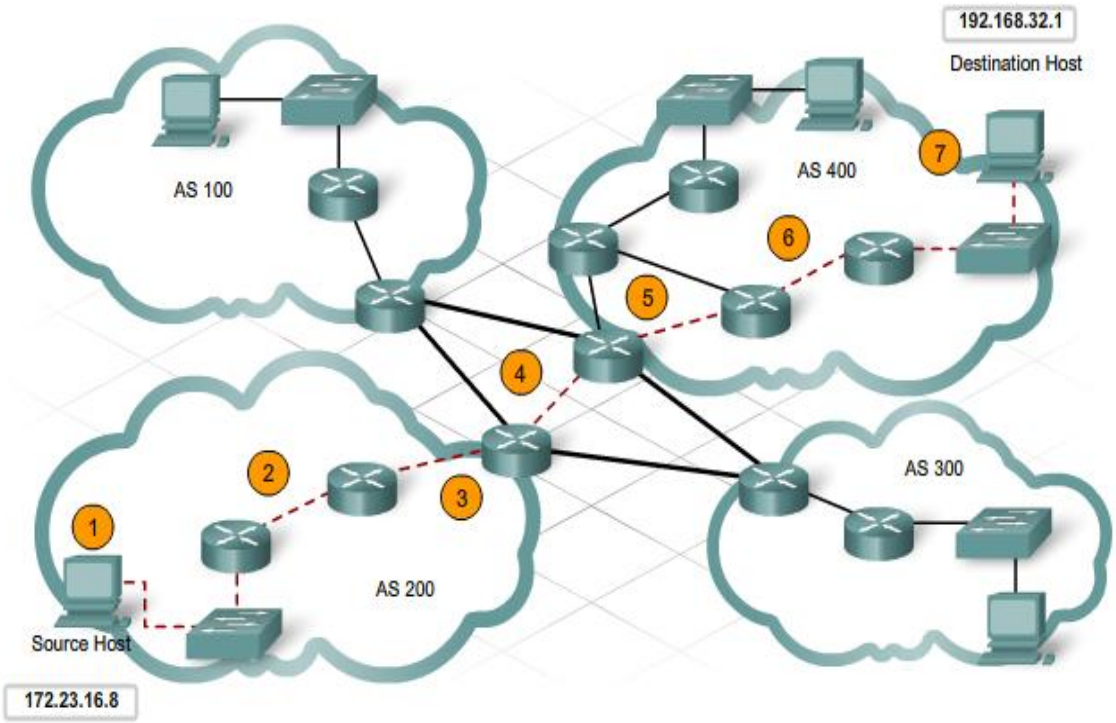
Η σωστή δρομολόγηση στο Internet βασίζεται αποκλειστικά στις IP διευθύνσεις. Κάθε συσκευή στο Internet έχει την δική της μοναδική IP διεύθυνση και με αυτό τον τρόπο μπορεί να αναγνωριστεί και να επικοινωνήσει με άλλες συσκευές (Εικόνα 8). Κάθε IPv4 διεύθυνση αποτελείται από 32 bits ή 4 Bytes. Ο κάθε κόμβος βρίσκεται στο δίκτυο στο οποίο καθορίζεται από την IP διεύθυνσή του. Οι κύριες συσκευές του Internet (Ραχοκοκαλιά του Internet) οι οποίες είναι υπεύθυνες να δρομολογούν τα δεδομένα προς τον σωστό προορισμό ονομάζονται δρομολογητές ή routers. Οι δρομολογητές για να μπορούν να εκτελούν σωστά αυτή την μεταπτυχιακή εργασία, λαμβάνουν υπόψη τους την IP διεύθυνση προορισμού των δεδομένων. Οι δρομολογητές χρησιμοποιούν τα λεγόμενα Routing protocols για να μπορούν να λαμβάνουν αποφάσεις για την καλύτερη διαδρομή (best path) που μπορούν να δρομολογήσουν τα δεδομένα [12].



Εικόνα 1.7: Routing across the Internet A [12]

Το Internet χωρίζεται στην πραγματικότητα σε πολλά αυτόνομα συστήματα (AS-εικόνα 1.7). Ένα αυτόνομο σύστημα είναι ένα σύνολο από πολλά δίκτυα τα οποία ελέγχονται

από μια ενιαία διοικητική αρχή με την ίδια την εσωτερική πολιτική δρομολόγησης. Κάθε AS χαρακτηρίζεται από έναν μοναδικό αριθμό AS (ASN) ο οποίος ελέγχεται και εγγράφεται στο Διαδίκτυο. Αυτόνομα συστήματα μπορεί να είναι οι internet providers , μεγάλοι οργανισμοί που έχουν γραφεία σε διάφορες χώρες και για αυτό το λόγο έχουν δικά τους ASN. Το ίδιο ισχύει και για τράπεζες που τα καταστήματά τους είναι διασκορπισμένα σε διάφορες χώρες με διαφορετικούς internet providers. Η επικοινωνία μεταξύ αυτόνομων συστημάτων γίνεται μέσω των Border Routers. Τα πρωτόκολλα που διακινούν τα δεδομένα μεταξύ των Border Routers (μεταξύ AS) ονομάζονται Exterior Gateway Protocols (π.χ BGP). Τα πρωτόκολλα που διακινούν τα δεδομένα εσωτερικά του κάθε αυτόνομου συστήματος ονομάζονται Interior Gateway Protocols και χρησιμοποιούνται διαφορετικού τύπου πρωτόκολλα δρομολόγησης (π.χ. OSPF, EIGRP,RIP…) [12].

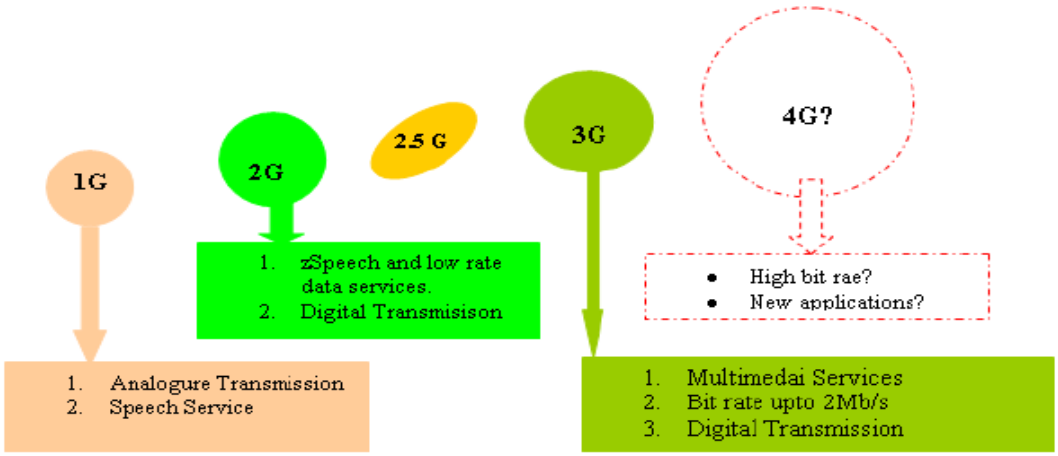


Εικόνα 1.8: Routing across the Internet B [12].

Κεφάλαιο 2
Ετερογενή Δίκτυα

Τα τελευταία χρόνια έχουν σημειωθεί ριζικές αλλαγές στα κυψελοειδή συστήματα κινητής τηλεφωνίας όπως και στη συντριπτική πλειοψηφία των τηλεπικοινωνιακών δικτύων (Cellular Networks) [06].

2.1 Εξέλιξη Κυψελοειδών Δικτύων



Εικόνα 2.1: Evolution of Cellular Networks [25].

Τα ασύρματα δίκτυα 1ης γενιάς μετέδιδαν μόνο αναλογικό σήμα. Σχεδιάστηκαν και λειτούργησαν στα τέλη της δεκαετίας του 70 στην Αμερική και Ιαπωνία. Στην Ευρώπη εμφανίστηκαν στις αρχές της δεκαετίας του 80. Οι δυνατότητές τους ήταν λίγες και βασικά μετεδίδετο μόνο φωνή. Ένα βασικό χαρακτηριστικό των συστημάτων 1ης γενιάς, ήταν ότι τόσο ο πομπός όσο και ο δέκτης εξέπεμπαν και λάμβαναν αντίστοιχα με χρήση της ίδιας συχνότητας. Όταν ο χρήστης περνούσε έξω από την περιοχή που ήταν η εμβέλεια της κυψέλης, τότε τερματιζόταν η κλήση, αφού δεν ήταν δυνατό να παραμείνει η κλήση ανοιχτή κατά την φάση μετάβασης σε άλλο κύτταρο (handover). Στην συνέχεια εμφανίστηκαν τα ασύρματα δίκτυα 2ης γενιάς (GSM). Εδώ τώρα έχουμε ψηφιακή μετάδοση. Οι χρήστες διαχωρίζονταν με Time Division Multiple Access (TDMA) ή Code Division Multiple Access (CDMA). Στην Ευρώπη εφαρμόστηκε ένα ενιαίο σύστημα το λεγόμενο GSM με περίπου 350 εκατ. Χρήστες. Το GSM ξεκίνησε να λειτουργεί στην ζώνη των 800-900 MHz. Με το GSM ξεκίνησε περιορισμένη πρόσβαση στο internet και η αποστολή σύντομων μηνυμάτων.

Η ανάγκη για μεγαλύτερη πρόσβαση προς το internet έφερε μια νέα γενιά δικτύων, την λεγόμενη γενιά 2.5. Σε αυτή την νέα τεχνολογία που είχε σαν βάση της τον εξοπλισμό της 2ης γενιάς, υπήρχε η δυνατότητα χρήσης πολλών υπηρεσιών του internet, όπως π.χ. πλοήγηση στο internet, αποστολή μηνυμάτων (e-mails) κλπ. Με την γενιά 2.5 προέκυψαν και νέα συστήματα με πιο διαδεδομένο το General Packet Radio Service (GPRS). Μερικές εφαρμογές ακολουθούν στον πίνακα πιο κάτω.

ΕΦΑΡΜΟΓΗ	**ΠΑΡΑΔΕΙΓΜΑ ΕΦΑΡΜΟΓΗΣ**
WWW	Ανάκτηση σελίδων
FTP	Μεταφορά αρχείων
E-mail	Αποστολή μηνυμάτων
Telnet	Πρόσβαση σε απομακρυσμένα τερματικά
Video	Τηλεσυνδιάσκεψη

Πίνακας 2.1: Πίνακας Εφαρμογών

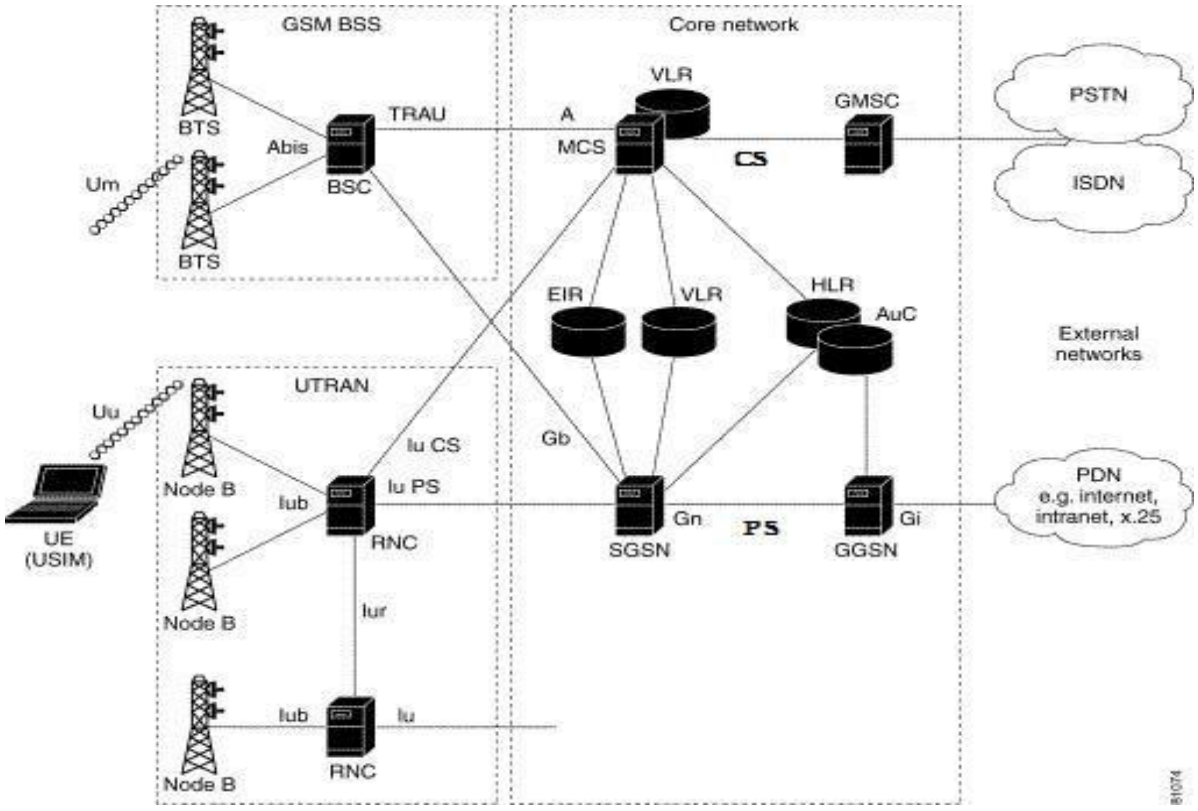
Ένα σημαντικό πλεονέκτημα του GPRS είναι ότι δεσμεύει τους πόρους του δικτύου μόνο όταν υπάρχουν δεδομένα που πρέπει να μεταδοθούν.

Με την εμφάνιση της 3ης γενιάς ασύρματων δικτύων έχουμε την χρήση περισσοτέρων υπηρεσιών στο internet όπως Voice over Internet Protocol (VoIP), το κατέβασμα μουσικής καθώς και άλλες υπηρεσίες. Οι υπηρεσίες αυτές είναι υπηρεσίες internet καθώς και υπηρεσίες πολυμέσων (multimedia) με μεγάλες ταχύτητες μετάδοσης. Τα πιο βασικά συστήματα 3ης γενιάς είναι, το Universal Mobile Telecommunications System (UMTS-Ευρώπη), που είναι μια αναβάθμιση του GSM, το CDMA2000 (USA). Το UMTS αποτελείται από τον συνδυασμό GSM (2G δίκτυο μεταγωγής κυκλώματος – Circuit Switch CS) και το GPRS (2.5G δίκτυο – Packet Switch – PS). Όταν έχουμε υπηρεσίες φωνής, τις εκτελεί το GSM ενώ όταν πρόκειται για υπηρεσίες δεδομένων τις εκτελεί το GPRS (PS).

Το σύστημα UMTS αποτελείται από τα εξής μέρη [28]:

1. Το UTRAN (Σύστημα ραδιοπρόσβασης) το οποίο χωρίζεται επίσης στους σταθμούς πρόσβασης Node B και στον RNC (Radio Network Controller). Αντίστοιχα οι ονομασίες στους 2G σταθμούς είναι BTS και BSC.

2. Το δίκτυο κορμού CN (Core Network), το οποίο αποτελείται από το CS και το PS δίκτυο.



Εικόνα 2.2: Συστατικά μέρη συστήματος UMTS [28].

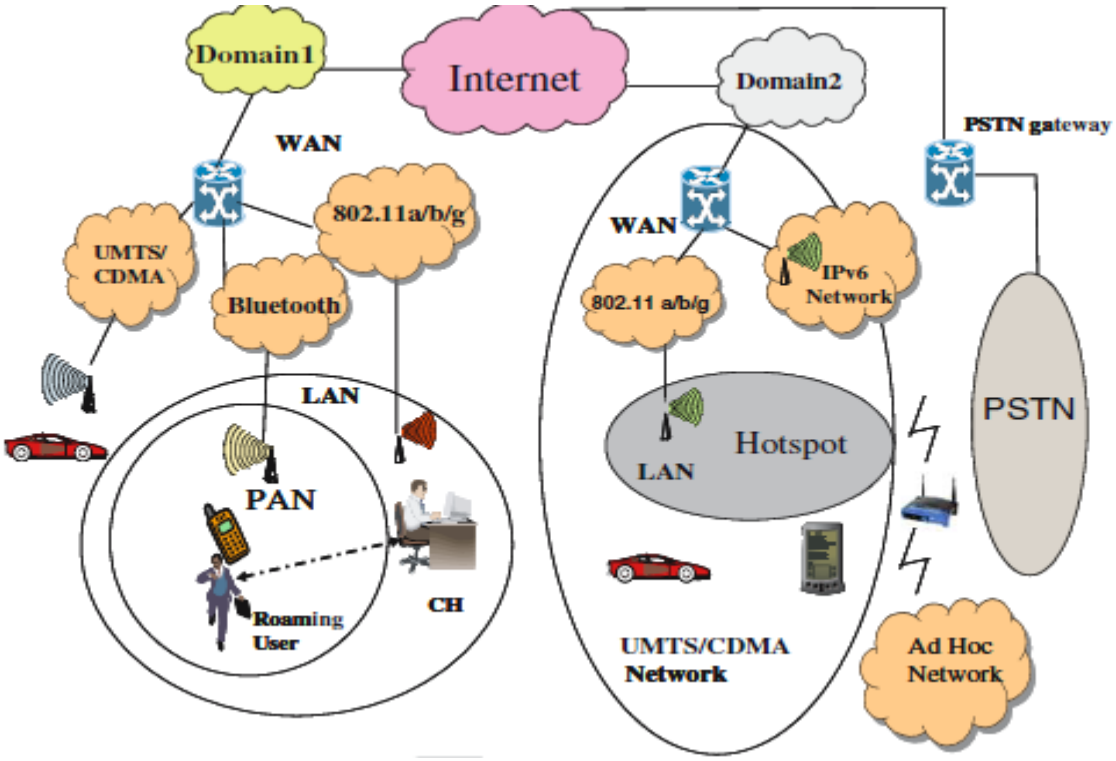
Στο δίκτυο CS, πολλοί RNC (ή BTS) είναι ενωμένοι σε ένα Mobile Switching Center (MSC). Το MSC μεταξύ άλλων διαχειρίζεται τη βάση δεδομένων (ΒΔ) Visitor Location Register (VLR). Σε αυτή την ΒΔ καταγράφονται οι χρήστες που βρίσκονται στη περιοχή του MSC. Επίσης οι MSC, ενημερώνουν τη κεντρική βάση δεδομένων HLR (Home Location Register) για αυτούς τους χρήστες. Η HLR φυλάει πληροφορίες για όλους τους χρήστες και συνεργάζεται με το Authentication Centre (AuC). Το AuC είναι υπεύθυνο για την πιστοποίηση αυθεντικότητας και τα δικαιώματα πρόσβασης του κάθε συνδρομητή. Τέλος μέσω της GMSC (Gateway - Mobile Switching Center) συνδέονται οι MSC στο PSTN δίκτυο.

Στο δίκτυο PS, πολλοί RNC είναι ενωμένοι σε ένα Serving GPRS Support Node (SGSN). Οι SGSN με τη σειρά τους, ενώνονται μέσω των πυλών Gateway GPRS Support Node (GGSN) στα δίκτυα δεδομένων Packet Data Network (PDN). Οι SGSN παραλαμβάνουν/παραδίδουν πακέτα από/προς τους RNC και τα δρομολογούν στο CN. Επίσης είναι συνδεδεμένοι με διάφορες ΒΔ, όπως με την ΒΔ VLR για τοπικό έλεγχο εντοπισμού θέσης (location), με την ΒΔ HLR που φυλάει πληροφορίες για όλους τους χρήστες, καθώς και με την AuC, για την πιστοποίηση αυθεντικότητας και τα δικαιώματα πρόσβασης του κάθε συνδρομητή και τέλος με την ΒΔ EIR που έχει καταγραμμένες πληροφορίες για τα κλεμμένα κινητά και τον αποκλεισμό τους από τις επικοινωνίες.

Τα δίκτυα 3G κινητής Τηλεφωνίας μπορούν να καλύψουν μεγάλες γεωγραφικές περιοχές.

Είναι αποδεκτό πλέον ότι η αρχιτεκτονική των ασύρματων δικτύων 4ης γενιάς θα συμπεριλάβει διαφορετικά δίκτυα ασύρματης πρόσβασης, με κοινό στρώμα αναφοράς, το στρώμα δικτύου και το πρωτόκολλο IP που υλοποιείται σ' αυτό. Το επονομαζόμενο κινητό IP (mobile IP) θα παρέχει ενιαία πρόσβαση διαδικτύου στους κινητούς χρήστες.
Σύμφωνα με τον ορισμό της ITU, ετερογενές δίκτυο καλείται ένα δίκτυο μεταγωγής πακέτων ικανό να παρέχει υπηρεσίες, συμπεριλαμβανομένων των υπηρεσιών Τηλεπικοινωνίας και ικανό να αξιοποιεί πολλαπλές ευρυζωνικές, QoS τεχνολογίες μεταφοράς στις οποίες οι σχετιζόμενες με υπηρεσίες λειτουργίες είναι ανεξάρτητες από τις υποκείμενες σχετιζόμενες με μεταφορά τεχνολογίες. Επίσης εξασφαλίζει στους

χρήστες απεριόριστη πρόσβαση σε διαφορετικούς παροχείς υπηρεσιών και υποστηρίζει γενικευμένη κινητικότητα η οποία εξασφαλίζει διαρκή και απανταχού παροχή υπηρεσιών στους χρήστες. Πρακτικά αποτελεί την ενοποίηση της τηλεφωνίας PSTN, των ασύρματων (WiFi/WiMAX/GSM/UMTS) και του δικτύου δεδομένων (Internet) (Εικόνα 2.3).



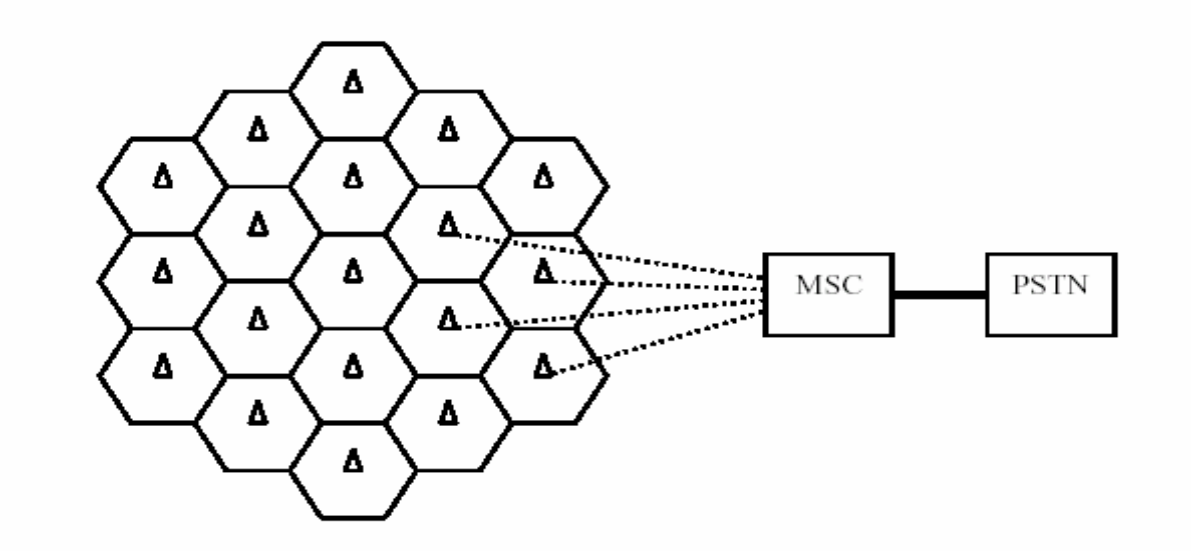
Εικόνα 2.3: Wireless internet roaming scenario [09]

Μελλοντικές συσκευές δικτύου θα μπορούν να στέλλουν/δέχονται voice calls, να στέλλουν/δέχονται πληροφορίες ή να χρησιμοποιούν άλλες υπηρεσίες, ενώ μετακινούνται σε περιοχές γεωγραφικά έξω από το home network τους και δια μέσου ετερογενώνs δικτύων όπως 802.11 (WLAN), WiMAX, CDMA, UMTS, και GSM, μεταξύ ενσύρματων δικτύων όπως xDSL και cable, όπως επίσης μεταξύ packet switched και circuit switched (PSTN) δικτύων [10].

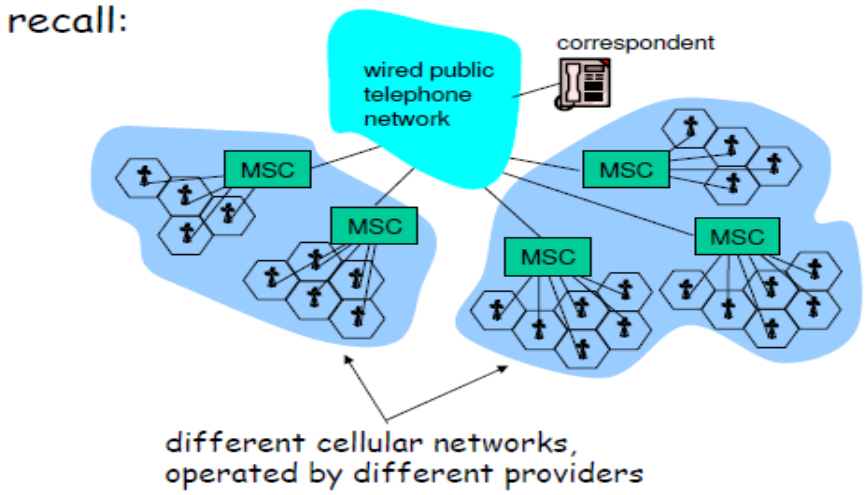
2.2 Συστατικά της Κυψελοειδούς Αρχιτεκτονικής Δικτύου

Σε ένα κυψελοειδές δίκτυο (Εικόνα 2.4), μια περιοχή κάλυψης μιας υπηρεσίας χωρίζεται σε μικρότερες περιοχές σε εξαγωνικό σχήμα, που αναφέρονται ως κύτταρα. Κάθε κύτταρο εξυπηρετείται από ένα σταθμό βάσης. Ο σταθμός βάσης είναι σταθερός.

Ο σταθμός βάσης μπορεί να επικοινωνεί με κινητούς σταθμούς, όπως κινητά τηλέφωνα που χρησιμοποιούν πομποδέκτη με τις ραδιοσυχνότητες του. Ο σταθμός βάσης είναι συνδεδεμένος με το κινητό κέντρο μεταγωγής (MSC), το οποίο με τη σειρά του, συνδέεται με το δημόσιο τηλεφωνικό δίκτυο μεταγωγής (PSTN). Το φάσμα των συχνοτήτων που διατίθενται για ασύρματες επικοινωνίες είναι πολύ περιορισμένο. Κάθε κύτταρο έχει έναν ορισμένο αριθμό καναλιών. Για την αποφυγή παρασίτων τα κανάλια που καταχωρούνται σε μία κυψέλη πρέπει να είναι διαφορετικά από τα κανάλια έχουν ανατεθεί σε γειτονικά κελιά της. Ωστόσο, τα ίδια κανάλια μπορούν να επαναχρησιμοποιηθούν από δύο κύτταρα, τα οποία είναι πολύ μακριά μεταξύ τους. Με τη μείωση του μεγέθους των κυττάρων, το κυψελοειδές δίκτυο είναι σε θέση να αυξήσει την ικανότητά του και επομένως, να εξυπηρετεί περισσότερους συνδρομητές.



Εικόνα 2.4: Κυψελοειδές δίκτυο. Κάθε τρίγωνο αντιπροσωπεύει ένα σταθμό βάσης.



Εικόνα 2.5: Components of cellular network architecture [17]

Κάθε κύτταρο (cell) διαθέτει το δικό του σταθμό εδάφους (BTS) ο οποίος στέλλει ή δέχεται σήματα από ένα κινητό σταθμό. Η περιοχή που μπορεί να καλύψει ένα κύτταρο εξαρτάται από πολλούς παράγοντες. Μερικοί βασικοί παράγοντες είναι η ισχύς του σήματος που μεταδίδει ο BTS, η ισχύς του σήματος του κινητού χρήστη που μεταδίδει και το ύψος της αντένας του σταθμού εδάφους. Το mobile switching center (MSC) παίζει ένα σημαντικό ρόλο στα cellular Networks (Εικόνα 2.5). Μερικά καθήκοντα του MSC είναι:

1. User Authorization

2. User accounting (αποφασίζει αν θα επιτραπεί σε μια κινητή συσκευή να ενωθεί με το cellular δίκτυο)

3. Handoff

2.3 Τεχνολογία WiMAX

Οι WiMAX τεχνολογίες ανήκουν στην οικογένεια των IEEE 802.16 standard οι οποίες μπορούν να μεταφέρουν wireless πληροφορίες σε μεγάλο αριθμό χρηστών σε μεγάλη απόσταση. Το 802.16e standard υποστηρίζει mobility σε ταχύτητες 70-80 μίλια την ώρα. Το WiMAX μοιάζει με το WiFi στη υποδομή και με τα κυψελώδη (cellular) τηλεφωνικά δίκτυα [17] (Εικόνα 2.6).

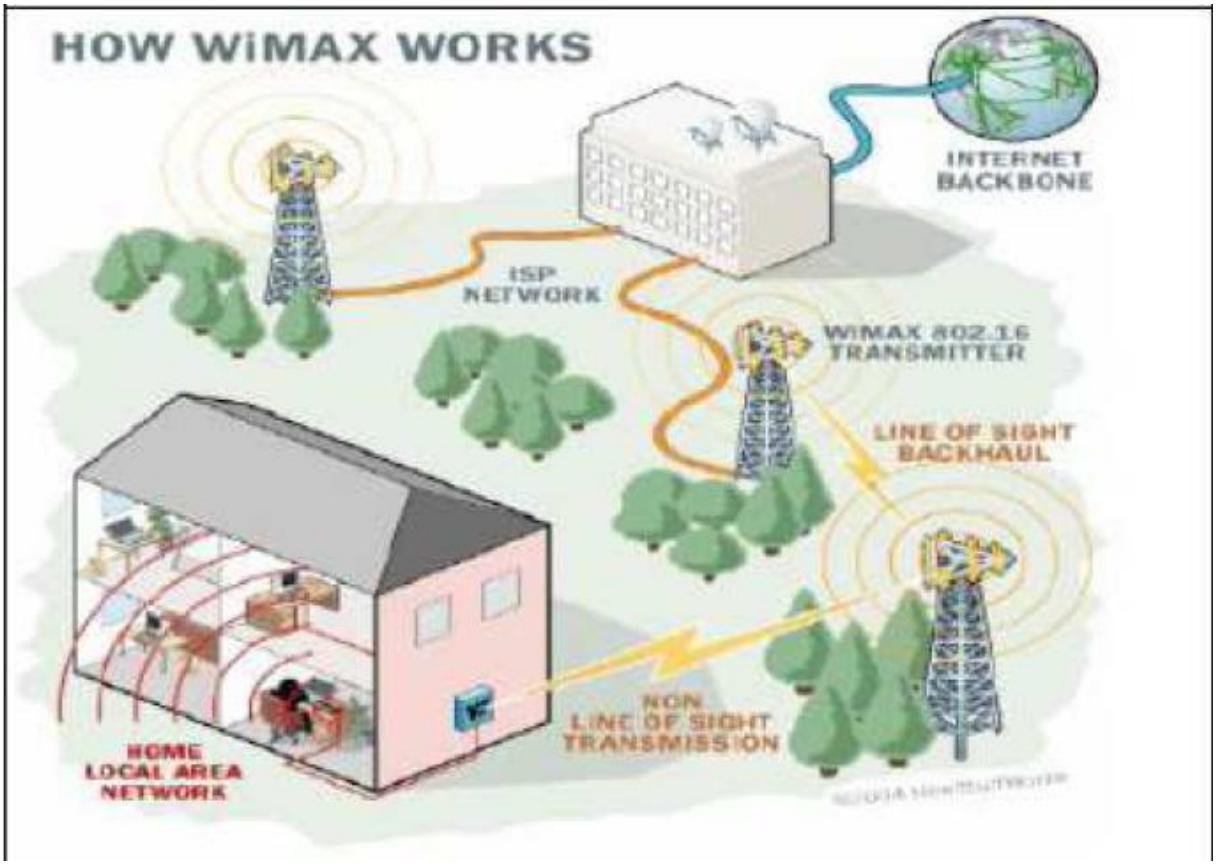
Οι τεχνολογίες WiMAX δουλεύουν ακριβώς όπως οι τεχνολογίες WiFi αλλά με μεγαλύτερη εμβέλεια. Μπορούν να καλύψουν περιοχές μέχρι και κάποιες δεκάδες χιλιόμετρα. Θα μπορεί δηλ. κάποιος χρήστης τοποθετώντας στον υπολογιστή του μια κάρτα WiMAX όπως κάνει τώρα με το WiFi, να ενώνεται με το internet ενώ βρίσκεται σε μεγάλη απόσταση από το Access Point.

Ένα σύστημα WiMAX αποτελείται από δύο μέρη [26]:

1. Ένα Σταθμό Βάσης (BS) ο οποίος αποτελείται από τα ηλεκτρονικά κυκλώματα και την αντένα WiMAX. Ένας BS καλύπτει μέχρι 10 χλμ. Έτσι κάθε ασύρματος

κόμβος μπορεί να ενώνεται μέσω της αντένας με το internet εφόσον φυσικά είναι μέσα στο πεδίον κάλυψης της αντένας.

2. Ένα δέκτη WiMAX (Subscriber Station - SS). Ο δέκτης μπορεί να είναι ένα laptop (κινητός κόμβος), ή ένας υπολογιστής με μια ειδική κάρτα PCMCIA για επικοινωνία με την αντένα.



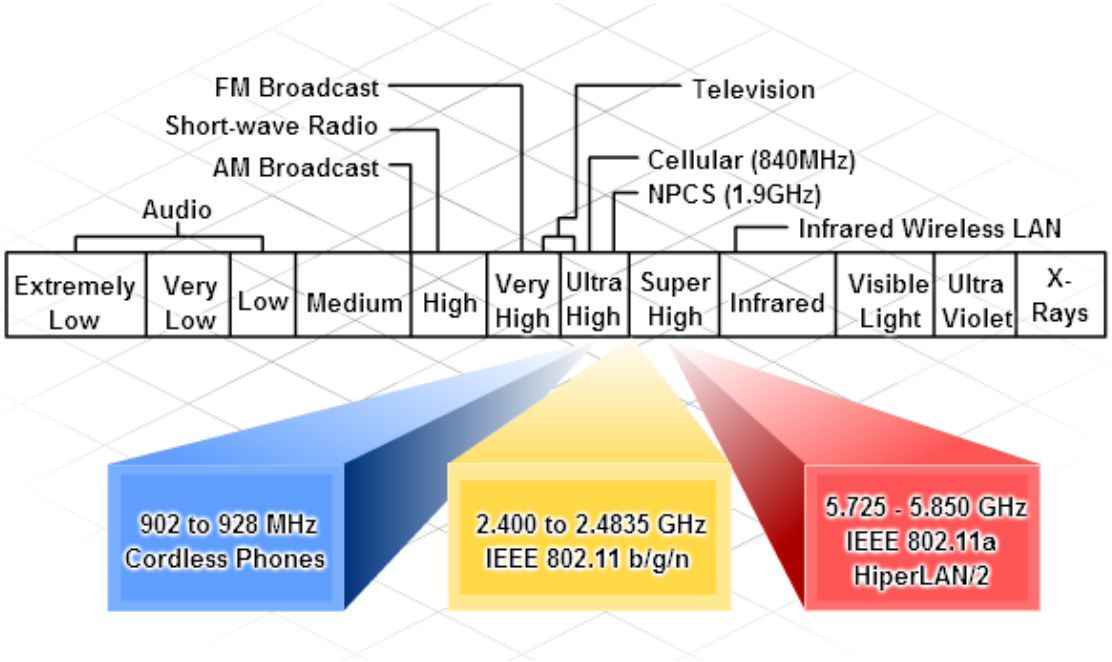
Εικόνα 2.6: 802.16 WiMAX υποδομή [26].

Οι διάφοροι σταθμοί βάσεων μπορούν και επικοινωνούν μεταξύ τους μέσω μικροκυμάτων μεγάλης ταχύτητας. Αυτό επιτρέπει την κινητικότητα των χρηστών WiMAX από ένα σταθμό βάσης, σε ένα άλλο όπως συμβαίνει στα δίκτυα κινητής τηλεφωνίας. Μερικά χαρακτηριστικά της τεχνολογίας αυτής είναι η επεκτασιμότητα (scalability), η εμβέλεια (coverage), η παροχή υψηλής ποιότητας υπηρεσιών (QoS) και η ασφάλεια (security).

2.4 Ασύρματα Τοπικά Δίκτυα (WiFi)

Στην συγκεκριμένη μεταπτυχιακή εργασία θα διερευνηθούν διάφορα χαρακτηριστικά των ασύρματων τοπικών δικτύων (WiFi) που αφορούν την ποιότητα του σήματος (QoS).

2.4.1 WLAN (Wireless Local Area Network) [20]



Εικόνα 2.7: Radio Frequency (RF) διαφόρων wireless συσκευών [20]

Ασύρματα τοπικά δίκτυα (WiFi) συμπληρώνουν ενσύρματα δίκτυα ή ακόμη αντικαθιστούν τέτοια δίκτυα. Ασύρματες συσκευές σε ένα ασύρματο δίκτυο χρησιμοποιούν RF (Radio frequency) κύματα που μπορούν να διαπερνούν τους τοίχους ή άλλα εμπόδια και με αυτό τον τρόπο διευρύνεται η απόσταση κάλυψης τους, εν σχέση με τα κύματα υπέρυθρων. Διάφορα είδη ασύρματων τεχνολογιών χρησιμοποιούν διαφορετικά φάσματα συχνοτήτων που ξεκινούν από 900 MHz και φτάνουν μέχρι 5GHz. Όπως φαίνεται στην εικόνα14 π.χ. τα Cordless τηλέφωνα χρησιμοποιούν συχνότητες από 902 – 928 MHz ενώ τα wireless LANs χρησιμοποιούν συνήθως τις συχνότητες από 2.400-2.4835 GHz. Bluetooth τεχνολογίες (IEEE 802.15.1) χρησιμοποιούν μπάντες των 2.4GHz. Συσκευές Bluetooth τεχνολογίας επικοινωνούν με χαμηλές ταχύτητες (4Mbps) και η απόσταση επικοινωνίας τους είναι μικρή (10m diameter) Το πλεονέκτημά που έχει όμως αυτή η τεχνολογία είναι η ταυτόχρονη

επικοινωνία πολλών συσκευών μαζί. Αυτό το πλεονέκτημα της Bluetooth, one to many, την κάνει χρήσιμη στην επικοινωνία ενός υπολογιστή με τις περιφερειακές του συσκευές όπως keyboards, mice και printers. 802.15.1 δίκτυα είναι ad hoc δίκτυα. Χρησιμοποιούν την frequency-hopping spread spectrum (FHSS) channel hopping [17].

Άλλες τεχνολογίες που κάνουν την χρήση της μπάντας 2.4 GHz και 5GHz είναι οι μοντέρνες wireless LAN τεχνολογίες οι οποίες τηρούν τα διάφορα 802.11 κριτήρια.
Μερικά πλεονεκτήματα/Μειονεκτήματα των wireless δικτύων φαίνονται στον πιο κάτω πίνακα.

Πλεονεκτήματα	**Μειονεκτήματα**
Κινητικότητα : Ασύρματα δίκτυα παρέχουν την δυνατότητα στους χρήστες να κινούνται και να επικοινωνούν μεταξύ τους.	Χρήση μη αδειούχων περιοχών του RF spectrum
Scalability**:** Μπορούν εύκολα να προστεθούν νέοι χρήστες.	Interference**:** Ευαίσθητα σε παρεμβολές π.χ. cordless phones, microwaves
Flexibility**:** Υπάρχει σύνδεση οποιαδήποτε ώρα και οπουδήποτε.	Security**:** Υπάρχει ευκολία στη παράνομη πρόσβαση. encryption/authentication βοηθούν σημαντικά στην ασφάλεια των wireless networks.
Cost**:** Χαμηλό το κόστος εγκατάστασης	

Πίνακας 2.2: Πλεονεκτήματα/Μειονεκτήματα wireless networks.

2.4.2 Τύποι Ασύρματων δικτύων

WPAN : Wireless Personal Area Network : Είναι το μικρότερο wireless δίκτυο. Χρησιμοποιείται για να ενώνει περιφερειακές συσκευές σε ένα υπολογιστή. Π.χ keyboards, PDAs. Χρησιμοποιούν υπέρυθρες *(Infrared*- IR), ή Bluetooth τεχνολογίες.
WLAN: Χρησιμοποιούνται για να επεκτείνουν το όριο των ενσύρματων τοπικών δικτύων LAN. Τα WLAN χρησιμοποιούν RF τεχνολογία και ανταποκρίνονται στις IEEE 802.11 απαιτήσεις. Επιτρέπουν σε πολλούς χρήστες να ενώνονται με ενσύρματα δίκτυα μέσω μιας συσκευής που ονομάζεται Access Point (AP) .

WWAN: Τα δίκτυα αυτά καλύπτουν πολύ μεγάλες γεωγραφικές περιοχές. Ένα παράδειγμα WWAN δικτύων είναι το δίκτυο κινητής τηλεφωνίας (cell phone network). Αυτά τα δίκτυα χρησιμοποιούν τεχνολογίες όπως Code Division Multiple Access (CDMA) ή Global System for Mobile Communication (GSM) (Εικόνα 2.8).

	WPAN	WLAN	WWAN
Standards	Bluetooth v2.0+ EDR**	IEEE802.11 a/b/g/n, HiperLAN, HiperLAN2	GSM, GPRS, CDMA
Speed		1-540 Mbps	10-384 Kbps
Range	Short	Medium	Long
Applications	Peer-to-Peer device to device	Home, small business and enterprise networks	PDAs, mobile phones, cellular access

** EDR is Enhanced Data Rate

Speed and ranges are constantly increasing with newer technologies.

Εικόνα 2.8: Πίνακας τύπων wireless δικτύων με τα χαρακτηριστικά τους

Common IEEE WLAN Standards

Standard	Release Date	Frequency	Data Rate (Max)	Maximum Range*
802.11	July 1997	2.4 GHz	2 Mbps	undefined
802.11a	October 1999	5 GHz	54 Mbps	50 m
802.11b	October 1999	2.4 GHz	11 Mbps	100 m
802.11g	June 2003	2.4 GHz	54 Mbps	100 m
**802.11n	Draft - Nov 2006 Release - Jan 2007 Approval - April 2007	2.4 GHz or 5 GHz	540 Mbps	250 m

*Maximum Range - This value can vary widely. ~ The 802.11n standard is still in draft and values may change.

Εικόνα 2.9: Wireless LAN standards

Στην εικόνα 2.9 παρατηρούμε ότι το νέο 802.11n standard έχουμε τον μεγαλύτερο ρυθμό δεδομένων (Data Rate) με ταχύτητες που φτάνουν τα 540 Mbps. Έχουμε επίσης μια περιοχή που καλύπτει το WLAN μέχρι 250m.

Γενικά ο ρυθμός δεδομένων σε κάθε τερματικό εξαρτάται σε μεγάλο βαθμό από διάφορους παράγοντες όπως π.χ., τις απαιτήσεις των ζητούμενων υπηρεσιών, τον αριθμό των χρηστών που είναι σε μια χρονική στιγμή ενεργοί στο WLAN (αλλά και το βαθμό απαιτητικότητας των υπηρεσιών τους), τη απόσταση του AP από το τερματικό, τις παρεμβολές από διάφορε πηγές, το θόρυβο και τη ισχύ εκπομπής του AP αλλά και του τερματικού [19].

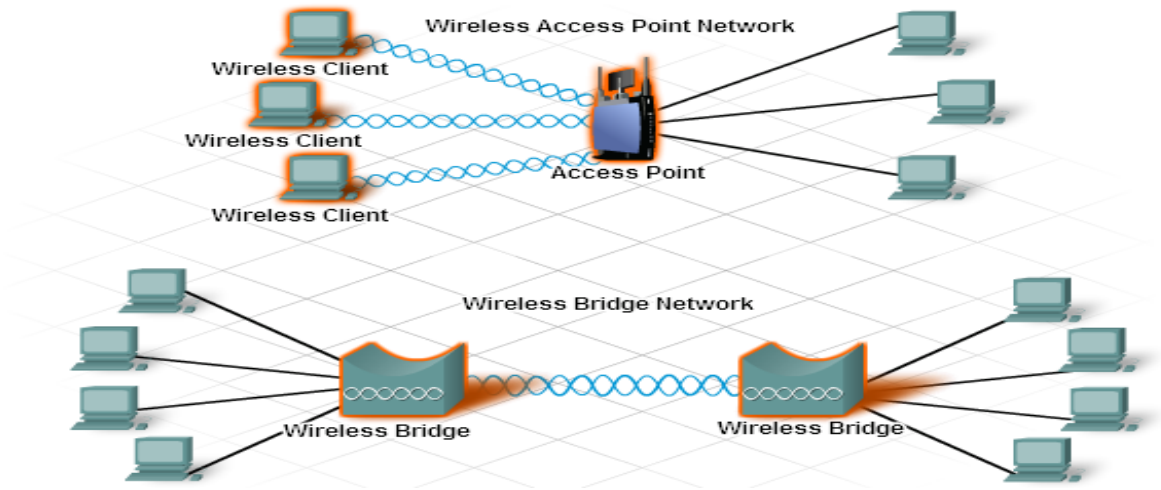
Η απόσταση κάλυψης της επικοινωνίας RF σε ένα WLAN εξαρτάται από την εκπεμπόμενη ισχύ του δέκτη τον αριθμό και τη φύση των εμποδίων που υπάρχουν ενδιάμεσα (ειδικά μέσα σε κτίρια). Η εμβέλεια ενός τυπικού AP είναι από 50 έως 250 μέτρα. Η κάλυψη μπορεί να επεκταθεί χρησιμοποιώντας κεραίες για ενίσχυση ή χρησιμοποιώντας περισσότερα AP [19].

2.4.3 Μέρη Ενός WLAN

Ένα WLAN αποτελείται από τέσσερα βασικά μέρη :

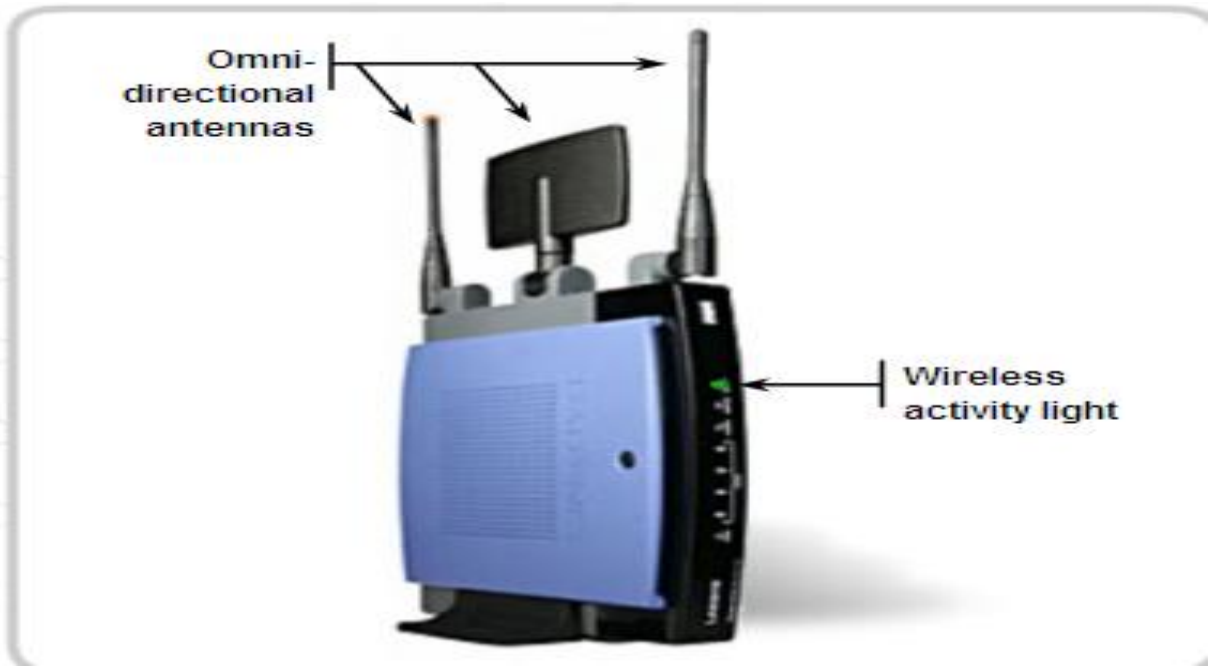
1. Wireless client or STA
2. Access Point
3. Wireless Bridge
4. Antenna

Ένας Wireless client μπορεί να είναι: laptops, PDAs, printers, projectors και storage devices. Μια τέτοια συσκευή μπορεί να είναι κινητή ή σταθερή. Ένα Access Point δημιουργεί και συντονίζει το traffic μεταξύ ενσύρματων και ασύρματων δικτύων. Μετατρέπει τα πακέτα πού έρχονται από ένα ενσύρματο δίκτυο σε μορφή που είναι συμβατή με τα κριτήρια του 802.11 στάνταρτ πριν να προωθηθούν προς το WLAN. Αυτή η μετατροπή μπορεί να γίνει και αντίθετα δηλ. 802.11 πακέτα να μετατραπούν σε μορφή Ethernet πακέτων πριν να προωθηθούν στο ενσύρματο δίκτυο. APs παρέχουν wireless συνδέσεις μέσα σε μια περιορισμένη περιοχή, που ονομάζεται cell ή Basic Service Set (BSS) (Εικόνα 2.12). Οι wireless Bridges επεκτείνουν ένα WLAN σε μια μεγάλη περιοχή (μέχρι και 40Km) (Εικόνα 2.10).



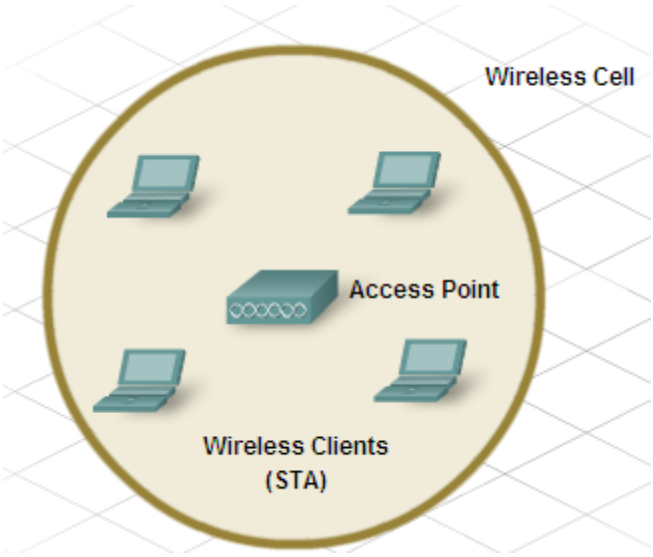
Εικόνα 2.10: Μέρη που αποτελείται ένα WLAN

Wireless Antennas χρησιμοποιούν τα AP και τα Wireless bridges. Αυτές οι Αντένες αυξάνουν την ένταση του σήματος (signal strength) που εκπέμπει μια wireless συσκευή (Εικόνα 2.11). Αυτή η αύξηση της έντασης του σήματος από μια αντένα ονομάζεται gain.



Εικόνα 2.11: Wireless Αντένα

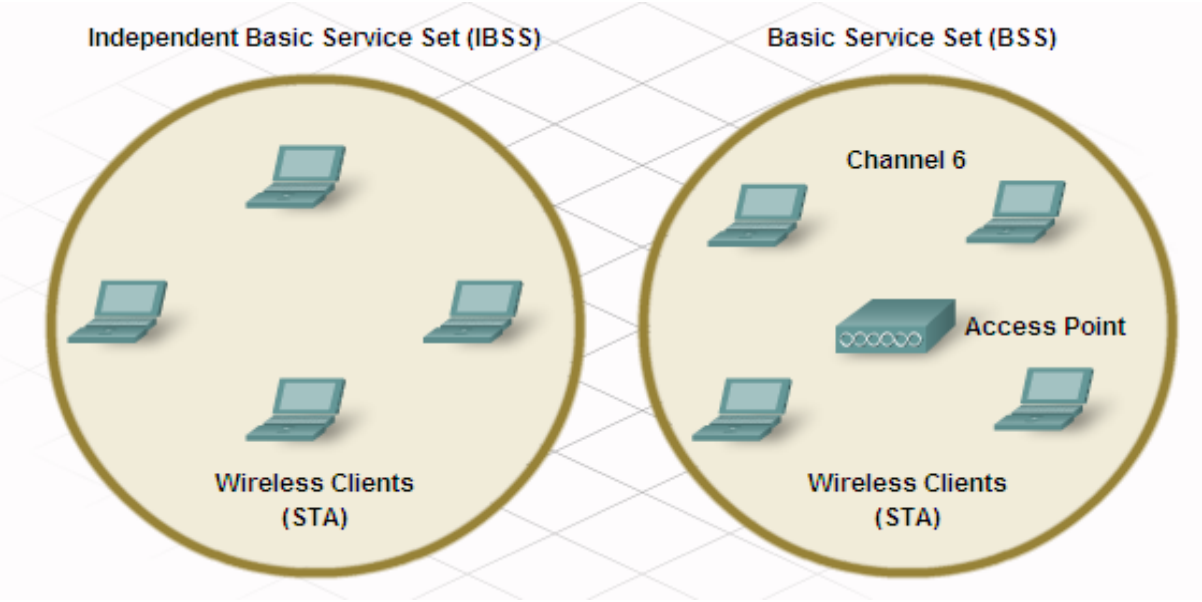
2.4.4 WLAN και SSID



Εικόνα 2.12: Wireless Cell

Είναι σημαντικό σε ένα wireless δίκτυο, ένας χρήστης να έχει ενωθεί στο σωστό WLAN. Αυτό επιτυγχάνεται με την χρήση του Service Set Identifier (SSID). Το SSID χρησιμοποιείται για να πληροφορήσει τη wireless συσκευή σε ποιο WLAN ανήκει (Εικόνα 2.12).

Υπάρχουν δύο βασικές τοπολογίες WLAN : Τα Ad-hoc και τα infrastructure mode.

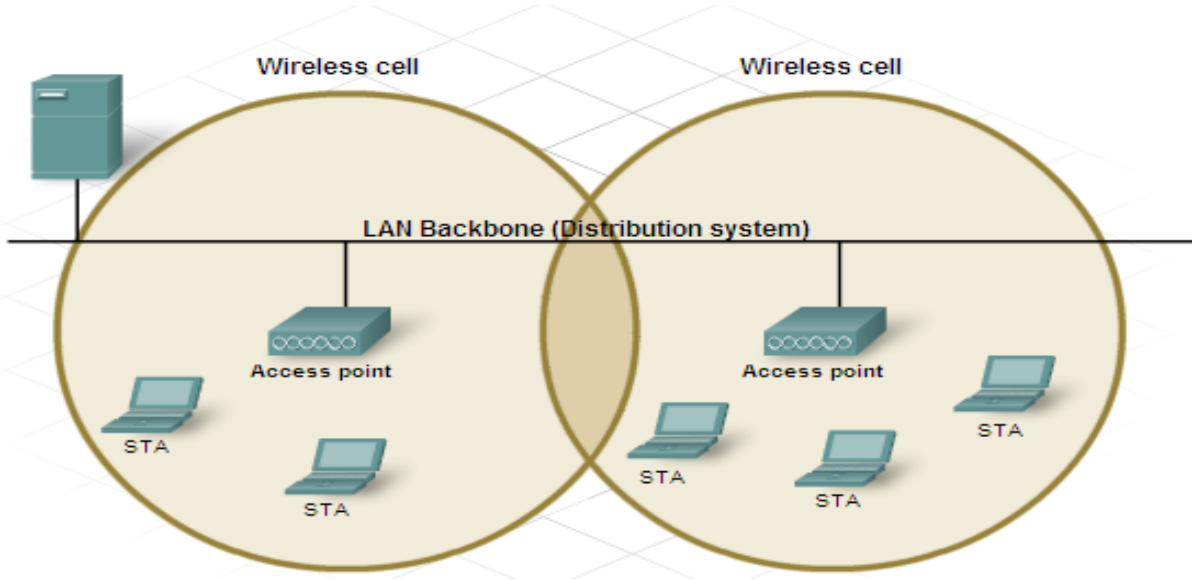


Εικόνα 2.13: Οι δυο βασικές τοπολογίες WLAN

Τα Ad-hoc WLAN δεν έχουν AP. Απλά ενώνουμε δύο ή περισσότερους χρήστες μαζί σε ένα peer-to-peer δίκτυο. Η περιοχή η οποία καλύπτει ένα Ad-hoc WLAN ονομάζεται Independent Basic Service Set (IBSS) (Εικόνα 2.13). Σε αυτή την περιοχή οι χρήστες μπορούν και επικοινωνούν μεταξύ τους απευθείας.

Στα infrastructure WLAN το AP ελέγχει την επικοινωνία μέσα στο δίκτυο δηλ. ελέγχει ποιος θα στέλλει δεδομένα και πότε θα τα στέλλει. Οι χρήστες δεν μπορούν να επικοινωνούν απευθείας αλλά μέσω του AP. Αυτή η μορφή επικοινωνίας χρησιμοποιείται πιο συχνά. Η περιοχή η οποία καλύπτεται από ένα AP ονομάζεται Basic Service Set (BSS) (Εικόνα 2.13).

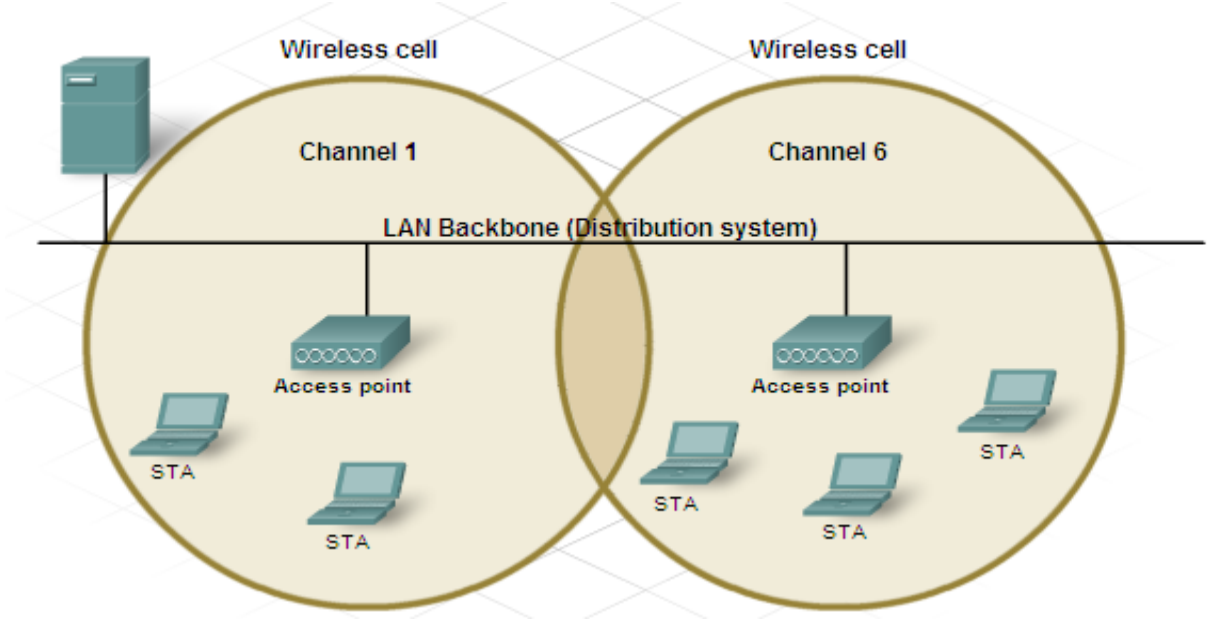
Για να επεκτείνουμε μια περιοχή ενός WLAN μπορούμε να ενώσουμε πολλές BSS μέσω ενός Distribution System (DS). Αυτή η περιοχή ονομάζεται Extended Service Set (ESS) και χρησιμοποιεί πολλά APs. Κάθε AP είναι ένα ξεχωριστό BSS. Για να υπάρχει η δυνατότητα μετακίνησης ενός χρήστη από cell σε cell χωρίς να διακόπτεται η επικοινωνία, κάθε BSS πρέπει να επικαλύπτει το επόμενο BSS περίπου 10%. Αυτό επιτρέπει στο χρήστη να ενωθεί με στο επόμενο AP πριν να διακοπεί η επικοινωνία με το πρώτο AP (Εικόνα 2.14).



Εικόνα 2.14: Extended Service Set (ESS).

2.4.5 Wireless Channels

Ο έλεγχος της συνομιλίας (επικοινωνίας) μεταξύ του αποστολέα και του παραλήπτη γίνεται μέσω της χρήσης των καναλιών (channels). Τα κανάλια δημιουργούνται χωρίζοντας το διαθέσιμο RF φάσμα. Κάθε κανάλι είναι ικανό να διαχειρίζεται μια διαφορετική συνομιλία (Εικόνα 2.15).



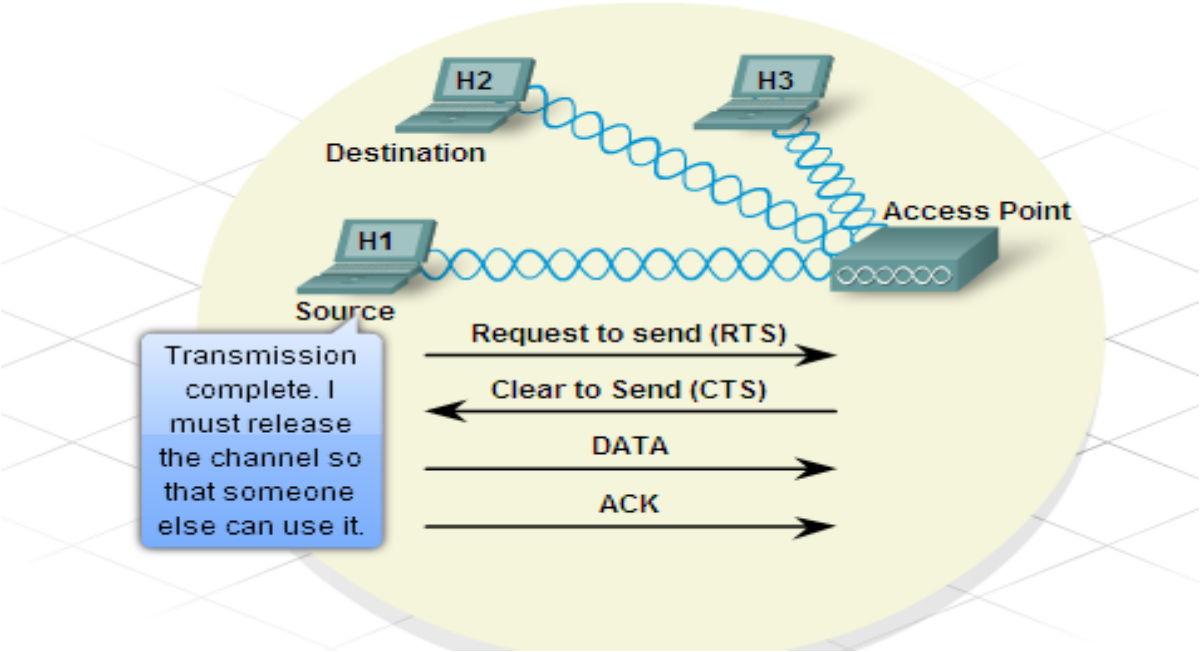
Εικόνα 2.15: Wireless Channels

Είναι δυνατό κάποιες συχνότητες που χρησιμοποιούνται από κάποια κανάλια να επικαλύπτουν συχνότητες που χρησιμοποιούνται από άλλα κανάλια. Θα πρέπει λοιπόν να προσεχθεί να μην συμβαίνει αυτό και για αυτό τον λόγο θα πρέπει να επιλέγονται κανάλια που χρησιμοποιούν διαφορετικές συχνότητες οι οποίες δεν επικαλύπτονται από άλλες. Η επιλογή των καναλιών μπορεί να γίνει αυτόματα ή manually. Φυσικά αν η διαχείριση των access points γίνεται από ιδιωτικές εταιρείες, τότε αυτό δεν μπορεί να ελεγχτεί και παρουσιάζεται το φαινόμενο του interference. Κάποιες νέες τεχνολογίες χρησιμοποιούν συνδυασμό καναλιών για να δημιουργήσουν ένα νέο κανάλι το οποίο δίνει περισσότερο Bandwidth και αυξάνει το data rate.

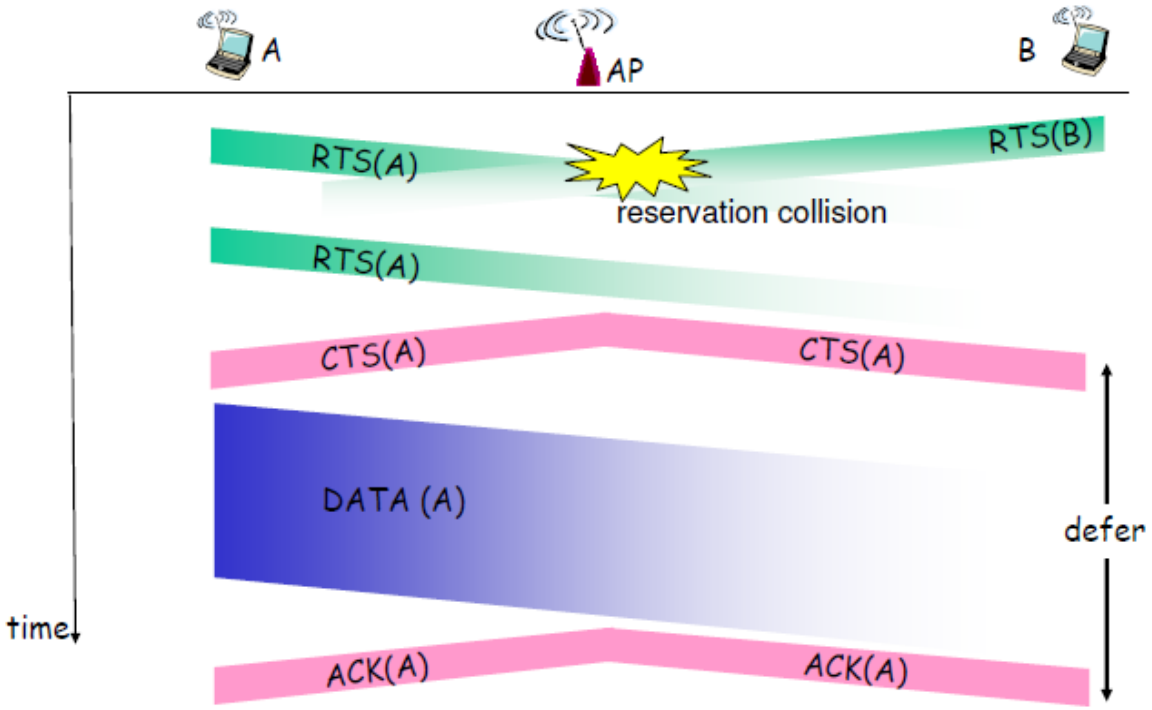
Είναι αναγκαίο να χρησιμοποιήσουμε μια μέθοδο πρόσβασης σε ασύρματο δίκτυο που να εξασφαλίζει ότι συγκρούσεις (collisions) δεν θα εμφανίζονται. Η ασύρματη τεχνολογία χρησιμοποιεί μια μέθοδο πρόσβασης που ονομάζεται Carrier Sense Multiple Access με αποφυγή σύγκρουσης (CSMA / CA). Η μέθοδος CSMA / CA εξασφαλίζει μια κράτηση σε ένα κανάλι, για χρήση του σε μια συγκεκριμένη συνομιλία που θέλει να

κάνει ένας χρήστης (τερματικό). Κατά τη διάρκεια της συνομιλίας αυτής κανένας άλλος χρήστης δεν μπορεί να εκπέμψει σε αυτό το κανάλι και έτσι με αυτό τον τρόπο αποφεύγονται συγκρούσεις. Υποθέτουμε ότι ένας ασύρματος σταθμός έχει 10000 μεγάλα πακέτα να μεταδώσει. Αρχικά ο σταθμός ανιχνεύει το μέσο αδρανές (idle) και αρχίζει την μετάδοση του πρώτου πακέτου μετά από μια μικρή χρονική περίοδο (Distributed Inter-Frame Space – DIFS). Κατά την διάρκεια της μετάδοσης υποθέτουμε ότι ένας δεύτερος σταθμός θέλει να μεταδώσει ένα πακέτο αλλά ανιχνεύει το μέσο κατειλημμένο. Τότε θα αρχίσει τον αλγόριθμο τυχαίας οπισθοχώρησης (Random Backoff Algorithm). Αν ο πρώτος σταθμός μπορούσε να μεταδώσει αμέσως το 2ο πακέτο, τότε αυτό θα οδηγούσε στην μονοπώληση του μέσου για την μετάδοση όλων των 10000 πακέτων. Για λόγους δίκαιας κατανομής των πόρων του μέσου, το CSMA/CA σχεδιάστηκε έτσι ώστε ο σταθμός να ακολουθεί τον αλγόριθμο τυχαίας οπισθοχώρησης όταν ολοκληρώνει την μετάδοση του πακέτου. Δηλ. ο σταθμός να επιλέγει μια random backoff τιμή την οποία μειώνει προς τα κάτω για όσο το κανάλι παραμένει ανενεργές. Κατά την διάρκεια που το κανάλι είναι απασχολημένο τότε η τιμή αυτή παραμένει σταθερή (frozen). Με αυτό τον τρόπο ο δεύτερος σταθμός έχει την ευκαιρία να μεταδώσει ενδιάμεσα. Όταν η τιμή του πρώτου σταθμού (random backoff τιμή) φτάσει το μηδέν (μόνο όταν το κανάλι είναι ανενεργές-idle), τότε ο σταθμός έχει το δικαίωμα να μεταδώσει το επόμενο πακέτο. Όταν ο παραλήπτης παραλάβει το πακέτο, περιμένει ένα μικρό χρονικό διάστημα (Short Inter-frame Spacing – SIFS) και στέλλει πίσω ένα acknowledgement (Ack).

Κάνοντας χρήση από ένα σταθμό ενός μικρού Request to Send (RTS) control frame και ενός επίσης μικρού Clear to Send (CTS) control frame, για να γίνει κράτηση ενός καναλιού, δίνεται λύση στο λεγόμενο hidden station problem (Εικόνα 2.17). Εάν μια συσκευή απαιτεί τη χρήση ενός ειδικού καναλιού επικοινωνίας σε ένα BSS, πρέπει να ζητήσει άδεια από το AP. Αυτό ονομάζεται αίτημα για αποστολή (RTS). Αν το κανάλι είναι διαθέσιμο, το AP θα ανταποκριθεί στη συσκευή στέλλοντας της το μήνυμα Clear to Send (CTS) που υποδεικνύει ότι η συσκευή μπορεί να εκπέμψει στο κανάλι. Το μήνυμα CTS μεταδίδεται σε όλες τις συσκευές εντός του BSS (Broadcast). Ως εκ τούτου, όλες οι συσκευές του BSS γνωρίζουν ότι το ζητούμενο κανάλι είναι αυτή τη χρονική στιγμή σε χρήση. Μετά το τέλος της συνομιλίας η συσκευή που κρατούσε το κανάλι στέλλει μήνυμα Acknowledgement (ACK) σε όλες τις συσκευές του δικτύου (Broadcast) πληροφορώντας τις έτσι ότι το κανάλι είναι ελεύθερο προς χρήση (Εικόνες 2.16, 2.17).



Εικόνα 2.16: Wireless Channels - Request to transmission



Εικόνα 2.17: Collision avoidance using the RTS and CTS frames – Hidden station problem

2.4.6 Wireless Security

Ένα από τα πρωταρχικά πλεονεκτήματα της ασύρματης δικτύωσης είναι η ευκολία σύνδεσης συσκευών. Δυστυχώς, η ευκολία σύνδεσης και το γεγονός ότι οι πληροφορίες μεταδίδονται μέσω του αέρα κάνει το ασύρματο δίκτυο ευάλωτο σε υποκλοπές και επιθέσεις. Ο εισβολέας μπορεί να έχει πρόσβαση στο δίκτυό μας, από οποιαδήποτε θέση που μπορεί να φτάσει το ασύρματο σήμα του δικτύου μας.

Έτσι αφού καταφέρει να εισβάλει στο δίκτυό μας, μπορεί να χρησιμοποιεί το internet μας δωρεά ή να κάνει οποιαδήποτε ζημιά στα αρχεία μας. Για αυτά τα τρωτά σημεία ασύρματης δικτύωσης απαιτείται να παρθούν ειδικά μέτρα ασφαλείας και να εφαρμοστούν μέθοδοι για την προστασία του WLAN από επιθέσεις. Αυτά τα μέτρα περιλαμβάνουν τα απλά βήματα που εκτελούνται κατά την αρχική εγκατάσταση της ασύρματης συσκευής, καθώς και πιο προχωρημένες ρυθμίσεις ασφαλείας. Μερικά μέτρα προστασίας ακολουθούν πιο κάτω:

1. Απενεργοποίηση της δυνατότητας SSID broadcast από τον δρομολογητή.

2. Απενεργοποίηση όλων των default settings του δρομολογητή

3. Αλλαγή του default password

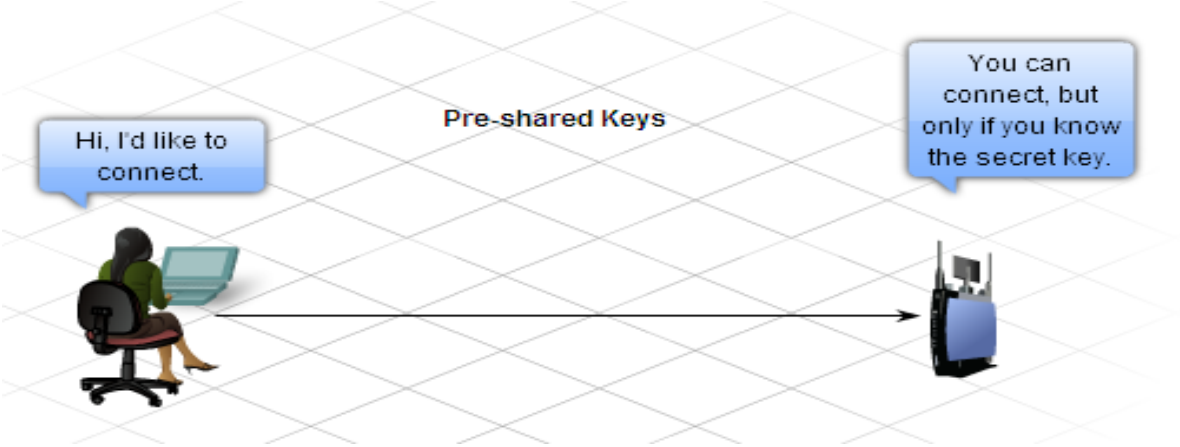
4. MAC Address Filtering

5. Ενεργοποίηση του authentication (username, password). Υπάρχουν τρία είδη authentication.

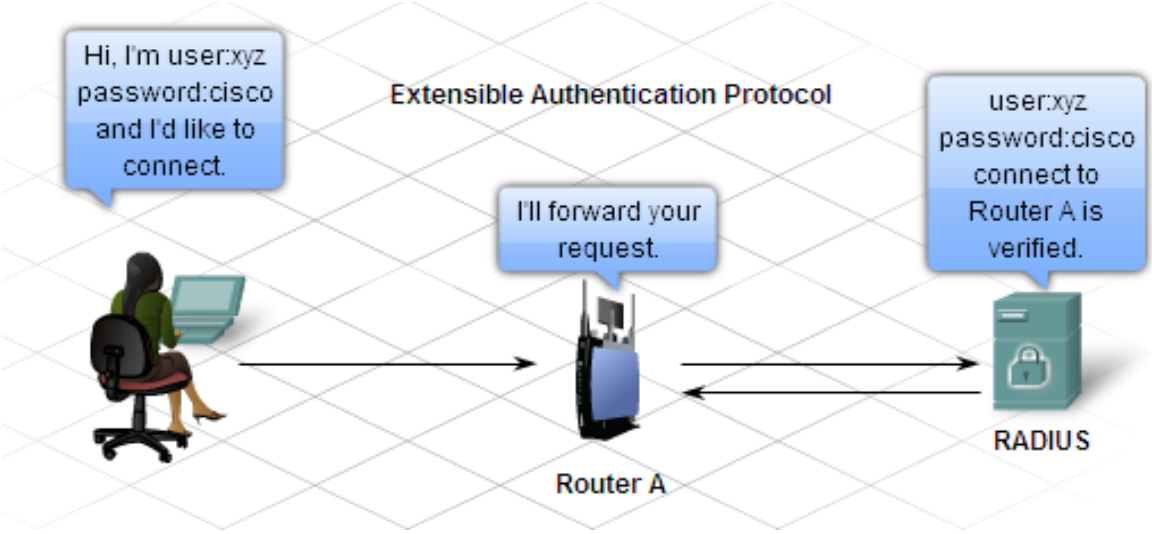
    5.1 Open

    5.2 PSK (Εικόνα 2.18)

    5.3 EAP (Εικόνα 2.19)

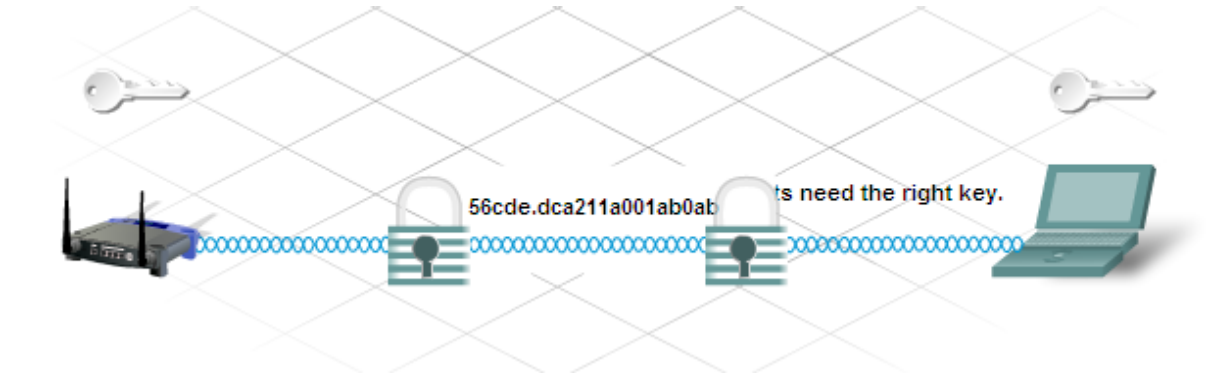


Εικόνα 2.18: Pre-share Keys



Εικόνα 2.19: Extensible Authentication Protocol (EAP)

Τα πιο πάνω μέτρα έχουν σαν σκοπό να αποτρέψουν attackers να εισβάλουν παράνομα στο δίκτυό μας. Αυτό όμως δεν είναι εμπόδιο για κάποιο hacker να υποκλέψει τις πληροφορίες ενώ ευρίσκονται στον αέρα. Για αυτό το λόγο υπάρχει η ανάγκη, οι πληροφορίες πριν την αποστολή τους να κωδικοποιούνται. Για το σκοπό αυτό υπάρχει ένα πρωτόκολλο για κωδικοποίηση δεδομένων που ονομάζεται Wired Equivalency Protocol (WEP). Το πρωτόκολλο αυτό χρησιμοποιεί κλειδί των 64 ή 128 ή ακόμη και 256 bits. Το κλειδί δίνεται σαν αλυσίδα (string) από γράμματα και αριθμούς (Εικόνα 2.20).

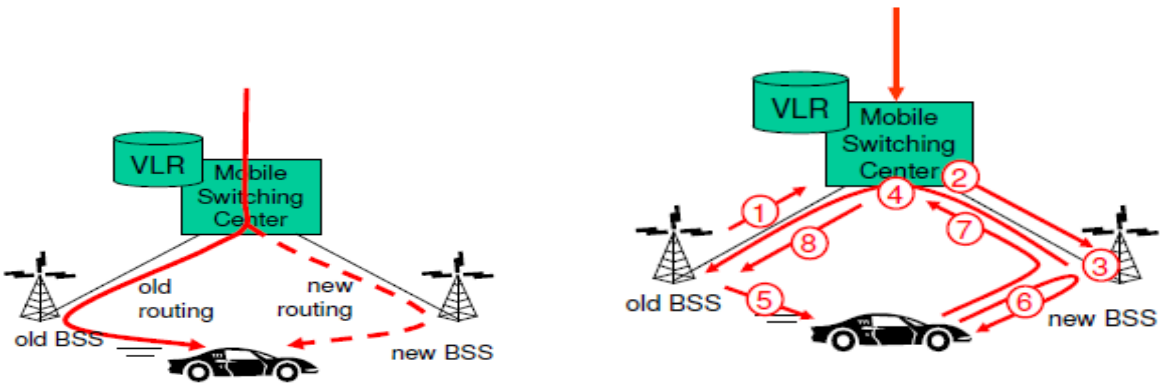


Εικόνα 2.20: Wired Equivalency Protocol (WEP)

2.5 Handovers

Η διαδικασία μεταφοράς ενός ασύρματου χρήστη σε άλλο ασύρματο δίκτυο χωρίς την διακοπή της επικοινωνίας ονομάζεται Handover.

2.5.1 Handoffs στα GSM Δίκτυα



Εικόνα 2.21: GSM handoff with common MSC [17]

Σε αυτό το κεφάλαιο θα εξηγηθεί περιληπτικά ο όρος Handover, καθώς και διάφορα είδη Handover που υπάρχουν και χρησιμοποιούνται σε διάφορες τεχνολογίες. Π.χ. GSM/WiMAX/WiFi.

Ένα handoff ή handover στην κινητή τηλεφωνία, εμφανίζεται όταν ένας κινητός κόμβος αλλάξει την θέση του από ένα σταθμό βάσης σε ένα άλλο, κατά την ώρα ενός τηλεφωνήματος. Αρχικά πριν το handoff, ο κινητός κόμβος επικοινωνούσε (receiving/transmitting) με το παλιό σταθμό βάσης (old BSS) και τα τηλεφωνήματα προς το κινητό, δρομολογούνταν από τον Mobile Switching Center (MSC) σύμφωνα με την παλιά διαδρομή (old routing). Μετά το handoff όμως επικοινωνεί (receiving/transmitting) με τον νέο σταθμό βάσης (new BSS) και η δρομολόγηση των τηλεφωνημάτων από τον MSC γίνεται σύμφωνα με την νέα διαδρομή. Ο παλιός και ο νέος σταθμός βάσης χρησιμοποιούν τον ίδιο MSC. Υπάρχουν πολλοί λόγοι που δημιουργείται ένα handoff [17]. Ένας λόγος είναι ότι χαλά η ποιότητα του σήματος επικοινωνίας του κινητού χρήστη με τον σταθμό βάσης και ταυτόχρονα ενισχύεται ένα άλλο σήμα με ένα άλλο σταθμό βάσης. Άλλος λόγος μπορεί να είναι ότι το δίκτυο στο συγκεκριμένο cell είναι βαρυφορτωμένο με πολλά τηλεφωνήματα και αυτό οδηγεί σε συμφόρηση. Αυτή η συμφόρηση μπορεί να μειωθεί αν κάποιοι κινητοί χρήστες μεταφερθούν (handoff) σε cells με λιγότερη συμφόρηση. Το handoff γίνεται από τον παλιό σταθμό βάσης.

Τα βήματα που γίνονται όταν ένας σταθμός βάσης αποφασίσει να κάνει handoff έναν κινητό χρήστη με κοινό MSC είναι [17] :

1. Ο παλιός BS πληροφορεί τον MSC ότι πρόκειται να κάνει handoff και τον πληροφορεί επίσης σε ποιό BS θα γίνει handoff το κινητό.

2. Ο MSC δημιουργεί μονοπάτι προς το νέο BS, κατανέμει τους πόρους που χρειάζονται για την μεταφορά του τηλεφωνήματος προς τον νέο BS και πληροφορεί το νέο BS για το επικείμενο handoff.

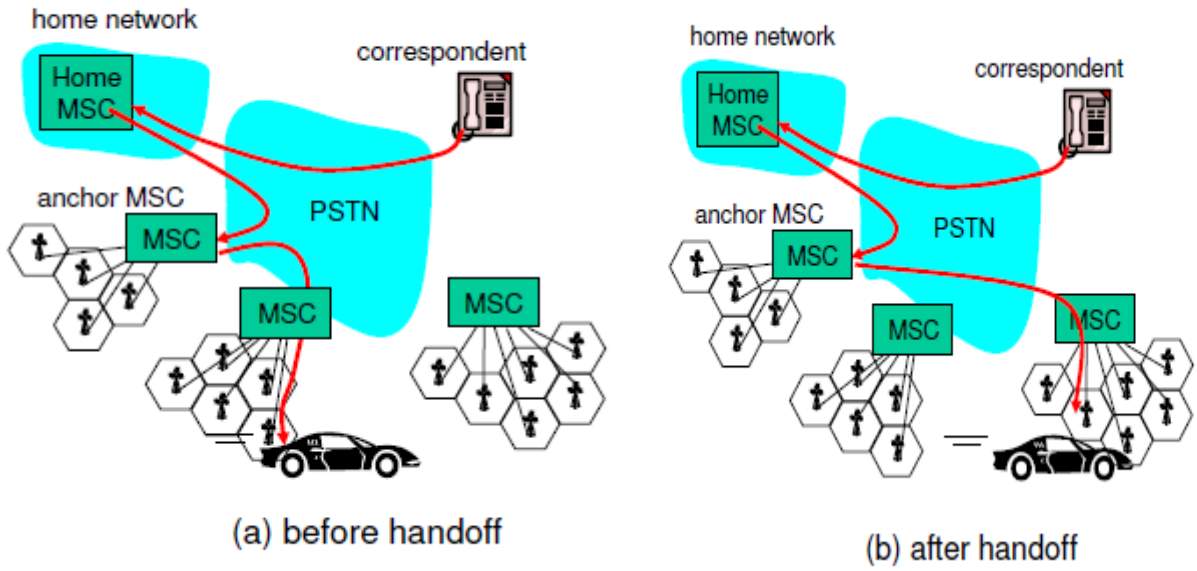
3. Ο νέος BS κατανέμει και ενεργοποιεί ένα radio κανάλι για χρήση του από το κινητό.
4. Ο νέος BS στέλλει σήμα στο MSC και στο παλιό BS και τους πληροφορεί ότι έχει δημιουργηθεί το νέο μονοπάτι MSC-to-new-BS . Ο νέος BS παρέχει όλες τις πληροφορίες που χρειάζεται το κινητό για τη σύνδεση μαζί του.

5. Ο παλιός BS πληροφορεί το κινητό ότι πρέπει να κάνει handoff στον νέο BS.

6. Κινητό και νέο BS ανταλλάσσουν μηνύματα για να ενεργοποιήσουν το νέο κανάλι στο νέο BS.

7. Το κινητό στέλλει σήμα στο νέο BS ότι έχει γίνει το handoff και αυτός με τη σειρά του πληροφορεί το MSC. Ο MSC με την σειρά του δρομολογεί το σε εξέλιξη (ongoing) τηλεφώνημα του κινητού μέσω του νέου BSS.

8. Οι πόροι που είχαν δεσμευτεί από το παλιό BS αποδεσμεύονται.

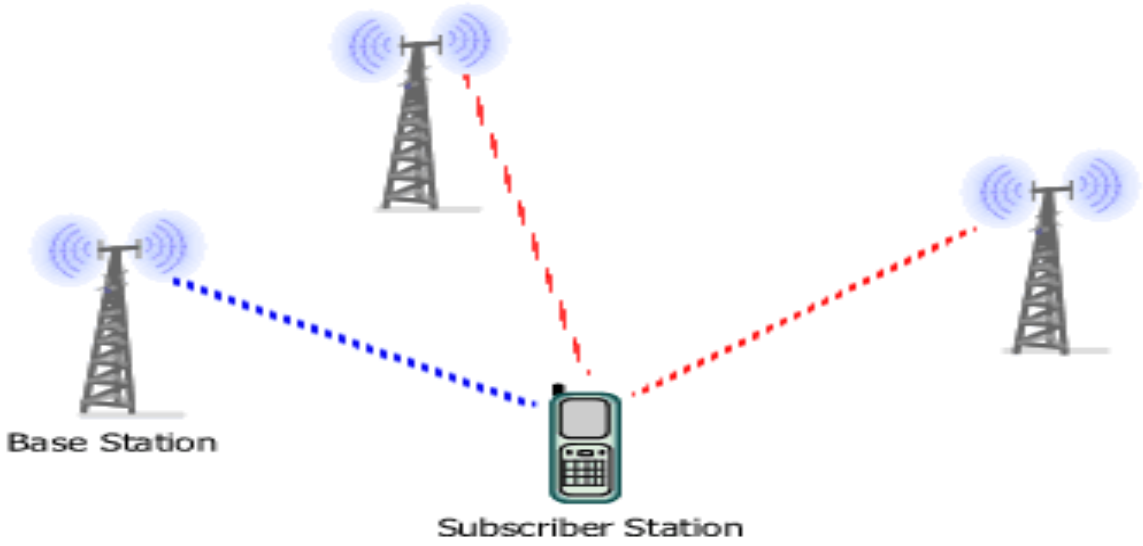


Εικόνα 2.22: GSM handoff between MSCs [17]

άγκυρα MSC: Το πρώτο MSC που επισκέφθηκε το κινητό μόλις άρχισε το τηλεφώνημα. Παραμένει αναλλοίωτο σε όλη την διάρκεια του τηλεφωνήματος. Το τηλεφώνημα δρομολογήθηκε αρχικά από το οικείο MSC προς το MSC άγκυρα και στη συνέχεια από το MSC άγκυρα προς το MSC του δικτύου που έχει εντοπιστεί το κινητό. Κατά την μετακίνηση του κινητού από δίκτυο σε δίκτυο (από MSC σε MSC), το σε εξέλιξη (ongoing) τηλεφώνημα επαναδρομολογείται από το MSC άγκυρα προς το νέο MSC που επισκέπτεται. Έτσι η αλυσίδα που δημιουργείται περιέχει τρία MSC (Home MSC, the Anchor MSC, visited MSC) μεταξύ του κινητού και του συνομιλητή (Εικόνα 2.22).

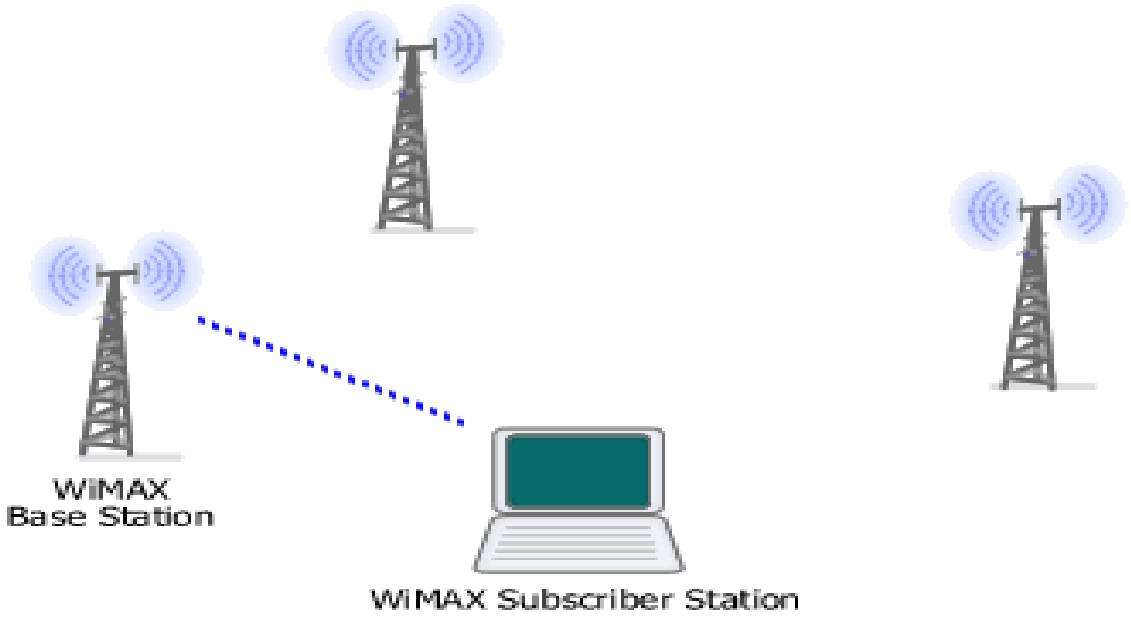
2.5.2 Handoff Μηχανισμοί στο Mobile WiMAX

Ο όρος Handoff στα κινητά δίκτυα (κινητές επικοινωνίες) αναφέρεται στο μηχανισμό ο οποίος χειρίζεται τη μεταφορά ενός χρήστη από ένα δίκτυο σε ένα άλλο δίκτυο χωρίς διακοπή της επικοινωνίας του. Handoff μηχανισμοί χειρίζονται την αλλαγή δικτύου συσκευών επικοινωνίας (subscriber station), μετακινούμενες από ένα Base Station (BS) σε άλλο Base Station. Το Handoff χωρίζεται σε soft handoff and hard handoff [14].



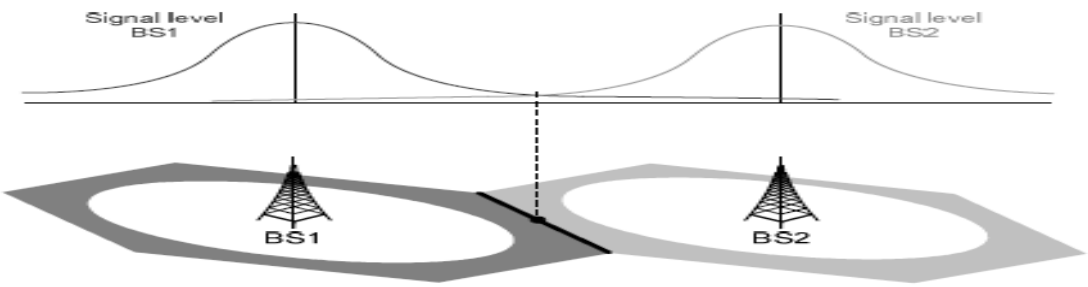
Εικόνα 2.23: Soft Handoff [14]

Soft handoff χρησιμοποιείται κυρίως στα voice-centric cellular networks όπως είναι το GSM ή το CDMA. Soft handoff έχουμε όταν η σύνδεση στο επόμενο Base Station (BS) πραγματοποιηθεί πριν διακοπεί η επικοινωνία με το αρχικό Base Station για αυτό και ονομάζεται make-before-break . Αυτή η τεχνική είναι κατάλληλη για να διαχειρίζεται voice και άλλες latency-sensitive υπηρεσίες όπως game και video conference. Στην Εικόνα 2.23 παρατηρούμε ότι στο Soft Handoff ο mobile user μπορεί να είναι συνδεδεμένος με περισσότερα από ένα Base Station. Το διάστημα κατά το οποίο υπάρχουν ταυτόχρονα περισσότερες της μίας συνδέσεις είναι μικρό.



Εικόνα 2.24: Hard Handoff (A) [14]

Hard handover έχουμε όταν ο mobile user επικοινωνεί με μόνο ένα base station (Εικόνα 2.24). Η επικοινωνία με το αρχικό Base Station διακόπτεται πριν αποκατασταθεί η επικοινωνία με το επόμενο base station (break-before-make). Hard Handover εκτελείται όταν η ένταση του σήματος του γειτονικού base station είναι πιο δυνατή από αυτή του current base station (Εικόνα 2.25).



Εικόνα 2.25: Hard Handoff (B) [15]

Πλεονεκτήματα Hard handoff

1. Hard handoff δεν απαιτεί επιπλέον Hardware με αποτέλεσμα οι συσκευές να είναι πιο φτηνές.
2. Σε κάθε χρονική στιγμή είναι συνδεδεμένο με μόνο ένα Base Station

3. Τα Hard handoffs είναι πολύ μικρά σε διάρκεια που δύσκολα γίνονται αντιληπτά

Ένα μειονέκτημα του Hard handoff είναι ότι αν αποτύχει, τότε πέφτει η ποιότητα της σύνδεσης λόγω παρεμβολών και στη συνέχεια διακόπτεται η επικοινωνία.

Πλεονεκτήματα Soft handoff

1. Με το Soft handoff η πιθανότητα ενός αποτυχημένου Handover με αποτέλεσμα να διακοπεί η σύνδεση είναι απομακρυσμένη, διότι η σύνδεση με το current Base Station διακόπτεται μόνο αν γίνει επιτυχημένη σύνδεση με τον επόμενο σταθμό (BS).
2. Η δυνατότητα διατήρησης επικοινωνίας με περισσότερους σταθμούς (BS) ταυτόχρονα μειώνει στο ελάχιστο τη πιθανότητα διακοπής της σύνδεσης. Για αυτό το λόγο η αξιοπιστία της σύνδεσης γίνεται μεγάλη με την χρήση Soft handoff.

Μειονεκτήματα Soft handoff

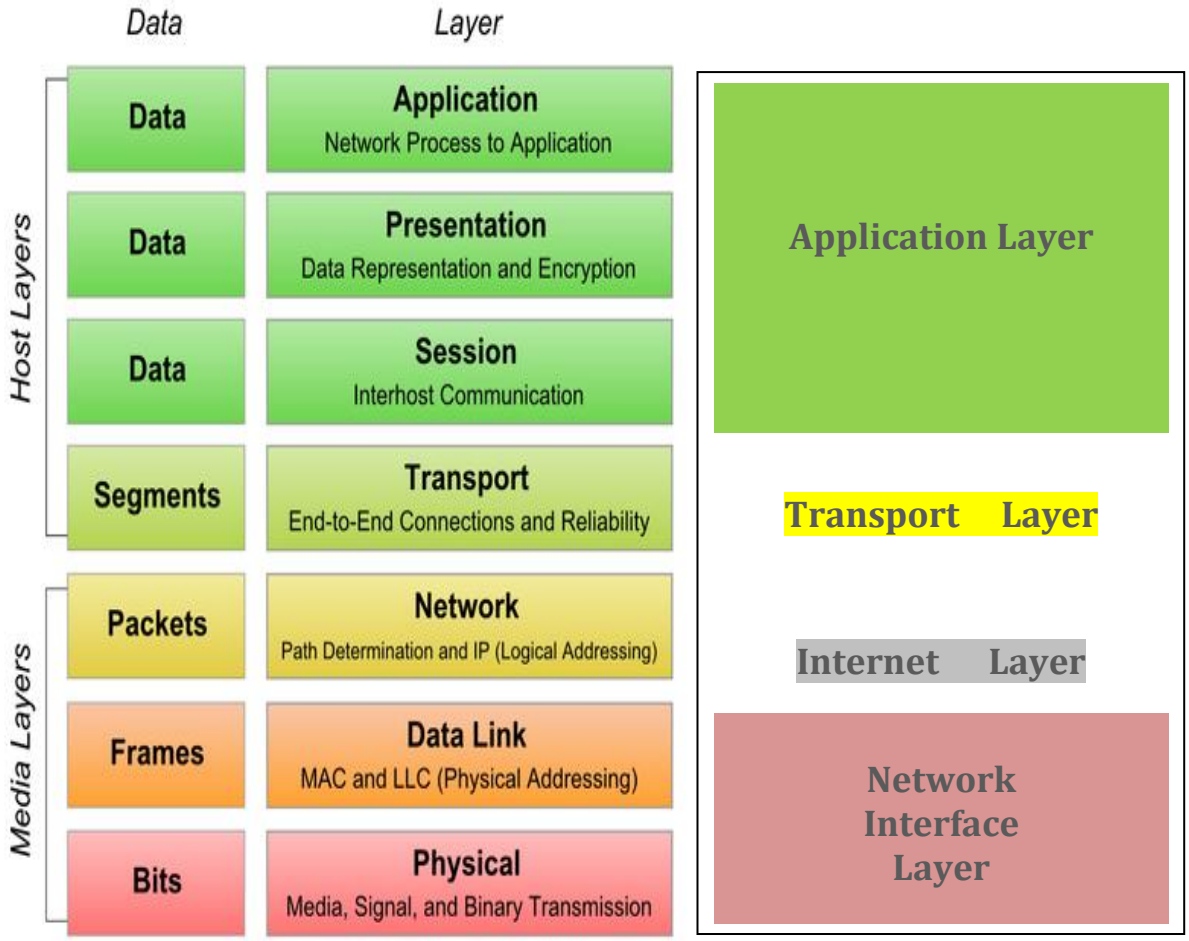
1. Η χρήση πιο ακριβών συσκευών λόγω του ότι πρέπει να έχουν την δυνατότητα να επεξεργάζονται πολλά κανάλια ταυτόχρονα.

2. Η δυνατότητα διατήρησης επικοινωνίας με περισσότερους σταθμούς (BS) για μια μόνο κλήση μειώνει τον αριθμό των ελεύθερων καναλιών για άλλες κλήσεις.

2.6 Layer 2 και Layer 3 Handover

Layer 2 Handover έχουμε όταν ο κινητός κόμβος κινείται στο ίδιο δίκτυο αλλά σε διαφορετικά BSS, ενώ Layer 3 Handover έχουμε όταν ο κινητός κόμβος κινείται σε διαφορετικά δίκτυα έχοντας κάθε φορά διαφορετικό MIP (CoA)

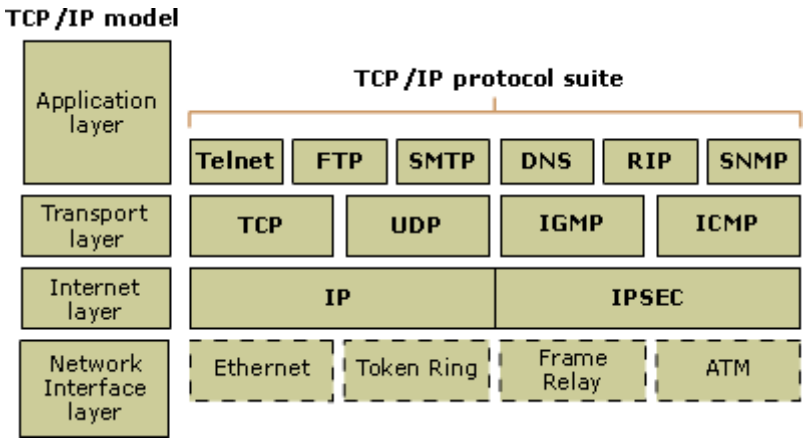
2.6.1 Το OSI και το TCP/IP Μοντέλο.



Εικόνα 2.26: OSI Model TCP/IP Model

Οι προδιαγραφές της επικοινωνίας δύο κόμβων μεταξύ τους μέσω ενός δικτύου (Internet) καθορίζεται από ένα μοντέλο το γνωστό OSI Model. Το μοντέλο OSI χωρίζεται σε εφτά επίπεδα (Layers) (Εικόνα 2.26). Κάθε επίπεδο είναι υπεύθυνο να διεκπεραιώσει ένα μέρος της όλης διαδικασίας δηλ. της επικοινωνίας δύο κόμβων που μπορεί να βρίσκονται σε μεγάλη απόσταση μεταξύ τους. Σε κάθε επίπεδο καθορίζεται ποια πρωτόκολλα χρησιμοποιούνται και ποια είναι η χρήση τους. Τα standards αυτού του μοντέλου έχουν καθοριστεί από το ISO , το Institute of Electrical and Electronic Engineers (IEEE) το American National Standards Institute (ANSI), και το International Telecommunications Union (ITU)[16].

Το μοντέλο TCP/IP βασίζεται πάνω σε τέσσερα επίπεδα αλλά εκτελεί ακριβώς τις ίδιες λειτουργίες όπως και το μοντέλο OSI (Εικόνα 2.27). Όλα τα πρωτόκολλα που ανήκουν στο μοντέλο TCP/IP καθορίζονται στα τρία ψηλότερα επίπεδα. Κάθε επίπεδο του μοντέλου TCP/IP αντιστοιχεί με ένα ή περισσότερα επίπεδα του μοντέλου OSI.

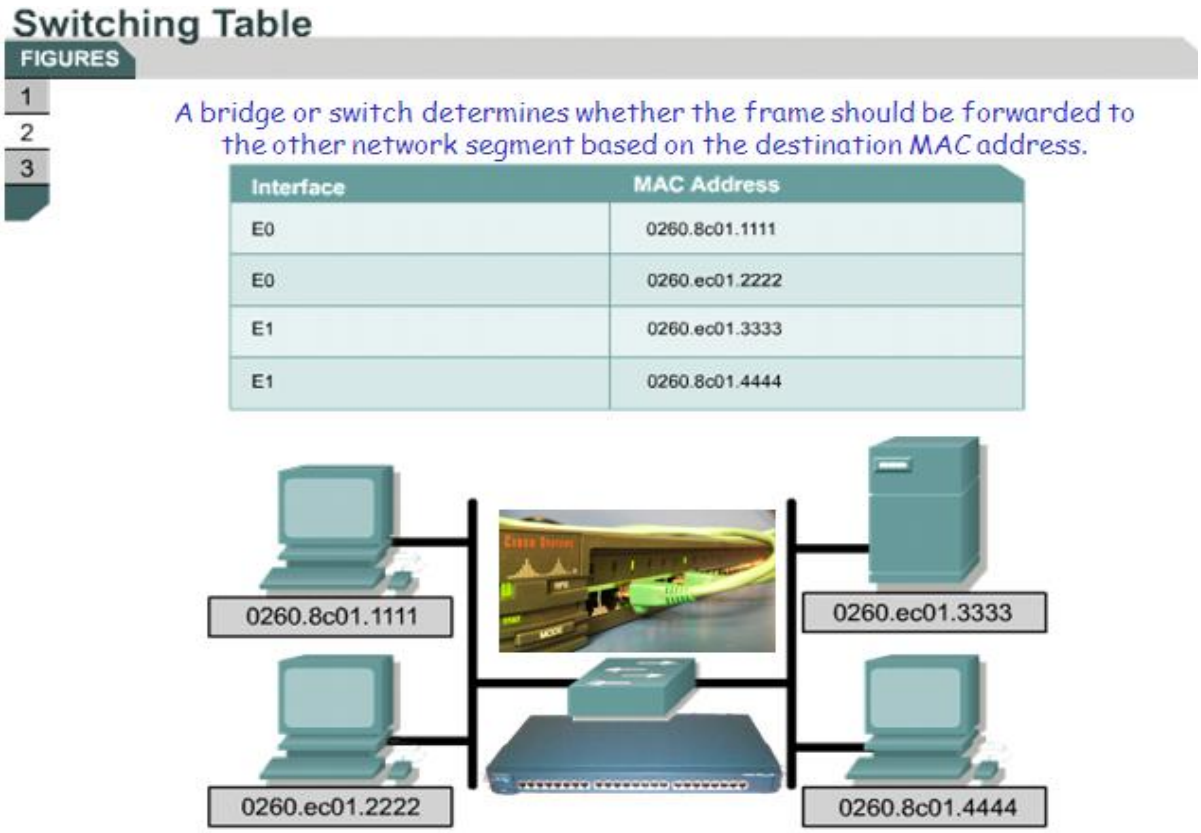


Εικόνα 2.27: TCP/IP Model

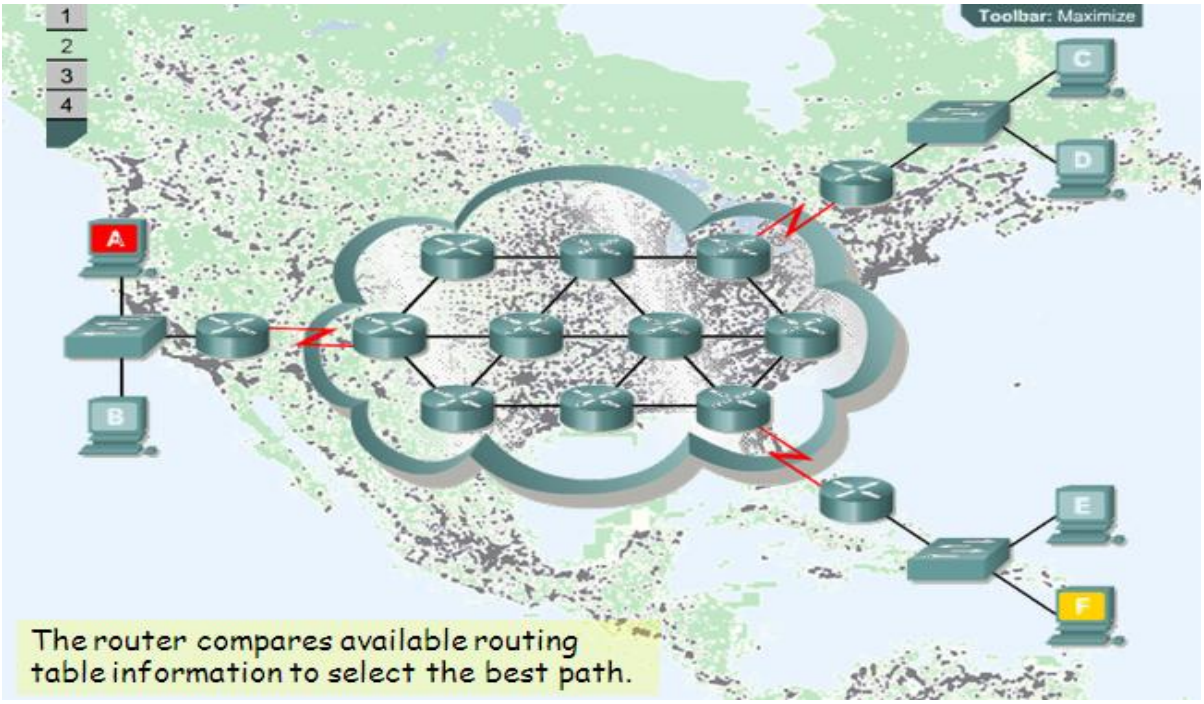
Στο μοντέλο TCP/IP, που είναι το μοντέλο που χρησιμοποιείται στο Internet, το επίπεδο ένα δηλ. το Network Interface layer αντιστοιχεί σε δύο επίπεδα του OSI μοντέλου και συγκεκριμένα στα επίπεδα ζεύξης δεδομένων ή Data Link Layer και στο φυσικό επίπεδο (Εικόνα 2.26). Το επίπεδο ζεύξης δεδομένων (Data Link Layer) παρέχει τα μέσα για την μεταφορά δεδομένων από μια συσκευή ενός τοπικού δικτύου σε μια άλλη συσκευή του ιδίου δικτύου. Αυτό γίνεται με τη χρήση της φυσικής διεύθυνσης ή mac-address των δύο συσκευών. Μια άλλη λειτουργία αυτού του επιπέδου είναι να μεταφέρει δεδομένα από το φυσικό επίπεδο προς το επίπεδο δικτύου. Σε αυτό το επίπεδο λειτουργούν οι δικτυακοί διακόπτες (switches) και οι δικτυακές γέφυρες (bridges). Είναι συσκευές οι οποίες διακινούν δεδομένα εσωτερικά ενός τοπικού δικτύου μόνο. Αποφάσεις για το από ποιά ports θα προωθήσουν τα δεδομένα προς τον προορισμό τους (destination host), λαμβάνουν με την βοήθεια πινάκων που έχουν καταγραμμένες πληροφορίες για αυτό τον σκοπό (εικόνα 2.28)[12].

Το επίπεδο δικτύου ασχολείται με την μεταφορά δεδομένων από και προς έναν προορισμό λαμβάνοντας υπόψη του τις IP-διευθύνσεις πηγής και προορισμού. Ασχολείται επίσης με την δρομολόγηση δεδομένων και αναφέρει τυχόν σφάλματα που μπορούν να εμφανιστούν κατά τις διαδικασίες αυτές. Σε αυτό το επίπεδο ο δρομολογητής (Router) διακινεί δεδομένα σε διάφορα δίκτυα λαμβάνοντας υπόψη την διεύθυνση προορισμού (destination IP-address). Χιλιάδες πακέτα διακινούνται σε μικρά χρονικά διαστήματα δια μέσου δρομολογητών για να πάνε στον προορισμό τους. Ο κάθε δρομολογητής διαθέτει ένα Routing table, με την βοήθεια του οποίου λαμβάνει αποφάσεις για την καλύτερη διαδρομή (best path) που πρέπει να προωθήσει τα πακέτα

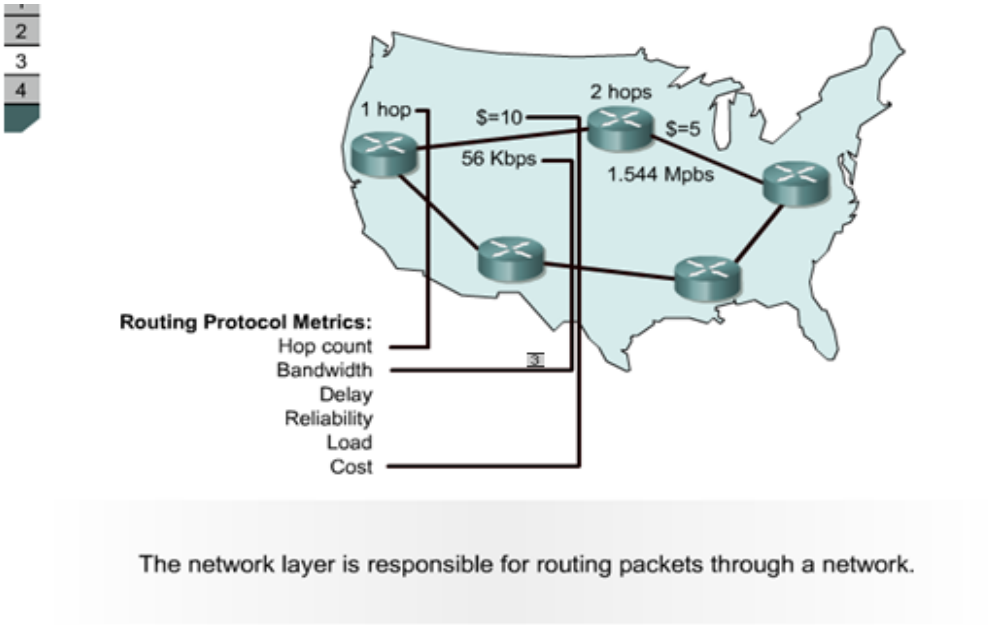
πληροφοριών για να πάνε γρήγορα και ασφαλισμένα προς τον προορισμό τους (Routing –Εικόνες 2.29-2.31)[12].



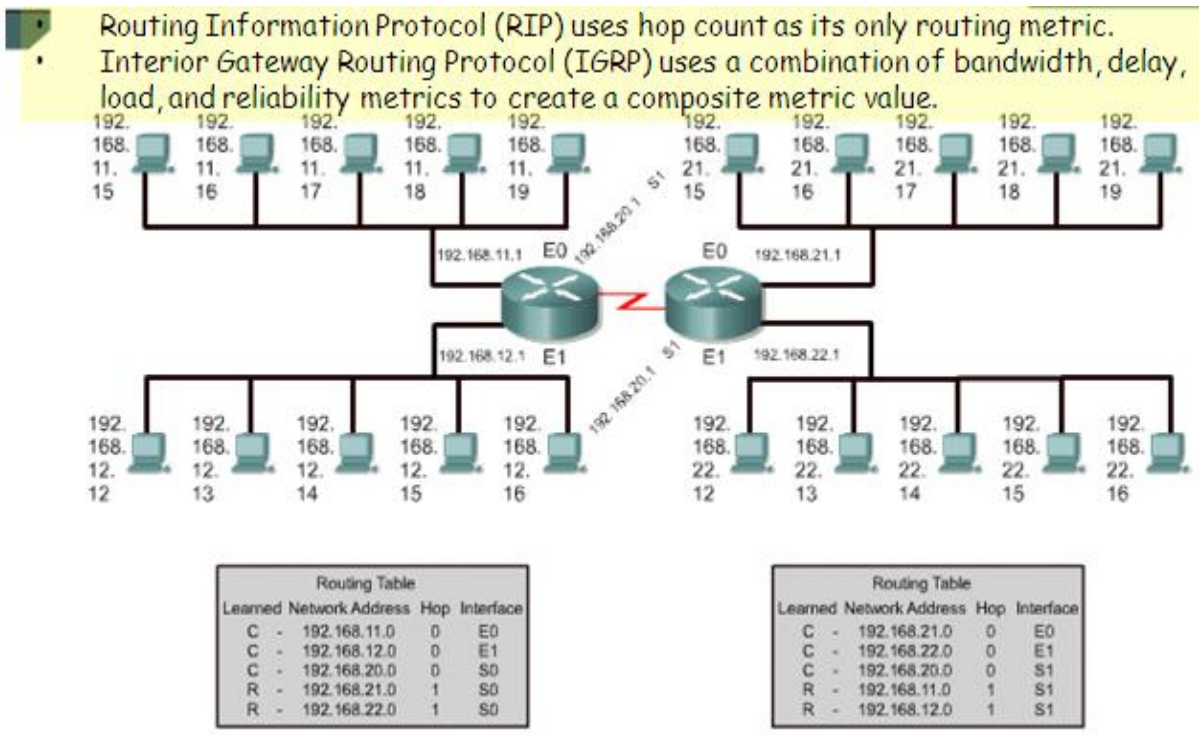
Εικόνα 2.28: Switching table [12]



Εικόνα 2.29 : Routing [12]



Εικόνα 2.30: Routing Protocols Metrics [12]

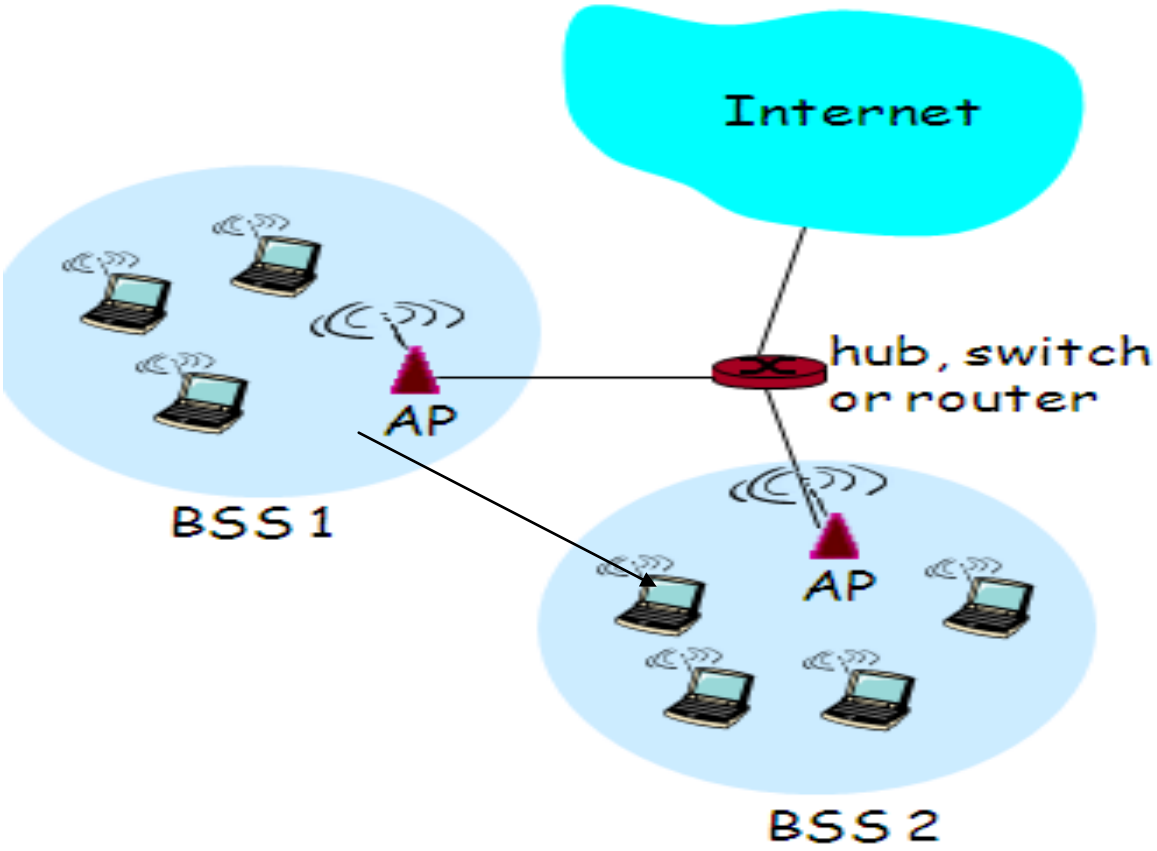


Εικόνα 2.31: Routing Tables [12]

Με την βοήθεια των πληροφοριών που ευρίσκονται μέσα στα routing tables τους, οι δρομολογητές αποφασίζουν την καλύτερη διαδρομή (best path) για να δρομολογήσουν τα δεδομένα προς τον προορισμό τους (destination network). Τα δίκτυα και οι διαδρομές προς αυτά, καθορίζονται από πρωτόκολλα τα λεγόμενα routing protocols (RIP,EIGRP,OSPF,IS-IS). Κάθε routing protocol καθορίζει βάσει κάποιων κριτηρίων (metrics π.χ. Number of hops, bandwidth, Transmission speed, Reliability) ποιες είναι οι καλύτερες διαδρομές (best paths) προς το δίκτυο προορισμού (destination network). Αυτές οι διαδρομές εισάγονται μέσα στα routing tables.

2.6.2 Data Link Layer (L2) Handover

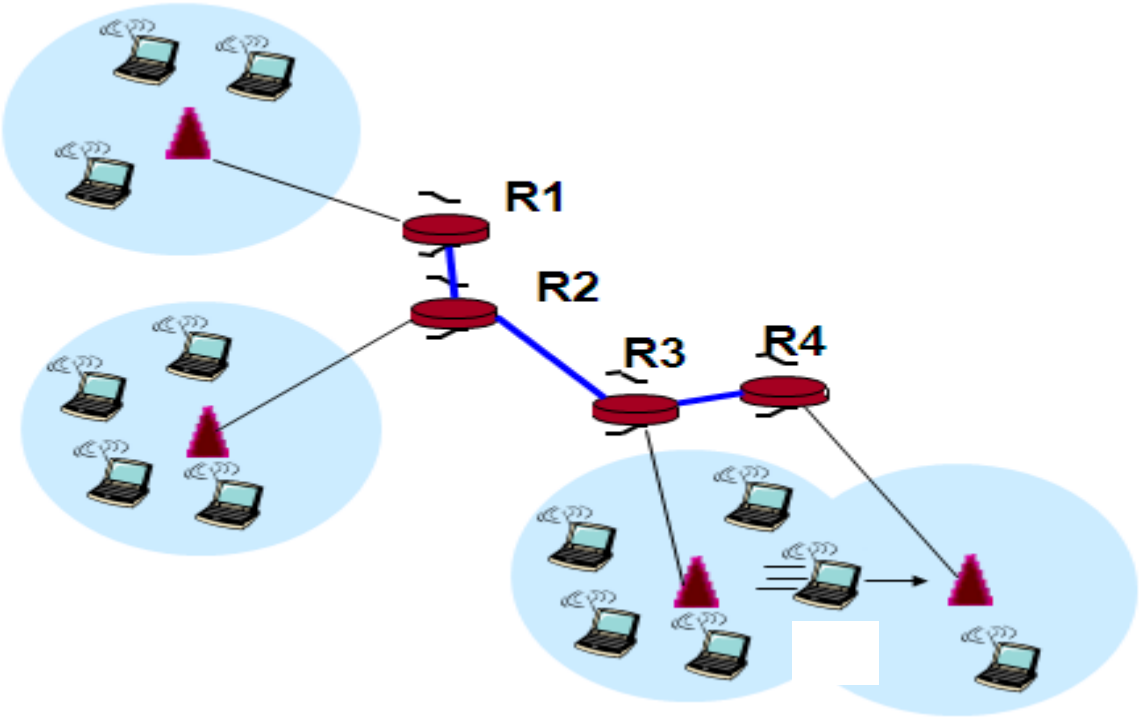
Ένα Data Link Layer (L2) Handover έχουμε όταν ένας κόμβος κινείται μεταξύ πολλών APs (2..N) τα οποία είναι συνδεδεμένα σε ένα switch και το switch είναι συνδεδεμένο με ένα δρομολογητή στο ίδιο subnet. Αυτό σημαίνει ότι όλοι οι κόμβοι των διαφόρων Basic Service Set (BSS) μαζί με όλα τα AP ανήκουν στο ίδιο Subnet (Εικόνα 2.32)[17]. Αυτό σημαίνει ότι ο κινητός κόμβος κατά την μετακίνηση του από το BSS1 προς το BSS2 θα διατηρήσει τη IP διεύθυνσή του. Απλώς θα χρειαστεί μόνο να γίνει το Authentication του στο νέο BSS που έχει μετακινηθεί.



Εικόνα 2.32: Data Link Layer handover

2.6.3 Network Layer (L3) Handover

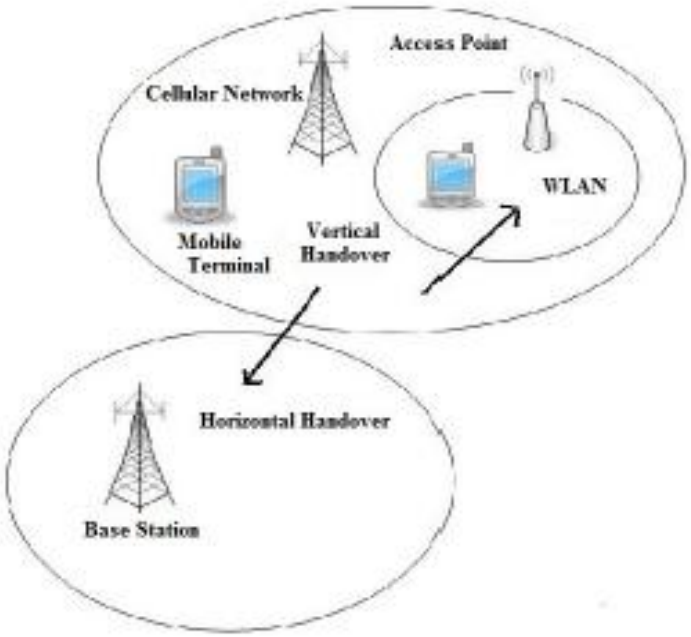
Ένα Network Layer (L3) Handover έχουμε όταν ένας κόμβος κινείται σε διαφορετικά υποδίκτυα, αφού κάθε φορά αλλάζει δρομολογητή (Εικόνα 2.33). Κατά την μετακίνησή του από δίκτυο σε δίκτυο ο κινητός κόμβος διατηρεί την μόνιμη διεύθυνσή του (Home Address HoA) καθώς και μια προσωρινή διεύθυνση (Care of Address CoA) την οποία χρησιμοποιεί όταν βρίσκεται σε κάποιο άλλο δίκτυο εκτός του οικείου δικτύου και αντιπροσωπεύει τον κινητό κόμβο στο δίκτυο στο οποίο ευρίσκεται την συγκεκριμένη χρονική στιγμή. Ο λόγος που διατηρεί και την μόνιμή διεύθυνση του είναι για να μην διακόπτεται η σύνδεσή του όταν μετακινείται σε άλλα δίκτυα [3].



Εικόνα 2.33: Network Layer handover

2.7 Vertical Handover

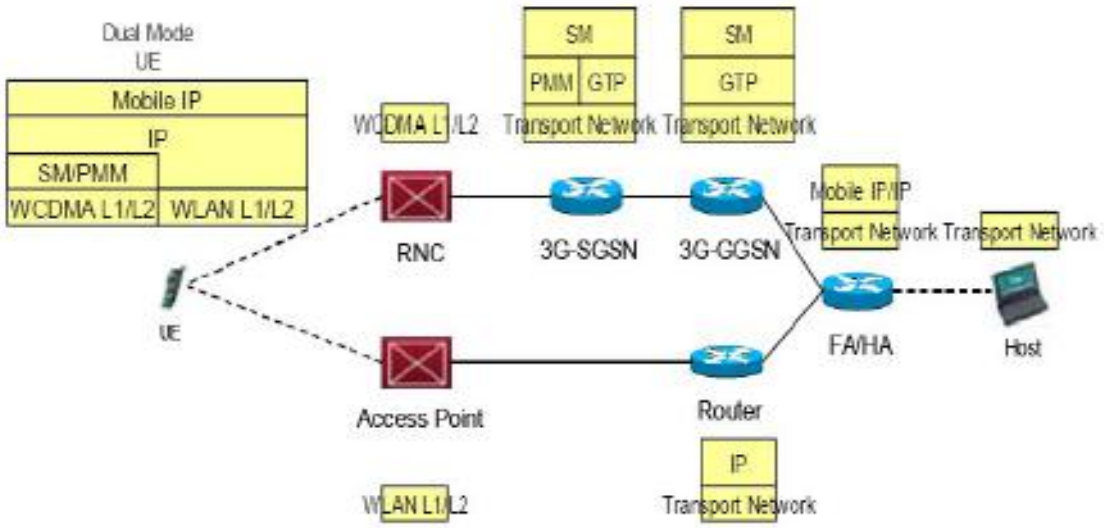
Ο όρος Vertical handover αναφέρεται στην διαδικασία μετάβασης, από μια τεχνολογία δικτύου σε άλλη τεχνολογία δικτύου (Vertical Handover), χωρίς την διακοπή της επικοινωνίας. Το Vertical handover διαφέρει από το Horizontal Handover στο ότι, το Horizontal Handover γίνεται μεταξύ δικτύων ίδιας τεχνολογίας (Εικόνα 2.34). Στα πλαίσια αυτής της μεταπτυχιακή εργασίας έχει γραφτεί ένα πρόγραμμα (DecideHandover.c), το οποίο ελέγχει αν υπάρχουν οι προϋποθέσεις και αποφασίζει αν ένας ασύρματος χρήστης θα γίνει Vertical Handover. Τις προϋποθέσεις και το πρόγραμμα θα τα δούμε αναλυτικά στο ΚΕΦ 6.



Εικόνα 2.34: Vertical Vs Horizontal handover σε ετερογενή δίκτυα [25]

2.7.1 Η Αρχιτεκτονική της Mobile IP Μεθόδου [27].

Σε αυτή την μέθοδο WLAN και 3G είναι δίκτυα peer to- peer.



Εικόνα 2.35: WLAN-3G Διασυνεργασία : Η αρχιτεκτονική της Mobile IP Μεθόδου [27]

1 Στα 3G δίκτυα, το User Equipment (UE) χρησιμοποιεί standart 3G Session Management (3G SM) και GPRS mobility management (GMM).

2 Στα WLAN, το UE χρησιμοποιεί απευθείας IP. Για την διαχείριση της κινητικότητας χρησιμοποιεί το mobile IP.

3 Κατά την περιαγωγή (roaming) του UE από το WLAN προς το 3G δίκτυο ή ανάποδα, το Mobile IP αναλαμβάνει να ξανακτίσει (restructure) την σύνδεση.

4 Η στοίβα πρωτοκόλλου για το UE είναι διπλής λειτουργίας η οποία περιέχει και τις δύο στοίβες. Την 3G καθώς και την WLAN στοίβα.

5 Το Handover από το 3G δίκτυο προς το WLAN δίκτυο γίνεται με απενεργοποίηση από το UE, της 3G στοίβας και χρήσης της IP στοίβας.

6 Το ίδιο IP μπορεί να διατηρηθεί σε περίπτωση WLAN-3G handover, ώστε να συνεχίσει η ίδια σύνοδος, με την περίπτωση 3G-WLAN (δηλ. να μην διακοπεί η σύνοδος)

7 Ο Foreign Agent (FA) και ο Home Agent (HA) είναι εγκατεστημένοι στο δρομολογητή πρόσβασης (AR) στο WLAN και στο GGSN στο 3G, έτσι ώστε οι FA / HA να μπορούν να βοηθήσουν τους δρομολογητές να χρησιμοποιούν την μέθοδο IP tunneling και να προωθούν τα πακέτα δεδομένων.

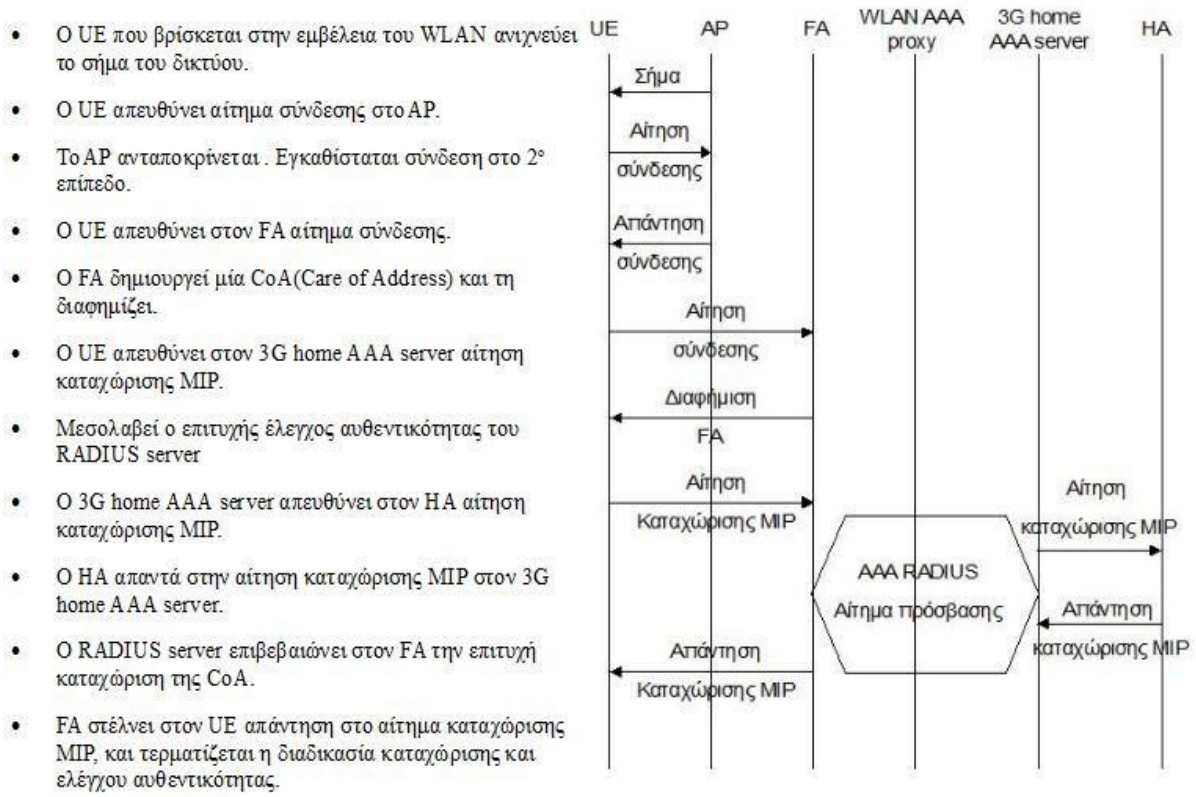
8 Όταν το User Equipment (UE) βρίσκεται έξω από το οικείο δίκτυο του, τότε αναγνωρίζεται από την Care Of Διεύθυνση (CoA) του. Αυτή η διεύθυνση δίνεται από το τοπικό δρομολογητή του συγκεκριμένου δικτύου (FA), ο οποίος διαχειρίζεται την αποθυλάκωση και την παράδοση των πακέτων στο UE. Το UE καταχωρεί την CoA στον Home Agent (HA) του, ο οποίος βρίσκεται στο οικείο δίκτυο του UE. Ο HA συλλαμβάνει όλα τα πακέτα που προορίζονται για το UE και τα δρομολογεί στη CoA του (IP Tunneling).

2.7.2 Η Πιστοποίηση Αυθεντικότητας στο 3G/WLAN [28]

Κατά την περιαγωγή (Roaming) κάποιου χρήστη από το 3G δίκτυο προς το WLAN, ή και αντίστροφα, είναι αναγκαία η πιστοποίηση αυθεντικότητας του χρήστη, για να μπορεί να έχει πρόσβαση στο WLAN/3G.

Στην Εικόνα 2.36 δίνεται περιγραφικά μια μέθοδος, για το πως γίνεται η απαραίτητη πιστοποίηση αυθεντικότητας στο 3G/WLAN. Το πλεονέκτημα αυτής της μεθόδου είναι ότι η πιστοποίηση αυθεντικότητας γίνεται παράλληλα με τη διαδικασία καταχώισης

MIP, συντομεύοντας το handover. Πιθανότερα η πιστοποίηση γίνεται από τον 3G παροχέα.



Εικόνα 2.36: Διαδικασία πιστοποίησης αυθεντικότητας στο 3G/WLAN [28]

Για πρόσβαση στα 3G δίκτυα ο έλεγχος πρόσβασης γίνεται με τον συνδυασμό EAP –AKA (Extensible Authentication Protocol – Authentication and Key Agreement). Επίσης συνδυασμός χρησιμοποιεί την εφαρμογή επίσης USIM (Universal Subscriber Identity Module), που τρέχει στη κάρτα UICC (Universal Integrated Circuit Card) επίσης συσκευής του χρήστη.

Στη συνέχεια δημιουργούνται τα κλειδιά κρυπτογράφησης και ακεραιότητας επίσης συνόδου, από το μυστικό κλειδί που είναι αποθηκευμένο στη μονάδα USIM, καθώς και στο AuC (κέντρο πιστοποίησης αυθεντικότητας).

Τι είναι οι κάρτες USIM : Είναι κάρτες που χρησιμοποιούν συσκευές που υποστηρίζουν δίκτυα 3G (UMTS) και είναι απαραίτητες για την επικοινωνία μέσω των δικτύων κινητής τηλεφωνίας 3G. Οι κάρτες αυτές περιέχουν τα στοιχεία του συνδρομητή, τον μοναδικό αριθμό του συνδρομητή (IMSI) και επίσης κάρτας, στοιχεία για την ασφάλεια

επίσης πρόσβασης, επίσης κωδικούς PIN και PUK, επίσης υπηρεσίες τις οποίες μπορεί να χρησιμοποιήσει ο εκάστοτε συνδρομητής κ.ά. Μπορούν να τρέξουν επίσης εφαρμογές, όπως πρόσβαση στον λογαριασμό του συνδρομητή στο δίκτυο κινητής τηλεφωνίας. Κάνουν επίσης κρυπτογράφηση των κλήσεων και των δεδομένων με κλειδιά που δημιουργεί η USIM.

2.7.3 Vertical Handover 3G/WLAN και WLAN/3G

Πιο κάτω θα γίνει μια περιγραφή του Vertical Handover μεταξύ ενός WLAN και 3G κυψελωτών δικτύων (UMTS) ή και αντίστροφα. Το πάνω κομμάτι του σχεδιαγράμματος (Εικόνα 2.37) εξηγεί το Handover από 3G σε WLAN και το κάτω κομμάτι (Εικόνα 2.37), το Handover από WLAN σε 3G (UMTS).

3G/ WLAN handover σενάριο

1 Υποθέτουμε ότι το 3G είναι το οικείο δίκτυο (Home Network) για το UE.

2 Μόλις αποφασιστεί (από το UE) το Handover στο WLAN, ξεκινά με ένα σύνολο Layer1/Layer2 (L1/L2) διαδικασιών Handover.

3 Το UE μπορεί να κινηθεί στο WLAN για ένα χρονικό διάστημα, και αργότερα να μετακινηθεί πίσω στο αρχικό 3G δίκτυο του (UMTS).

4 Για να εμποδίσει την αποσύνδεση του UMTS από το UE, επειδή το UMTS δεν λαμβάνει το περιοδικό Router Area (RA) μήνυμα ενημέρωσης από το UE, το UE στέλνει PDP / MM πλαίσιο αναμονής μήνυμα στον δικό του SGSN, για να διευκολύνει την προσπάθεια επανασύνδεσης του εάν μετακινηθεί πίσω στο UMTS, μετά από ένα χρονικό διάστημα.

5 Μετά από αυτό, το UE μπορεί να έχει πρόσβαση δικτύου IP και στέλνει ένα Solicitation Agent για να εντοπίσει τον τοπικό FA. Ο τοπικός FA αναθέτει μια CoA στον UE (Agent Advertisement).

6 Το UE στέλνει αίτηση εγγραφής της CoA του (Registration Request) στον HA του.

7 Μετά την καταχώρηση της CoA του UE στον HA και την ενημέρωση του UE (Registration Reply), τα πακέτα που αποστέλλονται στο οικείο δίκτυο του UE, θα προωθούνται από τον HA, στο δίκτυο επίσκεψης του UE (HA tunnel).

WLAN / 3G handover σενάριο.

1 Υποθέτουμε ότι το WLAN είναι το οικείο δίκτυο (Home Network) για το UE.

2 Μόλις αποφασιστεί (από το UE) το Handover στο 3G, ξεκινά με ένα σύνολο Layer1/Layer2 (L1/L2) διαδικασιών Handover.

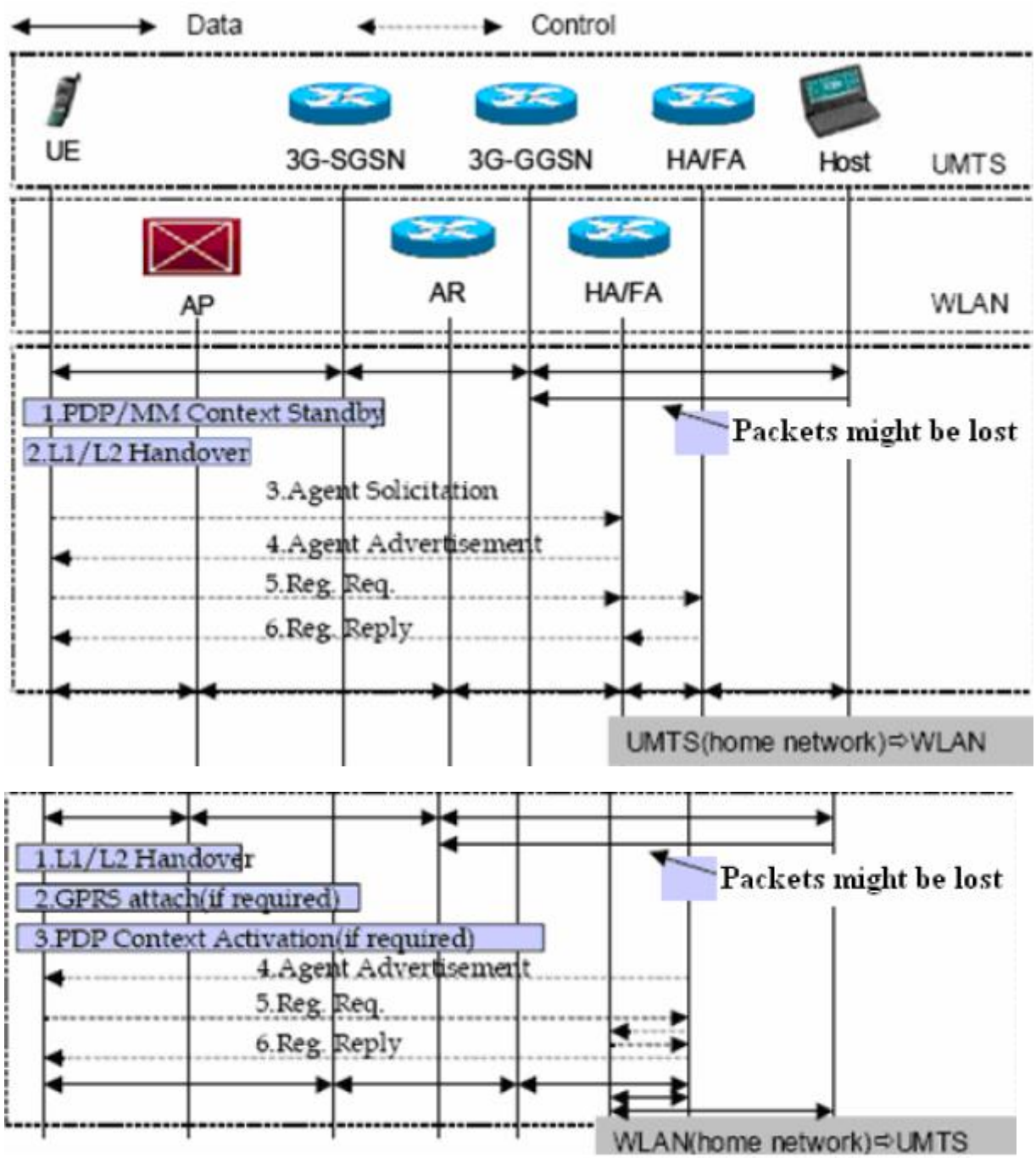
3 Το UE γίνεται attach με το GPRS (Διαδικασία δήλωσης του UE για την παρουσία του στο 3G δίκτυο και Authentication του UE από το SGSN).

4 PDP context activation (each context specifies one PDN it wants to access).

5 Ο τοπικός FA αναθέτει μια CoA στο UE (Agent Advertisement).

6 Το UE στέλνει αίτηση εγγραφής της CoA του (Registration Request) στον HA του.

7 Μετά την καταχώρηση της CoA του UE στον HA και την ενημέρωση του UE (Registration Reply). Τα πακέτα που αποστέλλονται στο οικείο δίκτυο του UE, θα προωθούνται από τον HA, στο δίκτυο επίσκεψης του UE (HA tunnel).

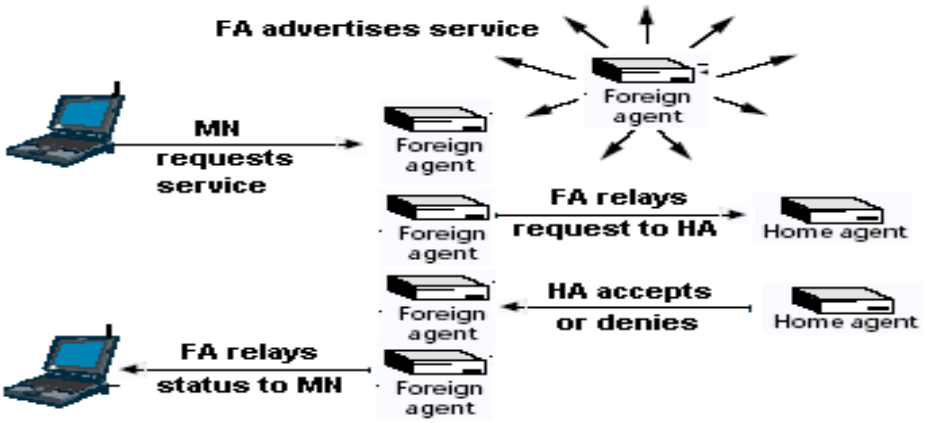


Εικόνα 2.37: WLAN-3G Vertical Handover χρησιμοποιώντας την μέθοδο Mobile IP [27].

Κεφάλαιο 3
IP Κινητικότητα

Mobile IP (ή IP κινητικότητα) είναι ένα Internet Engineering Task Force (IETF) πρότυπο πρωτόκολλο επικοινωνίας που έχει σχεδιαστεί για να επιτρέπει τους χρήστες κινητών συσκευών για να μετακινούνται από το ένα δίκτυο στο άλλο, διατηρώντας παράλληλα μια μόνιμη διεύθυνση IP χωρίς διακοπή της επικοινωνίας.

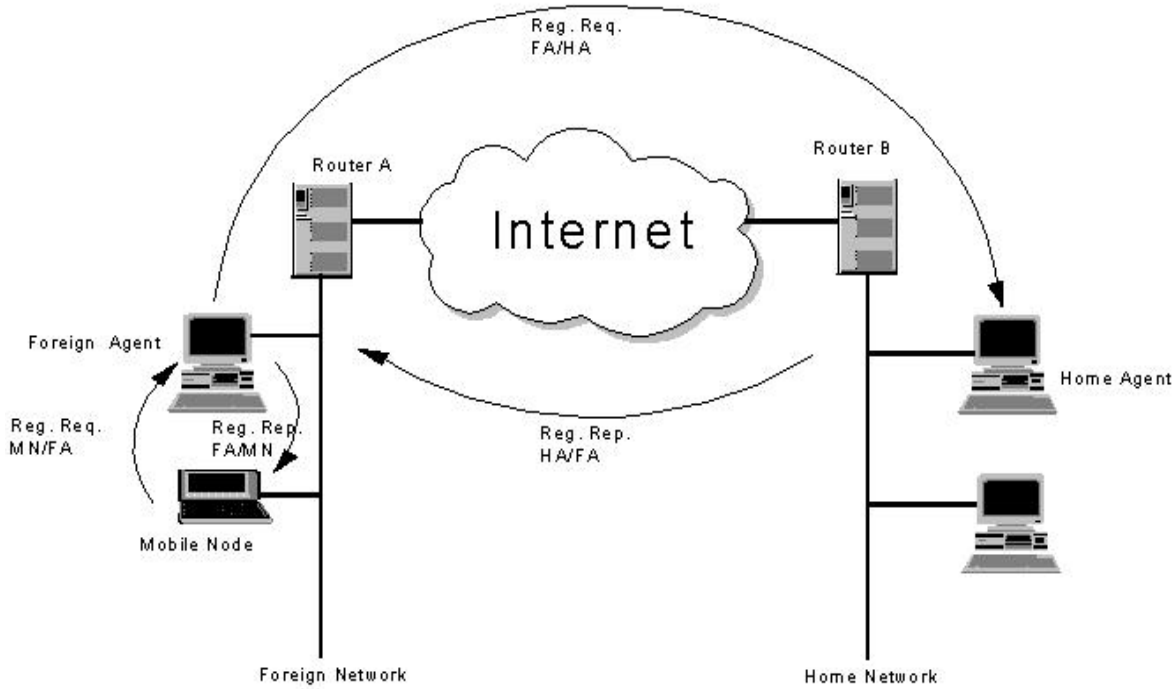
3.1 Mobile IPv4



Εικόνα 3.1: Registration overview 1

Το πρωτόκολλο διαδικτύου mobile IPv4 (MIPv4) έχει αναπτυχθεί από την IETF και υποστηρίζει την κινητικότητα των κόμβων (MN) με αναγνώριση των κόμβων μέσω της στατικής τους home address (HoA) ανεξάρτητα από την θέση τους στο internet. Το οικείο δίκτυο (Home Domain) στο οποίο ο MN ανήκει, ονομάζεται home network. Όταν ο MN μετακινείται μακριά από το οικείο δίκτυο σε κάποιο άλλο δίκτυο (foreign network), τότε πρέπει να στείλει πληροφορίες για την νέα του θέση και την νέα του προσωρινή IP διεύθυνση στον οικείο δρομολογητή που διαχειρίζεται το τοπικό δίκτυο. Ο οικείος αυτός δρομολογητής ονομάζεται home agent (HA). Ο home agent συλλαμβάνει και δρομολογεί τα πακέτα προς τον MN στη νέα του θέση. Η νέα προσωρινή IP διεύθυνση του MN στο foreign network ονομάζεται care-of address (CoA). Την CoA του ο MN την αποκτά από το λεγόμενο Foreign Agent (FA) (Εικόνες 3.1,3.2) , που είναι ο δρομολογητής που διαχειρίζεται το foreign network.

Ο MN καταγράφει την CoA στο HA μέσω binding update message. Ο HA πιστοποιεί την καταγραφή μέσω binding acknowledgement Η επικοινωνία μεταξύ MN και ενός απομακρυσμένου κόμβου CN (Correspondent Node) κινητού η σταθερού γίνεται μέσω του HA tunnel. Εάν κάποιος CN θέλει να επικοινωνήσει με τον MN τότε πρώτα στέλλει τα πακέτα στη HoA τα οποία συλλαμβάνει ο HA και τα δρομολογεί στη CoA του (IP Tunneling). Τότε τα παραλαμβάνει ο FA και τα προωθεί προς τον MN (εικόνα 3.2).



Εικόνα 3.2: Registration overview 2

Για να μπορεί ο HA να εντοπίζει εύκολα στο internet τον MN διατηρεί ένα πίνακα που ονομάζεται mobility binding table [3] ο οποίος πίνακας καταγράφει την αντιστοιχία μεταξύ της HoA και της CoA ενός MN. Κάθε εγγραφή που υπάρχει στον πίνακα αποτελείται από τρία πεδία: Home Address, Care-of-address, Lifetime (Διάστημα εγκυρότητας) (εικόνα 3.3).

Home Address	Care-of Address	Lifetime (in sec)
131.193.171.4	128.172.23.78	200
131.193.171.2	119.123.56.78	150

Εικόνα 3.3: Mobility binding table [3]

Ο Foreign Agent (FA) είναι ένας δρομολογητής που διαχειρίζεται ένα foreign network. Ο κάθε FA διατηρεί επίσης ένα πίνακα που ονομάζεται visitor table στον οποίο είναι καταχωρημένες πληροφορίες για όλους τους κινητούς κόμβους που βρίσκονται σε αυτό το δίκτυο.

Κάθε εγγραφή του πίνακα αυτού, αποτελείται από τέσσερα πεδία τα οποία είναι:

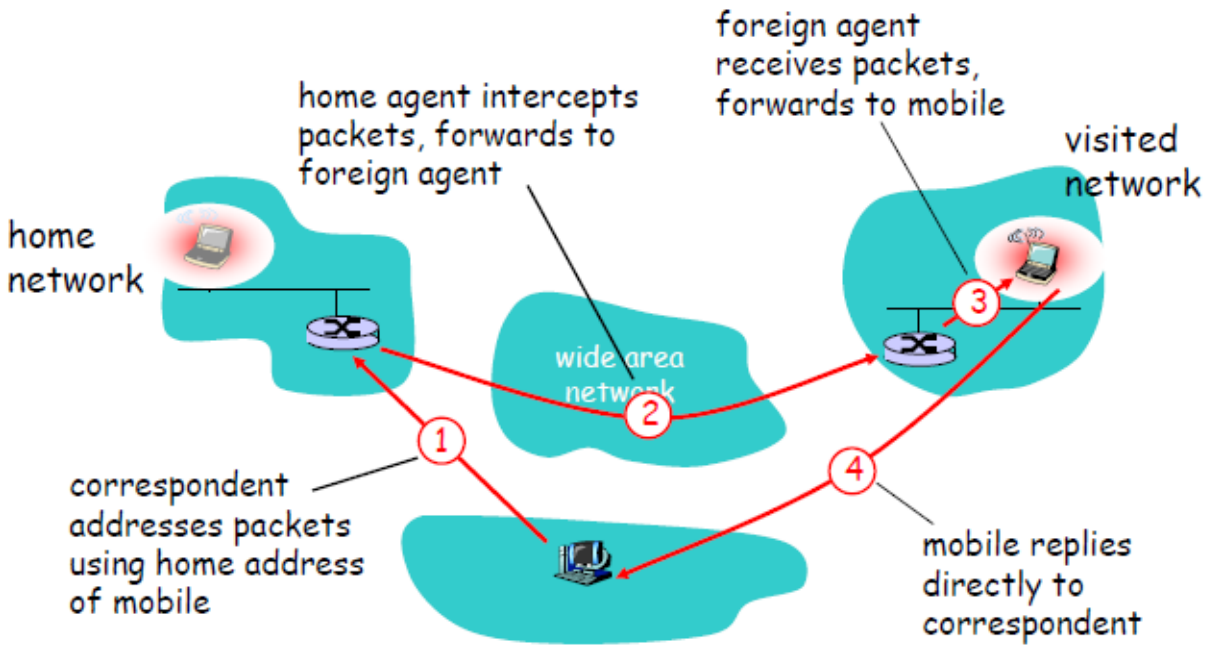
1 Home Address
2 Home Agent Address
3 MAC address
4 Lifetime (διάστημα εγκυρότητας)

Ένας τέτοιος πίνακας φαίνεται στην εικόνα 3.4

Home Address	Home Agent Address	Media Address	Lifetime (in s)
131.193.44.14	131.193.44.7	00-60-08-95-66-E1	150
131.193.33.19	131.193.33.1	00-60-08-68-A2-56	200

Εικόνα 3.4: Visitor table [3]

3.1.1 Επικοινωνία ενός Correspondent Node με τον Mobile Node.



Εικόνα 3.5: Mobility via Indirect Routing [17]

1 Ο Correspondent node (CN) θέλει να στείλει πληροφορίες στον Mobile node (MN). Τοποθετεί σαν destination IP την HoA του Mobile node που είναι η μόνιμη IP διεύθυνσή του.

2 Ο Home agent (HA) του Mobile node (MN) συλλαμβάνει τα πακέτα και κοιτάζει τον Mobility binding table του για να δει που βρίσκεται ο Mobile node (MN) εκείνη την χρονική στιγμή.

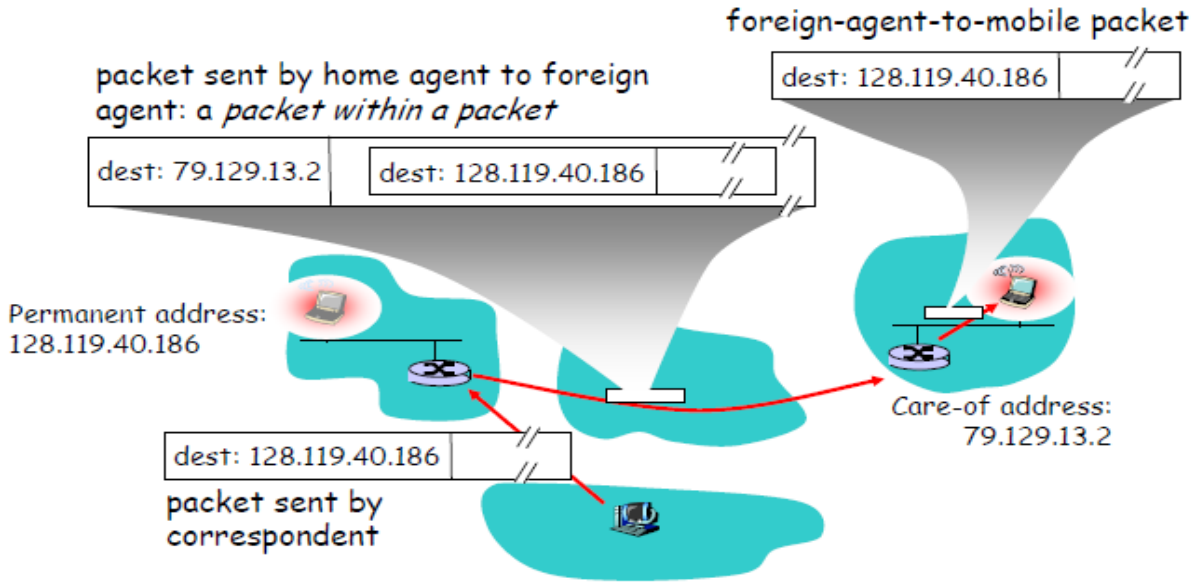
3 Ο Home agent (HA) βρίσκει την CoA του Mobile node (MN) . Στην συνέχεια δημιουργεί ένα νέο IP πακέτο με destination IP διεύθυνση, την CoA του Mobile node (MN). Το παλιό πακέτο τοποθετείται μέσα στο νέο και στη συνέχεια δρομολογείται μέσω τούνελ (IP within IP encapsulation-Tunneling [3]).

4 Όταν ο Foreign agent (FA) παραλάβει το πακέτο εξάγει το παλιό πακέτο και πληροφορείται την HoA του Mobile node (MN). Στη συνέχεια εξετάζει μέσα στο visitor table του αν υπάρχει αυτή η IP διεύθυνση καταχωρημένη. Αν υπάρχει,

τότε αλλάζει την destination MAC διεύθυνση του πακέτου με αυτή του Mobile node και προωθεί το πακέτο.

5 Εάν ο Mobile node θέλει να επικοινωνήσει με τον Correspondent node (CN), στέλλει το πακέτο αρχικά στο Foreign node και αυτός με την σειρά του το αποστέλλει απευθείας στον Correspondent node χρησιμοποιώντας IP δρομολόγηση.

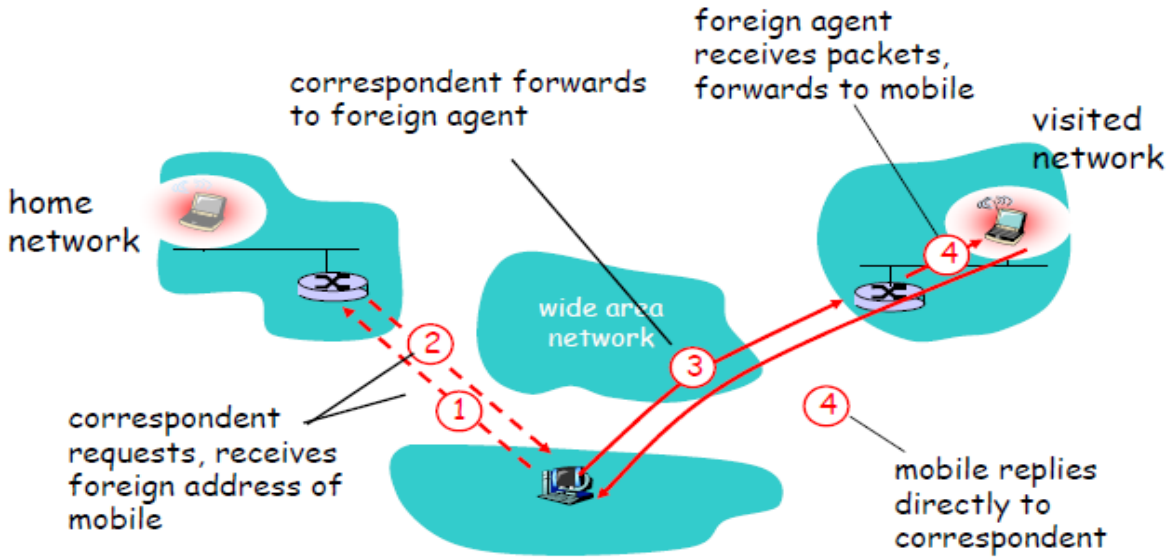
Παράδειγμα Mobile IP: indirect routing



Εικόνα 3.6: Mobile IP: indirect routing

Στη πιο πάνω εικόνα 3.6 ο CN θέλει να στείλει πακέτα στον MN. Ο CN τοποθετεί στο πακέτο σαν διεύθυνση προορισμού την μόνιμη IP διεύθυνση του MN (HoA-μόνο αυτή γνωρίζει) που είναι η 128.119.40.186. Το πακέτο πρώτα το παραλαμβάνει ο HA του MN και κοιτάζει στον πίνακά του (binding table) να δει την αντίστοιχη CoA του MN που είναι η 79.129.13.2. Αφού την βρει την ενθυλακώνει σε ένα νέο πακέτο (IP tunneling) και το αποστέλλει στον MN με διεύθυνση προορισμού την 79.129.13.2. Εκεί την παραλαμβάνει ο FA ο οποίος εξάγει το τελευταίο πακέτο που ήχε προστεθεί τελευταίο (IP tunneling). Ο FA πληροφορείται την HoA του MN (128.119.40.186) και ψάχνει στην συνέχεια στον δικό του πίνακα (Visitor table) να εντοπίσει την αντίστοιχη MAC-address της HoA. Αν υπάρχει τότε αλλάζει τη destination MAC διεύθυνση του πακέτου με αυτή του MN και προωθεί το πακέτο προς αυτό [17].

3.1.2 Mobility μέσω Direct Routing

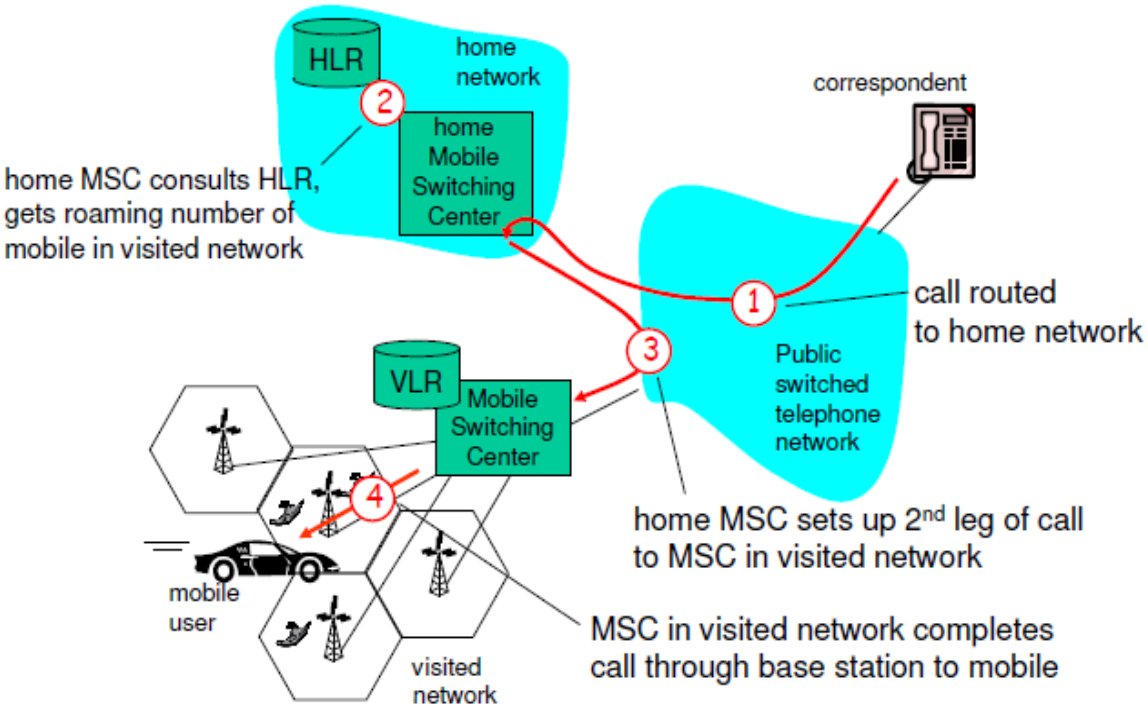


Εικόνα 3.7: απευθείας επικοινωνία του CN με τον MN (route optimization) [17]

Η λειτουργία του MIPv4 δεν είναι και τόσο αποδοτική όσο φαίνεται για τον πιο κάτω λόγο. Υποθέτουμε ότι ένας κόμβος (CN) θέλει να στείλει δεδομένα στον κινητό κόμβο (MN). Και τα δύο nodes βρίσκονται στο ίδιο δίκτυο αλλά ο Home agent του MN βρίσκεται σε κάποιο απομακρυσμένο δίκτυο. Αυτό σημαίνει ότι τα δεδομένα θα πρέπει να δρομολογηθούν πρώτα από το CN στον Home agent του MN και στη συνέχεια αυτός χρησιμοποιώντας την διαδικασία που εξηγήθηκε πιο πάνω (IP Tunneling) θα δρομολογήσει τα δεδομένα στον Foreign agent και αυτός με την σειρά του στον MN (Εικόνα 3.7). Αυτή η διαδικασία θα οδηγήσει σε μεγάλη end to end καθυστέρηση (Latency) μεταξύ του CN και του MN και αυτό στη συνέχεια θα οδηγήσει σε απώλεια πληροφοριών. Σε εφαρμογές όπως video conference ή video on demand που έχουν μεγάλες απαιτήσεις όσο αναφορά την ταχύτητα μεταφοράς δεδομένων και απαιτούν όσο το δυνατό μικρό Latency, θα οδηγήσει σε απώλεια πακέτων που αυτό σημαίνει χαμηλή ποιότητα της εικόνας. Επίσης σε κάθε αλλαγή δικτύου που γίνεται από τον MN αποκτάται και μια νέα CoA που αυτό σημαίνει και μια νέα ενημέρωση των mobility binding tables των δύο κόμβων. Αυτό προϋποθέτει και νέα handover καθυστέρηση, που μπορεί να προκαλέσει και προσωρινή διακοπή της σύνδεσης. Αυτό θα έχει ως αποτέλεσμα την απώλεια πακέτων που συνεπάγεται κακή ποιότητα της σύνδεσης [3].
Μια λύση του πιο πάνω προβλήματος θα μπορούσε να ήταν η απευθείας επικοινωνία του CN με τον MN (route optimization). Αυτό προϋποθέτει ότι ο CN θα διατηρεί ένα

πίνακα εγγραφών που θα εισάγονται όλες οι αναγκαίες πληροφορίες που αφορούν τον MN (π.χ CoA) που επικοινωνεί. Παράλληλα θα πρέπει ο MN να ενημερώνει για την νέα του CoA και τον CN και τον Home agent του. Με αυτό τον τρόπο θα μπορεί ο CN να επικοινωνεί απευθείας με τον MN χωρίς την διαμεσολάβηση του Home agent (Εικόνα 3.7).

3.1.3 GSM : Indirect Δρομολόγηση Τηλεφωνημάτων σε Κινητό Χρήστη



Εικόνα 3.8: GSM: indirect routing to mobile [17]

home network: Δίκτυο κινητής τηλεφωνίας στο οποίο έχει εγγραφεί ο χρήστης από τον παροχέα.

home location register (HLR): Βάση δεδομένων στο οικείο δίκτυο περιέχοντας τον αριθμό του κινητού, πληροφορίες για το προφίλ (Υπηρεσίες, προτιμήσεις, χρεώσεις), πληροφορίες για για την τωρινή τοποθεσία του κινητού.

visited network: Δίκτυο στο οποίο το κινητό ευρίσκεται εκείνη την χρονική στιγμή. Δεν μπορεί να είναι το οικείο δίκτυο.

visitor location register (VLR): Β.Δ. που περιέχει πληροφορίες για κάθε χρήστη που ευρίσκεται εκείνη την ώρα στο δίκτυο. Μπορεί να είναι και το οικείο δίκτυο.

Βήματα εντοπισμού ενός mobile user κατά την διάρκεια μια τηλεφωνικής κλήσης [17]:

1. Ο correspondent τηλεφωνεί στον mobile user. Τα πρώτα ψηφία του αριθμού προσδιορίζουν το οικείο δίκτυο του κινητού. Το τηλεφώνημα δρομολογείται μέσω του κινητού τηλεφωνικού δικτύου (PSTN) στο οικείο mobile switching center (MSC) στο οικείο δίκτυο του κινητού που έχει δεχτεί το τηλεφώνημα.

2. Το MSC λαμβάνει το τηλεφώνημα και αναθέτει στο HLR να προσδιορίσει την θέση του κινητού. Στη εύκολη περίπτωση ο HLR επιστρέφει το λεγόμενο mobile station roaming number (MSRN)-roaming number. Ο roaming number είναι ένας προσωρινός αριθμός που δίνεται στο κινητό κατά την επίσκεψή του στο visited network, είναι όμως άγνωστος στον correspondent. Εξυπηρετεί τον ίδιο σκοπό όπως η CoA στο mobile IP. Υπάρχει όμως η περίπτωση που ο HLR δεν έχει τον roaming number του κινητού. Σε αυτή την περίπτωση ο HLR επιστρέφει την διεύθυνση του VLR στο visited network. Ο MSC του οικείου δικτύου αιτείται το roaming number του κινητού από το VLR του visited network[1].

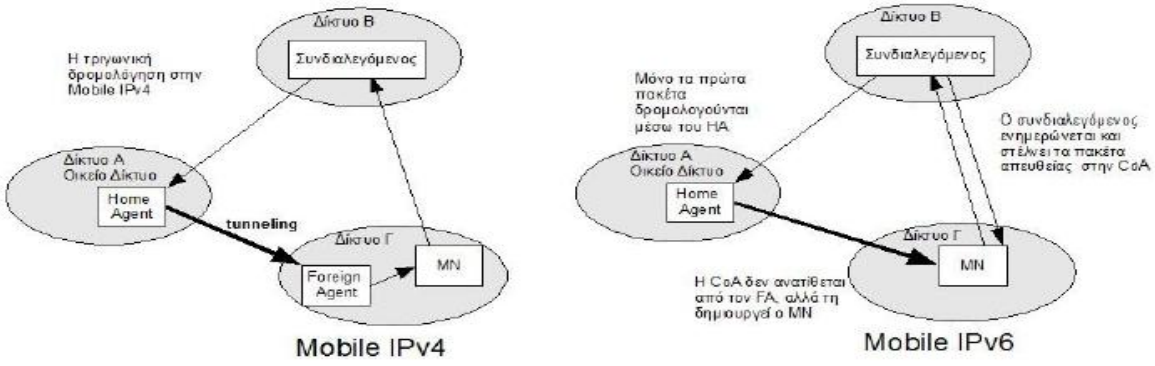
3. Αφού ο οικείος MSC παραλάβει τον roaming number από το VLR του visited network, το τηλεφώνημα συμπληρώνεται . Το τηλεφώνημα δρομολογείται από τον correspondent στον οικείο MSC και από τον οικείο MSC στον visited MSC και από εκεί στο σταθμό βάσης που εξυπηρετεί εκείνη την στιγμή το κινητό.

[1] Ένα ερώτημα που υπάρχει είναι πως μαζεύει ο οικείος HLR πληροφορίες για τον κινητό χρήστη. Όταν ο κινητός χρήστης επισκεφθεί ένα νέο δίκτυο (visited network) τότε ο κινητός χρήστης καταγράφεται από τον VLR του δικτύου που έχει επισκεφτεί και ταυτόχρονα του δίνεται ένα roaming number. Επίσης καταγράφεται το δίκτυο στο οποίο ευρίσκεται. Κατόπιν αιτήσεως του οικείου HLR του mobile , οι πληροφορίες αυτές αποστέλλονται στο οικείο HLR. Έτσι όταν ζητηθούν οι πληροφορίες αυτές από τον οικείο MSC τότε είναι διαθέσιμες [17].

3.1.4 Η Κινητικότητα στο 3G/WLAN

Στα 3G δίκτυα η διαχείριση της κινητικότητας γίνεται κυρίως στο 2ο επίπεδο, αλλά και στο επίπεδο δικτύου. Το δημοφιλέστερο πρωτόκολλο κινητικότητας σε επίπεδο δικτύου, είναι το MIP (Mobile IP). Το πρωτόκολλο διαδικτύου mobile IPv4 (MIPv4) έχει αναπτυχθεί από την IETF και υποστηρίζει την κινητικότητα των σταθμών (MS) με αναγνώριση των σταθμών μέσω της στατικής τους home address (HoA) ανεξάρτητα από την θέση τους στο internet. Το οικείο δίκτυο (Home Domain) στο οποίο ο MS ανήκει, ονομάζεται home network. Όταν ο MS μετακινείται μακριά από το οικείο δίκτυο σε κάποιο άλλο δίκτυο (foreign network), τότε πρέπει να στείλει πληροφορίες για την νέα του θέση και την νέα του προσωρινή IP διεύθυνση στον οικείο δρομολογητή που διαχειρίζεται το τοπικό δίκτυο. Ο οικείος αυτός δρομολογητής ονομάζεται home agent (HA). Ο home agent συλλαμβάνει και δρομολογεί τα πακέτα προς τον MS στη νέα του θέση. Η νέα προσωρινή IP διεύθυνση του MS στο foreign network ονομάζεται care-of address (CoA). Την CoA του ο MS την αποκτά από το λεγόμενο Foreign Agent (FA), που είναι ο δρομολογητής που διαχειρίζεται το foreign network.

Η επικοινωνία μεταξύ MS και ενός απομακρυσμένου σταθμού CS (Correspondent Station) κινητού η σταθερού γίνεται μέσω του HA tunnel. Εάν κάποιος CS θέλει να επικοινωνήσει με τον MN τότε πρώτα στέλλει τα πακέτα στη HoA τα οποία συλλαμβάνει ο HA και τα δρομολογεί στη CoA του (IP Tunneling). Τότε τα παραλαμβάνει ο FA ο οποίος τα αποθυλακώνει και τα προωθεί προς τον MS. Το μειονέκτημα αυτής τη μεθόδου είναι η αύξηση της διαδρομής και της καθυστέρησης εξαιτίας της τριγωνικής δρομολόγησης. Το πρόβλημα μπορεί να αντιμετωπισθεί με βελτιστοποίηση της διαδρομής, όπου εγκαθίσταται απευθείας διαδρομή ανάμεσα στους σταθμούς που επικοινωνούν (Direct Routing). Η διαδικασία αυτή υποστηρίζεται από το MIPv6 (Εικόνα 3.9), πρωτόκολλο όπου εξηγείται πιο κάτω.



Εικόνα 3.9: MIPv4 vs MIPv6

3.2 Mobile IPv6

Εδώ και αρκετά χρόνια υπήρχε η ανάγκη ενός πρωτοκόλλου το οποίο να συμπλήρωνε τα κενά του Mobile IPv4 και παράλληλα να έλυνε και το πρόβλημα της έλλειψης IP διευθύνσεων. Έτσι πριν μερικά χρόνια εμφανίστηκε το Mobile IPv6 (MIPv6) που θεωρείται η εξέλιξη του Mobile IPv4 (MIPv4). Το πρωτόκολλο αυτό διαθέτει διευθύνσεις των 128 bit, δηλ. τέσσερις φορές όσες μια IPv4 διεύθυνση. Γενικά τα πλεονεκτήματα του πρωτοκόλλου IPv6 είναι:

1 Η IP διεύθυνση πλέον αποτελείται από 128 bits. Αυτό μας δίνει τον τετραπλάσιο αριθμό διευθύνσεων.

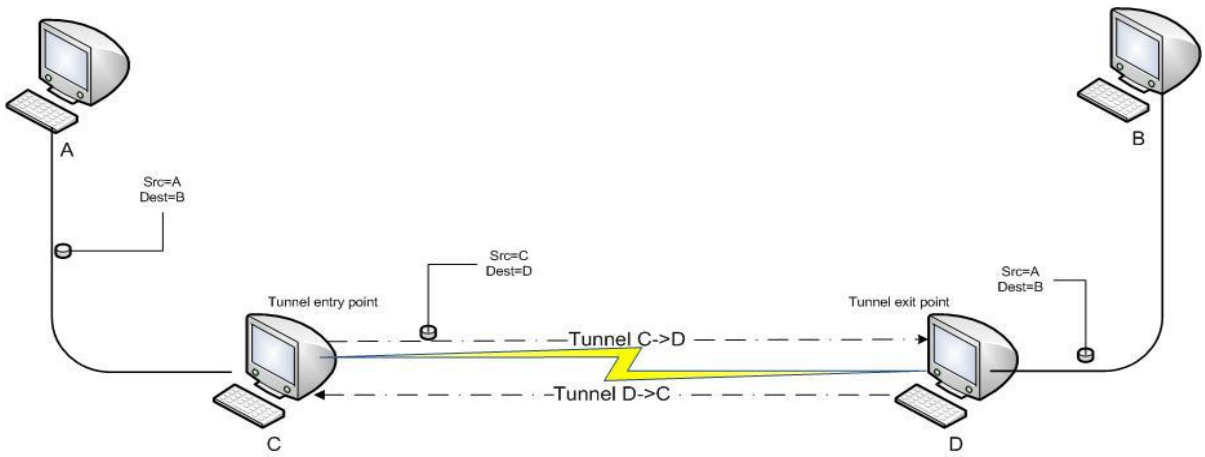
2 Απλοποίηση της κεφαλίδας με αποτέλεσμα μικρότερη καθυστέρηση και μείωση του κόστους δρομολόγησης.(κάποια πεδία του IPv4 δεν υπάρχουν πια).

3 Κατάργηση του NAT μηχανισμού ο οποίος βοήθησε στην μείωση της σπατάλης IP διευθύνσεων αλλά δημιουργούσε άλλα προβλήματα[3].

4 Παρέχει Ασφάλεια στο επίπεδο IP. Διαθέτει Πρωτόκολλα για Ασφάλεια όπως το IPsec το οποίο παρέχει ασφαλή ανταλλαγή IP πακέτων. Το IPsec παρέχει δύο encryption modes: Το transport mode κωδικοποιεί μόνο τα δεδομένα (payload) του πακέτου και όχι το header. Το Tunnel mode παρέχει κωδικοποίηση και στο header και στα δεδομένα.
5 Παρέχει ενσωματωμένη υποστήριξη για κινητικότητα (mobility). Διαθέτει ενσωματωμένους μηχανισμούς για τον σκοπό αυτό.

Η λειτουργία του MIPv6 είναι παρόμοια με αυτή του MIPv4. ¨Έχουμε τον κινητό κόμβο (MN) ο οποίος αρχικά βρίσκεται στο οικείο δίκτυο. Ο πράκτορας του οικείου δικτύου (Home Agent, HA) τροφοδοτεί τον MN με μια IP διεύθυνση η οποία αντιστοιχεί στο υποδίκτυο, την οποία διατηρεί μόνιμα, ανεξαρτήτως σε ποιο δίκτυο έχει μετακινηθεί. Ταυτόχρονα ο MN διατηρεί και μια προσωρινή διεύθυνση (Care-of Address,CoA) η οποία του παραχωρείται κάθε φορά που επισκέπτεται ένα ξένο δίκτυο και ισχύει μόνο για αυτό το δίκτυο. Ο MN φροντίζει κάθε φορά να ενημερώνει τον HA για την CoA που διατηρεί. Αυτό γίνεται για τον λόγο ότι όταν υπάρχουν πακέτα που προορίζονται για

τον MN, να μπορεί ο HA να τα προωθεί σε αυτόν στην σωστή IP διεύθυνση. Έτσι με αυτό τον τρόπο επιτυγχάνεται η επικοινωνία του MN με οποιονδήποτε χρήστη (CN) θέλει να επικοινωνήσει μεταξύ του, ανεξαρτήτως σε ποιο δίκτυο βρίσκεται εκείνη την χρονική στιγμή. Απλά ο χρήστης στέλλει τα δεδομένα στην HoA του MN (που πρέπει να του είναι γνωστή). Με αυτό τον τρόπο τα δεδομένα κατευθύνονται πρώτα προς το οικείο δίκτυο του MN, όπου ο HA του δικτύου τα παραλαμβάνει και τα προωθεί προς την CoA διεύθυνση του MN που του είναι γνωστή (IPv6 tunneling). Η επικοινωνία του MN με τον CN γίνεται ανάλογα. Ο MN επικοινωνεί με τον CN αφού πρώτα στείλει τις πληροφορίες προς τον HA (Reverse Tunneling) [19]. Στην πιο κάτω Εικόνα 3.10 γίνεται χρήση δύο IPv6 κατευθυνόμενων τούνελ για πραγματοποίηση αμφίδρομης επικοινωνίας.



Εικόνα 3.10: IPv6 Tunneling [3]

Στη Εικόνα 3.10 ο A θέλει να στείλει πληροφορίες προς τον B. Αρχικά ο C λαμβάνει τις πληροφορίες που στη συνέχεια τις ενθυλακώνει (encapsulation) σε ένα νέο πακέτο με διεύθυνση πηγής (source address) την διεύθυνση του και διεύθυνση προορισμού (destination address) την IP διεύθυνση του D. Στη συνέχεια προωθεί τις πληροφορίες μέσα στο tunnel. Μόλις ο D παραλάβει τις πληροφορίες τότε αφαιρεί το νέο πακέτο που προστέθηκε (de-encapsulation) και προωθεί τις πληροφορίες προς τον τελικό προορισμό που είναι το B[3].

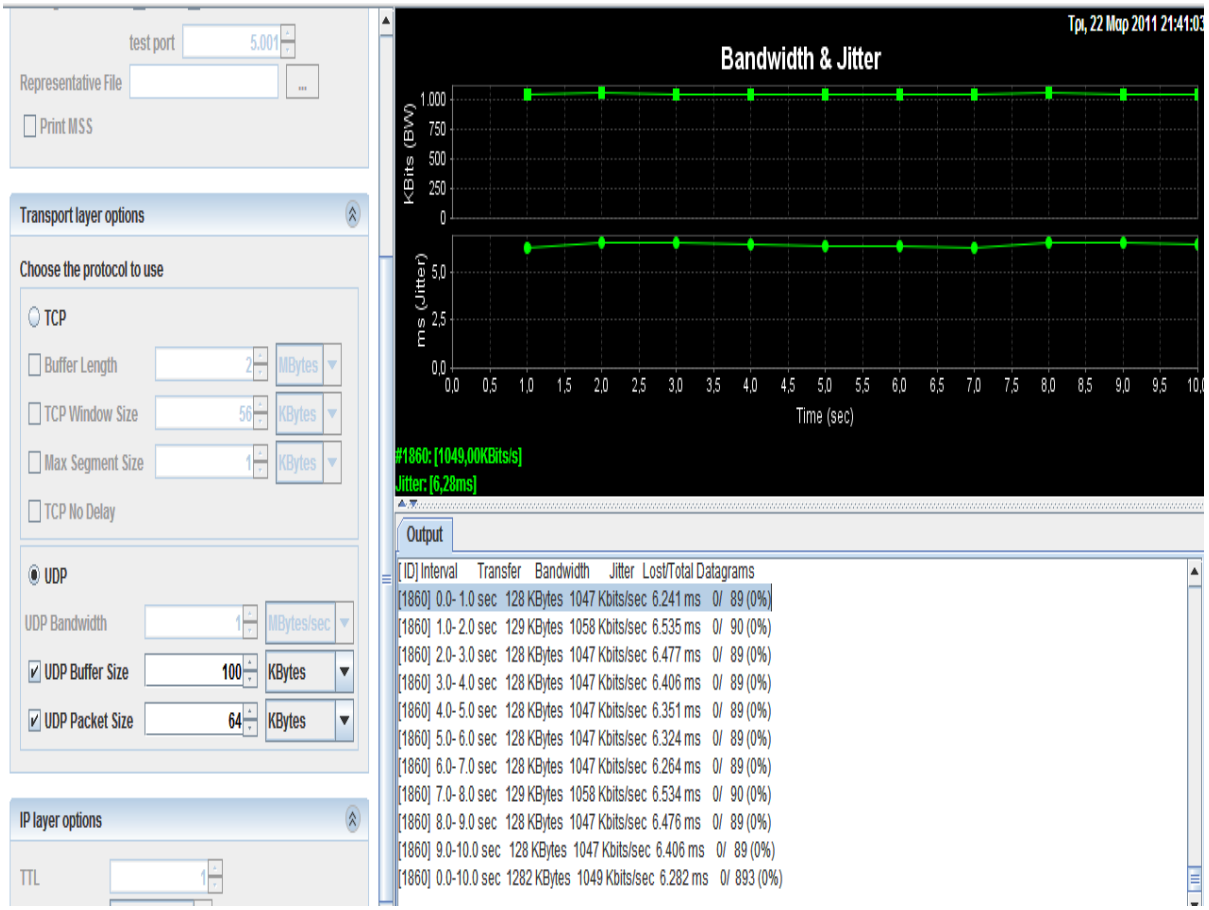
Δεν θα ήθελα να επεκταθώ με μεγαλύτερη λεπτομέρεια στο MIPv6 διότι σκοπός της μεταπτυχιακής εργασίας αυτής είναι να ασχοληθεί με την κινητικότητα κάνοντας χρήση του πρωτοκόλλου MIPv4. Θα μπορούσε κάποιος σε μια νέα μεταπτυχιακή εργασία να ασχοληθεί με τη κινητικότητα σε ετερογενή ασύρματα δίκτυα με χρήση του MIPv6 κάνοντας χρήση των πολλών πλεονεκτημάτων του MIPv6 έναντι του MIPv4.

Κεφάλαιο 4
Παρουσίαση Εργαλείων

Στην παρούσα μεταπτυχιακή εργασία όλες οι μετρήσεις που έγιναν για να διερευνηθούν τα χαρακτηριστικά ενός ασύρματου τοπικού δικτύου (WLAN) και να ελεγχθεί η ποιότητα του σήματος (QoS) μεταξύ ασύρματων κόμβων μέσα στο WLAN και του Router (AP- Network link), έγιναν με χρήση του προγράμματος iperf.

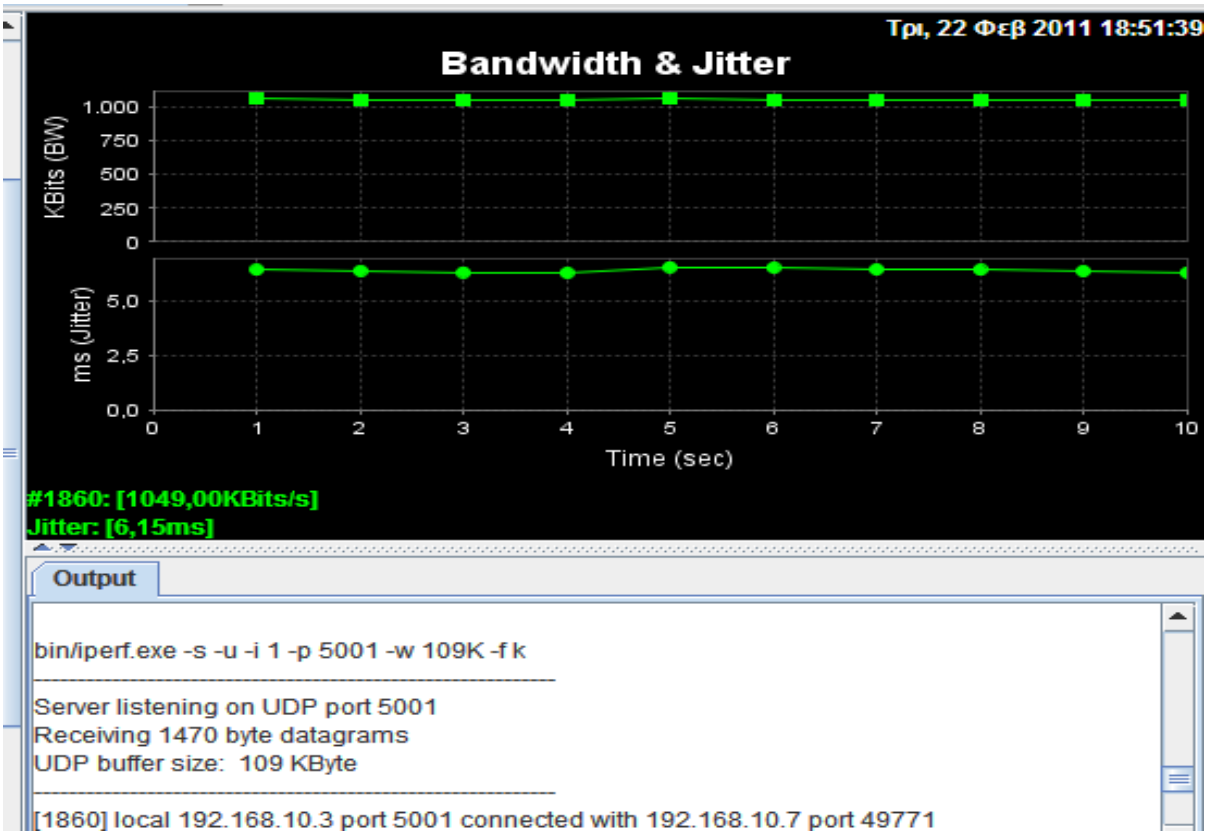
4.1 Παρουσίαση του Εργαλείου Iperf

Το Iperf είναι ένα εργαλείο που μπορεί να χρησιμοποιηθεί για την αξιολόγηση της απόδοσης ενός δικτύου, όσο αφορά την μέτρηση της ποιότητας του σήματος (QoS) μεταξύ διαφόρων κόμβων. Το Iperf μπορεί να δημιουργήσει TCP και UDP ροές δεδομένων και στη συνέχεια να μετρήσει την απόδοση του δικτύου που τις μεταφέρει. Το Iperf είναι γραμμένο σε C + +.



Εικόνα 4.1: Γραφική αναπαράσταση της ποιότητας της επικοινωνίας μεταξύ ενός Jperf server (windows) και ενός iperf linux client.

Στην εικόνα 4.1 παρατηρούμε στην γραφική παράσταση, την ποιότητα του σήματος μεταξύ δύο σημείων (end points). Στο πάνω μέρος της γραφικής παράστασης βλέπουμε το Bandwidth και στο κάτω μέρος το Jitter. Στο κάτω μέρος της οθόνης δεξιά το 1860 είναι το ID της μέτρησης , το 0.0-10.0 είναι το συνολικό χρονικό interval σε sec που διαρκεί η μέτρηση, το 1282 Kbytes είναι το σύνολο των KBytes που έγιναν transfer στο χρονικό διάστημα 0.0-10.0 sec, το 1049 Kbits/sec είναι το Bandwidth, το 6.146 ms είναι το Jitter , το 0/ είναι τα packet loss, το 893 είναι τα πακέτα που έγιναν transfer και τέλος το (0%) είναι το ποσοστό επί τοις % των packet loss. Σε μια καλή ποιοτική σύνδεση το packet loss δεν πρέπει να υπερβαίνει το 1% [22]. Packet loss rate μεταξύ 1% και 20% όμως είναι αποδεχτό[17]. Αριστερά παρατηρούμε ότι δουλεύουμε με UDP πρωτόκολλο Buffer Size=100 KBytes UDP Packet size=64Kbytes και τέλος πάνω βλέπουμε ότι το listening port που χρησιμοποιείται είναι το 5001 (default).



Εικόνα 4.2: Γραφική αναπαράσταση της ποιότητας της επικοινωνίας μεταξύ Jperf server (windows) και ενός iperf linux client.

Οι πληροφορίες που μας δίνει η πιο πάνω εικόνα 4.2 είναι αρκετά χρήσιμες για να εξαχθεί η ποιότητα της σύνδεσης. Βλέπουμε γραφικά ότι το Bandwidth ισούται περίπου με 1049 Kbits/sec. Το Jitter ισούται περίπου 6.146 ms. Το Jitter είναι η διακύμανση του latency και είναι πολύ βασικός παράγοντας σε network links που υποστηρίζουν voice over IP (VoIP). Ψηλό Jitter προκαλεί διακοπή της σύνδεσης (call). Στο παράθυρο output βλέπουμε στη πρώτη γραμμή την ενεργοποίηση του iperf μαζί με κάποια arguments που χρησιμοποιούμε για να εξάξουμε κάποιες πληροφορίες που μας είναι χρήσιμες. Στη 2η γραμμή το πρόγραμμα μα ς πληροφορεί το port number που χρησιμοποιεί ο server. Στη 3η γραμμή μα πληροφορεί για το μέγεθος των datagram's. Στη 4η γραμμή μας πληροφορεί για το μέγεθος του buffer. Τέλος στη τελευταία γραμμή έχουμε την source ip-address, το source port number, την destination ip-address και το destination port number.

-c	run in client mode
-u	use UDP rather than TCP
-i	seconds between periodic bandwidth reports
-p 5001	listening port number

-fk	format to report: Kbits, Mbits, KBytes, MBytes
-d	Simultaneous bi-directional

Εικόνα 4.3: Επεξήγηση των arguments του iperf

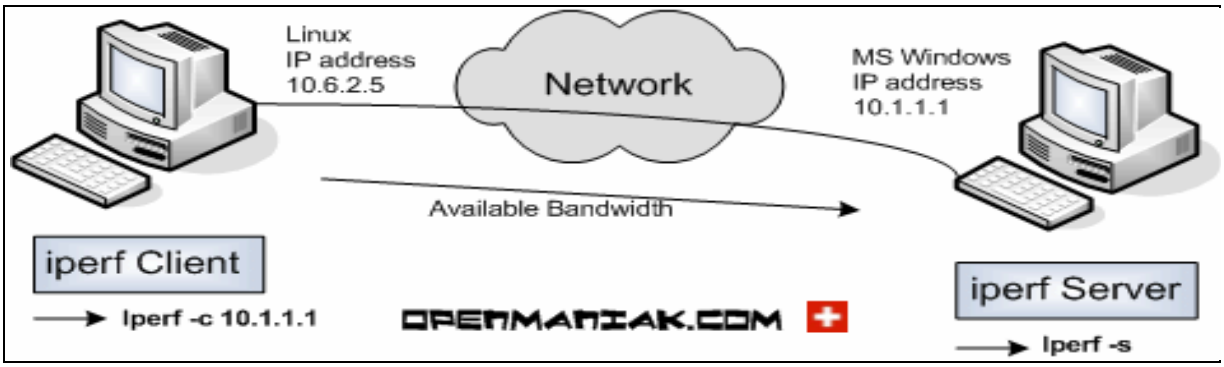
Το Iperf επιτρέπει στο χρήστη να ρυθμίσει διάφορες παραμέτρους που μπορούν να χρησιμοποιηθούν για τη δοκιμή ενός δικτύου, ή εναλλάξ, για βελτιστοποίηση ή βελτίωση ενός δικτύου. Το Iperf μπορεί να λειτουργήσει σαν client και σαν server, και μπορεί να μετρήσει τη διακίνηση μεταξύ των δύο άκρων, είτε προς μια κατεύθυνση ή αμφίδρομα**.** Είναι λογισμικό ανοικτού κώδικα και τρέχει σε διάφορες πλατφόρμες όπως Linux, Unix και Windows.

Όταν χρησιμοποιείται για τη δοκιμή UDP χωρητικότητας, το Iperf επιτρέπει στο χρήστη να καθορίσει το μέγεθος του datagram και παρέχει αποτελέσματα για το datagram throughput και την απώλεια πακέτων (packet loss). Όταν χρησιμοποιείται για τις δοκιμές TCP χωρητικότητας, το Iperf μετρά την απόδοση του ωφέλιμου φορτίου (payload).

Το Jperf είναι μια διεπαφή χρήστη (GUI) στο μπροστινό άκρο του Iperf (Εικ. 4.1/4.2). Το Iperf μπορεί να χρησιμοποιηθεί για τη σύγκριση των ενσύρματων και ασύρματων συσκευών δικτύωσης και τεχνολογιών με έναν αμερόληπτο τρόπο. Δεδομένου ότι είναι επίσης ανοικτή πηγή, η μεθοδολογία μέτρησης μπορεί να ελέγχεται από τον χρήστη. Ο πρωταρχικός στόχος του Ipef είναι να βοηθήσει στη ρύθμιση TCP συνδέσεων πάνω από ένα συγκεκριμένο μονοπάτι. Το πιο θεμελιώδες ζήτημα συντονισμού για το TCP είναι το μέγεθος του παραθύρου TCP, το οποίο ελέγχει τον όγκο των δεδομένων**.** Αν είναι πολύ μικρό, ο αποστολέας θα είναι αδρανής κατά περιόδους κατάσταση που μπορεί να οδηγήσει σε χαμηλές επιδόσεις. Σημειώστε ότι πολλά λειτουργικά συστήματα έχουν ανώτατα όρια για το μέγεθος του παραθύρου TCP. Αυτό μπορεί να είναι τόσο χαμηλό όσο 64 KB ή μέχρι MB.

Ακολουθεί παράδειγμα επικοινωνίας iperf Client σε πλατφόρμα Linux με iperf Server σε πλατφόρμα MS Windows [22]

Στην εικόνα 4.4 το iperf έχει γίνει installed σε Linux και Microsoft Windows. Στο Linux χρησιμοποιείται σαν client και στα Windows σαν server.



Εικόνα 4.4: iperf tests [22]

Παράμετροι που μπορούν να χρησιμοποιηθούν μαζί με το iperf για την εξαγωγή συγκεκριμένων πληροφοριών:

Iperf tests:			
no	Default settings	-p, -t, -i	Port, timing and interval
arg.	Data format	-u, -b	UDP tests, bandwidth settin
-b	Bi-directional bandwidth	-m	Maximum Segment Size disp
-r	Simultaneous bi-directional	-M	Maximum Segment Size sett
-d	bandwidth	-P	Parallel tests
-w	TCP Window size	-h	help
Iperf:			
no arg.	Default settings		
-d	Simultaneous bi-d		
-u, -b	UDP tests, bandwi		

Default Iperf settings:

By default, ο Iperf client ενώνεται με τον Iperf server στο TCP port 5001 και το bandwidth που εμφανίζεται στο Iperf είναι το bandwidth από τον client στον server. Εάν θέλουμε να χρησιμοποιήσουμε UDP tests, τότε χρησιμοποιούμε το -u argument.
Τα -d και -r Iperf client arguments μετρούν το bi-directional bandwidths.

```
Usage: iperf [-s|-c host] [options]
     iperf [-h|--help] [-v|--version]

Client/Server:
 -f, --format    [kmKM]   format to report: Kbits, Mbits, KBytes, MBytes
 -i, --interval  #        seconds between periodic bandwidth reports
 -l, --len       #[KM]    length of buffer to read or write (default 8 KB)
 -m, --print_mss          print TCP maximum segment size (MTU - TCP/IP header)
 -o, --output    <filename> output the report or error message to this specified file
 -p, --port      #        server port to listen on/connect to
 -u, --udp                use UDP rather than TCP
 -w, --window    #[KM]    TCP window size (socket buffer size)
 -B, --bind      <host>   bind to <host>, an interface or multicast address
 -C, --compatibility      for use with older versions does not sent extra msgs
 -M, --mss       #        set TCP maximum segment size (MTU - 40 bytes)
 -N, --nodelay            set TCP no delay, disabling Nagle's Algorithm
 -V, --IPv6Version        Set the domain to IPv6

Server specific:
 -s, --server             run in server mode
 -U, --single_udp         run in single threaded UDP mode
 -D, --daemon             run the server as a daemon

Client specific:
 -b, --bandwidth #[KM]    for UDP, bandwidth to send at in bits/sec
                          (default 1 Mbit/sec, implies -u)
 -c, --client    <host>   run in client mode, connecting to <host>
 -d, --dualtest           Do a bidirectional test simultaneously
 -n, --num       #[KM]    number of bytes to transmit (instead of -t)
 -r, --tradeoff           Do a bidirectional test individually
 -t, --time      #        time in seconds to transmit for (default 10 secs)
 -F, --fileinput <name>   input the data to be transmitted from a file
 -I, --stdin              input the data to be transmitted from stdin
 -L, --listenport #       port to recieve bidirectional tests back on
 -P, --parallel  #        number of parallel client threads to run
 -T, --ttl       #        time-to-live, for multicast (default 1)
 -Z, --linux-congestion <algo>  set TCP congestion control algorithm (Linux only)

Miscellaneous:
 -x, --reportexclude [CDMSV]   exclude C(connection) D(data) M(multicast) S(settings)
V(server) reports
 -y, --reportstyle C      report as a Comma-Separated Values
 -h, --help               print this message and quit
 -v, --version            print version information and quit
```

Εικόνα 4.5: iPerf command line arguments [22]

[KM] Indicates options that support a K or M suffix for kilo- or mega- Bytes

Ακολουθούν παραδείγματα χρήσης της εντολής iperf με διαφόρους παραμέτρους και παρουσίαση των αντίστοιχων εξαγόμενων πληροφοριών [22].

Το TCP window size είναι η ποσότητα πληροφοριών η οποία μπορεί να αποθηκευτεί προσωρινά κατά την διάρκεια της επικοινωνίας χωρίς την επισημοποίηση (Acknowledgment) από τον παραλήπτη. Μπορεί να είναι μεταξύ 2 και 65,535 bytes. Στο σύστημα Linux , όταν δίνεται το μέγεθος του TCP buffer δίνοντας -w argument, ο πυρήνας κατακρατεί διπλάσιο μέγεθος από ότι έχει ζητηθεί.

➔Client side:

#iperf -c 10.1.1.1 -w 2000

WARNING: TCP window size set to 2000 bytes. A small window size will give poor performance. See the Iperf documentation.
--
Client connecting to 10.1.1.1, TCP port 5001
TCP window size: 3.91 KByte (WARNING: requested 1.95 KByte)
--
[3] local 10.6.2.5 port 51400 connected with 10.1.1.1 port 5001
[3] 0.0-10.1 sec 704 KBytes 572 Kbits/sec

➔Server side:

#iperf -s -w 4000

Server listening on TCP port 5001

TCP window size: 3.91 KByte

---

[852] local 10.1.1.1 port 5001 connected with 10.6.2.5 port 51400

[ID] Interval Transfer Bandwidth

[852] 0.0-10.1 sec 704 KBytes 570 Kbits/sec

Communication port (-p), timing (-t) and interval (-i):

Το Iperf server port επικοινωνίας μπορεί να αλλάξει με τη χρήση του -p argument. Πρέπει να γίνει configured στον client και στον server με την ίδια τιμή, default είναι το TCP port 5001.

Το -t argument υποδηλώνει την χρονική διάρκεια σε seconds, default είναι 10 secs.

Το -i argument υποδηλώνει το διάστημα σε seconds μεταξύ περιοδικών bandwidth αναφορών.

→Client side:

#iperf -c 10.1.1.1 -p 12000 -t 20 -i 2

```
------------------------------------------------------------
Client connecting to 10.1.1.1, TCP port 12000
TCP window size: 16.0 KByte (default)
------------------------------------------------------------
[ 3] local 10.6.2.5 port 58316 connected with 10.1.1.1 port 12000
[ 3]  0.0- 2.0 sec   224 KBytes   918 Kbits/sec
[ 3]  2.0- 4.0 sec   368 KBytes   1.51 Mbits/sec
[ 3]  4.0- 6.0 sec   704 KBytes   2.88 Mbits/sec
[ 3]  6.0- 8.0 sec   280 KBytes   1.15 Mbits/sec
[ 3]  8.0-10.0 sec   208 KBytes   852 Kbits/sec
[ 3] 10.0-12.0 sec   344 KBytes   1.41 Mbits/sec
[ 3] 12.0-14.0 sec   208 KBytes   852 Kbits/sec
[ 3] 14.0-16.0 sec   232 KBytes   950 Kbits/sec
[ 3] 16.0-18.0 sec   232 KBytes   950 Kbits/sec
[ 3] 18.0-20.0 sec   264 KBytes   1.08 Mbits/sec
[ 3]  0.0-20.1 sec   3.00 MBytes   1.25 Mbits/sec [SUM]
```

→Server side:

#iperf -s -p 12000

```
------------------------------------------------------------
Server listening on TCP port 12000
TCP window size: 8.00 KByte (default)
------------------------------------------------------------
[852] local 10.1.1.1 port 12000 connected with 10.6.2.5 port 58316
[ ID] Interval Transfer Bandwidth
[852]  0.0-20.1 sec   3.00 MBytes   1.25 Mbits/sec [SUM]
```

→Client side:

#iperf -c 10.1.1.1 -p 12000 -t 20 -i 2

```
------------------------------------------------------------
Client connecting to 10.1.1.1, TCP port 12000
TCP window size: 16.0 KByte (default)
------------------------------------------------------------
[ 3] local 10.6.2.5 port 58316 connected with 10.1.1.1 port 12000
[ 3]  0.0- 2.0 sec   224 KBytes   918 Kbits/sec
[ 3]  2.0- 4.0 sec   368 KBytes   1.51 Mbits/sec
[ 3]  4.0- 6.0 sec   704 KBytes   2.88 Mbits/sec
```

[3] 6.0- 8.0 sec 280 KBytes 1.15 Mbits/sec
[3] 8.0-10.0 sec 208 KBytes 852 Kbits/sec
[3] 10.0-12.0 sec 344 KBytes 1.41 Mbits/sec
[3] 12.0-14.0 sec 208 KBytes 852 Kbits/sec
[3] 14.0-16.0 sec 232 KBytes 950 Kbits/sec
[3] 16.0-18.0 sec 232 KBytes 950 Kbits/sec
[3] 18.0-20.0 sec 264 KBytes 1.08 Mbits/sec
[3] 0.0-20.1 sec 3.00 MBytes 1.25 Mbits/sec [SUM]

UDP tests: (-u), bandwidth settings (-b)

Το UDP tests με το -u argument μας δίνει σημαντικές πληροφορίες για το jitter και το packet loss. Εάν δεν ορίσουμε το -u argument, Το Iperf χρησιμοποιεί το πρωτόκολλο TCP. Για να έχουμε καλή ποιότητα σύνδεσης, το packet lost δεν πρέπει να υπερβαίνει 1 %[22]. Τυχόν μεγάλος αριθμός packet loss, θα δημιουργήσει μεγάλο αριθμό TCP segment retransmissions γεγονός που θα επηρεάσει το bandwidth.

Το jitter είναι η διακύμανση της καθυστέρησης (latency) και δεν βασίζεται στη καθηστέρηση. Μπορεί να έχουμε ψηλό χρόνο ανταπόκρισης και πολύ χαμηλό jitter. Η τιμή του jitter είναι σημαντική στα network links που μεταφέρουν voice over IP (VoIP) για το λόγο ότι ψηλή τιμή του jitter μπορεί να διακόψει τηλεφωνική επικοινωνία (call).

Το -b argument επιτρέπει τον καθορισμό του bandwidth. Π.χ 10 Mbits/sec

Client side:

#iperf -c 10.1.1.1 -u -b 10m

Client connecting to 10.1.1.1, UDP port 5001
Sending 1470 byte datagrams
UDP buffer size: 108 KByte (default)
---
[3] local 10.6.2.5 port 32781 connected with 10.1.1.1 port 5001
[3] 0.0-10.0 sec 11.8 MBytes 9.89 Mbits/sec
[3] Sent 8409 datagrams
[3] Server Report:
[3] 0.0-10.0 sec 11.8 MBytes 9.86 Mbits/sec 2.617 ms 9/ 8409 (0.11%) [SUM]

Server side:

#iperf -s -u -i 1

Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size: 8.00 KByte (default)
---
[904] local 10.1.1.1 port 5001 connected with 10.6.2.5 port 32781
[ID] Interval Transfer Bandwidth Jitter Lost/Total Datagrams
[904] 0.0- 1.0 sec 1.17 MBytes 9.84 Mbits/sec 1.830 ms 0/ 837 (0%)
[904] 1.0- 2.0 sec 1.18 MBytes 9.94 Mbits/sec 1.846 ms 5/ 850 (0.59%)
[904] 2.0- 3.0 sec 1.19 MBytes 9.98 Mbits/sec 1.802 ms 2/ 851 (0.24%)
[904] 3.0- 4.0 sec 1.19 MBytes 10.0 Mbits/sec 1.830 ms 0/ 850 (0%)
[904] 4.0- 5.0 sec 1.19 MBytes 9.98 Mbits/sec 1.846 ms 1/ 850 (0.12%)
[904] 5.0- 6.0 sec 1.19 MBytes 10.0 Mbits/sec 1.806 ms 0/ 851 (0%)
[904] 6.0- 7.0 sec 1.06 MBytes 8.87 Mbits/sec 1.803 ms 1/ 755 (0.13%)
[904] 7.0- 8.0 sec 1.19 MBytes 10.0 Mbits/sec 1.831 ms 0/ 850 (0%)
[904] 8.0- 9.0 sec 1.19 MBytes 10.0 Mbits/sec 1.841 ms 0/ 850 (0%)
[904] 9.0-10.0 sec 1.19 MBytes 10.0 Mbits/sec 1.801 ms 0/ 851 (0%)
[904] 0.0-10.0 sec 11.8 MBytes 9.86 Mbits/sec 2.618 ms 9/ 8409 (0.11%) [SUM]

Maximum Segment Size (-m argument) display:

Το Maximum Segment Size (MSS) είναι η μεγαλύτερη ποσότητα πληροφοριών, σε bytes, την οποία μπορεί ένα computer να παρέχει σε ένα μονό, ατεμάχιστο TCP segment. Υπολογίζεται όπως πιο κάτω:

MSS = MTU - TCP & IP headers

The TCP & IP headers are equal to 40 bytes. Το MTU ή Maximum Transmission Unit είναι η μεγαλύτερη ποσότητα πληροφοριών την οποία μπορεί να μεταφερθεί σε ένα frame.

Ακολουθούν μερικά default MTU size διαφορετικών network topology:

Ethernet - 1500 bytes: used in a LAN.
PPPoE - 1492 bytes: used on ADSL links.
Token Ring (16Mb/sec) - 17914 bytes: old technology developed by IBM.
Dial-up - 576 bytes

Γενικά, μεγαλύτερο MTU (and MSS) φέρνει μεγαλύτερο bandwidth efficiency Το πιο κάτω παράδειγμα μας εξηγεί πως μπορώ να στέλλω 200-byte datagrams στα 100 Mbits/second:

carla@xena:~$ iperf -su -i 1
terry@uberpc:~$ iperf -c xena -u -l 200 -b 100m
[3] 0.0-10.0 sec 106 MBytes 88.9 Mbits/sec 0.219 ms 2683/187644 (1.4%)

Η επιλογή-i εμφανίζει την πρόοδο στην οθόνη κάθε δευτερόλεπτο. Ακόμη πιο σημαντικό σε VoIP είναι η τιμή jitter, η οποία σε αυτό το παράδειγμα είναι 0.219 χιλιοστά του δευτερολέπτου.

Κεφάλαιο 5

Διερεύνηση των Λειτουργιών Ασύρματων Τοπικών Δικτύων (WLAN)

Η διεξαγωγή των μετρήσεων γίνεται μόνο σε ασύρματο τοπικό δίκτυο WLAN, θεωρώντας ότι ο χρήστης θα μετακινηθεί από δίκτυο WLAN σε άλλο δίκτυο. Ο λόγος οφείλεται στην έλλειψη της αναγκαίας υποδομής σε άλλες τεχνολογίες. Στόχος είναι να ευρεθούν όλοι οι παράγοντες που επιδρούν θετικά ή αρνητικά, στην κακή ποιότητα του σήματος (QoS) μέσα σε ένα ασύρματο δίκτυο. Αναμένεται ότι παρόμοιοι παράγοντες θα υπάρχουν και στις άλλες ασύρματες επικοινωνίες.

Θα διεξαχθούν διάφορες μετρήσεις, για να διερευνηθούν τα χαρακτηριστικά ενός τοπικού ασύρματου δικτύου και θα εντοπισθούν οι παράγοντες που επηρεάζουν την ποιότητα του σήματος (QoS), μεταξύ των ασύρματων κόμβων και του Router (AP-Nework link) ενός ασύρματου τοπικού δικτύου (WLAN). Η διεξαγωγή αυτών των μετρήσεων έχει χωριστεί σε διάφορα σενάρια (18), για να μελετηθούν όσο το δυνατόν περισσότεροι παράγοντες και συνθήκες που επηρεάζουν το QoS. Αυτοί οι παράγοντες

θα ληφθούν υπόψη από το πρόγραμμα DecideHandover.c, που έχει γραφτεί για να αποφασίζει βάσει κάποιων προϋποθέσεων (packet loss), αν πρέπει να γίνει ένας χρήστης handover ή όχι. Δύο βασικοί παράγοντες που επηρεάζουν την ποιότητα του σήματος (QoS), είναι το Jitter και το Packet loss. Αυτοί οι δύο παράγοντες θα μελετηθούν στις μετρήσεις που θα διεξαχθούν.

5.1 Τι είναι το jitter

Στο πλαίσιο των δικτύων υπολογιστών, ο όρος jitter χρησιμοποιείται συχνά ως ένα μέτρο της μεταβλητότητας (variation) με την πάροδο του χρόνου, της καθυστέρησης πακέτων σε ένα δίκτυο. Ένα δίκτυο με σταθερή λανθάνουσα κατάσταση δεν έχει καμία μεταβολή (ή jitter). Αυτή η μεταβλητότητα της καθυστέρησης άφιξης των πακέτων προς τον προορισμό τους (packet delay), οφείλεται κυρίως σε μια πιθανή συμφόρηση ενός δικτύου άρα γίνεται πιο αργό, ή στην διαφορετική διαδρομή που ακολουθούν τα πακέτα μέχρι να φτάσουν στον προορισμό τους[18]. Αυτή η αυξομείωση του packet delay, είναι ένας παράγοντας που επηρεάζει την ποιότητα του σήματος (QoS),

Παράδειγμα [18]:
Υποθέτουμε ότι μια συσκευή VoIP στέλνει ένα RTP (Real-time Transport Protocol) πακέτο κάθε 20 χιλιοστά του δευτερολέπτου. Η εικόνα 5.1 δείχνει την χρονική άφιξη των πακέτων στο σημείο παραλαβής. Παρατηρούμε ότι τα πακέτα δεν φθάνουν ακριβώς κάθε 20 χιλιοστά του δευτερολέπτου. Αυτό σημαίνει ότι αν παίξουμε τον ήχο απευθείας όπως έρχεται, τότε θα έχουμε κακή ποιότητα του ήχου.

Εικόνα 5.1: Άφιξη πακέτων συσκευής VoIP

Για να λυθεί το πρόβλημα αυτό πρέπει να γίνει χρήση ενός buffer (jitter buffer). Μπορούμε να δημιουργήσουμε ένα buffer για να αποθηκεύει, π.χ. 100 χιλιοστά του δευτερολέπτου του ήχου - με το ρυθμό δειγματοληψίας π.χ των 8000 Hz, 100 χιλιοστά του δευτερολέπτου αντιστοιχούν σε 800 δείγματα. Αποθηκεύουμε τα εισερχόμενα ηχητικά καρέ στο buffer και αρχίζουμε το playout, όταν ο buffer είναι, τουλάχιστον γεμάτος μέχρι τη μέση.

5.1.1 Υπολογισμός του Jitter [18]

J(i) = J(i-1) + (|D(i-1,i)| - J(i-1))/16

Για τον υπολογισμό του jitter J(i) μετά που έχουμε παραλάβει το i-th πακέτο, υπολογίζουμε την αλλαγή του χρόνου άφιξης, και τη διαιρούμε με το 16 για να μειώσουμε το noise, και τον προσθέτουμε στη προηγούμενη τιμή του jitter. Η διαίρεση με το 16 βοηθά στη μείωση της επιρροής των μεγάλων τυχαίων αλλαγών.

Η τιμή D(i-1, i) είναι η διαφορά του χρόνου μεταφοράς για δύο πακέτα. Η διαφορά υπολογίζεται με τον τύπο που ακολουθεί:

$D(i,j) = (R_j - R_i) - (S_j - S_i) = (R_j - S_j) - (R_i - S_i)$

S_i είναι η ώρα αναχώρησης του πακέτου i και R_i είναι η ώρα άφιξης του πακέτου i.

Θεωρούμε ότι ο sender στέλλει ένα πακέτο κάθε 20 milliseconds και ότι ο αναγκαίος χρόνος μεταφοράς του πακέτου είναι 10 milliseconds. Θα χρησιμοποιούμε milliseconds στη θέση των timestamp units. Ξεκινούμε από το μηδέ (zero), και όχι από κάποια τυχαία τιμή. Ο πιο κάτω πίνακας δείχνει τους υπολογισμούς.

παράδειγμα για την δημιουργία του πιο κάτω πίνακα :

$D(2,3)= (R_3 – R_2) – (S_3-S_2) = (R_3-S_3) – (R_2-S_2)$

$= (49-40) – (30-20)$

$= 9 – 10 = -1$

$D(3,4)= (R_4 – R_3) – (S_4-S_3) = (R_4-S_4) – (R_3-S_3)$

$= (74-60) – (49-40)$

$= 14 - 9 = 5$

$J(3) = (J2) + (|D(2,3)| - J(2))/16$

$= 0 + (|-1| - 0)/16 = 1/16 = 0.0625$

$J(4) = (J3) + (|D(3,4)| - J(3))/16$

$= 0.0625 + (|5| - 0.0625)/16 = 0.0625 + (4.937/16) =$

$= 0.0625 + 0.308 = 0.371$

I	S_i	R_i	D(i, i-1)	J(i)
1	0	10	0	0
2	20	30	0	0
3	40	49	-1	0.0625
4	60	74	5	0.3711
5	80	90	-4	0.5979
6	100	111	1	0.6230
7	120	139	8	1.0841
8	140	150	-9	1.5788
9	160	170	0	1.4802
10	180	191	1	1.4501
11	200	210	-1	1.4220
12	220	229	-1	1.3956
13	240	250	1	1.3709
14	260	271	1	1.3477

Πίνακας 5.1 : Υπολογισμός του jitter

Όπως φαίνεται στον πίνακα, η τιμή του jitter ξεκινά να μεγαλώνει αργά (to grow slowly) παρά τη μεγάλη διαφορά (D) — Αυτό οφείλεται στη μείωση του noise. Όταν μειωθεί η διαφορά (D) (I> 8), παρατηρούμε ότι το jitter πλησιάζει τη μέση (mean) τιμή.

5.2 Σενάρια Εξέτασης Χαρακτηριστικών των WLAN

Αρχικά θα ερευνήσουμε διάφορα σενάρια για να δούμε πόσο επηρεάζεται το jitter και το packet loss από διάφορους παράγοντες:

1 Τον αριθμό των Access Points (AP)

2 Την μεταξύ τους απόσταση

3 Τον αριθμό των χρηστών μέσα στο ίδιο δίκτυο

4 Την ταχύτητα του κινητού κόμβου

5 Εμπόδια μεταξύ κόμβου και AP

6 Απόσταση κινητού κόμβου και AP (Ένταση του σήματος dBm)

7 Παραπλήσια BSS με χρήση και από τα δύο, του ιδίου καναλιού

8 Αυξομείωση του Bandwidth

Α/Α Σεναρίων	Protocol	Αρ. χρηστών	Ταχύτητα κίνησης	Αριθμός Εμποδίων Wall / Floor	Απόσταση από AP(m)	Αριθμός APs	Απόσταση των AP(m) μεταξύ τους	Iperf-Bandwidth Mbps	Signal strength dBm
1	UDP	1	0	OXI	1	1	0	1	-36
2	UDP	1	0	2 walls	10	1	0	1	-83
3	UDP	1	0	1 wall/floor	15	1	0	1	-87
4	UDP	1	3m/sec	2 walls	10	1	0	1	-82
5	UDP	2	0	OXI	1	2	0.5	1	-36/-33
6	UDP	2	0	2 walls	10	2	0.5	1	-83/-72
7	UDP	2	0	1 wall/floor	15	2	0.5	1	-87/-88
8	UDP	2	3m/sec	2 walls	10	2	0.5	1	-83/-72
9	UDP	2	0	OXI	1	2	10	1	-36/-33
10	UDP	2	0	2 walls	10	2	10	1	-83/-72
11	UDP	2	0	1 wall/floor	15	2	10	1	-87/-88
12	UDP	2	3m/sec	2 walls	10	2	10	1	-83/-72
13	UDP	2	0	OXI	1	3	1	1	-36/-33
14/ 14*	UDP	2	0	2 walls	10	3	10	1	-83/-72
15	UDP	2	3m/sec	2 walls	10	3	10	1	-83/-72
16/ 16*	UDP	2	0	OXI*	1	2	1	100	-36/-33
17/ 17*	UDP	2	0	1wall/floor*	10	2	10	100	-83/-72
18	UDP	1	0	OXI	1	1	0	0	-36

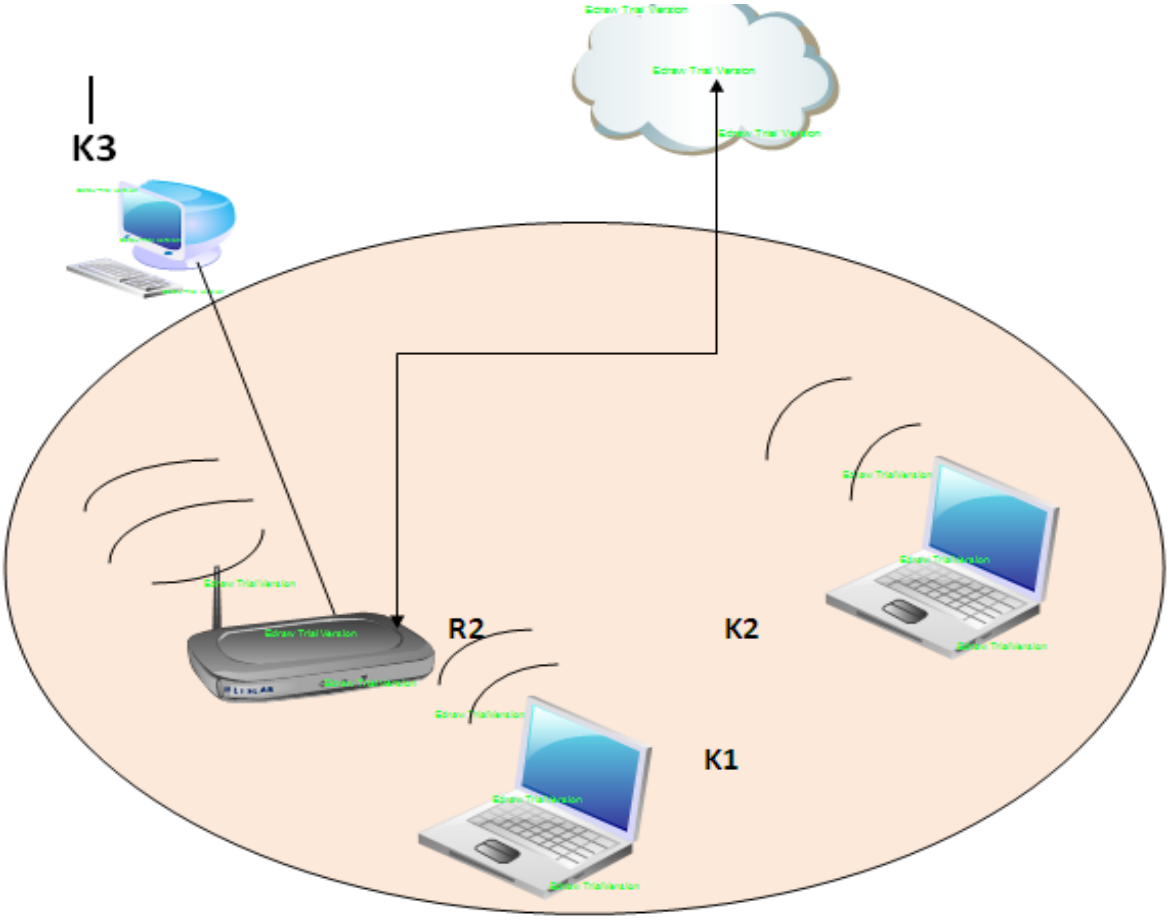
Πίνακας 5.2: Πίνακας σεναρίων

Σημείωση: Όλες οι μετρήσεις του signal strength γίνονται με την βοήθεια του προγράμματος inSSIDer 2.0.

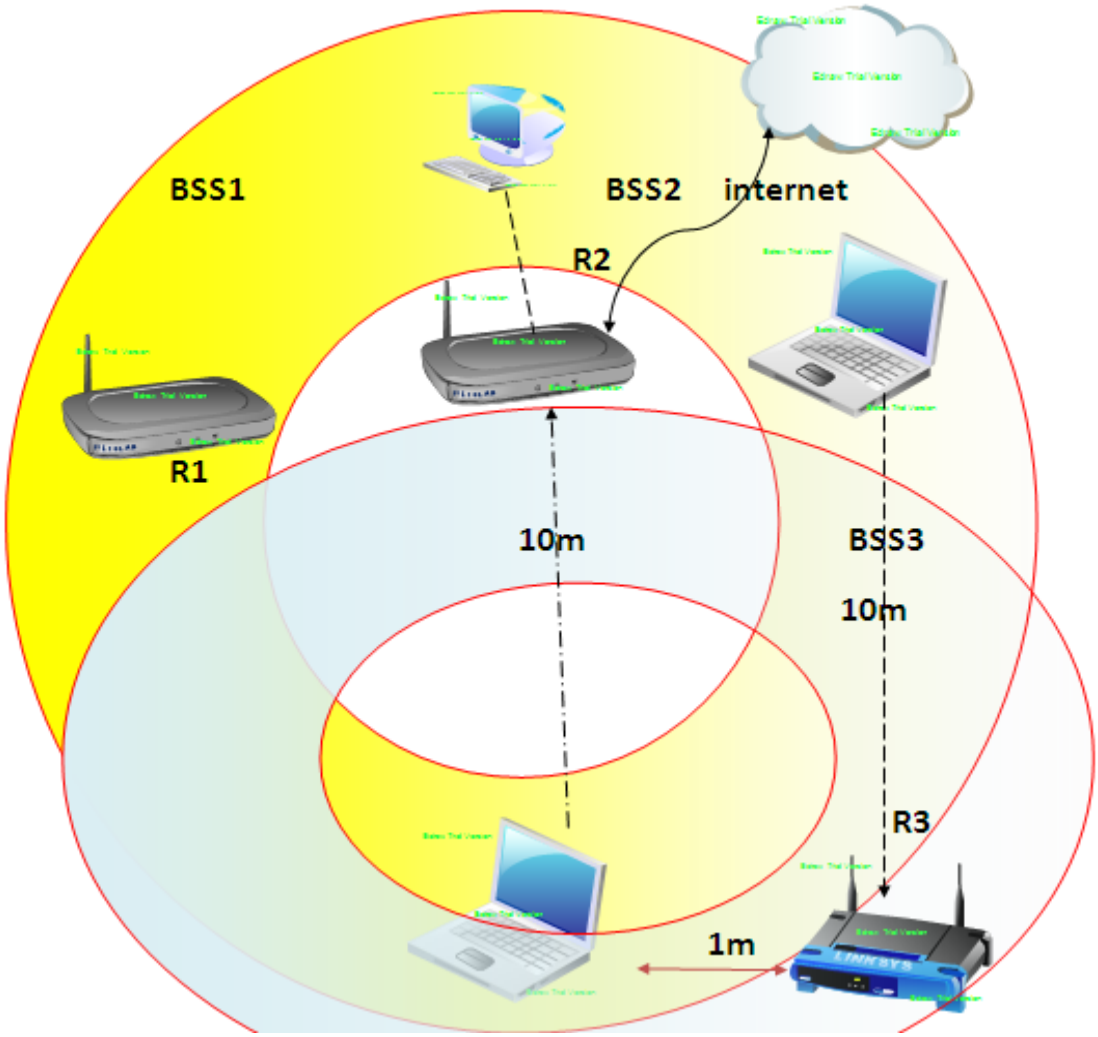
Για κάθε σενάριο γίνονται πέντε μετρήσεις για κάθε χρήστη προκειμένου να έχουμε πιο αξιόπιστα αποτελέσματα. Οι πέντε μετρήσεις γίνονται ανά Χ δευτερόλεπτα η κάθε μία. Τα Access Points (APs) μέχρι το σενάριο 15 έχουν διαφορετικά Channels. Το σενάριο 14* έγινε σε εξωτερικό χώρο ενώ τα σενάρια 16*,17* τα AP2, AP3 χρησιμοποιούν το ίδιο channel (channel 6).

5.2.1 Τεχνικά Χαρακτηριστικά (Test bed)

R1 : Linksys 802.11n Integrated router 2.4 GHz with 4 port switch , Bandwidth : 54 Mbps R2 : The SpeedTouch 585 is an ADSL modem with integrated 4-port switch and 802.11a/g wireless LAN access point. Bandwidth : 54 Mbps R3: Linksys 802.11g Integrated router 2.4 GHz with 4 port switch , Bandwidth : 54 Mbps 1 Desktop : Pendium 4 cpu 3.2 Ghz, Lan card : broadcom 440x 10/100, OS : Linux ubundu 2 Laptops hp intel centrino Duo with Pro/wireless 3945ABG and OS : windows xp



Εικόνα 5.2: Σχεδιάγραμμα Test bed1 (ένα AP + 2 ασύρματοι κόμβοι)



Εικόνα 5.3: Σχεδιάγραμμα Test bed2 (Τρία APs + 2 ασύρματοι κόμβοι)

ΛΟΓΙΚΟ ΔΙΑΓΡΑΜΜΑ ΔΙΚΤΥΟΥ (Test bed)

IP Address R2 (AR): 192.168.10.254 (DGW)

IP Address Desktop (K3)(Ethernet 0) : 192.168.10.4

IP Address R2: 192.168.10.6 (DGW : 192.168.10.254)

IP Address R3: 192.168.10.3 (DGW : 192.168.10.254)

IP Address wireless Κόμβου 1 (K1): 192.168.10.1

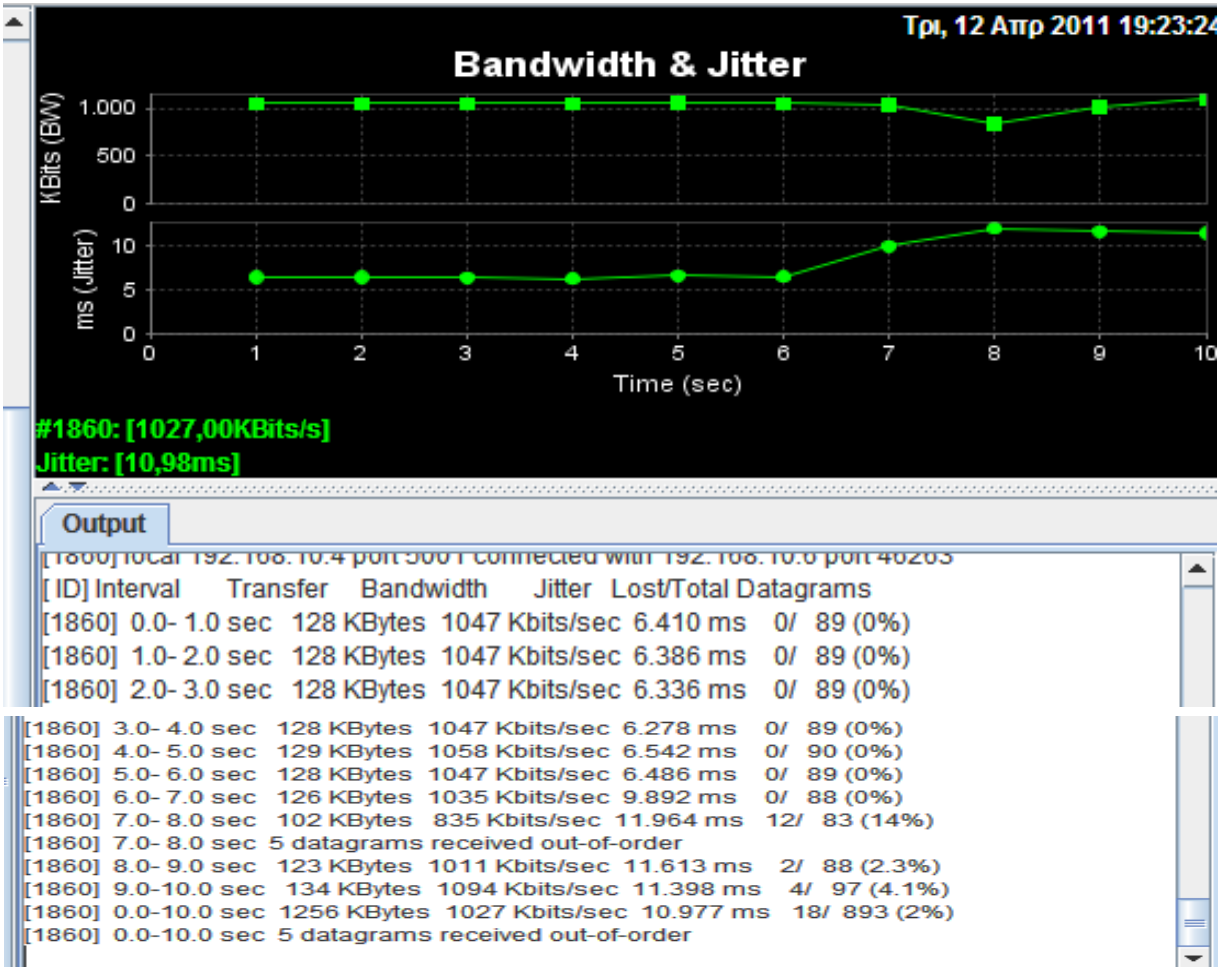
IP Address wireless Κόμβου 2 (K2): 192.168.10.2

: AP connected

: APs επικοινωνούν με τον κεντρικό δρομολογητή

5.3 Σχέση Packet Loss , Jitter και Απόστασης από το Access Point (AP).

Στα επόμενα σενάρια (1-4) θα εξετάσουμε ποια είναι η σχέση και πόσο επιδρά η απόσταση των ασύρματων κόμβων από το Access Point (AP), στη αύξηση/μείωση του αριθμού των χαμένων πακέτων (packet loss). Η απόσταση από το AP φυσικά επιδρά πάνω στο signal strength (dBm). Τα UDP πακέτα στον iperf-server (windows xp) έχουν μέγεθος 1470 bytes. Το buffer size έχει μέγεθος 8K (default). Το buffer size στον iperf-client (Linux) έχει μέγεθος 128K. Τα αποτελέσματα φαίνονται στις Εικόνες των σεναρίων 1-4. Σε κάθε μέτρηση (διαρκ.10 sec) στέλλονται συνολικά από και προς τους ασύρματους κόμβους 893 UDP πακέτα. Σε κάθε χρονικό διάστημα 1 sec στέλλονται περίπου 128KBytes τα οποία τεμαχίζονται (segmentation) σε 89 πακέτα των 1470 Bytes.

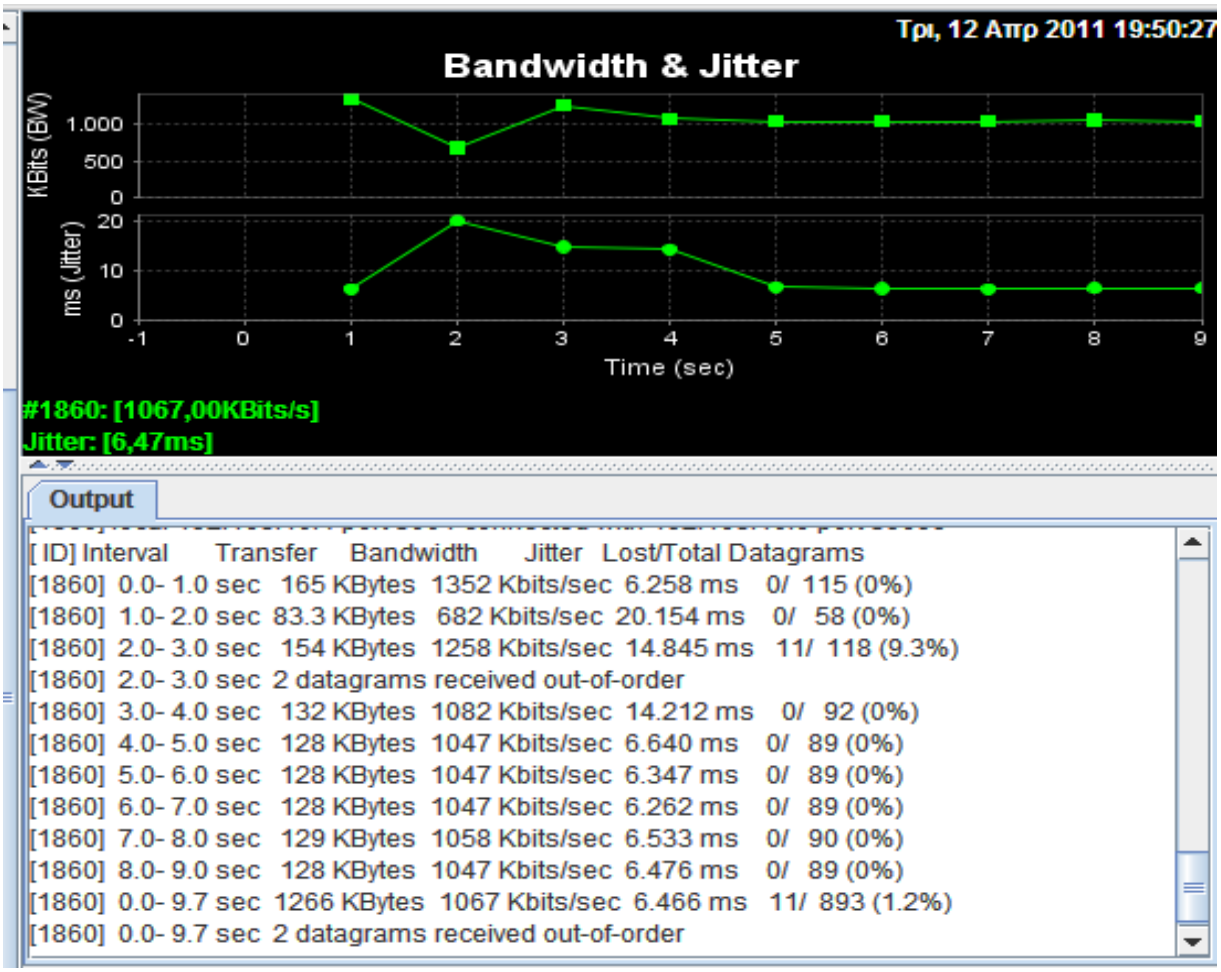


Εικόνα 5.4: Σενάριο 1

Στα χρονικά διαστήματα 7-11 sec που έχουμε packet loss (MO = 2%), παρατηρούμε ότι το jitter βρίσκεται σε ψηλά επίπεδα δηλαδή > 11ms. Το Bandwidth σε αυτά τα χρονικά

διαστήματα κάποτε είναι πιο χαμηλό από τον μέσο όρο (ΜΟ) δηλ. 835 Kbps και κάποτε πιο ψηλό (1094 Kbps). Σε αυτές τις περιπτώσεις έχουμε χαμένα πακέτα. Συνολικά από τα 893 πακέτα έχουν χαθεί τα 20 δηλαδή packet loss = 2%. Πέντε πακέτα έχουν έρθει με out-of-order. Το signal strength = -36dBm.

Συμπέρασμα: Όσο η απόσταση των ασύρματων κόμβων από το AP δεν είναι μεγάλη, και το signal strength είναι δυνατό (-36dBm) δεν παρατηρείται μεγάλη αύξηση του αριθμού των packet loss (<= 2% Εικόνα 5.4)



Εικόνα 5.5: Σενάριο 2

Εδώ παρατηρούμε ότι το jitter δεν είναι σταθερό αλλά οι τιμές του κυμαίνονται μεταξύ 6.258ms και 20.154ms. Ένδεκα (11) από τα 893 πακέτα έχουν χαθεί, δηλαδή packet loss = 1.2%. Επίσης παρατηρούμε ότι στο χρονικό διάστημα [1-2 sec] το jitter=20.154 αλλά δεν έχουμε χαμένα πακέτα. Έχουμε επίσης 2 πακέτα out-of-order. Παρατηρούμε ότι στο χρονικό διάστημα [2-3 sec] το Bandwidth = 1258 Kbps είναι αρκετά πιο ψηλό από τις άλλες μετρήσεις , το jitter=14.845ms που είναι επίσης πιο ψηλό από μερικές άλλες μετρήσεις και τέλος τα packet loss = 9.3% στην ίδια μέτρηση. Στο χρονικό

διάστημα [3-4 sec] έχουμε ψηλό jitter=14.212ms αλλά δεν έχουμε packet loss. Το signal strength = -83 dBm.

Συμπέρασμα: Δεν φαίνεται να συνδέεται η αύξηση/μείωση του jitter με αύξηση/μείωση του αριθμού των packet loss. Όμως λόγω εξασθένησης του signal strength = -83dBm, παρατηρούμε αύξηση του packet loss.

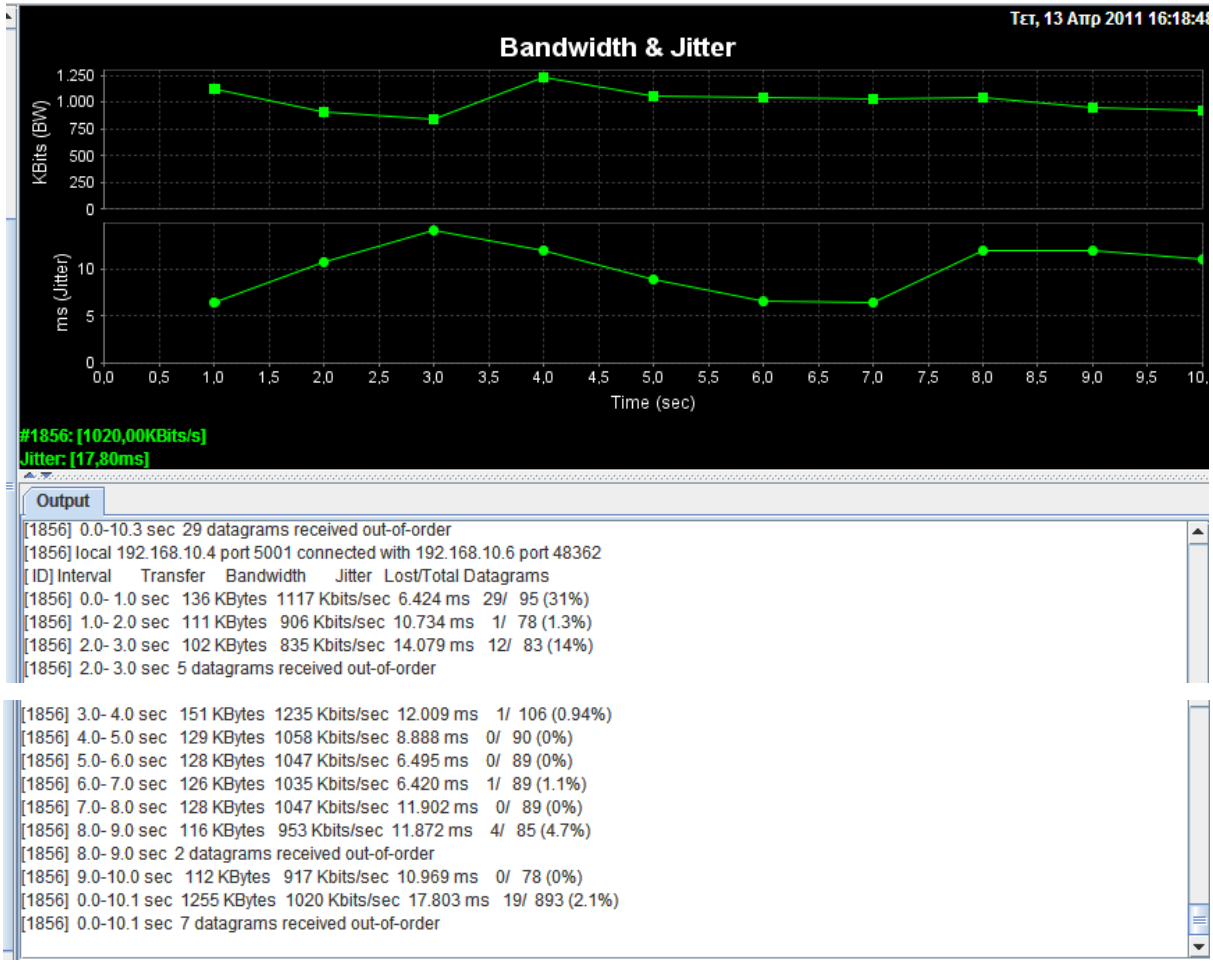
Εικόνα 5.6: Αύξηση του jitter χωρίς Packet loss

Η διακύμανση της καθυστέρησης (jitter) επηρεάζει όμως αρκετά το VoIP (γενικά τις εφαρμογές πραγματικού χρόνου), διότι τα πακέτα φωνής πρέπει να εκτελεστούν στον χρήστη σε συγκεκριμένη χρονική στιγμή. Αυτή η διακύμανση της καθυστέρησης οδηγεί στην κακή ποιότητα του ήχου. Έτσι για να διορθωθεί το πρόβλημα αυτό χρησιμοποιείται μια τεχνική (jitter buffer) κατά την οποία εξαλείφεται το jitter, αλλά αυξάνεται η συνολική καθυστέρηση, η οποία με την σειρά της προκαλεί μεγάλο packet loss (μεγαλώνοντας τον χρόνο αποθήκευσης μεγαλώνει και η συνολική καθυστέρηση μειώνοντας έτσι την ποιότητα της συνδιάλεξης).

Εικόνα 5.7: Σενάριο 3

Εδώ παρατηρούμε στο χρονικό διάστημα [0-1 sec] το jitter είναι σε χαμηλά επίπεδα και είναι κάτω από τον μέσο όρο = 6.355ms, εντούτοις έχουμε αρκετά ψηλό αριθμό packet loss=20%. Ταυτόχρονα στο χρονικό διάστημα [3-4 sec] παρατηρούμε το Bandwidth =917 kbps και είναι κάτω από τον MO, το jitter = 38.534 που είναι πολύ ψηλό και έχουμε packet loss=13%. Το συνολικό packet loss=3.9% (35 packets from 893). Το signal strength= -87dBm

Συμπέρασμα : Όσο η απόσταση των ασύρματων κόμβων από το AP μεγαλώνει, τόσο εξασθενεί το signal strength (=-87dBm) με αποτέλεσμα να παρατηρείται μεγάλη αύξηση του αριθμού των packet loss (= 3.9% Εικόνα 5.7). Επίσης παρατηρούμε ότι σε περιπτώσεις που το jitter γίνεται πολύ μεγάλο, έχουμε αριθμό datagrams received out-of-order.



Εικόνα 5.8: Σενάριο 4

Στο Σενάριο 4 έχουμε κίνηση. Ο κινητός κόμβος κινείται (κίνηση με τα πόδια) και ευρίσκεται σε απόσταση 10m από το AP, με εμπόδια ενδιάμεσα (2 Τοίχους) . Ο αριθμός των packet loss = 3.54. Το jitter = 13.73. Συγκρίνοντάς το με το Σενάριο 2 που είναι παρόμοιο, αλλά χωρίς κίνηση παρατηρούμε ότι ο μέσος όρος των χαμένων πακέτων είναι αρκετά ψηλότερος (από 0,48 έγινε 3,54) και ο μέσος όρος του jitter έγινε επίσης πιο ψηλός (από 7,309 έγινε 13,73). Επίσης παρατηρούμε ότι 2 πακέτα που έχουν παραληφθεί είναι out-of-order. Το signal strength= -82dBm.

Συμπέρασμα: : Όταν ο κόμβος κινείται μέσα σε ένα BSS και ευρίσκεται σε απόσταση 10m από το AP, με διάφορα εμπόδια ενδιάμεσα (2 τοίχους + έπιπλα), το signal strength εξασθενεί (-82dBm), με αποτέλεσμα η ποιότητα του σήματος να μην είναι καλή και να έχουμε μεγαλύτερο αριθμό packet loss (3.54%).

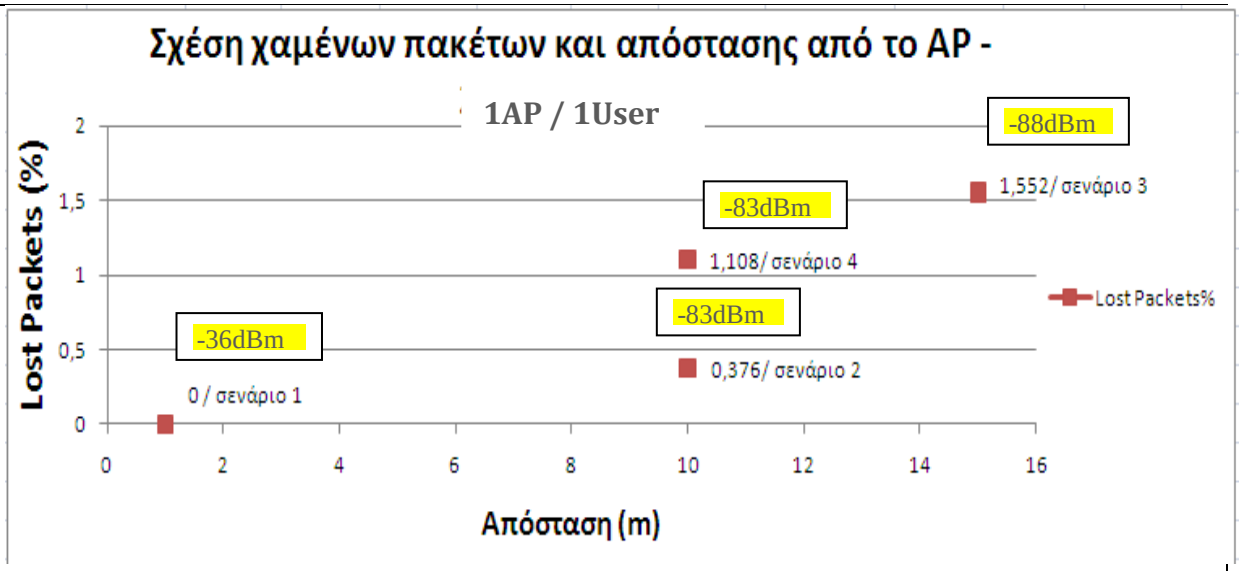
5.4 Εξάρτηση του Packet Loss και του Jitter από την Απόσταση από το Access Point (signal strength)

Στα επόμενα σενάρια θα εξετάσουμε πόσο ρόλο παίζει η απόσταση του κινητού κόμβου από το access point (AP), στη συμπεριφορά του jitter και του αριθμού των χαμένων πακέτων (packet loss). Η απόσταση φυσικά επιδρά πάνω στο signal strength **(**dBm**).** Όσο απομακρυνόμαστε από το AP τόσο αδυνατίζει το signal strength. Τα UDP πακέτα στον iperf-server (windows xp) έχουν μέγεθος 1470 bytes. Το buffer size έχει μέγεθος 8K. Το buffer size στον client (Linux) έχει μέγεθος 128K. Τα αποτελέσματα φαίνονται στις Εικόνες των σεναρίων 1-4. Σε κάθε μέτρηση στέλλονται συνολικά 893 UDP πακέτα. Σε κάθε χρονικό διάστημα 1 sec στέλλονται περίπου 128KBytes τα οποία τεμαχίζονται σε 89 πακέτα των 1470 Bytes. 128KB= 89*1470. Το Bandwidth = 1Mbps.

	Μέτρηση	Μέτρηση	Μέτρηση	Μέτρηση	Μέτρηση5		Απόσταση	Lost Packets	Απόσταση	Jitter	Ένταση σήματος
Σενάριο 1	0	0	0	0	0		1	0	1	8,1402	-36dBm
jitter	14,788	6,37	6,48	6,527	6,536						
Σενάριο 2	0,78	0	0	1,1	0		10	0,376	10	6,59	-83dBm
jitter	7,657	6,262	6,35	6,335	6,346						
Σενάριο 3	3,2	0,22	2,1	0,34	1,9		15	1,552	15	6,9182	-88dBm
jitter	6,560	6,487	6,235	6,518	8,791						
Σενάριο 4	0,9	0,22	1,8	0,22	2,4		10	1,108	10	9,2522	-82dBm
jitter	6,288	6,29	21,229	6,166	6,288						

Πίνακας 5.3: Αριθμητικά δεδομένα σεναρίων 1-4

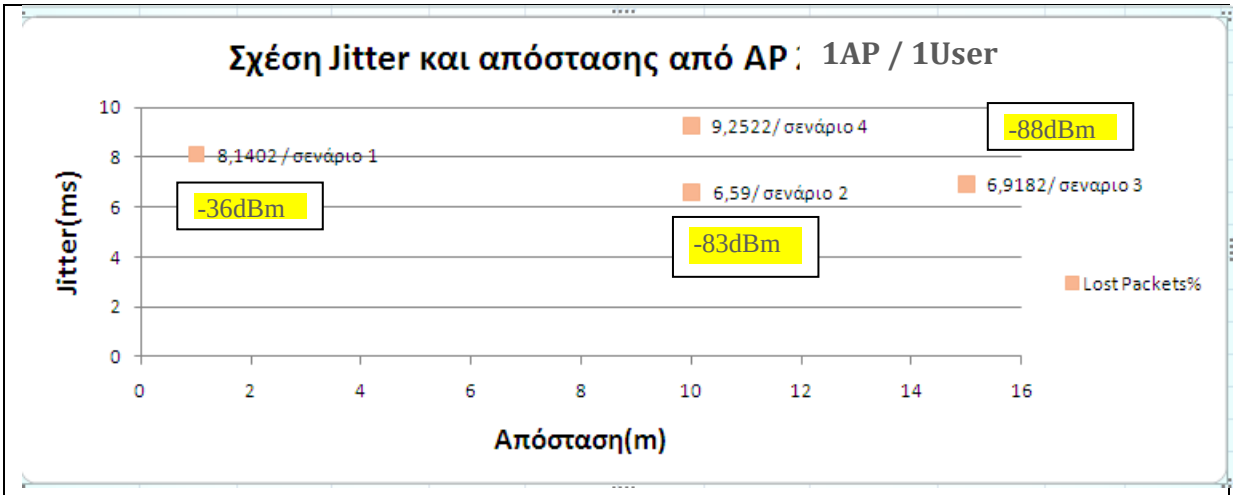
Παραθέτουμε πιο πάνω και τα αριθμητικά αποτελέσματα των Σεναρίων 1-4. Η στήλη Packet loss % παραθέτει τον μέσο όρο των 5 μετρήσεων που καταμετρούνταν σε κάθε σενάριο σε σχέση με τις μετρήσεις των χαμένων πακέτων . Τα ίδιο ισχύει και για την τελευταία στήλη Jitter. Δηλ. παραθέτει τον μέσο όρο των 5 μετρήσεων για κάθε σενάριο σε σχέση με τις μετρήσεις του Jitter. Το ίδιο ισχύει και για τα υπόλοιπα σενάρια σε σχέση με τις στήλες Packet loss και Jitter.



Εικόνα 5.9: Σχέση χαμένων πακέτων και απόστασης από το AP. Σενάρια 1-4

Στη πιο πάνω γραφική παράσταση (Εικόνα 5.9) παρατηρούμε ότι όσο απομακρύνεται ο κινητός κόμβος από το AP με εμπόδια ενδιάμεσα (2 τοίχους), τόσο μειώνεται η ένταση του σήματος (-83dBm) με αποτέλεσμα να αυξάνεται ο αριθμός των χαμένων πακέτων (packet loss). Επίσης στο σενάριο 4 (κινητός κόμβος) παρατηρούμε ότι, όταν κινείται ο κόμβος αυξάνεται και ο αριθμός των χαμένων πακέτων (packet loss=1,108%) σε σύγκριση με το σενάριο 2 όπου έχουμε την ίδια απόσταση από το AP,

Συμπέρασμα: Η απόσταση του κινητού κόμβου από το AP (10m) με μείωση του signal strength (-83dBm) λόγω εμποδίων (2 τοίχοι ενδιάμεσα + έπιπλα), επιδρά στη αύξηση του αριθμού των packet loss. Επίσης όπως συμπεράναμε προηγουμένως, η κίνηση επιδρά στη αύξηση του αριθμού των packet loss.



Εικόνα 5.10: Σχέση Jitter και απόστασης από το AP. Σενάρια 1-4.

Στη πιο πάνω γραφική παράσταση (Εικόνα 5.10) παρατηρούμε ότι η απόσταση του κινητού κόμβου από το AP δεν επηρεάζει το jitter. Π.χ. Σε απόσταση 1m από το AP έχουμε jitter=8.14ms ενώ σε απόσταση 10m έχουμε jitter=6.59ms Σε απόσταση 10m αλλά με κίνηση έχουμε jitter=9.25 που είναι ψηλότερο από το σενάριο 2 που ήταν χωρίς κίνηση.

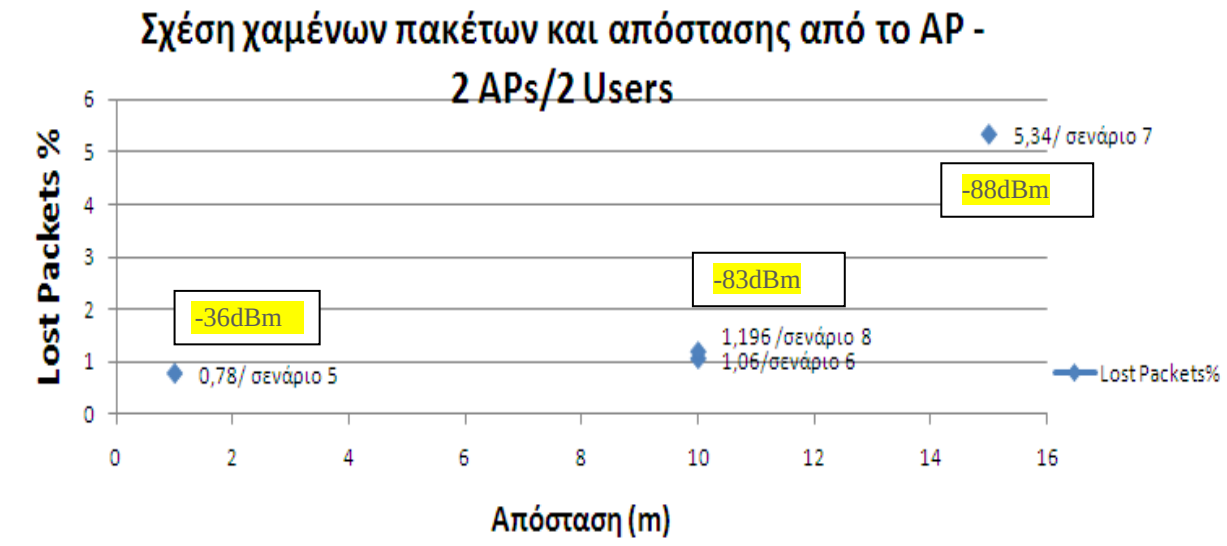
Συμπέρασμα: Το jitter δεν επηρεάζεται από την απόσταση του κινητού κόμβου από το AP. Ενδεχομένως όμως η κίνηση να επηρεάζει την αύξηση του jitter. Επειδή όμως η κίνηση ήταν χαμηλή για αυτό έχουμε και μικρή αύξηση.

	Μέτρηση	Μέτρηση	Μέτρηση	Μέτρηση	Μέτρηση5		Απόσταση	Lost Packets%	Απόσταση	Jitter	"Ενταση σήματος
Σενάριο 5	2,6	1,3	0	0	0		1	0,78	1	7,6894	-36dBm
jitter	6,147	13,303	6,472	6,391	6,134						
Σενάριο 6	3,5	0	0,9	0,9	0		10	1,06	10	6,2098	-83dBm
jitter	6,311	6,16	6,15	6,239	6,189						
Σενάριο 7	2	15	4,9	2,1	2,7		15	5,34	15	9,7572	-88dBm
jitter	10	6,14	12,285	14,241	6,171						
Σενάριο 8	2,4	1,7	0	0,78	1,1		10	1,196	10	6,8294	-82dBm
jitter	6,121	6,255	6,222	6,743	8,806						

Πίνακας 5.4: Αριθμητικά δεδομένα σεναρίων 5-8

Παραθέτουμε πιο πάνω και τα αριθμητικά αποτελέσματα των Σεναρίων 5-8. Η στήλη Packet loss % παραθέτει τον μέσο όρο των 5 μετρήσεων που γινόντουσαν σε κάθε

σενάριο σε σχέση με τις μετρήσεις των χαμένων πακέτων . Τα ίδιο ισχύει και για την προτελευταία στήλη Jitter. Δηλ. παραθέτει τον μέσο όρο των 5 μετρήσεων για κάθε σενάριο σε σχέση με τις μετρήσεις του Jitter.



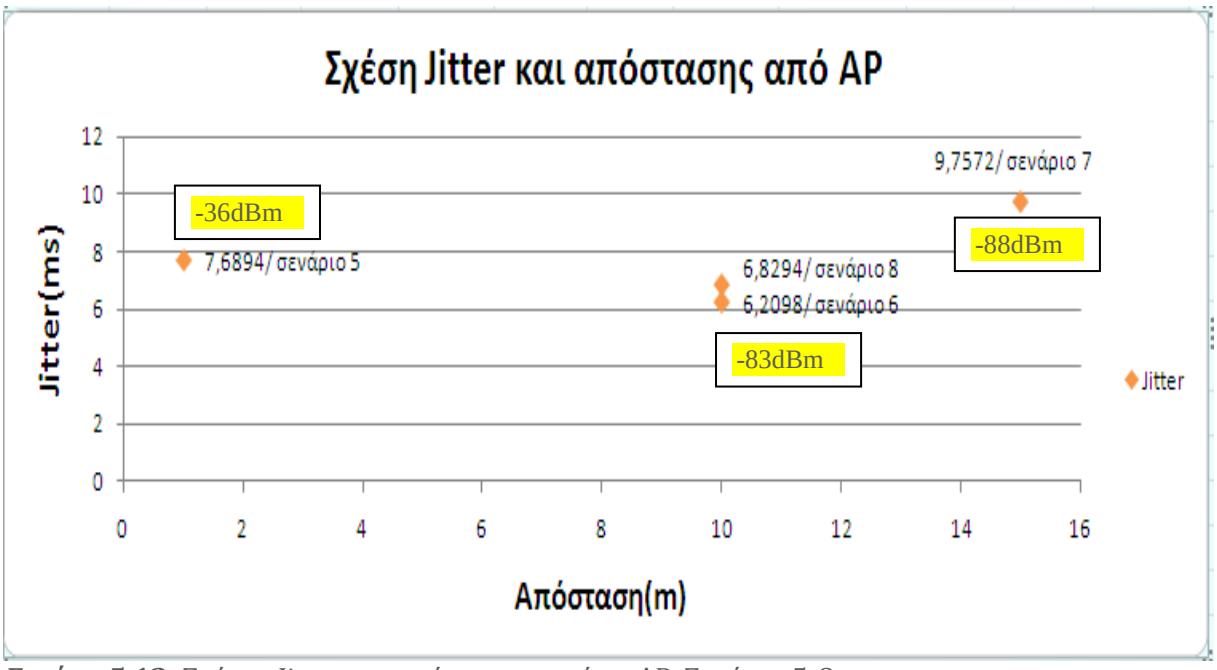
Εικόνα 5.11: Σχέσης χαμένων πακέτων και απόστασης από το AP. Σενάρια 5-8

Συγκρίνοντας το Σενάριο 1 με το Σενάριο 5 παρατηρούμε πολύ μικρές αυξομειώσεις (μικρή αύξηση του μέσου όρου) του αριθμού των packet loss κατά 0,5%, παρόλο που χρησιμοποιούμε 2 APs σε μικρή απόσταση το ένα από το άλλο (0.5m). Φαίνεται ότι δεν δημιουργούνται ιδιαίτερα προβλήματα στην ποιότητα του σήματος. Επιπρόσθετα χρησιμοποιούμε ακόμη ένα κινητό wireless κόμβο που επίσης δεν επηρεάζει την ποιότητα του σήματος (όλα τα APs χρησιμοποιούν διαφορετικό channels).

Συγκρίνοντας το Σενάριο 2 με το Σενάριο 6 παρατηρούμε πολύ μικρές αυξομειώσεις (μικρή αύξηση του μέσου όρου) του αριθμού των packet loss κατά 0,1%, παρόλο που χρησιμοποιούμε 2 Access Points σε μικρή απόσταση το ένα από το άλλο (0.5m) και λογικά το ένα παρεμβάλλει το άλλο. Φαίνεται ότι δεν δημιουργούνται ιδιαίτερα προβλήματα. Συγκρίνοντας το Σενάριο 3 με το Σενάριο 7 παρατηρούμε μια αύξηση του packet loss σε 5,34 (σενάριο 7). Ο συνδυασμός της απόστασης (10m) με εμπόδια (2 τοίχοι) ενδιάμεσα, την παρεμβολή ενός επιπρόσθετου AP σε μικρή απόσταση από το άλλο AP και ο επιπρόσθετος κινητός κόμβος φαίνεται ότι δεν επηρεάζουν την ένταση του σήματος σε σύγκριση με το σενάριο 2 (-83dBm).

Σημείωση: Τα δύο APs χρησιμοποιούν διαφορετικά κανάλια (11,6).

Συμπέρασμα: Και σε αυτά τα σενάρια επιβεβαιώνεται ότι η απόσταση του κινητού κόμβου από το AP σε συνάρτηση με την ένταση του σήματος (-36dBm / -83dBm) παίζει ένα ρόλο στην αύξηση του αριθμού των packet loss. Παρατηρούμε επίσης ότι με την προσθήκη και νέου AP (διαφορετικό channel) και επιπρόσθετου wireless κόμβου, δεν επηρεάζεται σε μεγάλο βαθμό η ποιότητα του σήματος, με το packet loss να μην μεταβάλλεται, εκτός από το σενάριο 7 (15m απόσταση από το AP).



Εικόνα 5.12: Σχέσης Jitter και απόστασης από το AP. Σενάρια 5-8.

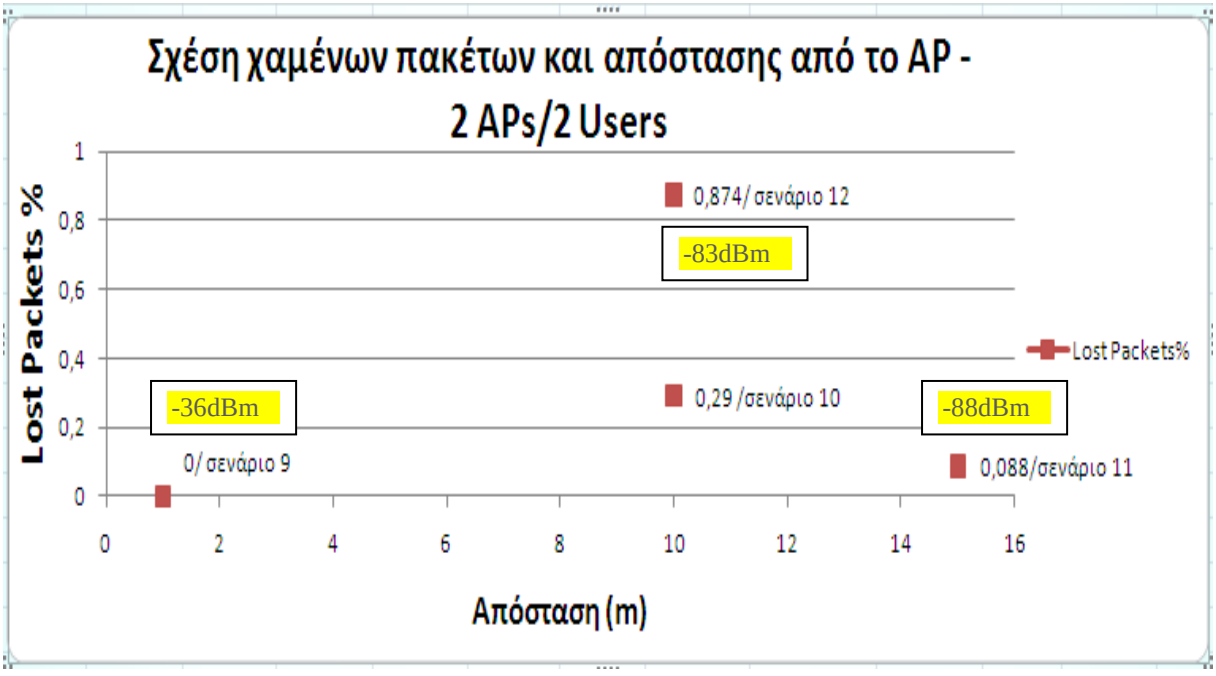
Στη πιο πάνω γραφική παράσταση (Εικόνα 5.12) παρατηρούμε ότι η απόσταση του κινητού κόμβου από το AP σε συνάρτηση με απώλεια της έντασης του σήματος (-36dBm / -83dBm / -88dBm) δεν επηρεάζει το jitter. Π.χ. Σε απόσταση 1m από το AP έχουμε jitter=7.68 (signal strength = -33dBm) ενώ σε απόσταση 10m (signal strength = -88dBm) έχουμε jitter=6.20ms Σε απόσταση 10m (signal strength = -83dBm) αλλά με κίνηση έχουμε jitter=6.82 που είναι ψηλότερο από το σενάριο 6 που ήταν χωρίς κίνηση.

Συμπέρασμα: Το jitter δεν επηρεάζεται από την απόσταση του κινητού κόμβου από το AP σε συνάρτηση με απώλεια της έντασης του σήματος (-36dBm / -83dBm / -88dBm). Επίσης ενδεχομένως η κίνηση του κόμβου να επηρεάζει την αύξηση του jitter. Επειδή όμως η κίνηση ήταν χαμηλή για αυτό έχουμε και μικρή αύξηση.

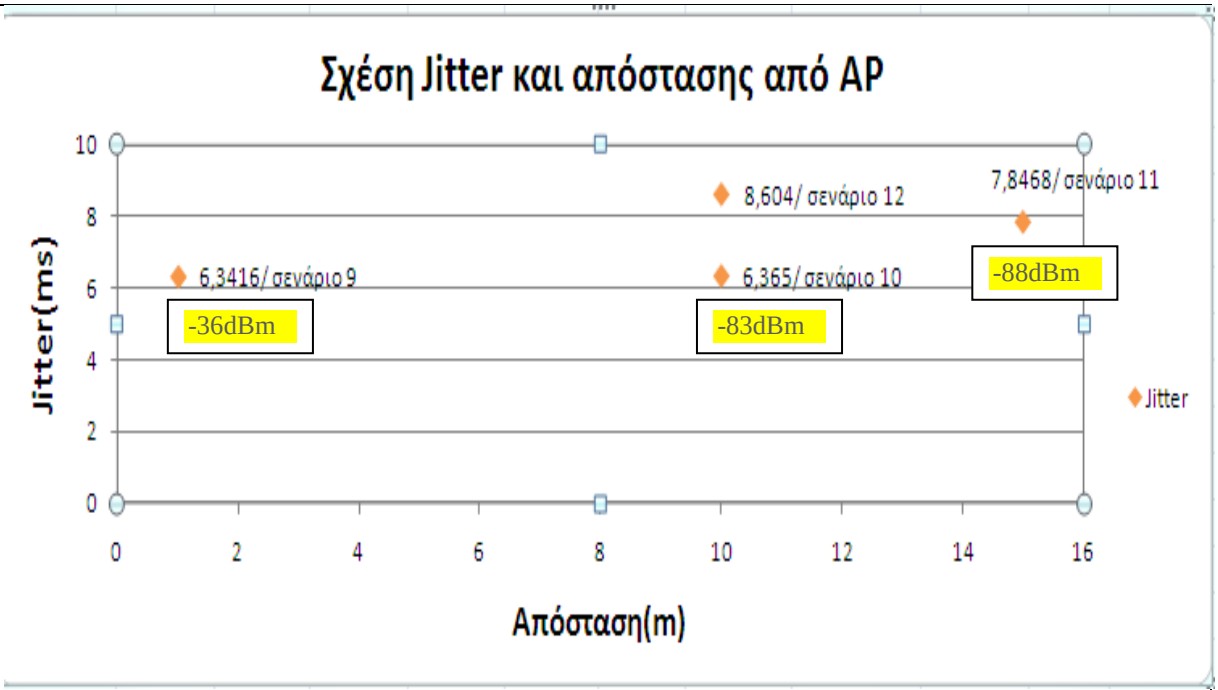
	Μέτρηση	Μέτρηση	Μέτρηση	Μέτρηση	Μέτρηση5	Απόσταση	Lost Packets%	Jitter	Ένταση σήματος
Σενάριο 9	0	0	0	0	0	1	0	6,3416	-36dBm
jitter	6,473	6,27	6,274	6,349	6,342				
Σενάριο 10	0,67	0	0	0	0,78	10	0,29	6,365	-83dBm
jitter	6,219	6,388	6,411	6,402	6,405				
Σενάριο 11	0,22	0	0	0	0,22	15	0,088	7,8468	-88dBm
jitter	13,566	6,391	6,453	6,35	6,474				
Σενάριο 12	0,56	1,1	0,45	0,56	1,7	10	0,874	8,604	-82dBm
jitter	6,373	14,412	6,334	6,342	9,559				

Πίνακας 5.5: Αριθμητικά δεδομένα σεναρίων 9-12

Παραθέτουμε πιο πάνω και τα αριθμητικά αποτελέσματα των Σεναρίων 9-12. Η στήλη Packet loss % παραθέτει τον μέσο όρο των 5 μετρήσεων που γινόντουσαν σε κάθε σενάριο σε σχέση με τις μετρήσεις των χαμένων πακέτων . Τα ίδιο ισχύει και για την προτελευταία στήλη Jitter. Δηλ. παραθέτει τον μέσο όρο των 5 μετρήσεων για κάθε σενάριο σε σχέση με τις μετρήσεις του Jitter.



Εικόνα 5.13: Σχέσης χαμένων πακέτων και απόστασης από το AP. 2APs/2Users



Εικόνα 5.14: Σχέσης Jitter και απόστασης από το AP. Σενάρια 9-12.

Συμπέρασμα: Το jitter δεν επηρεάζεται από την απόσταση του κινητού κόμβου από το AP σε συνάρτηση με απώλεια της έντασης του σήματος (-36dBm / -83dBm / -88dBm). Επίσης ενδεχομένως η κίνηση του κόμβου να επηρεάζει την αύξηση του jitter. Επειδή όμως η κίνηση ήταν χαμηλή για αυτό έχουμε και μικρή αύξηση.

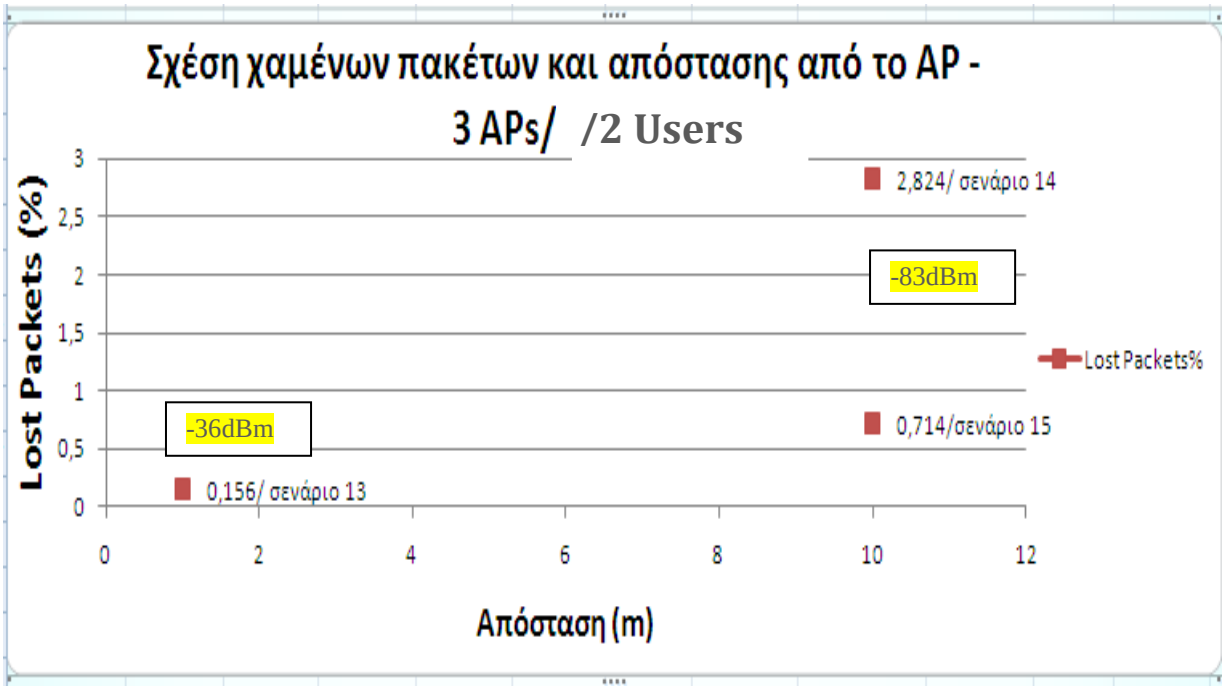
	Μέτρηση1	Μέτρηση2	Μέτρηση3	Μέτρηση4	Μέτρηση5	Απόσταση	Lost Packets%	Απόσταση	Jitter	Ένταση σήματος
Σενάριο 13	0,67	0	0	0,11	0	1	0,156	1	6,2358	-36dBm
jitter	6,156	6,181	6,395	6,236	6,211					
Σενάριο 14	12	0	1	0,56	0,56	10	2,824	10	6,2976	-86dBm
	6,486	6,33	6,333	6,266	6,073					
Σενάριο 15	0,9	2	0,56	0	0,11	10	0,714	10	8,3446	-83dBm
	6,487	15,944	6,181	6,514	6,597					

Πίνακας 5.6: Αριθμητικά δεδομένα σεναρίων 13-15

Στα σενάρια αυτά 13-15 χρησιμοποιούμε 3 AP καθώς και δύο wireless users. Το αξιοσημείωτο εδώ είναι ότι στο σενάριο 15, αν και έχουμε κίνηση έχουμε μικρότερο αριθμό packet loss=0.71 που είναι αρκετά πιο χαμηλός από το σενάριο 14 που δεν είχαμε κίνηση. Μια εξήγηση είναι ότι στο σενάριο 14 μπορεί να επηρέασε κάποια

στιγμιαία εξωτερική παρεμβολή με αποτέλεσμα να έχει εξασθενήσεις το signal strength (-86dBm) και να οδηγήσει σε αύξηση του αριθμού των packet loss=2.82%

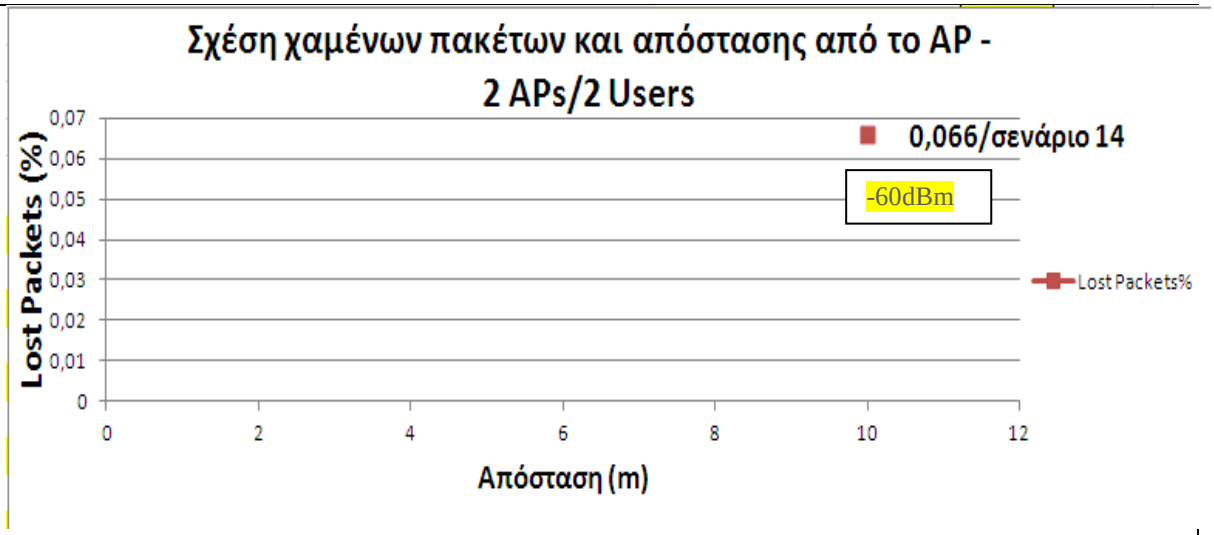
Παραθέτουμε πιο πάνω και τα αριθμητικά αποτελέσματα των Σεναρίων 13-15. Αν τα συγκρίνουμε με τα προηγούμενα σενάρια που χρησιμοποιούσαμε 1 ή 2 APs δεν παρατηρούμε καμιά αξιοσημείωτη αύξηση του αριθμού των packet loss και το ίδιο ισχύει και για το jitter.



Εικόνα 5.15: Σχέσης χαμένων πακέτων και απόστασης από το AP.

Στα σενάρια 13-15 χρησιμοποιούμε ακόμη ένα επιπρόσθετο AP και έναν επιπρόσθετο wireless user. Αυτό όμως φαίνεται να μην αλλάζει τα δεδομένα που συμπεράναμε στα προηγούμενα σενάρια.

Συμπέρασμα: Και σε αυτά τα σενάρια επιβεβαιώνεται ότι η απόσταση (10m) του κινητού κόμβου από το AP, με εμπόδια ενδιάμεσα (2 τοίχους) σε συνάρτηση με την εξασθένηση του signal strength (-36dBm / -83dBm) παίζει ένα ρόλο στην αύξηση του αριθμού των packet loss. Παρατηρούμε επίσης ότι με την προσθήκη και νέου AP (διαφορετικό channel) και επιπρόσθετου wireless κόμβου δεν επηρεάζεται καθόλου ο αριθμός των packet loss.



Εικόνα 5.16: Σχέσης packet loss και απόστασης από το AP σε εξωτερικό χώρο

Παρατηρήθηκε μια σημαντική μεταβολή στα αποτελέσματα, όταν το πείραμα έγινε εξωτερικά του σπιτιού κοντά σε δένδρα. Ο κόμβος τοποθετήθηκε μέσα σε δένδρα σε απόσταση 10m περίπου από το AP. Το packet loss έμεινε σε πολύ χαμηλά επίπεδα σε σύγκριση με το σενάριο 14 που έγινε σε εσωτερικό χώρο με εμπόδια τους τοίχους. Το signal strength είναι πιο δυνατό από ότι σε εσωτερικό χώρο (-60dBm).

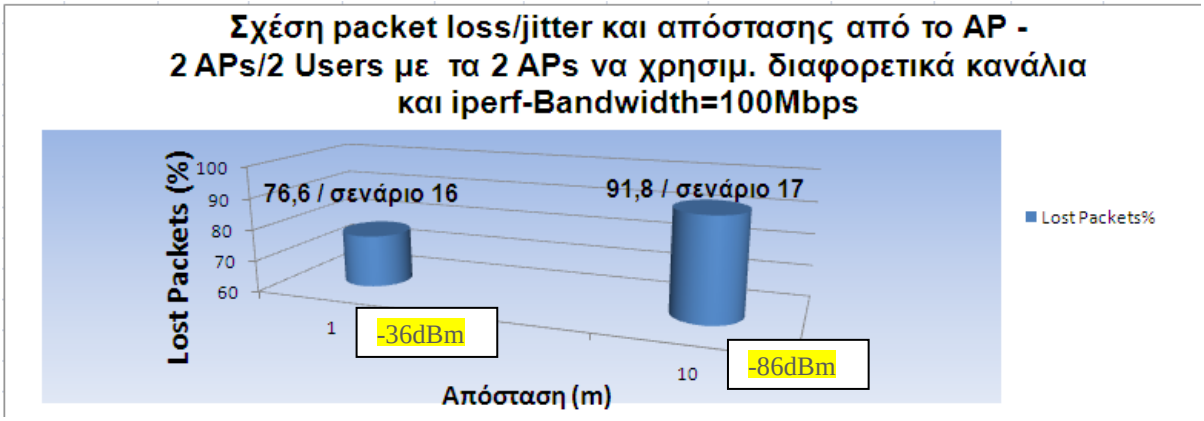
Συμπέρασμα: Παρατηρούμε ότι έχουμε καλύτερα αποτελέσματα (μικρότερο packet loss) όταν ο κόμβος βρίσκεται σε εξωτερικό χώρο με εμπόδια δένδρα και τραπέζια αντί με εμπόδια τοίχους. Ο λόγος είναι ότι το signal strength είναι μεγαλύτερο (-60 dBm) από ότι εσωτερικά (-83 dBm).

	Μέτρηση1	Μέτρηση2	Μέτρηση3	Μέτρηση4	Μέτρηση5	iperf-BW/ Mbps	Lost Packets%	Απόσταση	Jitter	Ένταση σήματος
K2 (R3)	76	76	76	77	78	100	76,6	1	20.451	-36dBm
jitter	6.166	3.924	5.524	82.187	4.454					
K2 (R3)	84	94	94	91	96	100	91,8	10	121.844	-83dBm
jitter	3.554	3.545	3.17	4.613	475.662					
K1 (R2)	62	63	65	66	63	100	63,8	1	11.835	-36dBm
jitter	14.499	15.853	14.166	1	14.657					

Πίνακας 5.7: Router R2=channel6, Router R3 channel=11 και το Bandwidth=100Mbps.

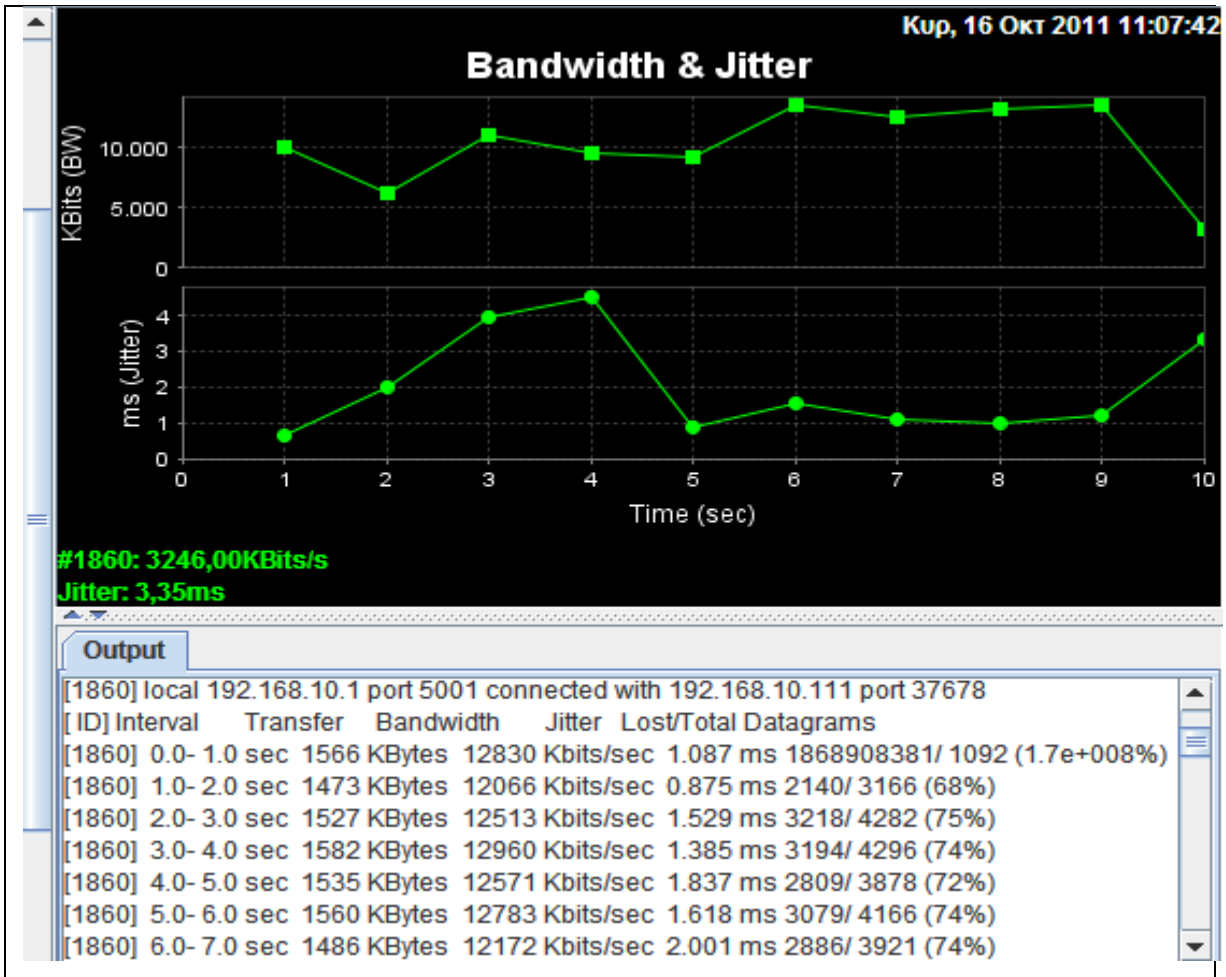
Σε αυτά τα σενάρια (16,17) χρησιμοποιήσαμε 2 APs, και δύο wireless users (Εικόνες 5.19,5.20). Το iperf-Bandwidth=100Mbps. Ο 1ος user (K1) ανήκει στο BSS 2 και επικοινωνεί με τον Router R2 (transmission rate=12Mbps). Ο 2os user (K2) ανήκει σε άλλο BSS (BSS 3) και επικοινωνεί με τον Router R3 (transmission rate =19Mbps). Ο Router R2 έχει το channel=6 και ο R3 το Channel=11, και band 2.4GHz. Ο K1 επικοινωνεί με τον Router R2. Παράλληλα ο K2 κατεβάζει ένα μεγάλο αρχείο. Επίσης έχουμε δοκιμάσει μια παραλλαγή του σεναρίου 16. Δηλ. έχουμε δοκιμάσει την ώρα που γίνονται οι μετρήσεις με το iperf μεταξύ του K1 και του R2, ο K1 να κατεβάζει video από το you tube. Παρατηρούμε ότι το packet loss και το jitter είναι αρκετά ψηλά. Ο λόγος είναι το πολύ υψηλό iperf-Bandwidth =100Mbps και το χαμηλό transmission rate των routers=12Mbps περίπου.

Συμπέρασμα: Έχουμε μεγάλο packet loss και jitter, όταν έχουμε μεγάλο iperf-Bandwidth (100Mbps), οι δύο wireless users είναι σε μικρή (1m) ή μεγάλη απόσταση από το AP (10m) (Εικόνα 5.17) και το transmission rate των δύο Routers (APs) είναι μικρότερο από το iperf-Bandwidth.



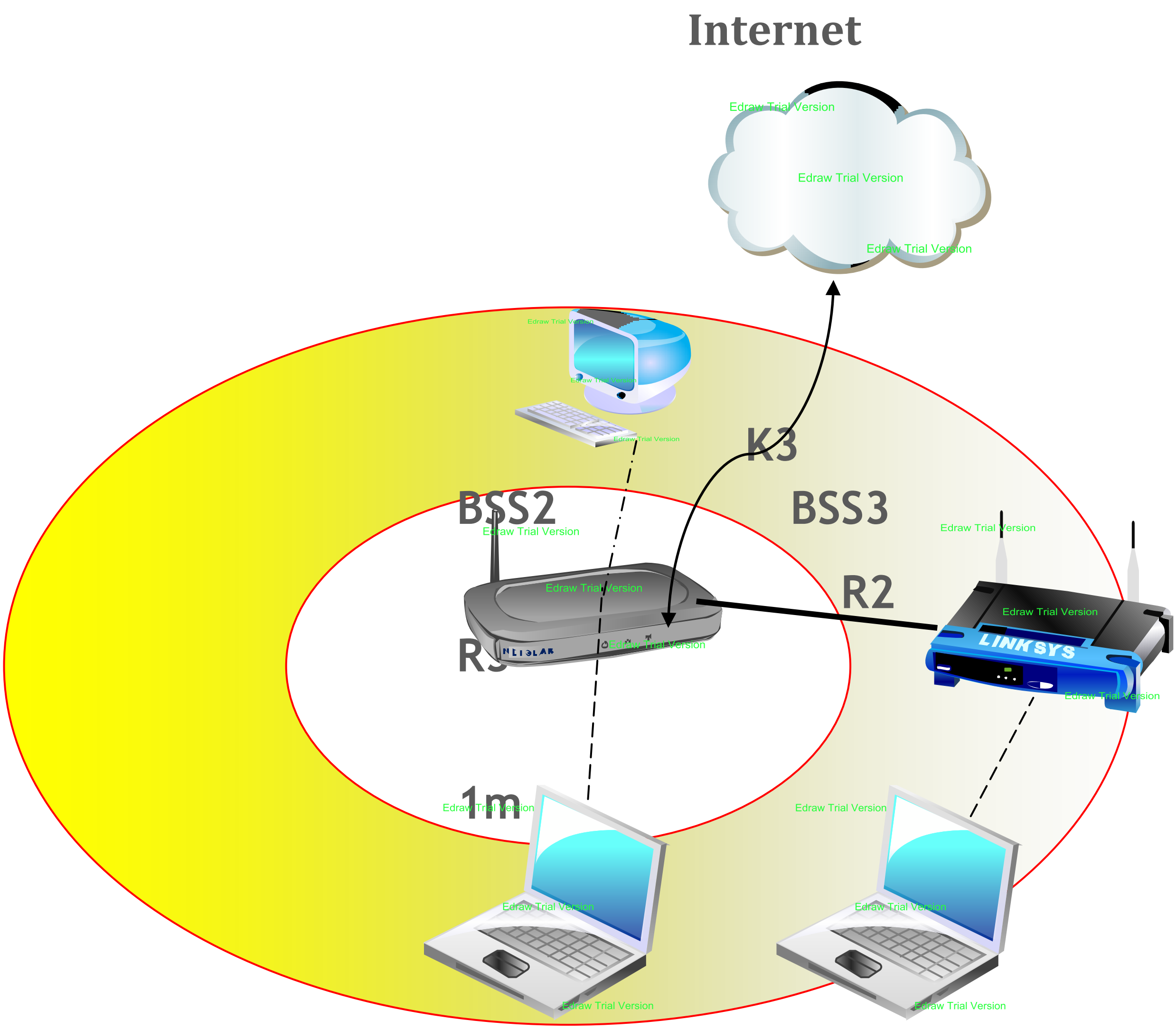
Εικόνα 5.17: Σχέσης packet loss/jitter και iperf-Bandwidth=100Mbps

Στην εικόνα 5.18 παρατηρούμε ότι όταν έχουμε 2 παραπλήσια APs σε απόσταση μόνο 0.5m, μαζί με μεγάλο iperf-Bandwidth (100Mbps), τότε έχουμε αύξηση στις τιμές του packet loss και του jitter και κακή ποιότητα του σήματος (QoS). Σύγκριση σεναρίων 13-15.



Εικόνα 5.18: Γραφική παράσταση Bandwidth και jitter με μεγάλο iperf-Bandwidth (100Mbps),

Το Bandwidth που χρησιμοποιούσε το Iperf για την ροή των δεδομένων ήταν 100Mbps. Παρατηρούμε τις μεγάλες αυξομειώσεις του jitter στην εικόνα 5.18. Τα test beds για τα τις πιο πάνω μετρήσεις φαίνονται στις εικόνες 5.19, 5.20.

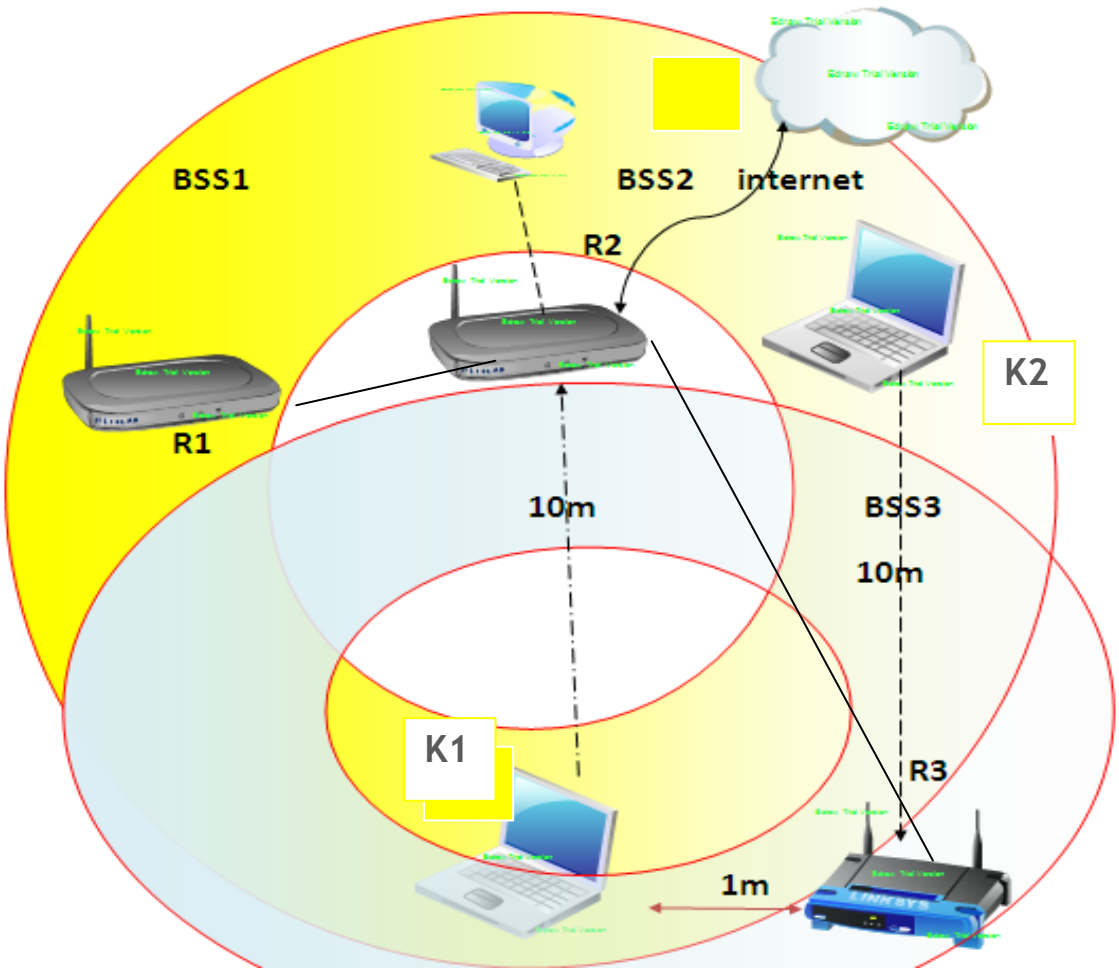


Εικόνα 5.19: Σχεδιάγραμμα του test bed σεναρίου 16

ΛΟΓΙΚΟ ΔΙΑΓΡΑΜΜΑ ΔΙΚΤΥΟΥ
IP Address R2 (AR): 192.168.10.254 (DGW)
IP Address Desktop K3 (Ethernet 0) : 192.168.10.4
IP Address R3: 192.168.10.3 (DGW : 192.168.10.254)
IP Address wireless Κόμβου 1 (K1): 192.168.10.1
IP Address wireless Κόμβου 2 (K2): 192.168.10.2

▬ · ▬ · ▬ · ▬ · ▬ · · : AP connected

▬▬▬▬▬▬ : APs επικοινωνούν με τον κεντρικό δρομολογητή



Εικόνα 5.20: Σχεδιάγραμμα του test bed σεναρίου 17

ΛΟΓΙΚΟ ΔΙΑΓΡΑΜΜΑ ΔΙΚΤΥΟΥ

IP Address R2 (AR): 192.168.10.254 (DGW)

IP Address Desktop K3 (Ethernet 0) : 192.168.10.4

IP Address R3: 192.168.10.3 (DGW : 192.168.10.254)

IP Address wireless Κόμβου 1 (K1): 192.168.10.1

IP Address wireless Κόμβου 2 (K2): 192.168.10.2

- - - - - - - - - - : AP connected

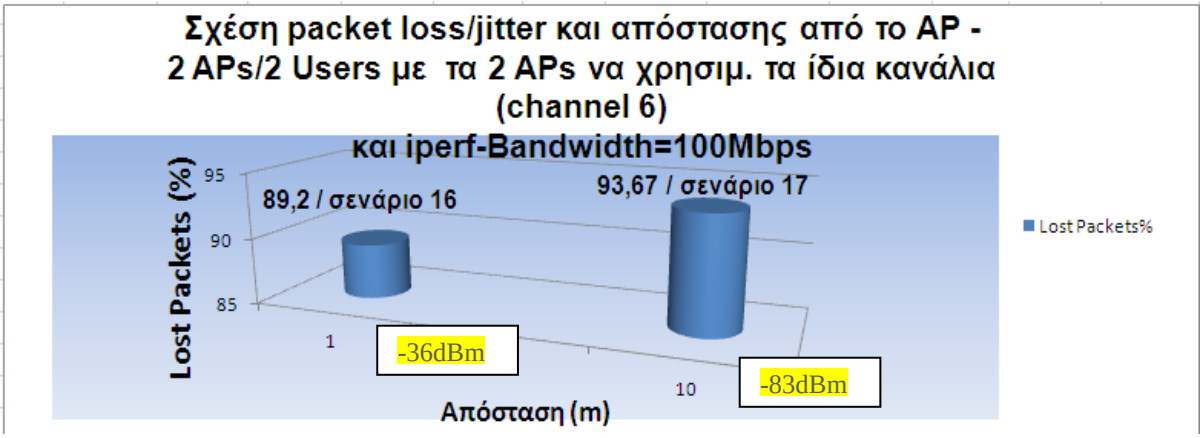
———————— : APs επικοινωνούν με τον κεντρικό δρομολογητή

	Μέτρηση1	Μέτρηση2	Μέτρηση3	Μέτρηση4	Μέτρηση5	iperf-BW/ Mbps	Lost Packets%	Απόσταση/ m	Jitter	Signal Strength
K2 (R3)	88	88	91	90	89	100	89,2	1	11.713	-31dBm
jitter	4.973	9.429	36.393	1.466	6.306					
K2 (R3)dd-wrt	N/A	N/A	92	97	92	100	93,67	10	25.858	-79dBm
jitter	N/A	N/A	6.714	63.318	7.543					
K1 (R2)	64	63	64	70	64	100	65	1	9.293	-27dBm
jitter	14.079	1.022	13.380	1.736	16.250					
K1 (R2)speed	99	98	98	99	98	100	98,4	10	26.999	-87dBm
jitter	14.749	6.326	22.413	81.018	10.489					

Πίνακας 5.8: Αριθμητικά αποτελέσματα σεναρίων με τους δύο Routers (R2,R3) να χρησιμοποιούν το ίδιο κανάλι (channel 6)

Στα σενάρια (16*,17*) χρησιμοποιήσαμε 2 APs, και δύο wireless users (Εικόνες 5.19, 5.20). Το iperf-Bandwidth=100Mbps. Ο ένας user (K1) ανήκει στο BSS 2 και επικοινωνεί με τον Router R2 (transmission rate=18Mbps). Ο 2os user (K2) ανήκει σε άλλο BSS (BSS 3) και επικοινωνεί με τον Router R3 (transmission rate =6Mbps). Οι Routers R2 και R3 χρησιμοποιούν το ίδιο κανάλι (Channel 6, band 2.4GHz). Ο K1 επικοινωνεί με τον Router R2. Παρατηρούμε ότι το packet loss και το jitter είναι ψηλότερα από τα σενάρια 16,17. Ο λόγος είναι ότι οι πόροι του καναλιού 6 μοιράζονται, με αποτέλεσμα κάθε wireless user να λαμβάνει μικρότερο εύρος ζώνης (δηλ. ταχύτητα σύνδεσης).

Συμπέρασμα: "Έχουμε πολύ μεγάλο packet loss και jitter, όταν έχουμε μεγάλο iperf-Bandwidth (100Mbps), τα δύο APs χρησιμοποιούν τα ίδια channels (=6), με αποτέλεσμα να μοιράζονται τους πόρους (R2 transmission rate=18Mbps και R3 transmission rate=6Mbps) < iperf-Bandwidth (100Mbps) και οι δύο wireless users είναι σε μικρή (1m) ή μεγάλη απόσταση από τα APs (10m) (Εικόνα 5.21).



Εικόνα 5.21: Γραφική παράσταση σχέσης packet loss και απόστασης από το AP όταν τα δύο APs χρησιμοποιούν το ίδιο κανάλι (channel 6).

Παρατηρήσεις για τις πιο πάνω μετρήσεις: Παρατηρούμε ότι έχουμε διαφορετικά αποτελέσματα (packet loss) στο Network link μεταξύ των δύο ασύρματων χρηστών, μολονότι έχουμε τις ίδιες αποστάσεις των δύο κόμβων από τους routers (APs). Ένας λόγος είναι ότι έχουν διαφορετικό signal strength (R3= -31dBm και R2= -27dBm) καθώς επίσης και διαφορετικό transmission rate (R3= 6Mbps και R2= 18Mbps). Έτσι φαίνεται ότι το signal strength και το iperf-Bandwidth σε συνδυασμό με το χαμηλό transmission rate των APs είναι δύο παράγοντες που καθορίζουν σε μεγάλο βαθμό το packet loss. Όσο πιο μεγάλο είναι το Bandwidth από το transmission rate τόσο πιο μεγάλο είναι το packet loss. Σε συνδυασμό με το signal strength, όσο πιο αδύνατο είναι το signal strength τόσο πιο μεγάλο είναι επιπρόσθετα το packet loss.

5.5 Εξάρτηση Packet loss/Jitter από το Μέγεθος των Πακέτων (UDP Segments) και του Μεγέθους του UDP Buffer.

Συνοψίζοντας τον πιο κάτω πίνακα 5.9 παρατηρούμε ότι δεν επηρεάζεται σχεδόν καθόλου ο αριθμός των packet loss από το μέγεθος του UDP Buffer και του μεγέθους των πακέτων που παραλαμβάνει ο iperf-server. Το Maximum Transfer Unit (MTU) στο δίκτυο είναι 1470 byte. Έχουν δημιουργηθεί όπως φαίνεται στον πίνακα πακέτα διαφόρων μεγεθών (από 1KB μέχρι 64KB) άρα γίνεται και τεμαχισμός των UDP Segments. Επίσης το μέγεθος του UDP Buffer είναι διαφόρων μεγεθών (8-32 MB). Ενώ η ένταση του σήματος της λήψης του κινητού κόμβου ήταν σχετικά χαμηλή λόγω απόστασης και εμποδίων (-83 dBm) από το AP, εντούτοις η ποιότητα του σήματος

φαίνεται να είναι αρκετά καλή διότι ο αριθμός των χαμένων πακέτων ήταν σε όλες τις περιπτώσεις < 1%. Επίσης το jitter κυμαινόταν σε χαμηλά επίπεδα (6,2 – 6,7).

Σημείωση: Δεν μπορούμε να έχουμε πακέτα με μέγεθος > 64KB

						Server	client				
	Μέτρηση1	Μέτρηση2	Μέτρηση3	Μέτρηση4	Μέτρηση5	Buffer/KB	Packet/KB	Lost Packets%	Απόσταση	Jitter	Ένταση σήματος
Σενάριο A	0	0	0	0	0	8	1	0	10	6,2412	-83dBm
jitter	6,491	6,169	6,171	6,223	6,152						
Σενάριο B	0	0	0	0	0	32	8	0	10	6,6378	-83dBm
jitter	6,372	6,276	6,387	6,402	7,752						
Σενάριο C	0	2,2	0	0	0,34	64	16	0,508	10	6,7622	-82dBm
jitter	6	6,389	8,814	6,153	6,113						

Πίνακας 5.9: Εξάρτηση του Packet loss/jitter από τα μεγέθη πακέτων/UDP Buffer

5.6 Εξάρτηση του Packet Loss/Jitter από το Bandwidth

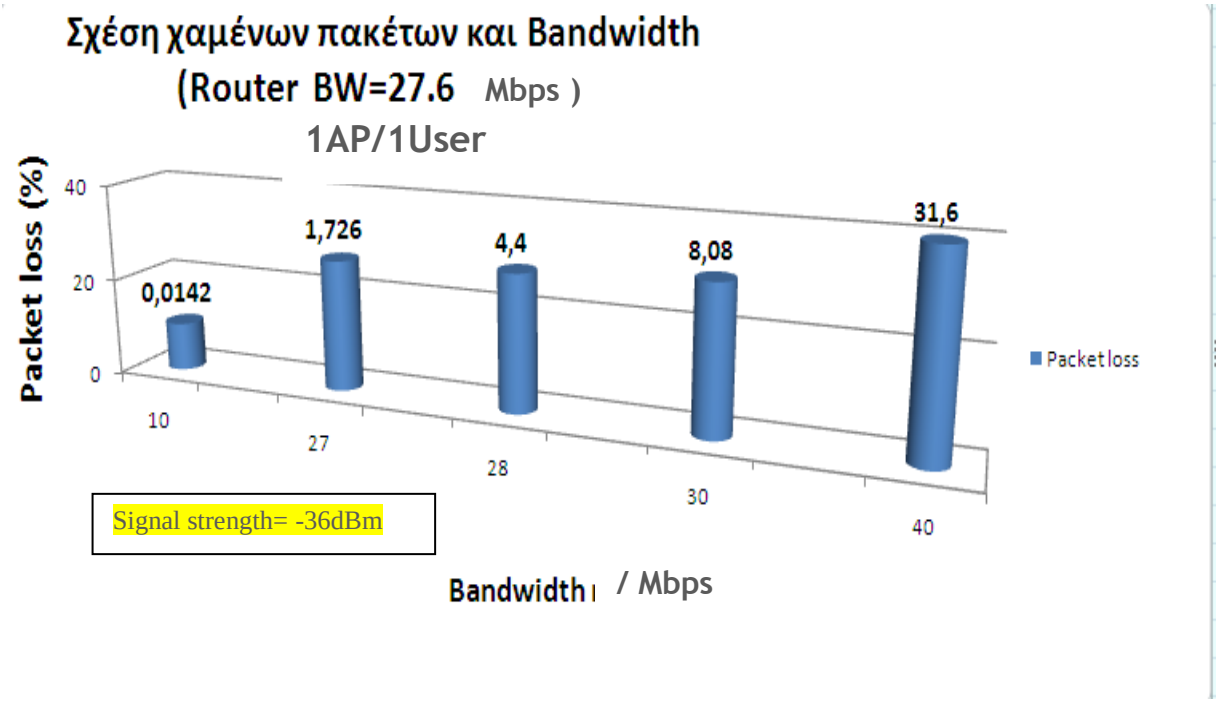
	Μέτρηση1	Μέτρηση2	Μέτρηση3	Μέτρηση4	Μέτρηση5	Bandwidth/ Mbps	Packet loss	Απόσταση	Jitter	Ένταση σήματος
Σενάριο A	0	0,047	0,012	0,012	0	10	0,0142	1	1,8968	-36dBm
jitter	1,989	1,983	1,797	1,885	1,83					
Σενάριο A	1,2	1,3	1,1	3,2	1,83	27	1,726	1	1,246	-36dBm
jitter	1,086	1,445	1,041	0,828	1,83					
Σενάριο A	1,6	8,3	4,7	2,7	4,7	28	4,4	1	3,7176	-36dBm
jitter	15,429	0,899	0,513	0,566	1,181					
Σενάριο A	8,4	7,9	7,3	8	8,8	30	8,08	1	6,6378	-36dBm
jitter	15,344	0,561	0,558	1,229	15,497					
Σενάριο A	33	31	32	31	31	40	31,6	1	9,9278	-36dBm
jitter	2,041	16,026	15,112	2,215	14,245					

Πίνακας 5.10: Εξάρτηση του Packet loss/jitter από το Bandwidth

Ο Router μας σε αυτές τις μετρήσεις έχει transmission rate =27,6 mbps, μολονότι επίσημα μας δίνεται ένα transmission rate = 54Mbps. Αυτή η μείωση οφείλεται σε

διάφορους παράγοντες (πχ. παρεμβολές). Συνοψίζοντας τον πιο πάνω πίνακα 5.10 παρατηρούμε ότι επηρεάζεται σε πολύ μεγάλο βαθμό ο αριθμός των χαμένων πακέτων, όταν το iperf-Bandwidth (BW) που αποστέλλονται οι πληροφορίες είναι μεγαλύτερο από το transmission rate του Router (=27.6 Mbps). Το signal strength διατηρείται σταθερό και ισούται με -36dBm. Σε αυτές τις μετρήσεις με το Bandwidth =10 Mbits/sec παρατηρούμε ότι ο αριθμός των packet loss <= 1% που θεωρείται μια πολύ καλή ποιότητα σήματος (QoS). Το jitter επίσης διατηρείται σε χαμηλά επίπεδα (1,8ms). Με την αύξηση του Bandwidth όμως (>=28Mbps) που ισούται περίπου με το transmission rate του Router, παρατηρούμε μια απότομη αύξηση του αριθμού των packet loss που ξεπερνά το 4%. Αυτό οφείλεται στο ότι ο Buffer του δρομολογητή έχει γεμίσει λόγω του μεγάλου Bandwidth >=28Mbps και όποια νέα πακέτα έρχονται γίνονται drop από τον δρομολογητή. Ο χρόνος μεταξύ των μετρήσεων ήταν 15sec. Επίσης σε πολύ υψηλό Bandwidth > 30 Mbps παρουσιάζεται πολύ μεγάλος αριθμός packet loss (>=8%).

Το jitter επίσης έχει αυξηθεί. Έτσι με την αύξηση του Bandwidth >= 28Mbps παρατηρούμε την ποιότητα του σήματος (QoS) να γίνεται σταδιακά πολύ κακή (Εικόνα 5.22). Η επεξήγηση των αποτελεσμάτων δίνεται στην παράγραφο 5.7.



Εικόνα 5.22: Σχέση Bandwidth / packet loss

Έχει γίνει και μια μέτρηση με Bandwidth (BW) =40Mbps με δύο users (K1,K2) να είναι ενωμένοι με τον ίδιο router R2 (BSS2) ταυτόχρονα (Εικόνα 5.2). Έχει παρατηρηθεί ότι

το packet loss έχει διπλασιαστεί και έχει φτάσει για τον K1=66.6% και τον K2=67%. Το jitter έχει επίσης αυξηθεί σημαντικά (Πίνακας 5.11). Η εξήγηση είναι ότι το transmission rate του Router έχει μειωθεί στο 1/2 για κάθε user. Δηλ. ισούται περίπου με 13Mbps/User, με αποτέλεσμα να αυξηθεί το traffic intensity=40/13 (>1). Επίσης έχουν γίνει και άλλες μετρήσεις και έχει διαπιστωθεί ότι με το BW=10Mbps το packet loss=1%. Με BW=15Mbps το packet loss=12%. Ο λόγος είναι ότι το Traffic intensity = 15/13>1. Το 13Mbps είναι το transmission rate του Router για τον κάθε user. Η απόσταση των ασύρματων χρηστών από το AP είναι μόνο 1m και το signal strength= -36dBm.

	Μέτρηση1	Μέτρηση2	Μέτρηση3	Μέτρηση4	Μέτρηση5	Bandwidth/ Mbps	Lost Packets%	Απόσταση	Jitter	Ένταση σήματος
K1	66	69	66	67	65	40	66,6	1	23256,2	-36dBm
jitter	17.409	1.119	79.943	1.254	16.556					
K2	67	70	66	66	66	40	67	1	16149,5	-36dBm
jitter	0.573	0.736	0.590	16.191,00	16.108,00					

Πίνακας 5.11: Εξάρτηση του Packet loss/jitter από το Bandwidth. 1AP/2 users

5.7 Εξάρτηση Packet Loss/Jitter από το Queuing Delay και το Traffic Intensity [17].

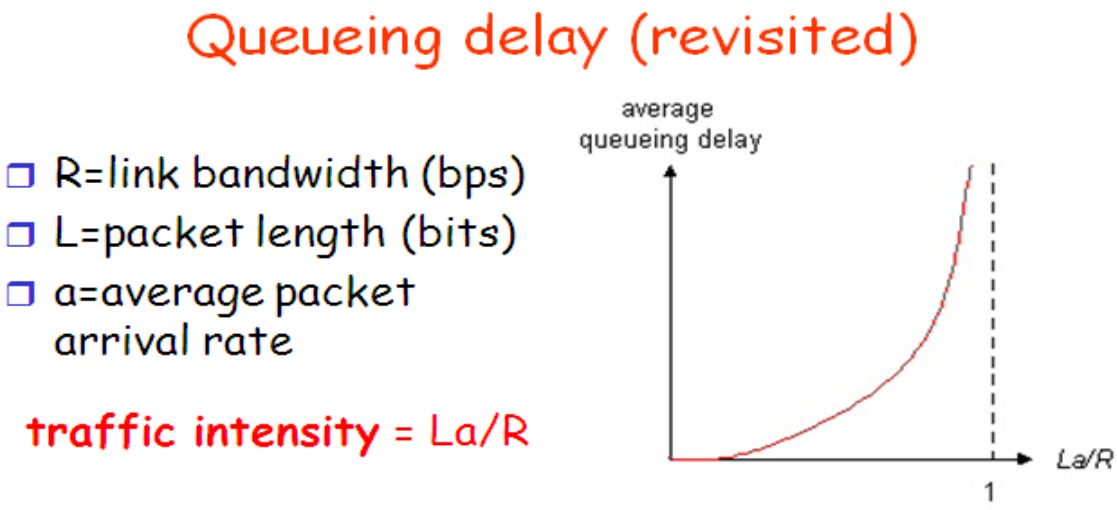
Τι είναι το Queuing Delay (d_{queue}); Είναι ο χρόνος που αναμένει ένα πακέτο από την άφιξή του σε ένα queue ενός Router, μέχρι να γίνει transmitted. Το queuing delay μπορεί να διαφέρει από πακέτο σε πακέτο. Για παράδειγμα αν 10 πακέτα αφιχθούν ταυτόχρονα σε ένα queue, το πρώτο πακέτο θα γίνει transmitted άμεσα και δεν θα έχει καθόλου queuing delay ενώ το τελευταίο πακέτο έχει αρκετά μεγάλο queuing delay διότι περιμένει τα υπόλοιπα 9 να γίνουν transmitted. Τώρα πότε θεωρείται το queuing delay μεγάλο και πότε πολύ μικρό; Αυτό εξαρτάται από το μέγεθος του queue, τη ταχύτητα που φτάνουν τα πακέτα στο queue (Bandwidth), τη ταχύτητα μετάδοσης (transmission rate) του link και από το αν τα πακέτα φτάνουν περιοδικά ή σε μεγάλο-bandwidth transmission σε μικρό χρονικό διάστημα (burst). Θεωρούμε το α το average rate της άφιξης των πακέτων στο queue που μετριέται σε packets/sec. R είναι το transmission rate (bits/sec). Θεωρούμε επίσης ότι τα πακέτα είναι μεγέθους L. Ο τύπος La/R μας δίνει το traffic intensity που η τιμή που παίρνει, καθορίζει το μέγεθος του

d_{queue}. Αν το La/R>1 τότε έχουμε πολύ μεγάλο d_{queue} που θα →∞ . Ο λόγος είναι ότι το average rate της άφιξης των πακέτων στο queue θα είναι μεγαλύτερο από το transmission rate και έτσι το d_{queue} →∞ . Αν το La/R<1 τότε επιδρά θετικά στο d_{queue} με αποτέλεσμα να είναι πολύ μικρό. Π.χ που τα πακέτα φτάνουν στο queue περιοδικά τότε θα βρίσκουν το queue άδειο με αποτέλεσμα το d_{queue} =0. Για παράδειγμα N πακέτα φτάνουν ταυτόχρονα στο queue με ταχύτητα (L/R)N seconds. Τότε το πρώτο πακέτο θα έχει d_{queue} =0. Στο δεύτερο πακέτο το d_{queue}=L/R και στο n-οστό το d_{queue} = (n-1)L/R. Αν τώρα νέα πακέτα φτάνουν σε ένα queue που είναι γεμάτο, τότε δεν θα βρίσκουν χώρο για να φυλαχτούν με αποτέλεσμα ο router να τα απορρίψει (drop) και έτσι να χαθούν (lost). Αυτή είναι η περίπτωση που το traffic intensity >1.

Έχει παρατηρηθεί ότι αν μειωθεί ο χρόνος διεξαγωγής των μετρήσεων σε κάθε 10 sec, τότε αυξάνεται δραστικά ο αριθμός των packet loss (87 packets loss = 125KByte) σε κάθε μέτρηση, με συνολικό packet loss στη κάθε μέτρηση = 6,32% (πίνακας 5.12). Αυτό οφείλεται στο ότι το queue του δρομολογητή έχει γεμίσει πλήρως και δεν μπορεί να δεχτεί νέα πακέτα, λόγω της αύξησης της ροής των δεδομένων. Από ένα σημείο και μετά όλα τα νέα πακέτα που καταφθάνουν γίνονται drop. Έτσι επαναλαμβάνεται το ίδιο σενάριο με εκείνο αύξησης του Bandwidth. Το jitter δεν φαίνεται να επηρεάζεται. Άρα ένας άλλος παράγοντας που συντείνει στην μείωση/αύξηση του packet loss είναι και το μέγεθος του Buffer του Router. Όσο πιο μεγάλος είναι τόσο πιο μεγάλη χωριτικότητα έχει με αποτέλεσμα να γίνονται λιγότερα πακέτα drop.

	Μέτρηση1	Μέτρηση2	Μέτρηση3	Μέτρηση4	Μέτρηση5		Απόστασι	Lost Packets%	Απόστασι	Jitter	Ένταση σήματος
Σενάριο 18	0	2,8	9,6	9,6	9,6		1	6,32	1	8,216	-36dBm
jitter	6,459	15,453	6,142	6,538	6,491						

Πίνακας 5.12: Αύξηση της ροής των δεδομένων και του packet loss



Εικόνα 5.23 : Queuing delay

Παράδειγμα υπολογισμού Queuing Delay, Average queuing delay , traffic intensity

Bandwidth=30 Mbps , 2550 packets, Transfer rate=26880 Kbps

R = 27.4 Mbps

L = 1470 bytes

α = 2550 packets/sec => La/R= 11760bits * 2550packets/sec/27.4Mbps= 1.09 >1 (traffic intensity)

d_{queue} = (n-1)L/R

1ο πακέτο d_{queue} =0

2ο πακέτο d_{queue} = L/R = 11760/27.4 Mbps=0.42ms

3ο πακέτο d_{queue} =2* L/R = 2*0.42 =0.84ms

.

2381ο πακέτο d_{queue} =2380* L/R = 2380*0.42=999.6ms = 1sec

Τα 2381 packets = 93% των πακέτων που έχουν σταλεί. => Τα υπόλοιπα πακέτα (7%) θα γίνουν trop από τον δρομολογητή διότι έχει γεμίσει ο buffer του Router (R) (Εικόνα 83).

2549ο πακέτο d_{queue} =2548* L/R = 2548*0.42=1070ms = 1.070sec

2550ο πακέτο d_{queue} =2549* L/R = 2549*0.42=1071ms = 1.071sec

Average queuing delay for packet N =2550

= 1/N [0 + L/R + 2L/R +……+ (N-1)L/R]

=L/NR[1 + 2 + …….+ (N-1)]

=(L/NR) (N-1) N/2 = (N-1)L/2R ➔ 2549*11760/2R= 535.5ms

Έτσι παρατηρούμε ότι το τελευταίο πακέτο από τα 2550 πακέτα και με Bandwidth 30Mbps θα έχει καθυστέρηση (Bandwidth 30Mbps) =1071ms και average queuing delay=535.5ms. Όπως φαίνεται στα αποτελέσματα της εικόνας 81 με το Bandwidth = 30Mbps έχουμε packet loss = 8% που θεωρείται σχετικά ψηλό ποσοστό. Ο λόγος είναι ότι το Buffer του Router είναι γεμάτο, λόγω μεγάλου traffic intensity (> 1) και έτσι τα τελευταία πακέτα (180) που εισέρχονται στον Buffer γίνονται drop από τον router. Στην εικόνα 5.23 παρατηρούμε ότι όταν το traffic intensity πλησιάσει το 1, τότε παρατηρείται μια απότομη αύξηση του average queuing delay (-> ∞). Είναι σημαντικό να τονίσουμε ότι ένας πολύ σημαντικός παράγοντας που σχετίζεται με το packet loss είναι και το μέγεθος του Buffer. Όσο πιο μεγάλος είναι, τόσο πιο μεγάλη είναι η χωρητικότητα του, άρα αυτό συνεπάγεται ότι πιο λίγα πακέτα θα γίνονται drop.

Κεφάλαιο 6
Παρουσίαση του Λογισμικού

Το Λογισμικό που έχει αναπτυχθεί αποτελείται από δύο βασικά μέρη. Το πρώτο μέρος (Calliperf.c) ασχολείται με την καταγραφή σε μια βάση δεδομένων (ΒΔ), της ποιότητας του σήματος μεταξύ ασύρματων κόμβων ενός WLAN και του Router (Network Link) και το δεύτερο μέρος (DecideHandover.c) αποφασίζει αν ένας ασύρματος κόμβος θα πρέπει να μεταφερθεί σε άλλο ασύρματο δίκτυο. Κριτήριο για αυτή την απόφαση είναι όταν το packet loss > όριο.

6.1 Επεξήγηση του Προγράμματος Calliperf.c

Σκοπός του προγράμματος (file parser) Calliperf.c είναι η καταμέτρηση της ποιότητας του σήματος επικοινωνίας (QoS), μεταξύ διαφόρων ασύρματων χρηστών και του Router (AP-Network link) ενός ασύρματου τοπικού δικτύου. Για σκοπούς μετρήσεων για την μεταπτυχιακή εργασία, χρησιμοποιούνται το test beds που παρουσιάζονται στο κεφάλαιο5.

Το πρόγραμμα calliperf.c είναι ένα πρόγραμμα αυτοματοποίησης της διαδικασίας μέτρησης και καταγραφής των μετρήσεων του iperf, στη Βάση Δεδομένων (ΒΔ) CENTRALDB και συγκεκριμένα στον πίνακα iperfmetriseis. Το πρόγραμμα αυτό έχει γραφτεί σε γλώσσα προγραμματισμού Anci C.

Η Βάση Δεδομένων (ΒΔ) CENTRALDB, όπου καταγράφονται οι μετρήσεις είναι μια ΒΔ MySQL και βρίσκεται στον ίδιο υπολογιστή με το iperf-client. Επίσης είναι εγκατεστημένο το PhpMyAdmin, ένα εργαλείο διαχείρισης της MySQL που επιτρέπει να δούμε και να επεξεργαστούμε τα δεδομένα της ΒΔ μέσω του browser.

Επειδή το πρόγραμμα χρησιμοποιεί SQL εντολές θα πρέπει να εισαγάγουμε την SQL βιβλιοθήκη mysql.h η οποία ευρίσκεται στο /usr/include/mysql/mysql.h

Μεταγλώττιση του προγράμματος.

Επειδή το πρόγραμμα χρησιμοποιεί εντολές για User-Level Threading θα πρέπει να εισαγάγουμε στο πρόγραμμα την POSIX Threads <pthread.h> βιβλιοθήκη για προγραμματισμό νημάτων (Threads) στο UNIX.

Για την μεταγλώττιση του προγράμματος πρέπει να χρησιμοποιηθούν οι επιλογές του GCC –lmysqlclient kai -lptread, δηλ.

gcc –o Calliperf Calliperf.c –lmysqlclient -lptthread

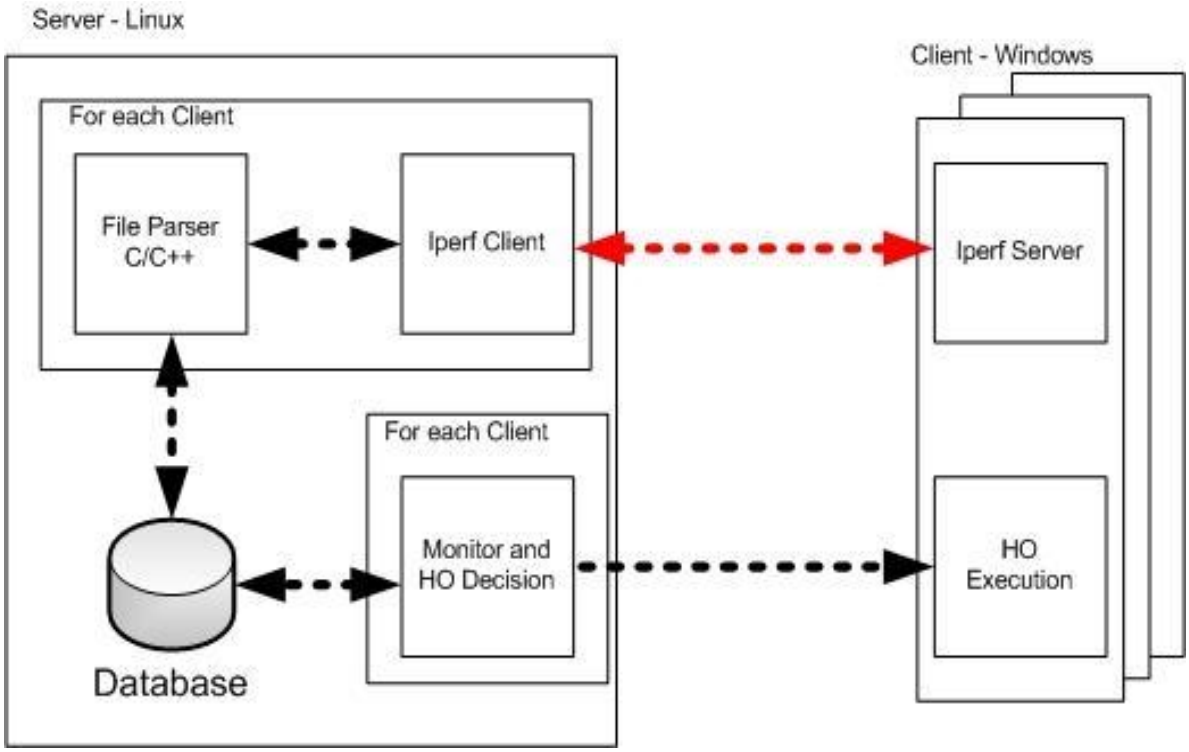
Πρώτος βασικός Πυλώνας του προγράμματος είναι η επικοινωνία του iperf-client (linux server) με τους iperf-servers (windows clients). Αρχικά δημιουργείται ένα text file για κάθε σύνδεση, το οποίο περιέχει μέσα όλες τις μετρήσεις της ποιότητας της επικοινωνίας (QoS) μεταξύ του Router (AP-Network link) και ενός κόμβου του WLAN.

Αρχικά για την ενεργοποίηση του προγράμματος καλούμε το πρόγραμμα με το όνομα **./**calliperf N TimeInt και παράλληλα δίνουμε σαν arguments 2 τιμές. Η πρώτη τιμή (N) είναι ο αριθμός των μετρήσεων που θέλουμε να κάνει το iperf για κάθε χρήστη, για να διαπιστωθεί η ποιότητα της σύνδεσης (QoS). Η δεύτερη τιμή (TimeInt) αφορά το χρονικό διάστημα μεταξύ των μετρήσεων. Αφού ενεργοποιηθεί το πρόγραμμα , πρώτα γίνεται έλεγχος του αριθμού των arguments, ότι δηλ. δόθηκαν σωστά (2) και στη συνέχεια δημιουργείται η σύνδεση με την ΒΔ CENTRALDB αφού πρώτα γίνουν όλα τα απαραίτητα βήματα για τον σκοπό αυτό και δοθούν τα αναγκαία arguments (Π.χ.

username, password, server-location, DB-name) που χρειάζεται η εντολή της MySQL mysql_real_connect() που είναι υπεύθυνη για την δημιουργία της σύνδεσης.. Στη συνέχεια γίνεται η κατασκευή και ενεργοποίηση της εντολής, για την σύνδεση του iperf-client με τους iperf-servers. Οι IP διευθύνσεις όλων των iperf-servers (windows users) που θα θέλουν να επικοινωνήσουν με τον iperf-client βρίσκονται καταχωρημένες στον πίνακα User. Για κάθε χρήστη δηλαδή υπάρχει ένα record στον πίνακα user. Το κάθε record περιλαμβάνει την IP διεύθυνση του χρήστη. Επιπρόσθετα διαθέτει και ένα flag με το όνομα status το οποίο χαρακτηρίζει την κατάσταση που βρίσκεται ο κάθε χρήστης. Αν δηλαδή είναι συνδεδεμένος με τον iperf-client ή όχι. Αν είναι συνδεδεμένος τότε το status=1 διαφορετικά το status=0. Σε μια χρονική στιγμή μπορούν πολλοί χρήστες (iperf-servers) να είναι συνδεδεμένοι με τον iperf-client, π.χ. όλοι οι χρήστες με status=1.

Δεύτερος βασικός πυλώνας του προγράμματος είναι η καταγραφή όλων των μετρήσεων μέσα στη Β.Δ. CENTRALDB. Αρχικά για κάθε ασύρματο user (iperf-server) δημιουργείται ένα Thread με το όνομα runner1(). Σκοπός του κάθε Thread runner1() είναι να δημιουργεί την επικοινωνία κάθε ασύρματου user (iperf-server) με τον iperf-client ξεχωριστά. Ένα άλλο Thread με το όνομα runner2() καταγράφει τις μετρήσεις της επικοινωνίας κάθε ασύρματου user (iperf-server) με τον Router (AP-Network link). Πρώτα τις διαβάζει (μόνο το σύνολο από το text-file iperfmetrisis) και μετά τις διαχωρίζει στη κατάλληλη δομή και στη συνέχεια τις φυλάσσει μέσα στην ΒΔ CENTRALDB στον πίνακα iperfmetriseis. Στη συνέχεια αυτές οι μετρήσεις διαβάζονται, από ένα ειδικό πρόγραμμα που περιγράφεται πιο κάτω, για να αποφασίσει αν ένας ασύρματος user (iperf-server) πληροί τις προϋποθέσεις (packet loss >10%) για να γίνει handover. Αυτό εξαρτάται από το πόσο ποιοτική είναι η σύνδεση (QoS) μεταξύ του Router (AP-Network link) και του iperf-server.

Διάγραμμα ροής της εργασίας 1



Περιγραφή: Ο iperf-Client (Mobile IP Server) είναι εγκατεστημένος σε linux πλατφόρμα και οι iperf-Servers (windows clients) είναι εγκατεστημένοι σε Windows XP. Η βάση δεδομένων MySQL Server είναι και αυτή εγκατεστημένη σε linux O.S. στον ίδιο υπολογιστή που είναι εγκατεστημένος και ο iperf-client. Μετά την ενεργοποίηση του iperf-Client γίνεται η επικοινωνία με τους iperf-servers. Γίνεται μια καταγραφή της ποιότητας του σήματος (QoS) μεταξύ του Router (AP-Network link) και των ασύρματων χρηστών και οι σχετικές πληροφορίες για την επικοινωνία φυλάγονται στη Β.Δ. CENTRALDB. Στη συνέχεια βάσει των πληροφοριών που έχουν φυλαχτεί στη ΒΔ, αποφασίζεται από το πρόγραμμα DecideHandover.c, εφόσον πληρούνται κάποια κριτήρια (HO Decision), ποιοι χρήστες θα γίνουν Vertical Handover (HO Execution).

Εικόνα 6.1: Διάγραμμα ροής της εργασίας 1

6.2 Επεξήγηση του Προγράμματος DecideHandover.c

Κατά την αξιολόγηση των μετρήσεων που έχουν εισαχθεί στη ΒΔ,, εάν διαπιστωθεί ότι πληρούνται οι προϋποθέσεις για Handover τότε το πρόγραμμα αποφασίζει να γίνει το handover. Η προϋπόθεση για να αποφασιστεί από το πρόγραμμα ότι πληρούνται οι συνθήκες για γίνει ένας χρήστης Handover, είναι όταν ο Μέσος Όρος (ΜΟ) του packet loss > 10% (ο ΜΟ για τις τελευταίες μετρήσεις του συγκεκριμένου χρήστη),, είναι μεγαλύτερος ενός ορίου που έχουμε θέσει (π.χ. ΜΟ > 10%).

Ένα ανεξάρτητο πρόγραμμα με το όνομα DecideHandover**.c** που επίσης γράφτηκε σε C θα διαβάζει τις μετρήσεις που είναι καταχωρημένες μέσα στη ΒΔ CENTRALDB. Οι μετρήσεις αυτές περιγράφουν την ποιότητα του σήματος (QoS) επικοινωνίας μεταξύ του Router (AP-Network link) του δικτύου και των iperf-servers. Συγκεκριμένα θα διαβάζει τις πέντε τελευταίες μετρήσεις (μπορεί να αποφασιστεί άλλος αριθμός μετρήσεων) που έγιναν μεταξύ του ασύρματου χρήστη (iperf-server) και του Router (AP-Network link) και θα υπολογίζει τον μέσο όρο του packet loss. Αν ο μέσος όρος ξεπερνά ένα όριο (π.χ. 10%, μπορεί να αλλάξει), τότε το πρόγραμμα αποφασίζει ότι ο ασύρματος χρήστης θα πρέπει να γίνει handover. Σε αυτή την περίπτωση το πρόγραμμα θα δημιουργήσει ένα string με όλες τις αναγκαίες πληροφορίες όπως, IP του χρήστη (iperf server) + την τεχνολογία του δικτύου που μπορεί μεταφερθεί ο χρήστης. Κριτήριο για την επιλογή τεχνολογίας δικτύου είναι το Signal strength (Επιλέγεται η τεχνολογία δικτύου με το μεγαλύτερο Signal strength). Αυτές οι πληροφορίες στέλλονται σε ένα κεντρικό υπολογιστή (Mobile IP Server) που στη συνέχεια θα εκτελέσει το handover. Το handover γίνεται μεταξύ διαφορετικών τεχνολογιών (Vertical Handover). Οι τεχνολογίες είναι όλες IP based π.χ. UMTS/HSDPA,WiFi, WiMAX. Ο κάθε χρήστης έχει καταχωρημένο μέσα στον πίνακα DiscoverNetworks της ΒΔ, ένα record για κάθε δίκτυο (Τεχνολογία) που έχει διαθέσιμη, δηλ. σε ποιο δίκτυο τεχνολογίας (WiFi, UMTS, WiMAX κλπ) μπορεί να γίνει handover. Σαν δεύτερο κριτήριο , για το που θα γίνει handover (δηλ. σε ποιο δίκτυο), είναι το Signal Strength . Αν δηλ. ένας χρήστης μπορεί να κάνει handover σε τρία δίκτυα (Τεχνολογίες δικτύου) θα επιλεγεί να γίνει handover σε εκείνο το δίκτυο που έχει το πιο δυνατό Signal Strength. Τέλος αφού αποφασιστεί από το πρόγραμμα DecideHandover.c ότι ένας χρήστης (iperf-server) πρέπει να γίνει handover, δημιουργεί ένα string με τις πληροφορίες (user IP + δίκτυο Τεχνολογίας) που είναι αναγκαίες για το handover. Αφού δημιουργήσει το string, το στέλλει μέσω socket στον mobile IP Server, ο οποίος με την σειρά του θα εκτελέσει το handover.

Σημείωση: Η εκτέλεση του Handover δεν είναι μέρος αυτής της μεταπτυχιακής εργασίας.

Μεταγλώττιση του προγράμματος.

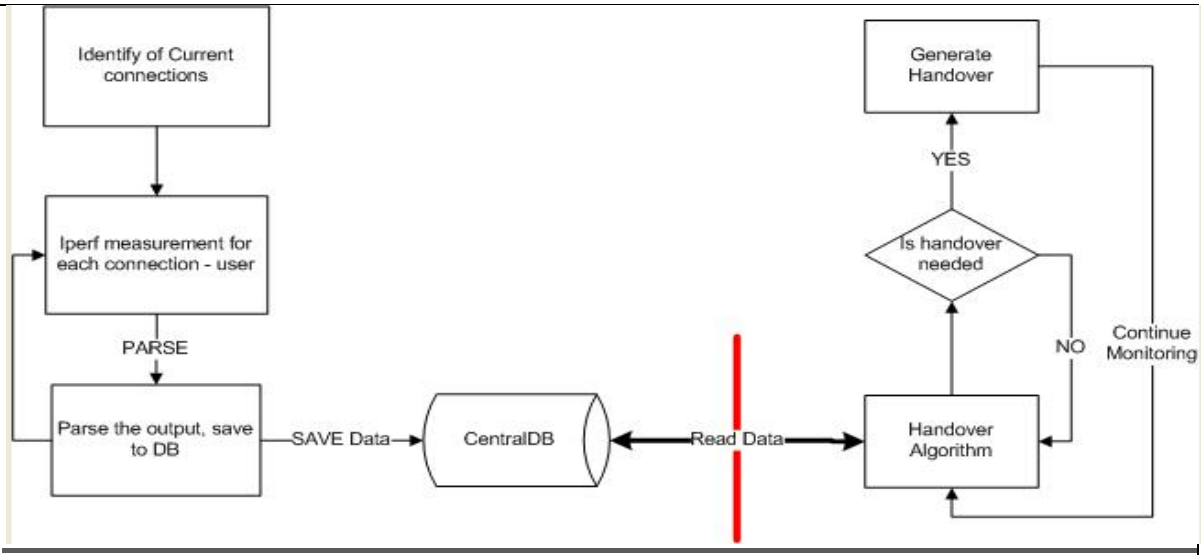
Για την μεταγλώττιση του προγράμματος πρέπει να χρησιμοποιηθούν οι επιλογές του GCC –lmysqlclient δηλ.

gcc –o DecideHandover DecideHandover.c –lmysqlclient

Για την ενεργοποίηση του προγράμματος καλούμε το πρόγραμμα με το όνομα

./DecideHandover server_ ip-address

Διάγραμμα ροής της εργασίας 2



Περιγραφή: Ένα πρόγραμμα με το όνομα DecideHandover.c διαβάζει τις μετρήσεις από την ΒΔ CentralDB και με κριτήριο ότι ο Μέσος Όρος (ΜΟ) του packet loss > 10% (ο ΜΟ για τις τελευταίες μετρήσεις του συγκεκριμένου χρήστη), δημιουργεί ένα string με τις αναγκαίες πληροφορίες για το handover, όπως το IP-address του user ο οποίος θα γίνει handover, καθώς επίσης και τη τεχνολογία του νέου δικτύου που θα μεταφερθεί. Κριτήριο για την επιλογή δικτύου, είναι το δίκτυο με το μεγαλύτερο Signal Strength από τα δίκτυα που είναι διαθέσιμα στον συγκεκριμένο χρήστη. Οι πληροφορίες αυτές θα σταλούν σε ένα κεντρικό υπολογιστή (Mobile IP Server) ο οποίος με την σειρά του θα εκτελέσει το handover.

Εικόνα 6.2: Διάγραμμα ροής της εργασίας 2

Κεφάλαιο 7
Επίλογος

Μελετώντας τα στοιχεία που έχουμε εξάγει από τις διάφορες μετρήσεις, βλέπουμε ότι πολλοί παράγοντες (Bandwidth, signal strength, Buffer length, traffic intensity) συμβάλουν στην ποιοτική επικοινωνία (QoS) μεταξύ των ασύρματων κόμβων ενός WLAN και του Router (AP-Network link). Μελετώντας τα αποτελέσματα που έχουμε εξάγει από τα διάφορα σενάρια που έχουμε πραγματοποιήσει, μπορούμε να λάβουμε κάποια μέτρα, ούτως ώστε να έχουμε μια ποιοτική επικοινωνία σε ένα ασύρματο περιβάλλον. Πιο κάτω ακολουθούν συνοπτικά, διάφορα συμπεράσματα που έχουμε εξάγει στα πλαίσια αυτής της μεταπτυχιακής διατριβής, όσο αναφορά τα χαρακτηριστικά ασύρματων τοπικών δικτύων (WLAN).

7.1 Συμπεράσματα

Το Bandwidth σε συνδυασμό με το μέγεθος του Buffer του Router που δέχεται την ροή των δεδομένων, είναι οι πιο βασικοί παράγοντες που συνδέονται με την αύξηση/μείωση του αριθμού του packet loss. Όσο μεγαλύτερο είναι το Bandwidth από το transmission rate του Router, τόσο αυξάνεται το traffic intensity (>= 1) με αποτέλεσμα να αυξάνεται

ο αριθμός του packet loss. Το jitter φαίνεται να αυξάνεται επίσης με την αύξηση του Bandwidth, λόγω της μεταβλητότητας (variation) με την πάροδο του χρόνου της καθυστέρησης των πακέτων σε ένα δίκτυο (πίνακες 5.10,5.11, εικόνα 5.22).

Παρατηρούμε ότι έχουμε διαφορετικά αποτελέσματα (packet loss) στο WLAN μεταξύ δύο ασύρματων χρηστών, μολονότι έχουμε τις ίδιες αποστάσεις (10m) των δύο ασύρματων κόμβων από τους routers (APs). Έτσι φαίνεται ότι το signal strength (-79 dBm/-87 dBm) και το transmission rate του Router (3Mbps/1.8Mbps) είναι δύο βασικοί παράγοντες που καθορίζουν επίσης σε μεγάλο βαθμό το packet loss (93,67%/98,4%). Όσο πιο μεγάλες είναι οι τιμές τους τόσο πιο χαμηλό είναι το packet loss (πίνακας 5.8). Ένας σημαντικός παράγοντας που πρέπει να ληφθεί υπόψη μας σε αυτή την περίπτωση με μεγάλο Bandwidth, είναι η χωρητικότητα του Buffer του Router. Όσο πιο μεγάλη είναι, τόσο πιο πολλά πακέτα μπορεί να αποθηκεύσει, με αποτέλεσμα μικρότερο packet loss.

Δεν φαίνεται να συνδέεται η αύξηση/μείωση του jitter με αύξηση/μείωση του αριθμού των packet loss. Επίσης παρατηρούμε ότι σε περιπτώσεις που το jitter γίνεται πολύ μεγάλο, έχουμε ένα αριθμό datagram's received out-of-order (εικόνα 5.7).

Η απόσταση (10m) του κινητού κόμβου από το AP με εμπόδια ενδιάμεσα (2 τοίχους), μειώνει το signal strength (-83dBm) με αποτέλεσμα, την αύξηση του αριθμού του packet loss (εικόνα 5.15).

Το jitter δεν επηρεάζεται από την απόσταση του κινητού κόμβου από το AP (εικόνα 5.14).

Με την προσθήκη και νέου AP (διαφορετικού Channel) και επιπρόσθετου wireless κόμβου δεν επηρεάζεται καθόλου ο αριθμός του packet loss. (εικόνα 5.15).

2 παραπλήσια BSS (2 APs) σε απόσταση μόνο 0.5m, που το ένα επικαλύπτει (overlap) το άλλο, τα οποία χρησιμοποιούν το ίδιο κανάλι (channel 6) και με μεγάλο data traffic μεταξύ τους, μεταβάλλουν προς τα πάνω τις τιμές του packet loss και του jitter (πίνακας 5.8, εικόνα 5.21). Ο λόγος είναι ότι οι πόροι του καναλιού μοιράζονται, με αποτέλεσμα ο κάθε user να λαμβάνει μικρότερο εύρος ζώνης (δηλ. ταχύτητα σύνδεσης).

Το jitter φαίνεται επίσης να επηρεάζεται από τις παρεμβολές δύο παραπλήσιων APs μεταξύ τους, που χρησιμοποιούν το ίδιο κανάλι (πίνακας 5.8).

Δεν επηρεάζεται σχεδόν καθόλου ο αριθμός των packet loss από το μέγεθος του UDP Buffer και του μεγέθους των πακέτων που παραλαμβάνει ο iperf-server (πίνακας 5.9).

Οι μετρήσεις που έγιναν σε εξωτερικούς χώρους με εμπόδια ενδιάμεσα (δένδρα), κατέδειξαν ότι στα 10m απόσταση από το AP, ο αριθμός των packet loss είναι πολύ μικρότερος, από ότι οι αντίστοιχες μετρήσεις που έγιναν σε εσωτερικούς χώρους με εμπόδια (τοίχους). Ο λόγος είναι ότι το signal strength είναι μεγαλύτερο (-60 dBm) από ότι στους εσωτερικούς χώρους με εμπόδια τοίχους (-83 dBm). Συνοψίζοντας μπορεί να εξαχθεί το συμπέρασμα ότι, σε εξωτερικούς χώρους το signal strength είναι πιο δυνατό (λόγω λίγων εμποδίων), άρα η επικοινωνία μεταξύ των ασύρματων κόμβων και του Router είναι καλύτερη από ότι σε κλειστούς χώρους. Σε πιο μικρές αποστάσεις οι μετρήσεις είναι σχεδόν οι ίδιες (εικόνα 5.16).

Το traffic intensity = Lα/R (>= 1) επηρεάζει σημαντικά τον αριθμό των packet loss (εικόνα 5.22). Λαμβάνοντας υπόψη μας τα αποτελέσματα των σεναρίων, θα πρέπει να επιλέγουμε το Bandwidth τόσο μεγάλο, ώστε να μην μας δίνει traffic intensity **>**=1**, γ**ια να μην έχουμε μεγάλο αριθμό packet loss (<=1%). Αυτό θα οδηγούσε σε κακής ποιότητας επικοινωνία (QoS) μεταξύ των ασύρματων κόμβων και του Router (AP-Network link) ενός WLAN. Το καλύτερο σενάριο έδειξε ότι, στην επικοινωνία μεταξύ των ασύρματων κόμβων και του Router, πρέπει το Bandwidth <= transmission rate του link (δηλ. traffic intensity<=1). Αυτή η σχέση μας δίνει μικρό αριθμό packet loss (<=1,7%), άρα καλής ποιότητας επικοινωνία μεταξύ των ασύρματων κόμβων και του Router (AP-Network link) ενός WLAN (πίνακας 5.9).

Επίσης ένας άλλος σημαντικός παράγοντας που πρέπει να ληφθεί υπόψη μας, είναι η απόσταση του κόμβου από το access point (AP). Όσο απομακρύνεται από το access point (AP) τόσο αδυνατίζει το σήμα μεταξύ τους (-83dBm). Αυτό έχει σαν αποτέλεσμα, το μεγάλο packet loss που επιδρά αρνητικά στην ποιότητα του σήματος (QoS) (εικόνες 5.11, 5.13, 5.15, 5.17).

7.2 Προτάσεις για Ποιοτική Επικοινωνία σε ένα Ασύρματο Περιβάλλον.

Οι προτάσεις για καλύτερη ποιότητα επικοινωνίας (QoS) στα ασύρματα δίκτυα, βάσει των πιο πάνω συμπερασμάτων είναι:

1. Traffic Intensity <1: Αυτό σημαίνει ότι η σχέση Data-Bandwidth/Link-Bandwidth πρέπει να είναι < 1. Διαφορετικά θα έχουμε μεγάλο Queuing Delay (Dqueuing-→∞) που οδηγεί σε μεγάλο packet loss και σε κακή ποιότητα της σύνδεσης (QoS).

2. Μεγάλο Router Buffer Length: Το Buffer Length του Router (AP-Network Link) πρέπει να είναι όσο γίνεται πιο μεγάλο, για να έχει μεγαλύτερη χωρητικότητα, ούτως ώστε λιγότερα πακέτα να γίνονται drop.

3. Δυνατό Signal Stength: Η μεγάλη απόσταση ενός ασύρματου χρήστη από το Access Point (AP) οδηγεί σε αδύνατο Signal Strength (-80/-90 dBm), με αποτέλεσμα μεγάλο packet loss. Επίσης η ύπαρξη εμποδίων μεταξύ του ασύρματου χρήστη και του AP οδηγεί σε αδύνατο Signal Strength με αποτέλεσμα μεγάλο packet loss. Όπως είδαμε στις μετρήσεις, μεγάλο packet loss οδηγεί σε κακή ποιότητα της σύνδεσης (QoS).

7.3 Σκέψεις για Μελλοντική Μεταπτυχιακή Διατριβή

Θα μπορούσε κάποιος σε μια μελλοντική μεταπτυχιακή διατριβή, να ασχοληθεί με τη διερεύνηση λειτουργίας άλλων ασύρματων δικτύων (όχι μόνο σε WiFi) με χρήση του MIPv6 κάνοντας χρήση των πολλών πλεονεκτημάτων του MIPv6 έναντι του MIPv4.

Μερικά πλεονεκτήματα του IPv6 έναντι του IPv4 είναι:

1. Η IP διεύθυνση πλέον αποτελείται από 128 bits. Αυτό μας δίνει τον τετραπλάσιο αριθμό διευθύνσεων.

2. Απλοποίηση της κεφαλίδας με αποτέλεσμα μικρότερη καθυστέρηση και μείωση του κόστους δρομολόγησης (κάποια πεδία του IPv4 δεν υπάρχουν πια).

3. Κατάργηση του NAT μηχανισμού ο οποίος βοήθησε στην μείωση της σπατάλης IP διευθύνσεων αλλά δημιουργούσε άλλα προβλήματα[3].

4. Παρέχει Ασφάλεια στο επίπεδο IP. Διαθέτει Πρωτόκολλα για Ασφάλεια όπως το IPsec το οποίο παρέχει ασφαλή ανταλλαγή IP πακέτων. Το IPsec παρέχει δύο encryption modes: Το transport mode κωδικοποιεί μόνο τα δεδομένα(payload) του πακέτου και όχι το header. Το Tunnel mode παρέχει κωδικοποίηση και στο header και στα δεδομένα.

5. Παρέχει ενσωματωμένη υποστήριξη για κινητικότητα (mobility). Διαθέτει ενσωματωμένους μηχανισμούς για τον σκοπό αυτό.

Βιβλιογραφία

[01] Νέες τάσεις στη χρήση του διαδικτύου για επικοινωνία, πληροφόρηση και ψυχαγωγία

[02] http://www.internetworldstats.com Ιούνιος 2010

[03] Διπλωματική εργασία Αριστομενόπουλου Γιώργου

[04] http://www.magicandroidapps.com Wiki

[05] C. Perkins, "RFC 3220 IP Mobility Support for IPv4", Ιανουάριος 2002

[06] U.S. Patent 4,144,411

[07] http://www.caida.org/research/id-consumption/whois-map/

[08] Cellular network Wikipedia

[09] Seamless proactive handover across heterogeneous access

[10] Networks Ashutosh Dutta · Subir Das · David Famolari · Yoshihiro Ohba · Kenichi Taniuchi Victor Fajardo · Rafa Marin Lopez · Toshikazu Kodama · Henning Schulzrinne

[11] Διπλωματική εργασία Κατερίνας Κουνούνη

[12] Cisco CCNA I,II,III,IV

[13] Performance Analysis of Mobile IPv4 and Mobile IPv6 Fayza Nada

[14] Handoff mechanism in Mobile WiMAX http://www.conniq.com/WiMAX/handoff.htm

[15] Handovers in the Mobile WiMAX Zdenek Becvar, Jan Zelenka

[16] http://el.wikipedia.org/wiki/Μοντέλο_αναφοράς_OSI

[17] Computer Networking Fifth Edition Dop Down approach Fifth edition from James F.

[18] VoIP Basics: About Jitter Vladimír Toncar

http://toncar.cz/Tutorials/VoIP/VoIP_Basics_Jitter.html

[19] Ανάπτυξη Αλγορίθμου Επίλυσης της Συμφόρησης της Κίνησης σε Σημεία

[20] Cisco CCNA Discovery I,II

[21] February 2011 Geoff Huston Transitioning Technologies – Part 2

[22] http://openmaniak.com

[23] February 2011 Geoff Huston Transitioning Protocols – Part 1

[24] http://en.wikipedia.org/wiki/IPsec

[25] QUALITY OF SERVICE DURING VERTICAL HANDOVER IN 3G/4G

[26] Ποιότητα Υπηρεσιών και Ασφάλεια σε Ασύρματα Δίκτυα 4ης Γενιάς (4G). Κωνσταντίνος

[27] WLAN-3G Interworking for future high data rate networks Mohammad Abualreesh

[28] Wireless LAN to Cellular Network Internetworking- Κοντόπουλος Γεώργιος

Κατάλογος Εικόνων-Πινάκων

Ορολογία (Γλωσσάριο)

ADSL (Asymmetric Digital Subscriber Line) : Καινούργια τεχνολογία για τη μετάδοση ψηφιακών πληροφοριών μέσα από τα ήδη υπάρχοντα τηλεφωνικά καλώδια. Πλεονεκτεί έναντι της τεχνολογίας ISDN στο ότι παρέχει συνεχή σύνδεση με το Internet επί 24ωρου βάσεως, χωρίς να χρειάζεται να κάνουμε κλήση (dial up) κάθε φορά που θέλουμε να συνδεθούμε. Ο συνδρομητής δεν χρεώνεται με το κόστος της κάθε κλήσης που κάνει για σύνδεση στο Internet αλλά μ' ένα σταθερό μηνιαίο πάγιο, ανάλογα με την ταχύτητα σύνδεσης που έχει επιλέξει απ' αυτές που του προσφέρει ο Παροχέας (ISP). Με την ADSL σύνδεση έχουμε και τη δυνατότητα για ταυτόχρονη χρήση δύο τηλεφωνικών γραμμών και το modem της ADSL γραμμής μπορεί να παίξει και τον ρόλο του δρομολογητή (router) σ' ένα τοπικό δίκτυο υπολογιστών (LAN). Η τεχνολογία ADSL παρέχει ασυμμετρικό εύρος δεδομένων (bandwidth) μέσω ενός ζεύγους καλωδίων, το οποίο πρακτικά σημαίνει ότι το εισερχόμενο bandwidth (από το δίκτυο προς τον χρήστη) είναι μεγαλύτερο από το εξερχόμενο (από τον χρήστη προς το δίκτυο).

AuC: **Authentication Center**. Αποτελεί έναν κόμβο που είναι συσχετισμένος με έναν HLR. Ο κόμβος αυτός αποθηκεύει πληροφορίες ταυτοποίησης και κρυπτογράφησης για τους συνδρομητές. Οι πληροφορίες αυτές φορτώνονται στον κόμβο κατά την έναρξη της συνδρομής από το χρήστη.

Bandwidth: A bit rate measure of available or consumed data communication resources expressed in bits/second or multiples of it (kilobits/s, megabits/s etc).

BSS : Basic Set Service είναι η περιοχή κάλυψης ενός AP. Κάθε BSS έχει ένα δικό του όνομα(Identifier) που ονομάζεται SSID (Service Set Identifier). Οι υπολογιστές που ανήκουν στο ίδιο BSS έχουν το ίδιο SSID.

CN: Το CN είναι το δίκτυο κορμού του συστήματος UMTS. Είναι συνδεδεμένο με άλλα δίκτυα όπως τηλεφωνικά δίκτυα Public Telephone Switched Network (PSTN), δίκτυα δεδομένων Public Data Networks (PDNs) όπως το Internet καθώς και με άλλα κινητά δίκτυα. Το CN είναι υπεύθυνο για τη δρομολόγηση, την ταυτοποίηση, τον εντοπισμό των χρηστών καθώς και για άλλες πολλές βασικές λειτουργίες. Το CN διαιρείται σε δύο πεδία: το πεδίο μεταγωγής κυκλώματος (CS) και το πεδίο μεταγωγής πακέτων (PS).

Delay: The delay of a network specifies how long it takes for a bit of data to travel across the network from one node or endpoint to another. It is typically measured in multiples or fractions of seconds.

GSM: (**Global System for Mobile Communications**, originally ***Groupe Spécial Mobile***), is a standard set developed by the European Telecommunications Standards Institute (ETSI) to describe technologies for second generation (or "2G") digital cellular networks.

GTP: Eίναι ένα πρωτόκολλο βασισμένο στο IP το οποίο χρησιμοποιείται στα δίκτυα UMTS. Το πρωτόκολλο αυτό δημιουργήθηκε και προτυποποιήθηκε από το ίδρυμα ETSI για το GSM. Στη συνέχεια, το 3GPP ενσωμάτωσε το GTP στο πρότυπο του UMTS. Το επίπεδο του GTP αντιστοιχεί στο επίπεδο πάνω από το UDP. Ουσιαστικά, πρόκειται για το πρωτόκολλο που είναι υπεύθυνο για τη διαχείριση των δομών του PDP, καθώς και για τη μεταφορά των δεδομένων που αντιστοιχούν σε κάθε σύνοδο. Για το σκοπό αυτό, υπάρχουν τρεις διαφορετικές μορφές του πρωτοκόλλου: η μορφή GTP-C, η GTP-U και η GTP'.

GMSC: Gateway Mobile Services Switching Center : Ο κόμβος GMSC είναι συνδεδεμένος με τους κόμβους MSC. Η λειτουργία του είναι να διασυνδέει το δίκτυο UMTS με άλλα δίκτυα μεταγωγής κυκλώματος όπως PSTN και ISDN.

HLR: Home Location Register Πρόκειται για μία βάση δεδομένων η οποία αποθηκεύει δεδομένα των χρηστών τα οποία μένουν σχετικά σταθερά στο χρόνο. Αυτά τα δεδομένα είναι αναγνωριστικά, πληροφορίες για τις υπηρεσίες του δικτύου στις οποίες συμμετέχει ο συνδρομητής κ.α.

Interworking: Διασυνεργασία

Internet Service Provider: An Internet service provider (ISP), also sometimes referred to as an Internet access provider (IAP), is a company that offers its customers access to the Internet.

Integrated services: IntServ or integrated services is an architecture that specifies the elements to guarantee quality of service (QoS) on networks. IntServ can for example be used to allow video and sound to reach the receiver without interruption.

IETF: **Internet Engineering Task Force.** The Internet Engineering Task Force develops and promotes Internet standards, cooperating closely with the W3C and ISO/IEC standards bodies and dealing in particular with standards of the TCP/IP and Internet protocol suite.

IMS: IP Multimedia Subsystem. For delivering Internet protocol (IP) multimedia services.

MSC: Mobile Services Switching Center (MSC): ο κόμβος MSC αποτελεί έναν κόμβο μεταγωγής ο οποίος δρομολογεί τα δεδομένα των υπηρεσιών μεταγωγής κυκλώματος εντός του δικτύου UMTS. Κάθε κόμβος MSC διαχειρίζεται πολλά RNCs τα οποία συνδέονται σε αυτόν μέσω της διεπαφής Iu-CS. Επίσης, είναι συνδεδεμένος με τις βάσεις δεδομένων του δικτύου όπως τη βάση δεδομένων Home Location Register (HLR) και τη Visitor Location Register (VLR). Τέλος, μία άλλη πολύ χρήσιμη λειτουργία του κόμβου MSC είναι η διαχείριση της κινητικότητας των χρηστών για τις υπηρεσίες μεταγωγής κυκλώματος.

Packet loss rate: Packet loss rate is defined as the fraction of the total transmitted packets that did not arrive at the receiver.

PDP : Packet Data Protocol. Προτού ένα UE μπορέσει να ανταλλάξει δεδομένα με ένα PDN, θα πρέπει να αποκατασταθεί μία εικονική σύνδεση μεταξύ του συγκεκριμένου UE και του PDN. Από τη στιγμή που το UE είναι γνωστό στο PDN, τα πακέτα μεταφέρονται μεταξύ του UE και του PDN μέσω του πρωτοκόλλου **Packet Data Protocol (PDP).** Το πρωτόκολλο αυτό αποτελεί το πρωτόκολλο επιπέδου δικτύου (3ο επίπεδο στο μοντέλο OSI) για το UMTS. Για κάθε σύνοδο του UE, δημιουργείται μία δομή του PDP, η οποία περιέχει τις παραμέτρους της συνόδου (διευθύνσεις εμπλεκόμενων κόμβων, επίπεδο QoS κ.α.). Το υπεύθυνο πρωτόκολλο για τη δημιουργία μίας δομής του PDP όπως και για τη μεταφορά της πληροφορίας, είναι το GPRS Tunnelling Protocol (GTP).

A PDP context contains routing information for packet transfer between an MS and a GGSN to have access to an external packet-switching network. It is identified by an exclusive MS PDP address (mobile's IP address). This means that the MS will have as many PDP addresses as activated PDP contexts.

PSTN: The **public switched telephone network** (**PSTN**) is the network of the world's public circuit-switched telephone networks. It consists of telephone lines, fiberoptic cables, microwave transmission links, cellular networks, communications satellites, and undersea telephone cables all inter-connected by switching centers which allows any telephone in the world to communicate with any other. Originally a network of fixed-line analog telephone systems, the PSTN is now almost entirely digital in its core and includes mobile as well as fixed telephones.

Packet - Αποδίδεται στα ελληνικά με τον όρο Πακέτο και αναφέρεται στα κομμάτια δεδομένων στα οποία διασπάται ένα μήνυμα ώστε να μπορέσει να φθάσει πιο αποτελεσματικά στον προορισμό του. Το κάθε πακέτο έχει μια δική του αρίθμηση έτσι ώστε να γίνεται σωστά η επανασύνδεση των πακέτων όταν αυτά φθάσουν στον τελικό παραλήπτη. Το κάθε πακέτο μπορεί να ακολουθήσει διαφορετική διαδρομή μέχρι τον τελικό προορισμό του και αν κάποιο πακέτο χαθεί ή δεν φθάσει έγκαιρα στον προορισμό του θα πρέπει να ζητηθεί από τον παραλήπτη η αποστολή του εκ νέου. Στη φιλοσοφία αυτή στηρίχθηκε το σύστημα άμυνας των ΗΠΑ απέναντι σε ενδεχόμενη σοβιετική πυρηνική επίθεση στις δεκαετίες του '50 και του '60 και αποτέλεσε και τη βάση για τη λειτουργία του Internet.

RNC: Κάθε κόμβος RNC ελέγχει έναν ή περισσότερους Node Bs. Ένας κόμβος RNC μαζί με τους συνδεδεμένους σε αυτόν Node Bs αποτελούν ένα Radio Network Subsystem(RNS). Ο RNC λαμβάνει τις πληροφορίες που συλλέγουν οι Node Bs του δικού του RNS και προσαρμόζει τις παραμέτρους του ασύρματου υποσυστήματος. Μία τέτοια παράμετρος μπορεί να είναι η ισχύς του ασύρματου σήματος στο UE ή στον Node B. Επίσης, ο RNC είναι υπεύθυνος για την ανάθεση του κώδικα WCDMA που θα χρησιμοποιήσουν ο Node B και το UE στη μεταξύ τους επικοινωνία, έτσι ώστε να μην υπάρξουν παρεμβολές από άλλους ασύρματους συνδέσμους. Τέλος, μία άλλη λειτουργία των κόμβων RNC είναι ο έλεγχος των handovers που λαμβάνουν χώρα μεταξύ διαφορετικών RNSs.

Router - Αποδίδεται στα ελληνικά με τον όρο Δρομολογητής και είναι ειδική δικτυακή συσκευή που αναλαμβάνει να δρομολογήσει (κατευθύνει) τα πακέτα των μηνυμάτων προς τον προορισμό τους καθώς και να διασυνδέσει τοπικά δίκτυα υπολογιστών (LANs). Ένας router διαθέτει στατική IP διεύθυνση και μπορεί να προγραμματισθεί με τη χρήση φορητού υπολογιστή ή και από μακριά (τηλεχειρισμός). Αν συνδεόμαστε στο

Internet μέσω τοπικού δικτύου (LAN) και router, τότε η IP διεύθυνσή μας που φαίνεται προς τα έξω είναι αυτή του router, ενώ τοπικά διαθέτουμε άλλη IP διεύθυνση που την αποδίδει ο router ανάλογα με τη σειρά που συνδέονται οι υπολογιστές του τοπικού δικτύου.

Quality of Service (QoS): The ability to provide specific guarantees to traffic flows.

SGSN: GPRS Support Node. Ο SGSN αποτελεί τον αντίστοιχο κόμβο του MSC στο πεδίο CS. Αυτό σημαίνει ότι αναλαμβάνει τη δρομολόγηση δεδομένων των υπηρεσιών μεταγωγής πακέτων εντός του δικτύου UMTS. Επιπλέον, διαχειρίζεται τους κόμβους RNCs οι οποίοι είναι συνδεδεμένοι σε αυτόν μέσω της διεπαφής Iu-PS. Επίσης, αλληλεπιδρά με βάσεις δεδομένων, όπως η βάση HLR. Τέλος, ο κόμβος SGSN είναι υπεύθυνος για τη διαχείριση της κινητικότητας των χρηστών για τις υπηρεσίες μεταγωγής πακέτων.

Transmission Control Protocol (TCP): The Transmission Control Protocol (TCP) is one of the core protocols of the Internet Protocol Suite. TCP is one of the two original components of the suite, complementing the Internet Protocol (IP) and therefore the entire suite is commonly referred to as TCP/IP. TCP provides the service of exchanging data reliably directly between two network hosts, whereas IP handles addressing and routing message across one or more networks.

UTRAN: Το UMTS Terrestrial Radio Access Network (UTRAN) είναι ένα νέο δίκτυο ασύρματης πρόσβασης το οποίο είναι ειδικά σχεδιασμένο για το σύστημα UMTS. Διαχωρίζεται από το UE μέσω της διεπαφής Uu και από το Core Network (CN) μέσω της διεπαφής Iu. Η βασικότερη λειτουργία του UTRAN είναι η εποπτεία και η διαχείριση των ασύρματων πόρων του δικτύου. Η λειτουργία αυτή συμπεριλαμβάνει την ευθύνη για τον έλεγχο της ισχύος καθώς και την υποστήριξη και διαχείριση των handovers.

VoIP: **Voice over IP**: Voice over Internet Protocol. is a general term for a family of methodologies, communication protocols, and transmission technologies for delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet.

Vertical handover: There are also inter-technology handovers where a call's connection is transferred from one access technology to another, e.g. a call being transferred from GSM to UMTS or from CDMA **IS-95** to **cdma2000**.

VLR : Visitor Location Register (VLR): Ο κόμβος VLR είναι μία βάση δεδομένων. Συνήθως κάθε VLR αντιστοιχεί σε έναν MSC. Η βάση VLR αποθηκεύει προσωρινή πληροφορία σχετικά με την ταυτοποίηση και την ασφάλεια καθώς και άλλες χρήσιμες πληροφορίες που σχετίζονται με όλους τους χρήστες που διαχειρίζεται κάθε δεδομένη στιγμή ο αντίστοιχος MSC. Η βάση VLR λαμβάνει την αρχική πληροφορία από τη βάση HLR και αναλαμβάνει να την ενημερώσει για τυχόν μεταβολές στα δεδομένα της. Όλες οι συναλλαγές μεταξύ VLR και HLR γίνονται μέσω ενός MSC.

WiFi: Wi-Fi, which stands for **WIRELESS FIDELITY**, in a play on the older term **HI-FI**, is a wireless networking technology used across the globe. Wi-Fi refers to any system that uses the 802.11 standard, which was developed by the Institute of Electrical and Electronics Engineers (IEEE) and released in 1997.

WiMAX: (**Worldwide Interoperability for Microwave Access**) is a telecommunications protocol that provides fixed and mobile Internet access. The current WiMAX revision provides up to 40 Mbit/s[1][2] with the IEEE 802.16m update expected to offer up to 1 Gbit/s fixed speeds.

UMTS: Stands for **UNIVERSAL MOBILE TELECOMMUNICATIONS SYSTEM**. UMTS is one of the emerging mobile phone technologies known as third-generation, or **3G**. Third-generation systems are designed to include such traditional phone tasks as calls, voice mail, and paging, but also new technology tasks such as Internet access, video, and SMS, or text messaging.

WCDMA: Wideband Code Division Multiple Access. is the radio access scheme used for third generation cellular systems that are being rolled out in various parts of the globe. The 3G systems to support wideband services like high-speed Internet access, video and high quality image transmission with the same quality as the fixed networks.

UE-User Equipment (κινητός χρήστης)

Ακρωνύμια

3G	3rd Generation
ANSI	American National Standards Institute
AP	Access Point
ARP	Address Resolution Protocol
BA	Binding Acknowledgments
BS	Base Station
BSS	Basic Set Service
BTS	base transceiver station
BU	Binding Update
CDMA	Code Division Multiple Access
CN	Correspondent Node
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CoA	Care of Address
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol Version 6
FA	Foreign Agent
GMM	GPRS mobility management
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HA	Home Agent
HoA	Home Address
HLR	home location register
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IMS	Internet Multimedia Service
IP	Internet Protocol
ITU	International Telecommunications Union
IPng	Next Generation Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6

ISO	International Organization for Standardization
L2	Layer 2 of OSI model, or Data Link layer
L3	Layer 3 of OSI model, or Network layer
LAN	Local Area Network
MIPv4	Mobile IPv4
MIPv6	Mobile IPv6
MN	Mobile Node
MSC	mobile switching center
MSRN	mobile station roaming number
NA	Neighbor Advertisement
NAT	Network Address Translation
NS	Neighbor Solicitation
OSI	Open System Interconnection reference model
PDP	Packet Data Protocol
PSTN	public switched telephone network
RA	Router Advertisement
RADIUS	Remote Authentication Dial-In User Service
RNC	Radio Network Controller
RS	Router Solicitation
RTT	Round Trip Time
SM	Session Management
SGSN	Serving GPRS Support Node
SSID	Service Set Identifier.
TCP	Transmission Control Protocol
TTL	Time To Live
VoIP	Voice over IP
VLR	visitor location register
WLAN	Wireless LAN
WCDMA	Wideband Code Division Multiple Access

Παράρτημα Α
Παρουσίαση Βάσης Δεδομένων και Λογισμικού

Παραθέτουμε όλα τα απαραίτητα αρχεία, ΒΔ, scripts, προγράμματα και ρυθμίσεις που χρησιμοποιήθηκαν για την αρχικοποίηση και λειτουργία των προγραμμάτων.

Α.1 To Shell Script

Είναι ένα text file αποτελούμενο από εντολές οι οποίες μεταφράζονται αμέσως και εκτελούνται χωρίς την δημιουργία ενδιάμεσων αρχείων. Μπορούν να δοθούν απευθείας στη shell. Κάθε shell μπορεί να χρησιμοποιηθεί για την δημιουργία του shell script. Για να μπορεί να γίνει αυτό πρέπει η πρώτη γραμμή κάθε script να είναι η πιο κάτω:

#!/path/to/shell (e.g. #!/bin/ksh).

Τα σύμβολα **#!** λένε στο σύστημα να εντοπίσει και να ακολουθήσει το πιο πάνω path μέχρι να εντοπίσει τη shell. Στη συνέχεια η shell ξεκινά και χρησιμοποιεί σαν input το υπόλοιπο περιεχόμενο του αρχείου (shell script).

Το shell script μπορεί να είναι ένα σύνολο από εντολές που χρησιμοποιούμε συχνά. Τοποθετώντας τις σε ένα script, τις μειώνουμε σε μια εντολή.

Παράδειγμα:

```
1: #!/bin/sh
2: date
3: pwd
4: du –k
```

A.1.1 Γιατί χρησιμοποιούμε Shell Scripts

1. Συνδυάζει μεγάλα και επαναλαμβανόμενα κομμάτια από εντολές σε μόνο μια εντολή
2. Δημιουργεί νέες εντολές χρησιμοποιώντας συνδυασμούς από utilities.
3. Δημιουργεί προσαρμοσμένες σειρές δεδομένων on the fly, και καλεί εφαρμογές (e.g. matlab, sas, idl, gnuplot) για να τα χρησιμοποιήσουν , ή δημιουργεί προσαρμοσμένες εντολές για εφαρμογές/διαδικασίες.

Τυπική χρήση των Shell Scripts

1. System boot scripts (/etc/init.d)

2. System administrators, για αυτοματοποίηση του computer maintenance, για δημιουργία user account κλπ.

3. Σε εργαλεία εγκατάστασης πακέτων εφαρμογών.

A.2 Επεξήγηση του shell script της Μεταπτυχιακής Διατριβής

Σε αυτή την μεταπτυχιακή διατριβή χρησιμοποιείται ένα shell script με το όνομα iperfsn.sh το οποίο καλεί το iperf, τροφοδοτώντας το με ορισμένα arguments για την εξαγωγή συγκεκριμένων πληροφοριών. Συγκεκριμένα το shell script ενεργοποιεί το iperf και με την χρήση κάποιων arguments που δίνονται από το command line του Linux, παίρνουμε πληροφορίες οι οποίες είναι χρήσιμες για την εξαγωγή συμπερασμάτων αναφορικά για την ποιότητα του σήματος μεταξύ των κόμβων του

δικτύου (QoS) και του Router (AP-Network link). Ο ένας κόμβος είναι ο iperf client (Linux machine) και οι άλλοι (1-N) οι iperf servers (windows machine).

Στο πιο κάτω παράδειγμα γίνεται η ενεργοποίηση του shell script και τρέχει σε περιβάλλον Linux.

Chmod 777 iperfsn.sh

./iperfsn.sh 192.168.10.4 –u -p 5001 -fk -d

Επεξήγηση των arguments του iperf που δίνονται πιο πάνω:

192.168.10.4 : Είναι το ip-address του υπολογιστή iperf **server** που θα ενωθεί ο iperf client.

-p 5001: port no

-f : format to report: Kbits, Mbits, KBytes, MBytes

-k : Kbits

-d : bi-directional

-u : use UDP rather than TCP

-c : client mode

Περιεχόμενο του shell script iperfsn.ksh

```
1#!/bin/sh
2# Script to call iperf server on mashine to communicate with server iperf on windows
3#arguments list iperf -c ip-address  -u -p  5001 -f k  -d
4iperf -c $1 $2 1 $3 1 $4 $5
5Exit 0
```

Επεξήγηση του shell script:

1. Ενεργοποίηση της shell sh
2. Επεξήγηση για το τι κάνει το shell script

3. Επεξήγηση για το τι arguments χρειάζεται το shell script

4. Ενεργοποίηση του iperf . Τα $.... χρησιμοποιούνται για την χρήση arguments κατά την ενεργοποίηση του shell script και να χρησιμοποιούνται σαν παράμετροι του iperf.

5. Έξοδος από το shell script.

Το πρόγραμμα καλεί το shell script το οποίο δημιουργεί ένα text file με το όνομα iperfmetrisis.txt με το πιο κάτω περιεχόμενο:

```
Client connecting to 192.168.10.3, UDP port 5001
Sending 1470 byte datagrams
UDP buffer size:   109 KByte (default)
------------------------------------------------------------
[  3] local 192.168.10.7 port 48579 connected with 192.168.10.3 port 5001
[  3]  0.0-10.0 sec  1282 KBytes  1049 Kbits/sec
[  3] Sent 893 datagrams
[  3] Server Report:
[  3]  0.0- 9.8 sec  1262 KBytes  1052 Kbits/sec  6.517 ms   14/  893 (1.6%)
```

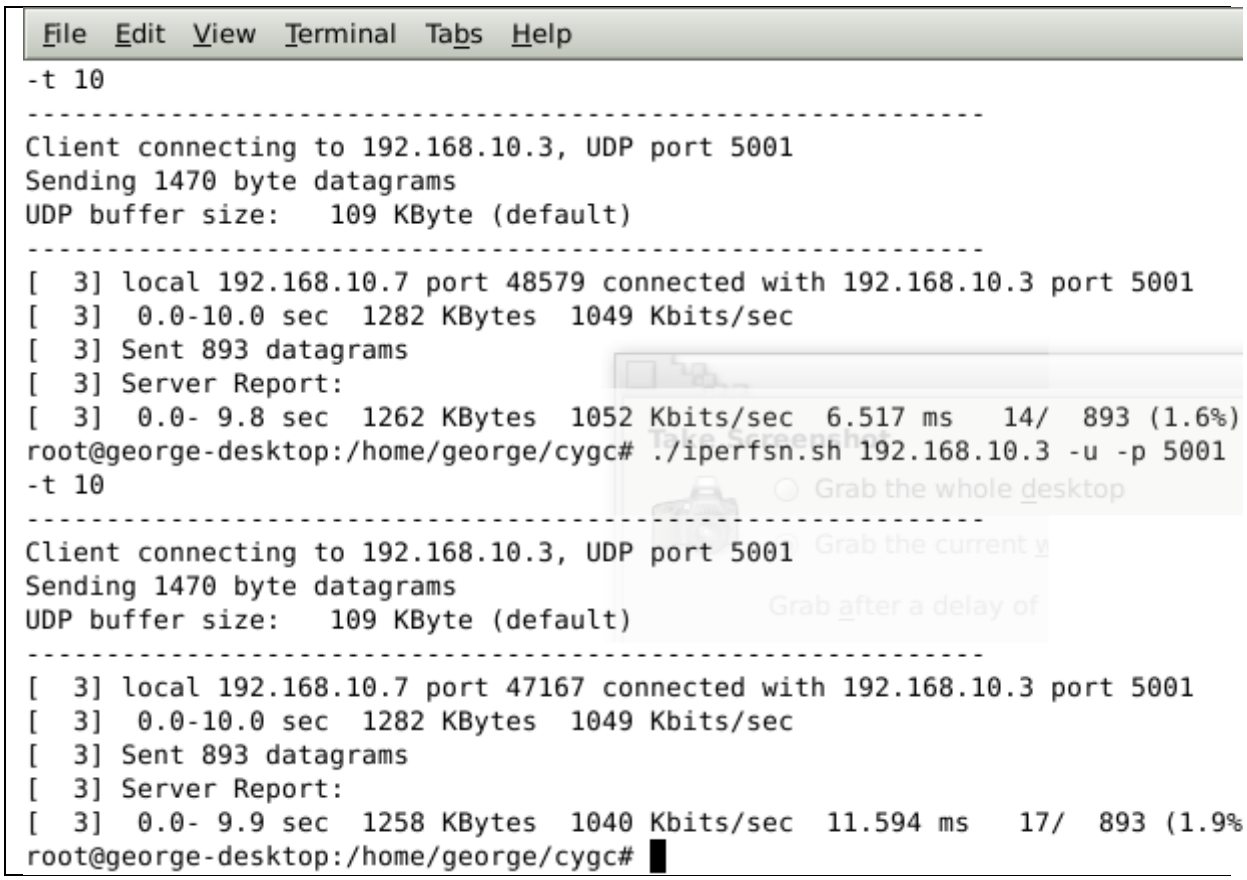
Εδώ παρατηρούμε ένα τυπικό output του iperf server σε ένα text file. Είναι μια πληροφόρηση από τον iperf server, που μας πληροφορεί ότι σε χρονικό διάστημα 10sec έχουν γίνει transfer από τον iperf client προς το iperf server 1262 KB με Bandwidth = 1052Kbps, jitter = 6.517 ms και τέλος ότι έχουμε 14 πακέτα loss, που αντιστοιχούν με το 1.9% των συνολικών πακέτων που έχουν αποσταλεί.

Iperf server side(windows xp)

```
bin/iperf.exe -s -u -P 0 -i 1 -p 5001 -f k
------------------------------------------------------------
Server listening on UDP port 5001
Receiving 1470 byte datagrams
UDP buffer size: 8.00 KByte (default)
------------------------------------------------------------
[1860] local 192.168.10.4 port 5001 connected with 192.168.10.6 port 59963
```

Client side (Linux ubundu)

Περιεχόμενο του δημιουργούμενου text file



Εδώ παρατηρούμε ένα τυπικό output του iperf server σε ένα text file. Είναι μια πληροφόρηση από τον iperf server, που μας πληροφορεί ότι σε χρονικό διάστημα 10sec έχουν γίνει transfer από τον iperf client προς το iperf server 1258 KB με Bandwidth = 1040 Kbps, jitter = 11.594 ms και τέλος ότι έχουμε 17 πακέτα loss που αντιστοιχούν με το 1.9% του συνόλου των 893 πακέτων που έχουν αποσταλεί.

Α.3 Το Σύστημα Β.Δ. MySQL

Η MySQL δουλεύει με την λογική client-server (πελάτης-εξυπηρετητής). Πρόκειται για έναν πολύ λογικό διαχωρισμό της λειτουργικότητας: ο server κρατά όλα τα δεδομένα και ο client ζητά ότι χρειάζεται, χρησιμοποιώντας τη γλώσσα SQL (Structure Query Language). Ο client μπορεί να βρίσκεται στο ίδιο μηχάνημα με το server της MySQL αλλά μπορεί και εύκολα να συνδέεται μέσω Δικτύου. Η MySQL συνήθως διαχωρίζεται σε τρία πακέτα.. Το mysql-server, mysql-client, libmysqlclient. Το πακέτο libmysqlclient χρησιμοποιείται από πολλά προγράμματα για να μπορούν να ενώνονται με το Mysql-server. Ένα χρήσιμο εργαλείο για την διαχείριση της Mysql είναι το PhpMyAdmin. Πρόκειται για ένα εργαλείο διαχείρισης της MySQL μέσω Apache/PHP που μας επιτρέπει να δούμε και να επεξεργαστούμε τα δεδομένα της Β.Δ. μέσω του browser.

Α.3.1 Initial Preparations

```
#include <stdio.h>
#include <stdlib.h>
#include <stdarg.h>
#include "mysql.h"
```

Οι τρείς πρώτες γραμμές είναι χρήσιμες για την γλώσσα προγραμματισμού C. Είναι header files που περιέχουν συναρτήσεις που χρησιμοποιεί η C. Η τέταρτη γραμμή είναι ένα header file που περιέχει συναρτήσεις, που είναι χρήσιμες για την επικοινωνία με τη MySQL Β.Δ. και τους πίνακές της.

```
MYSQL *mysql;            //create an object for accessing the db
MYSQL_RES  *results;    //for results set of a SELECT statement
MYSQL_ROW record;     //declaration of an array for temporarily holding a record or row
```

Η πρώτη γραμμή παραπάνω ορίζει ένα δείκτη που ονομάζεται mysql, βασισμένος στη δομή MYSQL, όπως ορίζεται στο mysql.h. Αυτός θα δημιουργήσει ένα αντικείμενο για την πρόσβαση στις βάσεις δεδομένων. Η επόμενη γραμμή δηλώνει μια σύνθετη δομή δεδομένων για τα αποτελέσματα που θα δώσει η εντολή SELECT, που θα εκτελεστεί αργότερα στο πρόγραμμα. Αυτό ακολουθείται από μια δήλωση ενός πίνακα, που η χρήση του θα είναι η προσωρινή φύλαξη μιας εγγραφής ή γραμμής, που θα διαβαστεί από τα αποτελέσματα αργότερα.

A.3.2 Connecting to a Database

Για να γίνει initialize ο ενσωματωμένος server και το mysql object

```
int main(void)
{
    char *server = "localhost";
    char *user = "george";
    char *password = "gi581806";
    char *database = "CENTRALDB";

  mysql = mysql_init(NULL);
    mysql_real_connect(mysql, server,user,password, database, 0,NULL,0))
```

Η πρώτη γραμμή initializes το MYSQL object το οποίο θα ονομάζεται mysql

Η δεύτερη γραμμή χρησιμοποιεί τη συνάρτηση mysql_real_connect(…….) για να ενωθεί με τη Β.Δ.

Η 2η παράμετρος καθορίζει τον υπολογιστή στον οποίο τρέχει ο server, η 3η παράμετρος καθορίζει το user name, η 4η το password , η 5η το DB name. Οι υπόλοιποι παράμετροι παίρνουν την τιμή NULL or 0 εφόσον η ΒΔ είναι local και δεν έχει γίνει accessed μέσω του δικτύου.

A.3.3 Querying a Database

Για να αντλήσουμε πληροφορίες από τη Β.Δ. MySQL , χρησιμοποιούμε τη συνάρτηση mysql_query() ή την συνάρτηση mysql_real_query(). Στο πιο κάτω παράδειγμα χρησιμοποιούμε την εντολή SELECT για να μας δώσει μια λίστα από βιβλία από το table με το όνομα books. Χρησιμοποιώντας τη συνάρτηση mysql_store_results(), το αποτέλεσμα του ερωτήματος φυλάγεται στο results array όπως φαίνεται πιο κάτω:

```
mysql_query(mysql, "SELECT book_id, title FROM books");

  results = mysql_store_result(mysql);

  while((record = mysql_fetch_row(results))) {
    printf("%s - %s \n", record[0], record[1]);
  }
```

Χρησιμοποιώντας τη while εντολή και τη συνάρτηση mysql_fetch_row(), διαβάζονται τα αποτελέσματα και εκτυπώνονται γραμμή με γραμμή. Μετά την εκτύπωση όλων των

αποτελεσμάτων ότι έχει ανοίξει πρέπει να κλείσει. Αυτό ισχύει και για την συνάρτηση main(). Αυτό γίνεται όπως πιο κάτω:

```
  mysql_free_result(results);
  mysql_close(mysql);
  mysql_server_end();

  return 0;
}
```

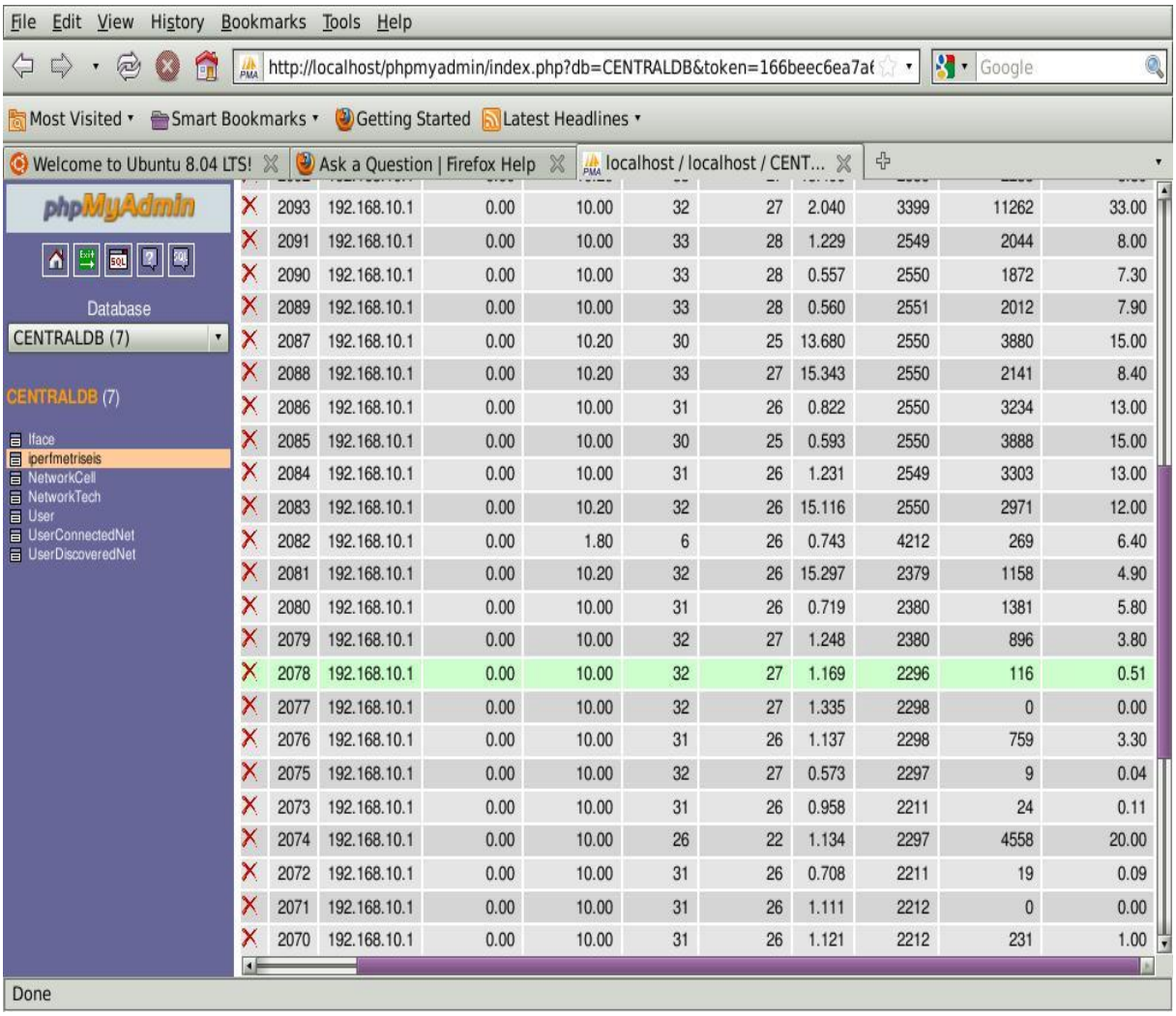
Η συνάρτηση mysql_free_result() χρησιμοποιείται για την απελευθέρωση της δεσμευμένης από το ερώτημα μνήμης. Η συνάρτηση mysql_close() θα κλείσει το mysql object. Η συνάρτηση mysql_server_end() χρησιμοποιείται για να κλείσει τον ενσωματωμένο server. Η εντολή return 0 χρησιμοποιείται για να κλείσει τη συνάρτηση main().

Παρουσίαση της δομής του πίνακα iperfmetriseis

```
-- Table structure for table `iperfmetriseis`

CREATE TABLE IF NOT EXISTS `iperfmetriseis` (

  `id` int(3) unsigned zerofill NOT NULL auto_increment,     // ID του Record

  `IPaddress` varchar(15) NOT NULL,                          // IP του κινητού κόμβου

  `ArxxronosT` float(5,2) NOT NULL,                          // Χρονικό διάστημα αρχής σε sec

  `TelxronosT` float(5,2) NOT NULL,                          //Χρονικό διάστημα  τέλους σε sec

  `PacketszKB` int(5) NOT NULL,                              // Μέγεθος πακέτου σε KB

  `Packetszkbs` int(5) NOT NULL,                             // Μέγεθος πακέτου σε Kbits

  `TransfXronosT` float(7,3) NOT NULL,                       // Χρόνος μετάδοσης των πακέτων

  `PacketNo` int(5) NOT NULL,                                //αριθμός πακέτων

  `Lostpackets` int(5) NOT NULL,                             // αριθμός χαμένων πακέτων

  `Lostpackpers%` int(5) NOT NULL,                           //αριθμός χαμένων πακέτων σε %

  PRIMARY KEY  (`id`)

) ENGINE=MyISAM  DEFAULT CHARSET=latin1 AUTO_INCREMENT=322 ;
```

Όλες οι μετρήσεις που γίνονται από το iperf μεταξύ των διαφόρων χρηστών ενός wireless δικτύου, φυλάγονται μέσα στην ΒΔ CENTRALDB στον πίνακα iperfmetriseis. Οι μετρήσεις αυτές καταδεικνύουν την ποιότητα του σήματος επικοινωνίας μεταξύ των ασύρματων κόμβων και του Router (AP-Network link) ενός WLAN. Μετρήσεις με μεγάλο αριθμό packet loss είναι ένδειξη ότι η επικοινωνία μεταξύ των δύο χρηστών είναι κακής ποιότητας και πρέπει ο mobile χρήστης να κάνει handover σε κάποιο άλλο δίκτυο (wimax,umts) το οποίο θα του παρέχει καλύτερης ποιότητας (QoS) επικοινωνία.

Οι πληροφορίες που φυλάγονται σε αυτόν τον πίνακα (iperfmetriseis) είναι σημαντικές και απαραίτητες για την λήψη απόφασης, αν θα πρέπει κάποιος mobile χρήστης να γίνει handover ή όχι.



X	2093	192.168.10.1	0.00	10.00	32	27	2.040	3399	11262	33.00
X	2091	192.168.10.1	0.00	10.00	33	28	1.229	2549	2044	8.00
X	2090	192.168.10.1	0.00	10.00	33	28	0.557	2550	1872	7.30
X	2089	192.168.10.1	0.00	10.00	33	28	0.560	2551	2012	7.90
X	2087	192.168.10.1	0.00	10.20	30	25	13.680	2550	3880	15.00
X	2088	192.168.10.1	0.00	10.20	33	27	15.343	2550	2141	8.40
X	2086	192.168.10.1	0.00	10.00	31	26	0.822	2550	3234	13.00
X	2085	192.168.10.1	0.00	10.00	30	25	0.593	2550	3888	15.00
X	2084	192.168.10.1	0.00	10.00	31	26	1.231	2549	3303	13.00
X	2083	192.168.10.1	0.00	10.20	32	26	15.116	2550	2971	12.00
X	2082	192.168.10.1	0.00	1.80	6	26	0.743	4212	269	6.40
X	2081	192.168.10.1	0.00	10.20	32	26	15.297	2379	1158	4.90
X	2080	192.168.10.1	0.00	10.00	31	26	0.719	2380	1381	5.80
X	2079	192.168.10.1	0.00	10.00	32	27	1.248	2380	896	3.80
X	2078	192.168.10.1	0.00	10.00	32	27	1.169	2296	116	0.51
X	2077	192.168.10.1	0.00	10.00	32	27	1.335	2298	0	0.00
X	2076	192.168.10.1	0.00	10.00	31	26	1.137	2298	759	3.30
X	2075	192.168.10.1	0.00	10.00	32	27	0.573	2297	9	0.04
X	2073	192.168.10.1	0.00	10.00	31	26	0.958	2211	24	0.11
X	2074	192.168.10.1	0.00	10.00	26	22	1.134	2297	4558	20.00
X	2072	192.168.10.1	0.00	10.00	31	26	0.708	2211	19	0.09
X	2071	192.168.10.1	0.00	10.00	31	26	1.111	2212	0	0.00
X	2070	192.168.10.1	0.00	10.00	31	26	1.121	2212	231	1.00

Πληροφορίες που καταγράφονται στην ΒΔ CENTRALDB στον πίνακα iperfmetriseis.

Α.4 Κώδικας των δύο Προγραμμάτων που έχουν γραφτεί σε C .

```
// Callipperf.c

#include <stdio.h>
#include <stdlib.h>
#include <stdarg.h>
#include <string.h>
#include <time.h>
#include <pthread.h>
//Το path αυτό δημιουργήθηκε κατά την εγκατάσταση του  mysql-server
#include "/usr/include/mysql/mysql.h"

#define NUM_THREADS       10 //maximum number of threads

#define perror2(s, e) fprintf(stderr, "%s: %s\n", s, strerror(e))


const lastline=10;            //last line output file
const Tint=1;                 //Time Intervall between Threads in sec
char **IpAddress=NULL;    //Array από IP-addresses /global variable accessible by all
threads!


int     loopnumber ;  //arithmos epanalipsewn
float timemetrisis;   //time between metrisis

pthread_mutex_t mutexsum,Recstruct;
 int rc;
 pthread_t thread[NUM_THREADS];
 pthread_attr_t attr;
```

```
//define ClientRecord
 struct ClientRec {
        int id;                    //record id
        float t1;                  //kato xroniko orio
        float t2;                  //pano xroniko orio
        int Transfer;              //Transfer
        int Bandwidth;             //Bandwidth
        float Jitter;              // Jitter
        int PacketNumber;      // packets number
        int Lostpacks ;            //Packet loss
        float Lostpackpers;        //Packet loss persentage rate

};

//define ServerRecord opos diabazete apo to metriseis.txt
struct ServerRec {
     char Firsts[2];
     char Secs[3];
     char Firstn[6]  ;
    char Stdash[1];
    char Secn[6];
    char MonXronou [4];
    char PacketszKB[6];
    char MonMetrKB[8];
    char  Packetszkb[8];
    char MonMetrkb[12];
    char Jitter[12];
    char Lostpackets[8];
    char MonXronou2[4];
    char Slash[2];
    char  PacketNumb[4];
    char  bracket[1];
    char  LostPers[8];
};
```

```
//interface with MYSQL database and tables
MYSQL *mysql; //create an object for accessing the db
MYSQL_RES  *results; //for results set of a SELECT statement
MYSQL_ROW record; //declaration of an array for temporarily holding a record or row



// Function Prototypes
void ReadResF(char * , int);
void errorandexit(char *);
void QueryUsers(char **);
int   QueryUsersStatus();
void Queryiperfmetriseis();
char **memoryalloc(char **,int );
void *CreateSystemRec(char *,char *);
void *runner1(void *); /* function prototype of thread's code */
void *runner2(void *); /* function prototype of thread's code */

void errorandexit(char *s) {
        /* Each program upon initialization opens by default three files
         * stdout (output), stderr (error), stdin  (input)
         * Whatever is printed to stderr, stdout appears in the console
         * however in reality we can select to direct these streams
         * into different files (e.g., stdout can be printed on screen and
         * stderr in a log file!). stderr should be utilized for
         * error messages while stdout for messages that go to the user.
         * Below we print error messages to stderr
         */
        fprintf(stderr,"Error: %s \n", s);
        exit(EXIT_FAILURE);
}
/*
Το Thread αυτό διαβάζει τις μετρήσεις του iperf μεταξύ Server-client και τις
```

```
καταχωρεί μέσα στη ΒΔ CENTRALDB στον πίνακα iperfmetriseis.
*/
void *runner2(void *arg){
    FILE *fp;

    int c,ti;
    int number;
    int lineno=1;
    char fname[20];

    //line fields
    struct ServerRec str;

     //Read file metrisewn sti line
     char line [200];
     //char linelast[200];

     //Write sqlbuffer into mysql DB
     char sqlbuffer[100];

     ti=(int)arg;
     strcpy(fname,"iperfmetrisis.txt");

     if ((fp=fopen(fname,"r"))==NULL) {
             errorandexit(" Input File cannot be read!\n");
     }

      //Read every line from file iperfmetrisis.txt.
     while ( fgets (line, 150, fp ) != NULL ) {  /* read a line until \n or the size of line or
eof*/

        //Read only the last line
        if (lineno==lastline) {
```

```
            sscanf(line,  "%s %s %[^-] %[-]  %s %s  %s %s %s %s %s  %s %[^/] %[/]
%s %[(]
                          %[^%]",
     str.Firsts, str.Secs, str.Firstn,str.Stdash,str.Secn,str.MonXronou, str.PacketszKB,
        str.MonMetrKB,str.Packetszkb,str.MonMetrkb, str.Jitter, str.MonXronou2,
            str.Lostpackets,str.Slash,str.PacketNumb,str.bracket,str.LostPers);

              //build the record for Mysql DB
              sqlbuffer[0]='\0';
                  strcat(sqlbuffer,"INSERT INTO iperfmetriseis  VALUES (");
                  strcat(sqlbuffer,"'");
                  strcat(sqlbuffer,",");
                  strcat(sqlbuffer,"'");
                  strcat(sqlbuffer,IpAddress[ti]);
                  strcat(sqlbuffer,"'");
                  strcat(sqlbuffer,",");
                  strcat(sqlbuffer,"'");
                  strcat(sqlbuffer,str.Firstn);
                  strcat(sqlbuffer,"'");
                  strcat(sqlbuffer,",");
                  strcat(sqlbuffer,"'");
                   strcat(sqlbuffer,str.Secn);
                   strcat(sqlbuffer,"'");
                   strcat(sqlbuffer,",");
                   strcat(sqlbuffer,"'");
                   strcat(sqlbuffer,str.PacketszKB);
                   strcat(sqlbuffer,"'");
                   strcat(sqlbuffer,",");
                   strcat(sqlbuffer,"'");
                   strcat(sqlbuffer,str.Packetszkb);
                   strcat(sqlbuffer,"'");
                   strcat(sqlbuffer,",");
                   strcat(sqlbuffer,"'");
                   strcat(sqlbuffer,str.Jitter);
```

```
                    strcat(sqlbuffer,"'");
                    strcat(sqlbuffer,",");
                    strcat(sqlbuffer,"'");
                    strcat(sqlbuffer,str.PacketNumb);
                    strcat(sqlbuffer,"'");
                    strcat(sqlbuffer,",");
                    strcat(sqlbuffer,"'");
                    strcat(sqlbuffer,str.Lostpackets);
                    strcat(sqlbuffer,"'");
                    strcat(sqlbuffer,",");
                    strcat(sqlbuffer,"'");
                    strcat(sqlbuffer,str.LostPers);
                    strcat(sqlbuffer,"'");
                    strcat(sqlbuffer,")");

       }//end if
     lineno++;
    }//while


     //printf("\n%s \n",sqlbuffer);

     mysql_query(mysql, sqlbuffer);

      printf("\n.....οι πληροφορίες έχουν καταχωρηθεί στη mysql DB\n");
      fclose(fp);

     pthread_exit( 0 );

}

//Create a system record to call iperf with arguments and user ip-address
//Call iperf with many  users (many ip-addressess)
void *runner1(void *arg) {
```

```
    char *ipaddress;
    int indext;
    int lcounter=1;    //metritis twn loops
    char scriptbuffer[50];
    int rc,t;
    pthread_t thread[NUM_THREADS];
    pthread_attr_t attr;
  //----------------------------------------Time variables-------------------
    time_t start, end, now;

    indext=(int)arg;

    //create the command to start automatically the iperf with some arguments
    //and create the output file
     scriptbuffer[0]='\0';
     strcat(scriptbuffer,""""" );
     strcat(scriptbuffer,"./iperfsn.sh " );
     strcat(scriptbuffer, IpAddress[indext]);
     //strcat(scriptbuffer, " -u  -b 4m -p 5001   -fk  -d  > iperfmetrisis.txt");   //test line
     strcat(scriptbuffer, " -u   -p 5001   -fk  -d  > iperfmetrisis.txt");
         strcat(scriptbuffer,""""" );
         strcat(scriptbuffer,"\0");

    //call a shell script to run iperf server
     system (scriptbuffer);

    //Call the Thread runner2 and read the file and write the results in mysql DB first
time
     if (rc = pthread_create(&thread[indext], NULL,  &runner2, (void *)indext)) {
           perror2("pthread_create", rc);
           exit(1);
     }
```

```
    start = time(&now);
    while(lcounter<loopnumber) {
          end=time(&now);

     // call the Thread runner2 every timemetrisis sec until loopnumber
        if  (difftime(end, start) == timemetrisis) {
          start = time(&now);
              system (scriptbuffer);

          if (rc = pthread_create(&thread[indext], NULL,  &runner2, (void *)indext)) {
             perror2("pthread_create", rc);
             exit(1);
          }
          lcounter++;

        }

    }//while
     pthread_exit( 0 );
}

//Querying the table Users and count the users  which they have
//status=1. Only this user will be connected with iperf-client
int  QueryUsersStatus() {
   int status;
   int counter=0;

   //Querying a Database table users
   mysql_query(mysql, "SELECT  * FROM User");

   results = mysql_store_result(mysql);

   //find the user with status=1.
   while((record = mysql_fetch_row(results))  !=NULL) {
```

```
            status=atoi(record[11]);
            if (status==1) {
                        counter++;       //count the users with status=1
            }
    }
   return counter;

}

//Querying the table Users and find the users  with
//status=1. Only this users will be connected with iperf-client
void QueryUsers(char **ipaddressQ) {
    int status;
    int i=0;
   char **ipaddress;

    //Querying a Database table users
    mysql_query(mysql, "SELECT  * FROM User");

    results = mysql_store_result(mysql);

    //find the user with status=1. Only one user has status=1
    while((record = mysql_fetch_row(results))  !=NULL) {

            status=atoi(record[11]);
            ///printf("status= %d\n",status);
            if (status==1) {
                        ipaddressQ[i]=record[5];     //ipaddresss[i]=The user ip-address with
status=1
               //printf("Connected with user %s \n",ipaddressQ[i]);
               i++;
            }
    }
```

```
}

char **memoryalloc(char **IperfArr,int arr_size){
    int i;

     //printf("memory allocation arr_size= %d\n",arr_size);
     IperfArr=malloc(8);
     for (i=0;i<arr_size;i++){

            //The first malloc allocates an array of IP-Addresses,
            IperfArr[i]=malloc(8);

    }
            return IperfArr;
}

int main(int argc, char *argv[]){

    FILE *fp;

    int j,arr_size,c,loop;
    //char **IpAddress=NULL;   //Array ??? IP-addresses

     char *server = "localhost";
     char *user = "george";
     char *password = "gi581806";
     char *database = "CENTRALDB";

      int lcounter=1;    //metritis twn loops
  //---------------Thread variables---------------------------------

    int t;
    //pthread_t thread[NUM_THREADS];
```

```
//pthread_attr_t attr;
void *status;



//----------------------------------------end ------------------------------

 printf("\n\n\n.....IperfResults  in P R O G R E S S    !!!!!!!!\n\n");
 //printf("arg= %d  \n",argc);
 //printf("input file name= %s  \n",argv[2]);

 if (argc!=3){
        errorandexit("input-parameters in main!\n");
}

loopnumber =atoi(argv[1]);  //arithmos epanalipsewn
timemetrisis=atoi(argv[2]);   //time between metrisis

mysql = mysql_init(NULL);

//Connecting to a Database
 if (!mysql_real_connect(mysql, server,user,password, database, 0,NULL,0)) {
    fprintf(stderr, "%s\n", mysql_error (mysql));
    exit(1);
}
printf("\n.....Connected to Mysql Data Base CENTRALDB   !!!!!!!!!! \n\n ");

 arr_size=QueryUsersStatus();  //To arr_size = αριθμότων users που έχουν status=1

 //Δυναμική δημιουργία ενός Array για IP-addresses μεγέθους arr_size
  IpAddress=memoryalloc(IpAddress,arr_size);

  //Γέμισμα του Array με τις users ip-addressess
  QueryUsers(IpAddress);
```

```
    /* Initialize and set thread detached attribute */
    pthread_attr_init(&attr);
    pthread_attr_setdetachstate(&attr, PTHREAD_CREATE_DETACHED);

    for(t=0; t<arr_size; t++){

      if (rc = pthread_create(&thread[t], NULL,  &runner1, (void *)t)) {
          perror2("pthread_create", rc);
          exit(1);
      }

     sleep(Tint);
    }

    // We're done with the attribute object, so we can destroy it
    pthread_attr_destroy(&attr);

     /* Free attribute and wait for the other threads */
    pthread_attr_destroy(&attr);
    for(t=0; t<arr_size; t++) {
       rc = pthread_join(thread[t], &status);
      if (rc) {
         printf("ERROR; return code from pthread_join()  is %d\n", rc);
         exit(-1);
      }
     //printf("Main: completed join with thread %ld having a status of
%ld\n",t,(long)status);
    }


   /* The main thread is done, so we need to call pthread_exit explicitly to
   *  permit the working threads to continue even after main completes.
   */
    printf("Main: program completed. Exiting.\n");
```

```
      pthread_exit(NULL);



    mysql_free_result(results); //free the memory where the relults set from the query
is store.
    mysql_close(mysql); //close the mysql object.
    mysql_server_end(); //close the embedded server.


  return 0;
}
```