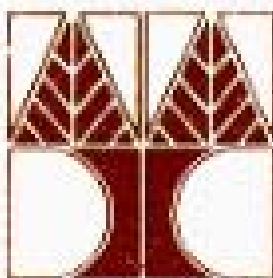


Ατομική Διπλωματική Εργασία

**ΤΡΙΤΗΣ ΓΕΝΕΑΣ ΚΙΝΗΤΑ ΔΙΚΤΥΑ:
ΜΕΛΕΤΗ ΧΡΗΣΗΣ MOBILE IPV6
ΣΕ UMTS ΠΕΡΙΒΑΛΛΟΝ**

Συμεού Ιωάννα

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ



ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Ιούνιος 2003

ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Τρίτης Γενεάς Κινητά Δίκτυα:
Μελέτη Πιθανής Χρήσης Mobile IPv6
σε UMTS Περιβάλλον

Συμεού Ιωάννα

Επιβλέπων Καθηγητής
Ανδρέας Πιτσιλλίδης

Η Ατομική αυτή Διπλωματική Εργασία υποβλήθηκε προς μερική εκπλήρωση
των απαιτήσεων απόκτησης του πτυχίου Πληροφορικής του
Τμήματος Πληροφορικής του Πανεπιστημίου Κύπρου

Ιούνιος 2003

Περιεχόμενα

Κεφάλαιο 1	Εισαγωγή	1
1.1	Τα κινητά δίκτυα σε γενικές γραμμές	1
1.2	Σύντομη Ιστορία των Δικτύων	2
1.3	Τι είναι, τι υπόσχεται και τι οδήγησε στο UMTS	4
1.4	Wireless LANs και UMTS	6
1.5	Το Mobile IP και πως μπορεί να εφαρμοστεί στο UMTS	6
Κεφάλαιο 2	Ένας IP Κόσμος	8
2.1	WLANs Εισαγωγή	9
2.2	IEEE 802.11	11
2.3	Bluetooth	13
2.4	HIPERLAN	17
2.5	Mobile IP	20
2.6	Γιατί IP σε UMTS	27
Κεφάλαιο 3	Περιγραφή Mobile IPv6	30
3.1	Εισαγωγή	30
3.2	Βασικές Ορολογίες	31
3.3	Σύντομο Overview του Mobile IPv6	32
3.4	Λειτουργία Mobile IPv6	34
3.5	QoS για Mobile IPv6	39
3.6	Μηχανισμοί Μετάβασης	40
3.7	Πλεονεκτήματα του Mobile IPv6	43
Κεφάλαιο 4	Περιγραφή Συστήματος UMTS	45
4.1	Σύντομο Overview του UMTS	46
4.2	UMTS Έκδοση 99	47
4.3	UMTS Έκδοση 2000 (Έκδοση 4 και Έκδοση 5)	50
4.4	All - IP UMTS	52
4.5	IP Έκδοση στο UMTS	57
Κεφάλαιο 5	Ανάλυση Δυνατών Σεναρίων Χρήσης UMTS με IPv6	58
5.1	Απαιτήσεις και Υποθέσεις	58
5.2	Σενάριο 1	59

5.3	Σενάριο 2	64
5.4	Σενάριο 3	70
5.5	Σενάριο 4	74
5.6	Σενάριο 5	77
5.7	Σενάριο 6	80
5.8	Συνοπτικός Πίνακας των Σεναρίων	85
Κεφάλαιο 6	Προσομοιώσεις Handover δικτύου UMTS με χρήση εργαλείου OPNET	86
6.1	UMTS Handover	86
6.2	Προσομοίωση με την χρήση του εργαλείου OPNET: Παράδειγμα Soft Handover	88
6.3	Προσομοίωση με την χρήση του εργαλείου OPNET: Σύγκριση Soft Handover και Hard Handover	90
6.4	Συμπεράσματα	100
Κεφάλαιο 7	Συμπεράσματα	101

Ευχαριστίες

Με το τέλος της φοίτησής μου και της ακαδημαϊκής μου ζωής στο Πανεπιστήμιο Κύπρου, θεωρώ υποχρέωσή μου να ευχαριστήσω πάνω από όλα την οικογένειά μου που με βοήθησε και με στήριξε σε όλη μου τη ζωή. Θέλω να ευχαριστήσω τους καθηγητές μου, ιδιαίτερα τον κ. Ανδρέα Πιτσιλλίδη για την καθοδήγησή του και την βοήθειά του στην μελέτη αυτή. Ιδιαίτερο ευχαριστώ και στον Χρυσόστομο Χρυσοστόμου και Josephina Αντωνίου για την βοήθειά τους. Ευχαριστίες και στα άτομα του προσωπικού μου κύκλου που ήταν πάντα εκεί και μου στάθηκαν ακαδημαϊκά και μη. Θέλω στο τέλος να ευχαριστήσω και τον εαυτό μου που πάντα προσπαθούσε και με έφτασε μέχρι εδώ.

Περίληψη

Τα κινητά δίκτυα είναι ένα μικρό, αλλά σημαντικό κομμάτι από τον κόσμο των δικτύων. Έχουν γίνει πλέον μέρος της καθημερινότητάς μας και συνεχώς αυξάνεται η ζήτηση για τις υπηρεσίες των κινητών δικτύων. Τα τρίτης γενεάς κινητά δίκτυα είναι η τελευταία εξέλιξη, μέχρι στιγμής, σε κινητά και ασύρματα δίκτυα. Ένα σύστημα τρίτης γενεάς δικτύων είναι και το Universal Mobile Telecommunications System (UMTS).

Τι προσφέρει όμως το UMTS; Ποιες είναι οι καινοτομίες του και οι υπηρεσίες του προς το μέσο χρήστη; Με ποια άλλα συστήματα μπορεί να συνλειτουργήσει; Αν θα προσφέρει μεταφορά πακέτων, ποιο πρωτόκολλο θα χρησιμοποιήσει; Αν θα είναι IP, θα είναι το IPv4 ή το IPv6; Είναι πάρα πολλά τα ερωτήματα που έρχονται με την νέα αυτή τεχνολογία. Στη μελέτη αυτή δίνονται κάποιες απαντήσεις και αναλύονται μερικά θέματα που αφορούν συνένωση των δικτύων κάτω από κοινό πρωτόκολλο network layer, την λειτουργία του Mobile IPv6 και προσομοιώσεις UMTS δικτύου για μελέτη των διαδικασιών Handover.

Κεφάλαιο 1

Εισαγωγή

1.1 Τα κινητά δίκτυα σε γενικές γραμμές	1
1.2 Σύντομη Ιστορία των Δικτύων	2
1.3 Τι είναι, τι υπόσχεται και τι οδήγησε στο UMTS	4
1.4 Wireless LANs και UMTS	6
1.5 Το Mobile IP και πως μπορεί να εφαρμοστεί στο UMTS	6

1.1 Τα κινητά δίκτυα σε γενικές γραμμές

Στο άκουσμα των λέξεων «Ηλεκτρονικός Υπολογιστής», ο μέσος άνθρωπος φέρνει στο μυαλό του την γνωστή εικόνα του Υπολογιστή που σχεδόν όλοι έχουμε στο σπίτι μας ή στο χώρο εργασίας μας. Είναι όμως σχεδόν σίγουρο ότι η μορφή του Ηλεκτρονικού Υπολογιστή δεν θα παραμείνει η ίδια στα επόμενα δέκα χρόνια και στον επόμενο αιώνα γενικότερα. Καμία ακριβής πρόβλεψη δεν μπορεί να γίνει, όμως σαν γενικό χαρακτηριστικό, πολύ πιθανόν όλοι οι Ηλεκτρονικοί Υπολογιστές θα είναι φορητοί και ασύρματοι καθώς πολλοί χρήστες θα είναι κινητοί, ήδη ένα χαρακτηριστικό της σημερινής κοινωνίας της πληροφορίας. [1]

Στις μέρες μας, υπάρχει μια εκθετική αύξηση στα συστήματα κινητής τηλεφωνίας, τα άτομα στην κοινωνία κινούνται όλο και περισσότερο και η αγορά απελευθερώνεται από το μονοπώλιο. Μαζί με τα παραδοσιακά σταθερά δίκτυα, συνυπάρχουν και τα κινητά δίκτυα όπως το GSM (Groupe Spéciale Mobile ή Global System for Mobile communications), με συστήματα σαν το GPRS (General Packet Radio Service). Για πολλές χώρες, η κινητή επικοινωνία είναι η μόνη λύση λόγω της μη επαρκούς υποδομής για σταθερά δίκτυα (για παράδειγμα δυσκολία καλωδιοποίησης).

Αυτό που βλέπουμε σήμερα όμως, είναι σχετικά μόνο η αρχή. Υπάρχουν πολλά καινούργια και συναρπαστικά συστήματα που αναπτύσσονται αυτή τη στιγμή σε εργαστήρια, σε πειραματικό επίπεδο. Το μέλλον θα δει πολλές νέες συσκευές (όπως

Προσωπικό Βοηθό Ταξιδιού – Personal Travel Assistant – στα αυτοκίνητα, Οδηγούς Ταξιδιού με Γνώση Τοποθεσίας – Location Aware Travel Guides – για ξεναγούς και τουρίστες, συσκευές σύνδεσης ασθενοφόρων με νοσοκομεία), την συγχώνευση των τεχνολογιών μετάδοσης φωνής και δεδομένων, την επέκταση των σημερινών εφαρμογών του Διαδικτύου και πολλά άλλα. Ήδη ένα βήμα προς το μέλλον έχει γίνει με το σύστημα UMTS (Universal Mobile Telecommunications System), το οποίο άρχισε να λειτουργεί δοκιμαστικά. [1]

1.2 Σύντομη Ιστορία των Δικτύων

Όσο απίστευτο κι αν φαίνεται, η κινητή και ασύρματη επικοινωνία χρονολογείται από πολύ παλιά. Με την χρήση σημάτων καπνού, του φωτός κατευθυνόμενο από καθρέφτες, με σημαίες και τα λοιπά, γινόταν δυνατή η επικοινωνία – και σταθερή και κινητή - μεταξύ των ανθρώπων χωρίς τη χρήση συρμάτων. Η ασύρματη επικοινωνία σε μεγάλη απόσταση έγινε δυνατή στο τέλος του 18 αιώνα (1794), με την εφεύρεση του Claude Chappe: τον οπτικό τηλέγραφο.

Η κινητή και ασύρματη επικοινωνία όμως δεν έγινε ιδιαίτερα δημοφιλής – λόγο των διάφορων προβλημάτων των οπτικών συστημάτων - μέχρι την ανακάλυψη των ηλεκτρομαγνητικών κυμάτων και την ανάπτυξη του εξοπλισμού για την χρησιμοποίηση και εκμετάλλευση των κυμάτων αυτών. Την εισαγωγή της έννοιας των ηλεκτρομαγνητικών κυμάτων έκανε ο Michael Faraday το 1831, ενώ ο James C. Maxwell έθεσε τις θεωρητικές αρχές των ηλεκτρομαγνητικών πεδίων. Την πρώτη μετάδοση ηλεκτρομαγνητικών κυμάτων πέτυχε ο Heinrich Hertz (εξού και η μονάδα μέτρησης Hz) το 1886.

Η πρώτη επίδειξη ασύρματου τηλεγράφου έγινε το 1895 από τον Guglielmo Marconi. Ακολούθως η πρώτη υπερατλαντική μετάδοση έγινε το 1901 και έξι χρόνια αργότερα το 1907 δημιουργήθηκαν οι πρώτες εμπορικές υπερατλαντικές συνδέσεις. Η πρώτη ραδιοφωνική μετάδοση έγινε το 1906 και το 1920 λειτούργησε ο πρώτος ραδιοφωνικός σταθμός.

Μέχρι το 1928 ακολούθησαν πολλές ανακαλύψεις, όπως τα short waves με την ιδιότητά τους να αντανακλούνται στην ιονόσφαιρα, την ηλεκτρονική λυχνία, τα τηλέφωνα στα

τραίνα, τα ραδιόφωνα στα αυτοκίνητα και η τηλεοπτική μετάδοση, οι οποίες βοήθησαν σημαντικά την διάδοση των κινητών κι ασύρματων δικτύων. Ένα μεγάλο βήμα προς την καλυτέρευση της ποιότητας των κινητών δικτύων έγινε το 1933 με την ανακάλυψη της μετατροπής συχνότητας (frequency modulation) από τον Edwin H. Armstrong.

Μετά τον δεύτερο παγκόσμιο πόλεμο οι βόρειες Ευρωπαϊκές χώρες συμφώνησαν στο NMT (Nordic Mobile System) σύστημα. Μετά την ανάπτυξη διαφόρων άλλων δικτύων στην Ευρώπη, η Ευρωπαϊκή Ένωση αποφάσισε το 1982 να αναπτύξει ένα πανευρωπαϊκό δίκτυο, το GSM (Groupe Spéciale Mobile). Σχεδόν τον ίδιο καιρό οι Η.Π.Α. ανέπτυξαν το αναλογικό AMPS (Advanced Mobile Phone System). Τα τηλέφωνα γίνονται ασύρματα με την χρήση του πρότυπου CT1 (Cordless Telephone) το 1984.

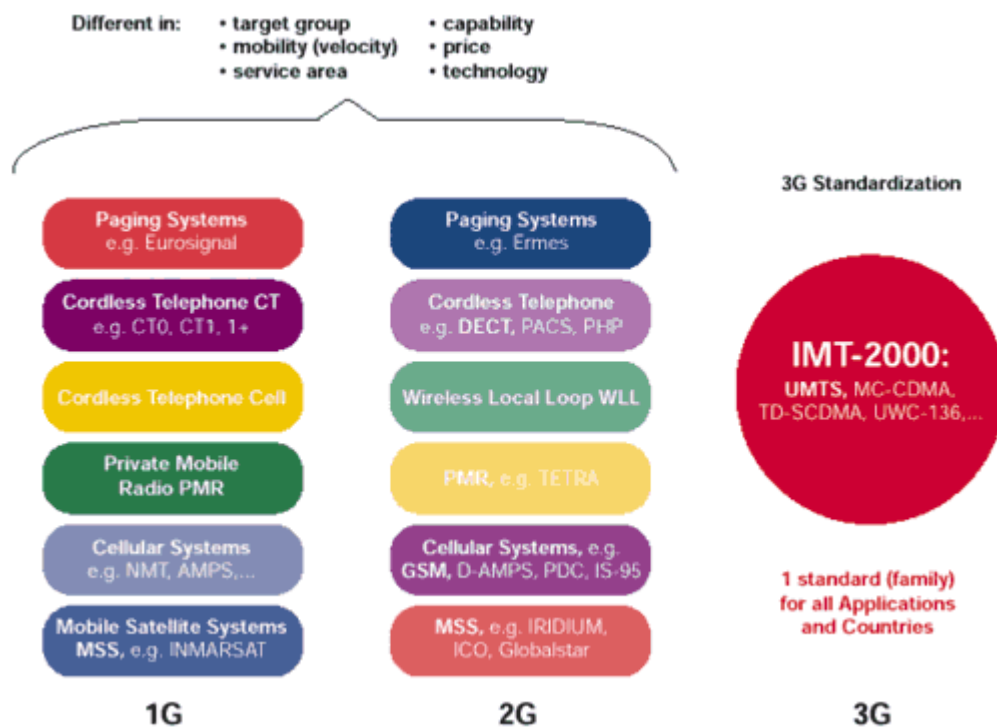
Στις αρχές του 1990 σηματοδεύτηκε η ανάπτυξη πλήρη ψηφιακών συστημάτων. Το 1991 το ETSI (European Telecommunications Standard Institute) χρησιμοποιεί το πρότυπο DECT (Digital European Cordless Telephone, γνωστό σήμερα σαν Digital Enhanced Cordless Telecommunications) για ψηφιακή ασύρματη τηλεφωνία. Το DECT λειτουργεί σε ένα φάσμα 1880 – 1900 MHz σε ακτίνα 100 – 150 μέτρα και προσφέρει κρυπτογράφηση και πιστοποίηση των δεδομένων. Το GSM γίνεται πρότυπο και μετονομάζεται σε Global System for Mobile communications, λειτουργεί στα 900 MHz και χρησιμοποιεί 124 full-duplex κανάλια.

Το 1998 χρησιμοποιήθηκε για πρώτη φορά δορυφόρος στην κινητή επικοινωνία με το σύστημα Iridium. Με το σύστημα αυτό γίνεται δυνατή η δημιουργία μικρών κινητών δορυφορικών τηλεφώνων που συμπεριλαμβάνουν και μεταφορά δεδομένων. Την ίδια χρονιά η Ευρώπη προτείνει στο International Telecommunications Union, IMT-2000 (International Mobile Telecommunications) το σύστημα UMTS (Universal Mobile Telecommunications System). Οι εισηγήσεις που δόθηκαν στο IMT-2000 καθορίζουν ένα κοινό, παγκόσμιο πλαίσιο εργασίας για μελλοντικές κινητές επικοινωνίες στα 2GHz. Αυτό συμπεριλαμβάνει πλαίσιο εργασίας για υπηρεσίες δικτύου, την αρχιτεκτονική του δικτύου λαμβάνοντας υπόψη και τις δορυφορικές επικοινωνίες, στρατηγικές για αναπτυσσόμενες χώρες, πλαίσιο εργασίας για αυξημένη ασφάλεια και άλλα. [1]

1.3 Τι είναι, τι υπόσχεται και τι οδήγησε στο UMTS

Οι τεχνικές δυσκολίες και μειονεκτήματα των κινητών δικτύων συνεχώς μειώνονται λόγω των τεχνολογικών εξελίξεων. Ήδη μελετούνται και εφαρμόζονται πειραματικά τρίτης γενεάς δίκτυα. Τα τρίτης γενεάς συστήματα κινητής επικοινωνίας δημιουργούν μια προοπτική εντελώς καινούργιων υπηρεσιών. Όλοι οι περιορισμοί των τεχνολογιών δεύτερης γενεάς πρέπει να ξεπεραστούν. Οι περιορισμοί αυτοί είναι κυρίως οι δυσκολίες που συναντιούνται στην ανάπτυξη ικανοποιητικών υπηρεσιών, για τις ακόλουθες εφαρμογές σε κινητά δίκτυα: ηλεκτρονικού ταχυδρομείου, πλοήγησης δικτύου, συνεταιρικής τοπικής πρόσβασης δικτύου (corporate local network access), τηλεσυνεδρίων, ηλεκτρονικού εμπορίου, πολυμέσων συμπεριλαμβανομένου και διάφορων άλλων εφαρμογών. [17]

Το UMTS είναι η πρόταση της Ευρώπης στο International Telecommunications Union, IMT-2000 και αποτελεί ένα τρίτης γενεάς δίκτυο. Το UMTS θα ενώσει τις ξεχωριστές υπηρεσίες σταθερής και κινητής τηλεπικοινωνίας, κάτω από ένα ψηφιακό περιβάλλον δεδομένων. Το σύστημα των UMTS συνδυάζει μεγάλες καινοτομίες στη ραδιο - πρόσβαση (radio access), συμπεριλαμβανομένου καινούργιων ραδιο – διαπροσωπικών (radio interface) και τεχνολογιών δικτύου για ραδιο – πρόσβαση. Παρουσιάζει μια καινούργια αρχιτεκτονική υπηρεσίας βάσει της οποίας επιτρέπεται η σύγκληση κινητών και σταθερών δικτύων. Σκοπός λοιπόν του UMTS είναι: η παροχή μιας παγκόσμιας και συνεχόμενης (seamless) επικοινωνίας πολυμέσων και υπηρεσίες δεδομένων σε υψηλό bit rate σε περιβάλλον τόσο τοπικής (local area) όσο και πλατιάς περιοχής (wide area). [19]. Η εξέλιξη από συστήματα πρώτης και δεύτερη γενεάς στο UMTS παρουσιάζεται στο ακόλουθο σχήμα.



Σχήμα 1.1 [9]

Ο χρήστης του UMTS θα μπορεί να διεξάγει όλες τις επικοινωνιακές δραστηριότητες από μια κινητή πλατφόρμα και να λαμβάνει παρόμοιες υπηρεσίες ανεξάρτητα από την τοποθεσία και το περιβάλλον του. Η μελλοντική κινητή επικοινωνία που καθίσταται δυνατή από το UMTS, θα συνδυάζει προσωπική επικοινωνία με παγκόσμιες υπηρεσίες. Υπάρχει και η δυνατότητα μιας «ανεξαρτησίας» από την συσκευή που χρησιμοποιεί ο χρήστης, το σύστημα πρόσβασης δικτύου και από το δίκτυο που εξυπηρετεί τον χρήστη καθώς και η ελευθερία επιλογής μέσου επικοινωνίας (ομιλία, κείμενο, δεδομένα, γραφικά, βίντεο και τα λοιπά) και τρόπου επικοινωνίας (real-time, two way, μήνυμα, paging, info retrieval και τα λοιπά).

Μια πραγματικά παγκόσμια επικοινωνία δεν μπορεί να γίνει δυνατή χωρίς δορυφορική σύνδεση. Έτσι έγινε πρόνοια για δορυφορική σύνδεση στο UMTS για να συμπληρωθεί το γήινο τμήμα του δικτύου. Με το Satellite UMTS να συμπληρώνει την γήινη κάλυψη του UMTS, καθίσταται δυνατή μια παγκόσμια και κινητή επικοινωνία.

Με λίγα λόγια, το UMTS είναι ένα σύστημα κινητής επικοινωνίας με πολλές λειτουργίες, εφαρμογές και υπηρεσίες που παρέχει προσωπικές επικοινωνίες από 144 kbps μέχρι 2Mbps, θα προσφέρει παγκόσμια κάλυψη και υπηρεσίες πολυμέσων ευρείας ζώνης [19]. Συνδυάζει αρχικά το καλύτερο κομμάτι από διαφορετικούς κόσμους δηλ:

circuit switching για παραδοσιακές υπηρεσίες τηλεφωνίας και packet switching για παροχή packet-based υπηρεσιών για επικοινωνία πολυμέσων σε πραγματικό χρόνο και μη, στον κινητό χρήστη.

1.4 Wireless LANS και UMTS

Από τα πιο σημαντικά συστήματα και εξελίξεις στον χώρο των δικτύων, είναι τα WLANs (Wireless Local Area Networks) τα οποία είναι και μια γρήγορα αναπτυσσόμενη τεχνολογία και αγορά. Ίσως το πιο ελκυστικό στα WLANs είναι το γεγονός ότι προσφέρουν την ευκολία της ασύρματης πρόσβασης σε πολλούς χώρους (στο γραφείο, το σπίτι, σε μεγάλες εταιρίες). Απώτερος σκοπός των WLANs είναι σταδιακά να αντικαταστήσουν τα LANs, να εξαλείψουν γενικά την καλωδιοποίηση, καθώς και να εισαγάγουν ευκαμψία στις ad hoc επικοινωνίες [1]. Είναι πιο περιορισμένα από άλλα δίκτυα από πλευράς έκτασης, όμως έχουν πολλά άλλα πλεονεκτήματα – καθώς και μειονεκτήματα. Ήδη υπάρχουν πάρα πολλές εφαρμογές των WLANs σε παγκόσμια κλίμακα και παρουσιάζεται μια αυξημένη τάση προς αυτά. Φαίνεται λοιπόν η ανάγκη συνύπαρξης και υποστήριξης του UMTS με τα WLANs. Εκτενέστερη αναφορά στα WLANs γίνεται σε επόμενο κεφάλαιο.

1.4 Το Mobile IP και πως μπορεί να εφαρμοστεί στο UMTS

Το Διαδίκτυο σχεδιάστηκε μια περίοδο όπου κανείς δεν είχε υπόψη του κινητούς υπολογιστές και χρήστες. Έτσι το Διαδίκτυο σήμερα είναι ελλιπές ως προς μηχανισμούς υποστήριξης κινητών χρηστών. Το πρωτόκολλο IP (Internet Protocol) είναι η πιο κοινή βάση για χιλιάδες εφαρμογές και τρέχει σε δεκάδες διαφορετικά δίκτυα. Αυτός είναι ο λόγος που τα κινητά δίκτυα βασίστηκαν στο πρωτόκολλο Mobile IP που είναι μια «προέκταση» του IP.

Το Mobile IP σχεδιάστηκε αρχικά για το IPv4 (IP version 4), αλλά το IPv6 (IP version 6) έκανε την εμφάνιση του στον κόσμο των σταθερών δικτύων. Πολλοί μηχανισμοί υποστήριξης κινητικότητας έρχονται μαζί με το IPv6. Γενικά, με το IPv6 δημιουργείται μια νέα έκδοση του Mobile IP η οποία παρέχει στα κινητά δίκτυα περισσότερη ασφάλεια, μεγαλύτερη απόδοση, καλύτερο handover, μικρότερη ανάγκη για επιπρόσθετους μηχανισμούς και άλλα πολλά τα οποία θα αναλυθούν αργότερα [1].

Όσον αφορά τα UMTS, για τις packet-based υπηρεσίες, είναι φανερό δεν θα είναι πολύ συνετή η χρήση αποκλειστικά του IPv4. Με το IPv4 παραμένουν ακόμη άλυτα ορισμένα θέματα ασφαλείας, άρχισε μια έλλειψη IPv4 διευθύνσεων, η παγκόσμια κάλυψη θα είναι δύσκολη και γενικά ακόμη το Mobile IPv4 σταματά σταδιακά να χρησιμοποιείται και στα κινητά συστήματα δεύτερης γενεάς. Λόγω της ένταξης του IPv6 στα σταθερά δίκτυα, προτείνεται το UMTS να υποστηρίζει το IPv6 (αλλά και το IPv4 για την μεταβατική περίοδο). Ακόμη, οι διάφορες υπηρεσίες του IPv6 είναι κατάλληλες για το UMTS και για τις εφαρμογές του. Έχουν μελετηθεί διάφορα σενάρια ένταξης του IPv6 και στο UMTS τα οποία θα αναλυθούν εκτενέστερα μαζί με άλλα σχετικά θέματα στα ακόλουθα κεφάλαια.

Κεφάλαιο 2

Ένας IP Κόσμος

2.1	WLANs Εισαγωγή	9
2.2	IEEE 802.11	11
2.3	Bluetooth	13
2.4	HIPERLAN	17
2.5	Mobile IP	20
2.6	Γιατί IP σε UMTS	27

Ένας άλλος τομέας που έχει ιδιαίτερο ενδιαφέρον είναι η ανάπτυξη των Wireless Local Area Networks (WLANs). Έχουν παρουσιαστεί τα τελευταία χρόνια πολλά καινούργια συστήματα, όπως το GSM, GPRS, και τελευταίως το Bluetooth, IEEE 802.11, HIPERLAN και το UMTS. Τα GSM και GPRS όμως είναι συστήματα 2^{ης} γενεάς και ήδη άρχισαν να καταρρέουν. Τα συστήματα 3^{ης} γενεάς συνδυάζουν όχι μόνο την παραδοσιακή φωνητική κλήση, αλλά και μεταφορά δεδομένων και πολυμέσων.

Μπορεί όμως κανείς να πει ότι και με την υπηρεσία WAP, τα συστήματα 2^{ης} γενεάς είχαν πρόσβαση στο Διαδίκτυο, όπου γινόταν μεταφορά δεδομένων. Η διαφορά όμως είναι ότι τότε, γινόταν σύνδεση από την συσκευή του χρήστη σε ένα base station, και από εκεί γινόταν η μεταφορά δεδομένων σε μορφή πακέτων με το πρωτόκολλο του Διαδικτύου. Στα νέα συστήματα, πρόκειται να ενσωματωθεί η δυνατότητα μεταφοράς πακέτων από τη συσκευή ενός χρήστη, απευθείας σε μια άλλη συσκευή. Για να γίνει αυτό, τα συστήματα 3^{ης} γενεάς, πρέπει να χρησιμοποιούν όλα ένα κοινό πρωτόκολλο και τι ποιό λογικό από τη χρήση του πρωτοκόλλου του Διαδικτύου, IP. Μιλούμε δηλαδή για μια σύνδεση IP end to end (από μια συσκευή στην άλλη).

Είναι όμως αναγκαίο να γίνουν κάποιες μετατροπές στο γνωστό IP, για να υποστηρίξει την κίνηση του χρήστη και την αλλαγή της τοποθεσίας του. Έτσι προέκυψε και το Mobile IP που χρησιμοποιείται στα κινητά δίκτυα. Ακόμη, με τη χρήση του Mobile IP

στα διάφορα συστήματα 3^{ης} γενεάς, είναι δυνατή η χρήση τους και η σύνδεσή τους με τα αναπτυσσόμενα και δημοφιλή WLANs. Στο κεφάλαιο αυτό πρόκειται να γίνει μια σύντομη παρουσίαση των WLANs, των συστημάτων Bluetooth, IEEE 802.11, HYPERLAN και του Mobile IP.

2.1 WLANs Εισαγωγή

Όπως έχει ήδη αναφερθεί, μια γρήγορα αναπτυσσόμενη αγορά και τεχνολογία είναι τα WLANs. Η τεχνολογία αυτή, προσφέρει την ευκολία της ασύρματης πρόσβασης στο γραφείο, το σπίτι, σε μεγάλες εταιρίες, σχεδόν παντού. Σε αντίθεση με τα μεγάλα δίκτυα (πχ Διαδίκτυο), τα WLANs περιορίζουν την διάμετρό τους σε ένα κτίριο, ένα πανεπιστήμιο, μια εταιρία, ένα δωμάτιο και διαχειρίζονται από ξεχωριστά άτομα κι όχι από large-scale network providers. Ο σκοπός των WLANs είναι να αντικαταστήσουν τα κανονικά LANs, να εξαφανίσουν γενικά την καλωδίωση αλλά και να εισαγάγουν την ευκαμψία στις ad hoc επικοινωνίες. Πιο κάτω αντιπαραθέτονται γενικά τα προτερήματα και τα μειονεκτήματα των WLANs σε σχέση με τα LANs:

Πλεονεκτήματα [1]:

- Ευκαμψία (Flexibility)

Με τα ραδιοκύματα, οι διάφορες συσκευές του δικτύου μπορούν να επικοινωνούν χωρίς άλλους περιορισμούς (τοίχους, πατώματα) και μπορούν να τοποθετηθούν παντού. Γίνεται ακόμη πιο εύκολη η επικοινωνία μεταξύ κτιρίων.

- Προσχεδίαση (Planning)

Μόνο τα wireless ad hoc δίκτυα επιτρέπουν την επικοινωνία χωρίς προηγούμενο σχεδιασμό – οποιοδήποτε wired δίκτυο χρειάζεται σχεδιασμό για σύρματα. Στα WLANs, οι συσκευές μπορούν να επικοινωνούν, φτάνει να ακολουθούν το ίδιο πρότυπο και πρωτόκολλο, ενώ στα LANs, χρειάζονται επιπρόσθετα σύρματα, ειδικές πρίζες, πιθανόν ακόμη και εσωτερικές συσκευές (πχ switches) για να γίνει δυνατή η επικοινωνία.

- Σχεδιασμός (Design)

Μόνο τα WLANs επιτρέπουν το σχεδιασμό μικρών φορητών συσκευών που θα ενώνονται με το δίκτυο. Τα καλώδια περιορίζουν όχι μόνο τους χρήστες αλλά και τους σχεδιαστές μικρών PDAs, notepads κτλ. Επιπλέον, ασύρματοι αποστολείς και παραλήπτες μπορούν να «κρυφτούν» σε ιστορικά κτίρια,

δηλαδή μπορεί η τρέχουσα τεχνολογία δικτύων να εφαρμοστεί χωρίς να είναι ορατή.

- Δύναμη (Robustness)

Τα WLANs, μπορούν να αντέξουν και να επιβιώσουν διάφορες καταστροφές, όπως σεισμούς. Με την επιβίωση της wireless συσκευής και του δικτύου, οι χρήστες μπορούν ακόμη να επικοινωνούν. Εδώ τα παραδοσιακά LANs με καλώδια, θα κατέρρεαν εντελώς.

Τα WLANs έχουν όμως και τα μειονεκτήματά τους, τα οποία καταγράφονται πιο κάτω [1]:

- Ποιότητα Υπηρεσίας (Quality Of Service)

Τα WLANs, τυπικά προσφέρουν χαμηλότερη ποιότητα υπηρεσίας από τα LANs. Ο κύριος λόγος για αυτό, είναι το χαμηλό τους bandwidth που οφείλεται σε περιορισμούς στην εκπομπή ραδιοκυμάτων και στα μεγαλύτερα ποσοστά λάθους (error rates) λόγω παρεμβολών.

- Κόστος (Cost)

Το κόστος των WLANs είναι καθαρά πιο ψηλό. Για παράδειγμα, ένα high-speed Ethernet adapter για LAN, κοστίζει περίπου 10 ευρώ, ενώ κάποιοι WLANs adapters, σαν μια PC-Card κοστίζουν περίπου 100 ευρώ.

- Ιδιοκτησιακές Λύσεις (Proprietary Solutions)

Λόγω της καθυστέρησης στις διαδικασίες προτυποποίησης, πολλές εταιρίες, έχουν βρει κάποιες ιδιοκτησιακές λύσεις και προσφέρουν προτυποποιημένες λειτουργίες με πολλές επιπρόσθετες υπηρεσίες. Όμως αυτά προσφέρονται μόνο για κάποια ομογενή περιβάλλοντα δηλαδή όταν adapters από τη συγκεκριμένη εταιρία χρησιμοποιούνται σε όλους τους ασύρματους κόμβους (wireless nodes).

- Περιορισμοί (Restrictions)

Όλα τα ασύρματα προϊόντα πρέπει να συμβιβάζονται με κρατικούς κανονισμούς. Πολλές κυβερνήσεις και μη κυβερνητικά ιδρύματα παγκόσμια, περιορίζουν κάποιες συχνότητες για να αποφεύγονται οι παρεμβολές. Έτσι θα περάσει πολύς καιρός μέχρι να βρεθούν κάποιες παγκόσμιες λύσεις όπως για παράδειγμα το IMT-2000.

- Ασφάλεια και Προστασία (Safety and Security)

Η χρήση ραδιοκυμάτων για μετάδοση δεδομένων, μπορεί να δημιουργήσει παρεμβολές σε κάποια άλλα μηχανήματα, όπως για παράδειγμα σε μηχανήματα που χρησιμοποιούνται σε νοσοκομεία. Έτσι πρέπει κάποια προληπτικά μέτρα να ληφθούν. Ακόμη με την ανοικτή ραδιομετάδοση, είναι πολύ εύκολο για κάποιον να «κρυφακούσει» και γενικά να υπάρξουν παρεμβολές στην μετάδοση.

Τα WLANs σε τελική ανάλυση έχουν πολύ περισσότερα πλεονεκτήματα και λύνουν πάμπολλα προβλήματα των δικτύων. Τα διάφορα συστήματα των WLANs προσπαθούν να ελαττώσουν όσο γίνεται τα μειονεκτήματά τους. Πιο κάτω ακολουθούν τρία κύρια συστήματα WLAN, το IEEE 802.11, το Bluetooth και το HYPERLAN.

2.2 IEEE 802.11

Το IEEE 802.11 είναι το πρότυπο για τα WLANs του IEEE, στο οποίο είναι ήδη διαθέσιμα πάρα πολλά προϊόντα. Ο πρωταρχικός σκοπός του IEEE 802.11 είναι ο καθορισμός ενός απλού και παράλληλα δυνατού WLAN που να προσφέρει τόσο ασύγχρονες, όσο και υπηρεσίες πραγματικού χρόνου. Ακόμη, τα MAC layers πρέπει να μπορούν να λειτουργούν με πολλαπλά physical layers, το καθένα από τα οποία θα έχει χρησιμοποιεί διαφορετικό μέσο μετάδοσης και θα έχει διαφορετικά χαρακτηριστικά μετάδοσης. Κάποια επιπλέον χαρακτηριστικά που θα προσφέρονται στα WLANs από το IEEE802.11, είναι η υποστήριξη διαχείρισης ενέργειας (power management) για διαφύλαξη μπαταρίας, ο χειρισμός κρυμμένων κόμβων, και δυνατότητα παγκόσμιας λειτουργίας. Έτσι το 2.4GHz ISM band το οποίο είναι διαθέσιμο παγκόσμια, επιλέχθηκε για το πρότυπο. Το πρότυπο οραματίζεται τα data rates 1Mbps υποχρεωτικά και 2Mbps προαιρετικά [1].

2.2.1 Αρχιτεκτονική Πρωτοκόλλου

Το IEEE 802.11 πρότυπο καλύπτει μόνο το physical layer (PHY) και το medium access layer (MAC).

MAC Layer

Οι βασικές λειτουργίες του MAC layer περιλαμβάνουν έλεγχο πρόσβασης μέσου διάδοσης, διάσπαση των δεδομένων του χρήστη και κρυπτογράφηση [6].

Physical Layer

Το physical layer χωρίζεται στο physical layer convergence protocol (PLCP) και στο physical medium dependent sublayer (PMD). Το PLCP sublayer παρέχει ένα carrier sense σήμα, το οποίο ονομάζεται clear channel assessment (CCA) για αποφυγή συγκρούσεων και ένα απλό PHY service access point (SAP) ανεξάρτητα από την τεχνολογία μετάδοσης. Τέλος, το PMD sublayer είναι υπεύθυνο για τη ρύθμιση και κωδικοποίηση / αποκωδικοποίηση του σήματος [6].

Layers Διαχείρισης

Εκτός από τα sublayers του πρωτοκόλλου, το IEEE 802.11 καθορίζει τόσο layers διαχείρισης όσο και την ίδια την διαχείριση του σταθμού. Η MAC διαχείριση, υποστηρίζει τη συσχέτιση ενός σταθμού (συσκευή) με ένα AP και την κινητικότητα μεταξύ διάφορων AP. Ακόμη ελέγχει τους μηχανισμούς πιστοποίησης, κρυπτογράφησης, συγχρονισμού ενός σταθμού με το AP και παρέχει διαχείριση ενέργειας. Τέλος, η διαχείριση MAC διατηρεί το MAC management information base (MIB).

Οι κύριες λειτουργίες της PHY διαχείρισης περιλαμβάνουν συντονισμό καναλιού και PHY συντήρηση του MIB. Τέλος, η διαχείριση σταθμού αλληλεπιδρά και με τα δυο sublayers διαχείρισης (του PHY και MAC) και είναι υπεύθυνη για κάποιες επιπρόσθετες λειτουργίες ψηλότερων layers [1].

2.2.2 Αρχιτεκτονική Συστήματος

Στο IEEE 802.11 υπάρχουν δυο διαφορετικοί τρόποι για να «σχηματιστεί» ένα δίκτυο: ad hoc και infrastructure.

Infrastructure WLANS

Στα infrastructure WLANs υπάρχουν κάποια σταθερά σημεία πρόσβασης (access points - AP) μέσω των οποίων μπορούν οι διάφορες συσκευές να επικοινωνούν. Οι συσκευές έχουν ενσωματωμένους μηχανισμούς πρόσβασης στο ασύρματο μέσο διάδοσης (wireless medium) και επικοινωνούν με τα AP μέσω ραδιοκυμάτων. Τα AP μαζί με τις συσκευές που βρίσκονται στη δική τους κάλυψη, σχηματίζουν ένα βασικό σετ υπηρεσιών (basic service set - BSS). Η σύνδεση των διάφορων BSS, γίνεται μέσω των

AP με ένα καταναμημένο σύστημα κι έτσι σχηματίζεται ένα δίκτυο. Με το καταναμημένο σύστημα, συνδέονται τα ασύρματα δίκτυα με μια πύλη μέσω των AP, σχηματίζοντας έτσι μια interworking μονάδα με άλλα LANs. Οι συσκευές μπορούν να επιλέξουν ένα AP και να συσχετιστούν μαζί του. Τα AP υποστηρίζουν την κινητικότητα και για την ανταλλαγή δεδομένων μεταξύ των συσκευών είναι υπεύθυνο το καταναμημένο σύστημα. Ακόμη, τα AP παρέχουν συγχρονισμό μέσα στα BSS, υποστηρίζουν διαχείριση ενέργειας και μπορούν να ελέγχουν το μέσο πρόσβασης για υποστήριξη υπηρεσιών με χρονικούς περιορισμούς [6].

Ad hoc WLANS

Στα ad hoc WLANs δεν υπάρχει κάποια συγκεκριμένη δομή στο δίκτυο, ούτε και κάποια σταθερά σημεία και συνήθως όλες οι συσκευές μπορούν να επικοινωνήσουν μεταξύ τους αυθαίρετα. Έτσι μεταξύ των συσκευών μπορούν να δημιουργηθούν διάφορα BSS. Σε αυτή την περίπτωση όμως, ένα BSS αποτελείται από συσκευές που λειτουργούν κι εκπέμπουν στην ίδια συχνότητα. Διαφορετικά BSS μπορούν να δημιουργηθούν είτε χρησιμοποιώντας την απόσταση μεταξύ τους, ή με χρήση διαφορετικών carrier συχνοτήτων. Υπάρχουν διάφοροι αλγόριθμοι για την διατήρηση τέτοιου είδους δικτύου όπως για παράδειγμα αλγόριθμοι εκλογής προέδρου, όπου ένας κόμβος λειτουργεί σαν σταθμός βάση (base station) ή «αφέντης» και οι άλλοι σαν «σκλάβοι», αλγόριθμοι υπερχείλισης (flooding) και ευρείας μετάδοσης για επικοινωνία μεταξύ των κόμβων και τα λοιπά [6].

2.3 Bluetooth

Η τεχνολογία του Bluetooth δημιουργήθηκε την άνοιξη του 1994 από τις Ericsson, Intel, IBM, Nokia και Toshiba. Πολλές άλλες εταιρίες και ινστιτούτα ερευνών ενώθηκαν με την αρχική ομάδα το 1998. Το Bluetooth αντιπροσωπεύει μια απλή radio-based ασύρματη τεχνολογία δικτύου με χαμηλό κόστος. Ο σκοπός της ομάδας αυτής είναι η εφαρμογή του Bluetooth σε κινητά τηλέφωνα, laptops, notebooks, headsets κτλ. Η τεχνολογία αυτή στοχεύει στη δημιουργία κάποιων ad hoc piconets, δηλαδή πολύ μικρά δίκτυα με περιορισμένη κάλυψη και καθόλου ανάγκη για υποδομή [1]. Αυτά τα δίκτυα χρειάζονται για να μπορούν να συνδεθούν διάφορες μικρές συσκευές που είναι σε κοντινές περιοχές, χωρίς την χρήση ακριβών καλωδίων και την κατάλληλη υποδομή για ασύρματη σύνδεση.

Η ιδέα των ασύρματων piconets είναι πολύ χρήσιμη και μπορούν να εφαρμοστούν σε πολλές περιπτώσεις [1]:

- Σύνδεση Περιφερειακών Συσκευών

Σήμερα οι περισσότερες συσκευές του Η/Υ συνδέονται με καλώδια (ποντίκι, πληκτρολόγιο, μεγάφωνα κτλ). Εκτός από το χώρο και την ακαταστασία των καλωδίων, χρειάζονται ξεχωριστά καλώδια για κάθε συσκευή, διαφορετικές εισδοχές κ.α. Με ένα ασύρματο δίκτυο όμως, δεν θα χρειάζονται τα καλώδια για μεταφορά δεδομένων απλά κάθε συσκευή θα θεωρείται σαν ένας κόμβος στο piconet. Θα πρέπει όμως να ενσωματωθούν μπαταρίες στις συσκευές αυτές.

- Υποστήριξη ad hoc δικτύωσης

Με τα ασύρματα δίκτυα, μπορούν διάφοροι άνθρωποι να ανταλλάζουν πληροφορίες μεταξύ τους οπουδήποτε, να συζητούν διάφορα θέματα μέσω κάποιων συσκευών (όπως για παράδειγμα ένας λέκτορας μπορεί να στέλνει δεδομένα στα PDAs των φοιτητών του την ώρα της διάλεξης). Οι μικρές συσκευές, μπορεί να μην έχουν WLAN adapters σύμφωνα με το IEEE 802.11 πρότυπο, αλλά πιο φτηνά Bluetooth chips ενσωματωμένα.

- Γεφύρωση δικτύων

Με την χρήση ασύρματων piconets, ένα κινητό τηλέφωνο μπορεί να συνδεθεί με ένα PDA ή με ένα laptop με απλό τρόπο. Τα κινητά τηλέφωνα δεν θα χρειάζεται να έχουν πλήρεις WLAN adapters αλλά Bluetooth chips. Έτσι το κινητό τηλέφωνο μπορεί να λειτουργήσει σαν ένα είδος γέφυρας μεταξύ του τοπικού piconet και του παγκόσμιου δικτύου (πχ του GSM). Για παράδειγμα ας σκεφτούμε το ακόλουθα σενάριο: με την άφιξη κάποιου στο αεροδρόμιο ένα email μπορεί αμέσως να παραληφθεί στο κινητό του μέσω του GSM και να το προωθήσει το laptop του που είναι μέσα στη βαλίτσα (το laptop και το κινητό είναι μέσα σε ένα piconet). Ή μέσω ενός piconet, ένας εξυπηρετητής αρχείων (fileserver) μπορεί να ενημερώσει τα αρχεία σε ένα laptop ή ένα PDA κάποιου ατόμου, καθώς αυτός εισέρχεται σε ένα γραφείο.

2.3.1 Αρχιτεκτονική Πρωτοκόλλου

Το Bluetooth λειτουργεί σε 5 επίπεδα του OSI μοντέλου: Session, Transport, Network, DataLink και Physical. Θα κοιτάξουμε λίγο τις λειτουργίες του Bluetooth στο Physical και DataLink Layer για να μπορεί ο αναγνώστης να κάνει σύγκριση με την λειτουργία του IEEE 802.11 στα επίπεδα αυτά.

Physical layer

Κατά τη σχεδίαση του physical layer του Bluetooth, λήφθηκαν υπόψη πολλοί περιορισμοί. Καταρχάς, οι μηχανισμοί του Bluetooth θα ενσωματώνονταν σε μικρές κινητές συσκευές και θα κατανάλωναν ισχύ της μπαταρίας. Γι' αυτό χρειάζονται μικρά chips, που απαιτούν λίγη ισχύ και μπορούν να ενσωματωθούν σε μικρές συσκευές. Οι συσκευές του Bluetooth έχουν ισχύ μετάδοσης 100mW σε μια ακτίνα 10m. Αφού βασίζονται σε ισχύ της μπαταρίας, οι συσκευές Bluetooth δεν μπορούν να είναι σε ενεργή κατάσταση μετάδοσης συνεχώς. Έτσι το Bluetooth καθορίζει ορισμένες καταστάσεις χαμηλής ισχύος για τις συσκευές. Για παράδειγμα κάθε συσκευή που δεν είναι σε ένα piconet βρίσκεται στην κατάσταση STANDBY, όπου η συσκευή «ακούει» περιοδικά για paging μηνύματα [1].

Ακόμη, για παγκόσμια λειτουργία, χρειάζεται η χρήση μια συχνότητας που είναι διαθέσιμη παντού. Γι' αυτό το Bluetooth λοιπόν χρησιμοποιεί την συχνότητα των 2.4 GHz που επιτρέπει παγκόσμια λειτουργία με μερικές μικρές προσαρμογές για κρατικούς περιορισμούς [15].

Οι συνδέσεις και κατά συνέπεια τα piconets μπορούν να δημιουργηθούν από οποιαδήποτε συσκευή η οποία γίνεται ο «αφέντης». Αυτό γίνεται με την αποστολή page μηνυμάτων, αν η συσκευή ήδη ξέρει τη διεύθυνση του παραλήπτη, ή με αποστολή inquiry μηνυμάτων ακολουθούμενα από ένα page μήνυμα αν η διεύθυνση του παραλήπτη είναι άγνωστη. Ο «αφέντης» στέλνει 16 μηνύματα σε 16 διαφορετικές hop συχνότητες οι οποίες καθορίζονται για την συσκευή που καλείται (που είναι «σκλάβος»). Αν ο «σκλάβος» δεν απαντήσει, ο «αφέντης» στέλνει page μηνύματα στους υπόλοιπους 16 wake-up hop carriers [18].

MAC layer

Αρκετοί μηχανισμοί ελέγχουν medium access στο Bluetooth σύστημα. Όπως έχει προαναφερθεί, μια συσκευή σε ένα piconet είναι «αφέντης» και οι υπόλοιπες (μέγιστος αριθμός 7) είναι «σκλάβοι». Ο «αφέντης» λοιπόν καθορίζει την hopping ακολουθία (χρησιμοποιώντας τον μοναδικό του αναγνωριστή συσκευής) καθώς και τη φάση της ακολουθίας (χρησιμοποιώντας το εσωτερικό του ρολόι). Αυτές οι μοναδικές ρυθμίσεις των παραμέτρων του «αφέντη» εμποδίζουν δυο διαφορετικά piconets από το να έχουν την ίδια hopping ακολουθία. Μέσα σε ένα piconet, ο «αφέντης» ελέγχει το medium access.

Το Bluetooth προσφέρει δυο ειδών υπηρεσίας [1]:

- Σύγχρονο συνδεδεμένο link (Synchronous connection-oriented link)
Συμπεριλαμβάνονται οι συνηθισμένες συνδέσεις τηλεφώνου, που απαιτούν συμμετρική, circuit-switched, από σημείο σε σημείο (point-to-point) σύνδεση.
- Ασύγχρονο μη συνδεδεμένο link (Asynchronous connectionless link)
Συμπεριλαμβάνονται οι μεταφορές δεδομένων, που μπορούν να γίνουν είτε συμμετρικά, είτε με ασυμμετρία και απαιτούν packet-switched, σημείο σε πολλαπλά σημεία (point-to-multipoint) μεταφορά.

2.3.2 Αρχιτεκτονική Δικτύου

Δικτύωση

Όλοι οι χρήστες σε ένα piconet έχουν την ίδια hopping ακολουθία, άρα μοιράζονται και το ίδιο 1MHz κανάλι. Καθώς περισσότεροι χρήστες συνδέονται με το piconet, το throughput ανά χρήστη πέφτει γρήγορα. Έτσι δεν είναι καθόλου αποδοτικό να υπάρχει μόνο ένα piconet μέσα στα διαθέσιμα 80MHz. Αυτό οδήγησε και στη δημιουργία ομάδων piconets, τα scatternets. Μόνο συσκευές που είναι απαραίτητο να μοιράζονται δεδομένα υπάρχουν στο ίδιο piconet κι έτσι πολλά piconets με επικαλυπτόμενη κάλυψη μπορούν να συνυπάρξουν [23].

Αν μια συσκευή θέλει να συμμετέχει σε περισσότερα από ένα piconets, πρέπει να συγχρονιστεί με την hopping ακολουθία του piconet με το οποίο θέλει να ενωθεί. Αν η συσκευή ήταν πριν «σκλάβος», μετά τον συγχρονισμό συνεχίζει να συμπεριφέρεται σαν «σκλάβος» στο καινούργιο piconet και δεν συμμετέχει στο παλιό piconet πλέον. Πριν

την αποχώρησή του από το piconet, ο «σκλάβος» πληροφορεί τον «αφέντη» ότι δεν θα είναι διαθέσιμος για κάποιο χρονικό διάστημα. Ένας «αφέντης» μπορεί επίσης να αποχωρήσει από το piconet και να ενωθεί με άλλο piconet σαν «σκλάβος». Όταν ο «αφέντης» αποχωρήσει από το piconet, όλη η κίνηση αναστέλλεται μέχρι να επιστρέψει ο «αφέντης» [1]. Έτσι η επικοινωνία μεταξύ των piconets γίνεται με συσκευές που «αλλάζουν» piconets συνεχώς.

Ασφάλεια

Είναι πολύ εύκολο για κάποιον να έχει παράνομη πρόσβαση σε ραδιομετάδοση. Ειδικά οι συσκευές Bluetooth μπορεί να μεταδίδουν προσωπικά δεδομένα. Έτσι το Bluetooth προσφέρει μηχανισμούς για πιστοποίηση και κρυπτογράφηση στο MAC layer οι οποίοι πρέπει να υλοποιούνται με τον ίδιο τρόπο σε κάθε συσκευή.

Τα κυριότερα χαρακτηριστικά ασφάλειας που προσφέρει το Bluetooth συμπεριλαμβάνουν μια ρουτίνα πρόκλησης-απάντησης (challenge-respond) για πιστοποίηση, ένα κωδικοποιητή ροής και μια session key γεννήτρια [23]. Παρόλα αυτά, οι εφαρμογές ψηλότερου επιπέδου πρέπει να προσφέρουν δυνατότερη κρυπτογράφηση αν χρειάζεται. Η ασφάλεια που παρέχει το Bluetooth είναι αρκετή για τη δημιουργία μιας ντόπιας περιοχής εμπιστοσύνης μεταξύ συσκευών.

2.4 HIPERLAN

Το 1996, το ETSI προτυποποίησε το HIPERLAN 1 (High Performance Local Area Network) σαν σύστημα για WLANs, επιτρέποντας κινητικότητα χρήστη και υποστηρίζοντας ad hoc τοπολογίες και τοπολογίες με υποδομή. Το HIPERLAN 1 ήταν αρχικά ένα από τα τέσσερα HIPERLANs που είχαν οραματιστεί, καθώς το ETSI αποφάσισε να έχει διαφορετικά δίκτυα για διαφορετικούς σκοπούς. Το κύριο χαρακτηριστικό όλων των τεσσάρων δικτύων, είναι ο συνδυασμός τους με time-sensitive υπηρεσίες μεταφοράς δεδομένων. Σήμερα τα HIPERLAN 3 και 4 ονομάζονται HIPERACCESS και HIPERLINK αντίστοιχα [1].

Το πρότυπο, περιγράφει ένα WLAN που υποστηρίζει προτεραιότητα και διάρκεια ζωής στα πακέτα για μεταφορά δεδομένων στα 23.5 Mbps, συμπεριλαμβανομένου μηχανισμού μεταβίβασης, ανακάλυψη τοπολογίας, κρυπτογράφηση δεδομένων,

αναγνώριση δικτύου, και μηχανισμούς διατήρησης ενέργειας. Γενικά τα HIPERLANs λειτουργούν στα 5.1 – 5.3GHz σε ακτίνα 50μ σε κτίρια με ισχύ μετάδοσης 1W [13].

Ένα ιδιαίτερο χαρακτηριστικό που άλλα wireless δίκτυα δεν φαίνεται να προσφέρουν είναι η δυνατότητα προώθησης πακέτων σε διάφορους χρόνους. Αυτό είναι αρκετά χρήσιμο για διατήρηση ενέργειας με τον εξής τρόπο: Μια συσκευή για παράδειγμα, μπορεί να ενεργοποιήσει ένα ειδικό wake-up μοτίβο. Αυτό το μοτίβο καθορίζει σε ποιά χρονική στιγμή η συσκευή είναι έτοιμη για παραλαβή δεδομένων, έτσι την υπόλοιπη ώρα η συσκευή μπορεί να έχει κλειστό τον παραλήπτη της, εξοικονομώντας ενέργεια. Αυτές οι συσκευές ονομάζονται p-savers και χρειάζονται τους λεγόμενους p-supporters που περιέχουν τις πληροφορίες για το wake-up μοτίβο όλων των p-savers για τους οποίους είναι υπεύθυνοι. Ένας p-supporter στέλνει δεδομένα σε ένα p-saver μόνο όταν αυτός είναι «ξύπνιος» [1].

2.4.1 HIPERLAN 2

Θα κοιτάξουμε λίγο το HIPERLAN 2, γιατί είναι κατάλληλο για να ενωθεί με UMTS δίκτυα. Αντίθετα με το HIPERLAN 1, το HIPERLAN 2 έχει αναπτυχθεί ειδικά για να έχει κυρίως μια καλωδιομένη υποδομή παρέχοντας μια μικρής ακτίνας ασύρματη πρόσβαση σε διάφορα δίκτυα (όπως IP, ATM και σε UMTS δίκτυα). Το HIPERLAN 2 λειτουργεί στα 5.2GHz σε ένα φάσμα 100MHz. Μια τυπική τοπολογία ενός HIPERLAN 2 περιλαμβάνει τα κινητά τερματικά (Mobile Terminals - MTs) τα οποία επικοινωνούν με ένα Access Point (AP) κάθε φορά μέσω ραδιοκυμάτων. Με την κίνηση του MT, το HIPERLAN 2 αυτόματα ενώνεται με το κοντινότερο AP. Μπορούν και να δημιουργηθούν ad hoc δίκτυα, όπου τα MT επικοινωνούν απευθείας μεταξύ τους [21].

Τα κύρια χαρακτηριστικά του HIPERLAN 2 είναι τα ακόλουθα [21]:

- Το HIPERLAN 2 έχει ένα πολύ ψηλό ρυθμό μετάδοσης, μέχρι και 54Mbps, Αυτό επιτυγχάνεται χρησιμοποιώντας μια μέθοδο συναρμολόγησης, το Orthogonal Frequency Digital Multiplexing (OFDM). Το OFDM είναι ιδιαίτερα αποδοτικό σε περιβάλλοντα εξοικονόμησης χρόνου.
- Οι συνδέσεις του HIPERLAN 2 είναι time-division multiplexed και connection – oriented, είτε διπλής κατεύθυνσης από σημείο σε σημείο, είτε μονής

κατεύθυνσης από σημείο σε πολλαπλά σημεία. Υπάρχει επίσης ένα κανάλι broadcast μέσω του οποίου η κίνηση από ένα AP φτάνει σε όλα τα MT.

- Αντίθετα με άλλα συστήματα ραδιομετάδοσης, η κίνηση σε ένα LAN είναι τυχαία και εκρηκτική. Αυτό μπορεί να προκαλέσει σοβαρά προβλήματα αναφορικά με το throughput, γιατί η απόδοση είναι ένας από τους πιο σημαντικούς παράγοντες στα WLANs. Στο HIPERLAN 2, σε κάθε σύνδεση μπορεί να ανατεθεί είτε ένα επίπεδο προτεραιότητας, είτε ένα συγκεκριμένο QoS σχετικά με το bandwidth, καθυστέρηση, τρέμουλα (jitter), bit error rate και τα λοιπά.
- Τα AP στο HIPERLAN 2 έχουν ενσωματωμένους μηχανισμούς υποστήριξης για αυτόματη μετάδοση κατανομής συχνότητας σε μια περιοχή κάλυψης ενός AP. Αυτό γίνεται με την Δυναμική Επιλογή Συχνότητας (Dynamic Frequency Selection - DFS). Ένα κατάλληλο κανάλι ραδιομετάδοσης διαλέγεται σύμφωνα με το ποιά κανάλια είναι διαθέσιμα και την ελαχιστοποίηση της παρέμβασης του περιβάλλοντος. Έτσι δεν υπάρχει ανάγκη για «χειρονακτική» επιλογή συχνότητας όπως σε άλλα δίκτυα σαν το GSM.
- Το HIPERLAN 2 υποστηρίζει πιστοποίηση και κρυπτογράφηση. Τόσο οι AP όσο και οι MT μπορούν να πιστοποιούν ο ένας τον άλλο, για να εγγυείται η εξουσιοδοτημένη πρόσβαση στο δίκτυο. Η κρυπτογράφηση μπορεί να χρησιμοποιηθεί σε υπάρχοντες συνδέσεις για προστασία εναντίον στο «κρυφάκουσμα». Κάθε κόμβος στο δίκτυο παίρνει ένα HIPELAN ID (HID) και ένα Node ID (NID). Ο συνδυασμός αυτών των δυο ταυτοτήτων καθορίζει μοναδικά κάθε συσκευή και περιορίζει τον τρόπο με τον οποίο μπορεί να συνδεθεί με άλλες συσκευές στο δίκτυο. Όλοι οι κόμβοι με το ίδιο HID μπορούν να επικοινωνούν μεταξύ τους χρησιμοποιώντας ένα δυναμικό μηχανισμό δρομολόγησης, Intra-HIPERLAN Forwarding.
- Η υποστήριξη για handover καθιστά δυνατή την κινητικότητα των MT. Το handover γίνεται από τα MT, δηλαδή το MT χρησιμοποιεί το AP με το καλύτερο σήμα και καθώς ο χρήστης κινείται όλες οι συνδέσεις μετακινούνται στον AP με την καλύτερη απόδοση ραδιομετάδοσης.
- Η αρχιτεκτονική του HIPERLAN 2 προσαρμόζεται εύκολα και μπορεί να συνδυαστεί με πολλά σταθερά δίκτυα. Όλες οι εφαρμογές που λειτουργούν στα σταθερά δίκτυα μπορούν να λειτουργήσουν και στο HIPERLAN 2.

- Η μέθοδος διατήρησης ενέργειας είναι όπως τη μέθοδο που έχει περιγραφεί πιο πάνω με το wake-up μοτίβο.

Έχουν περιγραφεί λοιπόν κάποια βασικά συστήματα των WLANs. Τα συστήματα αυτά χρησιμοποιούνται σχεδόν παντού και έχουν κοινό τους παράγοντα το πρότυπο IP στο network layer. Κατ' επέκταση χρειάζεται να μελετηθεί το πρότυπο αυτό και πιο συγκεκριμένα η επέκτασή του για τα κινητά δίκτυα, Mobile IP, αφού θέλουμε τόσο τα WLANS όσο και τα κινητά δίκτυα να λειτουργούν με κοινή βάση το πρωτόκολλο αυτό.

2.5 Mobile IP

Όπως έχει προαναφερθεί στο πρώτο κεφάλαιο, τα κινητά δίκτυα είναι καθαρά ένα μεγάλο μέρος του μέλλοντος. Επίσης, το Διαδίκτυο είναι το πιο μεγάλο δίκτυο διεθνούς επικοινωνίας δεδομένων με χιλιάδες εκατομύρια χρήστες. Γιατί λοιπόν να μην χρησιμοποιηθεί απλά ένας κινητός H/Y στο Διαδίκτυο; Ο λόγος είναι αρκετά απλός: δεν θα ληφθεί κανένα πακέτο μόλις ο H/Y βγει έξω από το home network του. Έχοντας υπόψη τους μηχανισμούς δρομολόγησης του Διαδικτύου, διαπιστώνουμε το λόγο που συμβαίνει αυτό: Ένας host στέλνει ένα πακέτο IP, στο header του οποίου συμπεριλαμβάνεται και η διεύθυνση του παραλήπτη, η οποία όχι μόνο καθορίζει τον παραλήπτη αλλά και το subnet του. Για παράδειγμα η διεύθυνση παραλήπτη 192.42.11.3 προσδιορίζει ότι ο παραλήπτης βρίσκεται στο subnet με το network prefix 192.42.11. Οι δρομολογητές του Διαδικτύου, έχουν αποθηκευμένα στους πίνακές τους μόνο τα network prefixes (για βελτιστοποίηση) κι έτσι το συγκεκριμένο πακέτο θα σταλεί στο subnet με το network prefix 192.42.11. Έτσι αν ο παραλήπτης μπορεί να βρεθεί στο subnet του, θα παραλάβει τα πακέτα που του στέλνονται · μόλις μετακινηθεί έξω από το subnet network, τα πακέτα χάνονται. Ο host λοιπόν χρειάζεται την λεγόμενη τοπολογικά ορθή διεύθυνση του κάθε χρήστη για να του αποστέλνει τα πακέτα του.

2.5.1 Ιδιαιτερότητες των κινητών δικτύων από πλευράς network layer

Στην σχεδίαση της αρχιτεκτονικής των κινητών δικτύων στο network layer έπρεπε να ληφθούν υπόψη κάποιοι παράγοντες και απαιτήσεις για να γίνει σωστά η ανάπτυξή τους [1].

Αυτοί οι παράγοντες είναι:

- Συμβατότητα (Compatibility)

Ο αριθμός των Η/Υ που χρησιμοποιούν το TCP/IP για σύνδεση και επικοινωνία μέσω του Διαδικτύου είναι τεράστιος. Έτσι ένα νέο πρωτότυπό, σαν το Mobile IP, δεν είναι σε θέση να απαιτεί αλλαγές για εφαρμογές ή για πρωτόκολλα που ήδη χρησιμοποιούνται. Δεν είναι ούτε πρακτικό να γίνεται χρήση διαφορετικών εφαρμογών αποκλειστικά για κινητούς Η/Υ. Το ίδιο ισχύει και για τα λειτουργικά συστήματα (O/S) · κανείς δεν επιθυμεί την χρήση διαφορετικού O/S στον φορητό του υπολογιστή. Το Mobile IP λοιπόν έπρεπε να γίνει μέρος των υπαρχόντων O/S ή τουλάχιστο να μπορεί λειτουργά στα O/S αυτά. Επίσης οι δρομολογητές του Διαδικτύου δεν ήταν σε θέση να αλλάξουν το λογισμικό τους για υποστήριξη της νέας αυτής εφαρμογής. Ακόμη, το Mobile IP έπρεπε να είναι συμβατό με τα χαμηλότερα επίπεδα που χρησιμοποιούνται από το κανονικό, μη κινητό IP. Αυτό όμως σημαίνει και την χρήση του ίδιου format για διευθύνσεις καθώς και τους ίδιους μηχανισμούς για δρομολόγηση.

- Διαφάνεια (Transparency)

Η κίνηση του χρήστη έπρεπε να παραμένει «αόρατη», διαφανής για πολλά πρωτόκολλα και εφαρμογές πιο ψηλών επιπέδων. Για το TCP για παράδειγμα, πρέπει ο Η/Υ να έχει πάντα την ίδια διεύθυνση IP, άσχετα από την θέση του και το δίκτυο στο οποίο βρίσκεται. Όμως, είναι γνωστό ότι σχεδόν όλες οι εφαρμογές δεν είχαν σχεδιαστεί με πρόνοια για κινητικότητα. Έτσι πρέπει η κίνηση του χρήστη να επηρεάζει το πολύ, σε θέματα μείωσης του bandwidth και αύξησης του χρόνου καθυστέρησης και να μην γίνεται αντιληπτή στον χρήστη. Υπάρχουν όμως και μερικές εφαρμογές, οι οποίες είναι καλύτερα να έχουν «γνώση» της κινητικότητας του χρήστη. Όπως για παράδειγμα εφαρμογές για τις οποίες ο χρήστης χρεώνεται ένα ποσό. Γνωρίζοντας ότι υπάρχει δυνατότητα χρησιμοποίησης κάποιου άλλου δικτύου, το λογισμικό/εφαρμογή μπορεί να διαλέξει το πιο φτηνό δίκτυο. Ήταν λοιπόν αναγκαίοι επιπρόσθετοι μηχανισμοί για να μπορούν οι εφαρμογές αυτές να ενημερώνονται για την κίνηση και τη θέση του χρήστη.

- Αποδοτικότητα (Efficiency)

Η ένταξη ενός νέου μηχανισμού στο Διαδίκτυο, δεν έπρεπε να διακινδύνευε την απόδοση του δικτύου. Η ενδυνάμωση του IP για την υποστήριξη κινητικότητας,

δεν πρέπει να συντελέσει στην αύξηση των πακέτων στο δίκτυο, προκαλώντας υπερχείλιση. Πολύ μεγάλη σημασία έπρεπε να δοθεί και στο γεγονός ότι κατά κανόνα, οι ασύρματες συνδέσεις έχουν πιο χαμηλό bandwidth και όλα σχεδόν τα κινητά συστήματα θα έχουν μια ασύρματη σύνδεση.

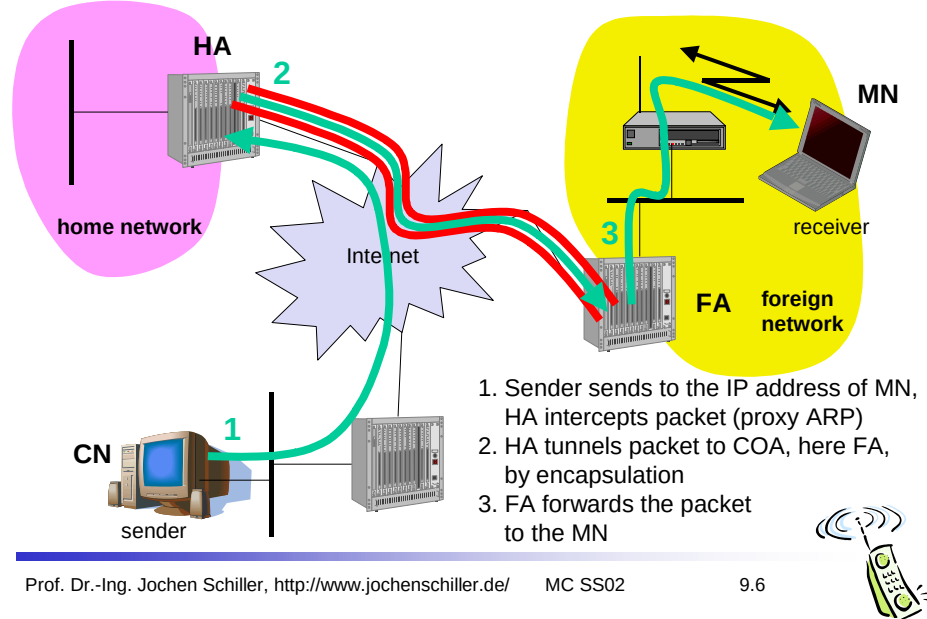
- Ασφάλεια

Αδιαμφισβήτητα, η κινητικότητα προβάλλει πολλά και καινούργια προβλήματα ασφάλειας. Είναι καταρχάς απαραίτητο, να γίνεται προτυποποίηση όλων των μηνυμάτων και πακέτων που αφορούν τη διαχείριση του Mobile IP. Πρέπει το IP layer να είναι σίγουρο πριν να στείλει ένα πακέτο σε ένα κινητό host, ότι ο host αυτός είναι πράγματι ο σωστός παραλήπτης του πακέτου. Το IP layer όμως όπως ήταν, μπορούσε μόνο να εγγυηθεί ότι η διεύθυνση IP του παραλήπτη ήταν σωστή.

Το Mobile IP με λίγα λόγια, είναι το πρωτόκολλο που χρησιμοποίησαν αρχικά τα κινητά δίκτυα στο network layer για να είναι δυνατή η επικοινωνία μεταξύ των χρηστών (τόσο μεταξύ χρηστών κινητών δικτύων, όσο και μεταξύ χρηστών κινητών με σταθερών δικτύων). Το πρωτόκολλο αυτό, είναι βασισμένο στο IPv4, το μέχρι στιγμής πρωτόκολλο που χρησιμοποιείται στο Διαδίκτυο. Μια σπουδαία ευθύνη του Mobile IP είναι να κάνει την κίνηση του χρήστη μη αντιληπτή από τα πιο ψηλά επίπεδα και τα πρωτόκολλά τους, όπως το TCP. Στη συνέχεια θα μελετηθούν οι ιδιαιτερότητες του Mobile IP, θα εξηγηθεί η αρχιτεκτονική του, η λειτουργία του και θα τεθούν ορισμένα προβλήματα που διαπιστώθηκαν.

2.5.2 Παραλαβή πακέτων Mobile IP

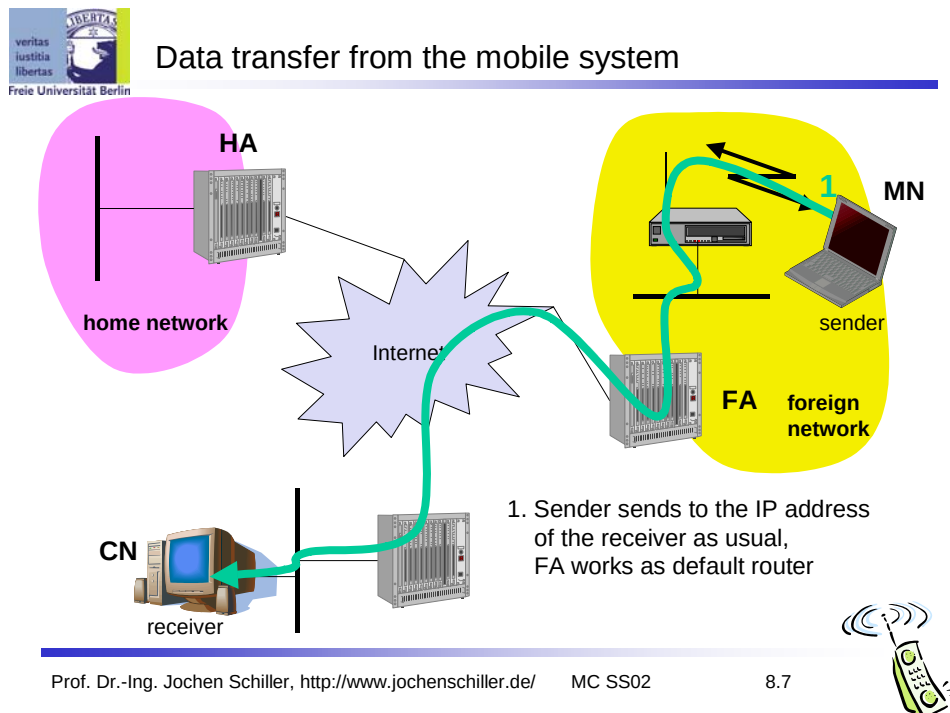
Στο σχήμα 2.1 παρουσιάζεται πως γίνεται η αποστολή των πακέτων, προς τον κινητό κόμβο (Mobile Node - MN).



Σχήμα 2.1 [20]

Έστω ότι ένας Corresponding Node (CN) επιθυμεί να στείλει ένα IP πακέτο σε ένα MN. Μια από τις απαιτήσεις στο Mobile IP είναι απόκρυψη της κίνησης στον MN. Έτσι ο CN δεν χρειάζεται να γνωρίζει τίποτα για την τοποθεσία του MN και στέλνει το πακέτο στη συνηθισμένη IP διεύθυνση του MN (βήμα 1). Αφού το Διαδίκτυο δεν έχει πληροφορίες για την θέση του MN, κατευθύνει το πακέτο στον δρομολογητή που είναι υπεύθυνος για το home network (HN), στον home agent (HA) του MN, με τους συνηθισμένους μηχανισμούς δρομολόγησης του Διαδικτύου. Όταν ο HA παραλαμβάνει το πακέτο, γνωρίζει ότι ο MN δεν βρίσκεται στο HN, έτσι το πακέτο δεν προωθείται στο subnet, αλλά στέλνεται στο Foreign Agent care-of address (FA COA) την οποία ο HA γνωρίζει. Αυτό γίνεται προσθέτοντας ένα νέο header στο πακέτο που παρουσιάζει τον FA σαν παραλήπτη και τον HA σαν αποστολέα (βήμα 2). Στη συνέχεια, ο FA αφαιρεί το καινούργιο header και προωθεί το αρχικό πακέτο με παραλήπτη τον MN και αποστολέα τον CN στο δικό του δίκτυο (βήμα 3) [20]. Έτσι για τον MN η κινητικότητα δεν είναι ορατή και παραλαμβάνει τα πακέτα του όπως θα γινόταν σε ένα σταθερό δίκτυο.

Στο σχήμα 2.2 παρουσιάζεται η αποστολή πακέτου από τον MN προς τον CN.



Σχήμα 2.2 [20]

Ο MN στέλνει το πακέτο ως συνήθως με διεύθυνση αποστολέα την δική του και διεύθυνση παραλήπτη, τη διεύθυνση του CN (βήμα 1). Ο δρομολογητής στον FA, λειτουργεί ως συνήθως και προωθεί κανονικά το πακέτο σύμφωνα με τη διεύθυνση παραλήπτη. Αν ο CN είναι σταθερός, τα υπόλοιπα γίνονται όπως κάθε αποστολή πακέτου στο διαδίκτυο. Αν ο CN είναι κινητός, θα γίνει η διαδικασία που έχει περιγραφεί πιο πάνω.

2.5.3 Διαφήμιση και ανακάλυψη πράκτορα (agent)

Ένα αρχικό πρόβλημα των MNs είναι να μπορούν να εντοπίζουν τους FAs. Έτσι, οι FAs καθώς και οι HAs «διαφημίζουν» περιοδικά την παρουσία τους στο δίκτυο χρησιμοποιώντας ειδικά μηνύματα. Κάποια σημαντικά μέρη του μηνύματος είναι τα ακόλουθα bits που καθορίζουν και τα χαρακτηριστικά του πράκτορα.: το R bit δείχνει αν η σύνδεση με αυτόν τον πράκτορα είναι αναγκαστική παρά με κάποιον άλλον FA κοντά στον MN, το B bit καθορίζει αν ο πράκτορας είναι βαρυφορτωμένος και δεν μπορεί να υποστηρίξει άλλους MN, τα H bit και F bit καθορίζουν αντίστοιχα αν ο πράκτορας προσφέρει υπηρεσίες σαν Home Agent ή σαν Foreign Agent (ένας πράκτορας με ενεργοποιημένο το F bit, πρέπει να διαφημίσει και τουλάχιστο μια COA),

τα M bit και G bit καθορίζουν τον τρόπο με τον οποίο γίνεται το encapsulation από το τούνελ και τέλος το V bit καθορίζει την χρήση του header compression [1].

Έτσι ένας MN σε ένα subnet, μπορεί να λαμβάνει «διαφημίσεις» είτε από τον HA του, ή από κάποιον FA. Αυτός είναι και ένας τρόπος για τον MN να γνωρίζει που βρίσκεται. Αν δεν λάβει «διαφημίσεις» και δεν έχει μια COA, ο MN πρέπει να στείλει μηνύματα «δελεασμού» πρακτόρων. Πρέπει να υπάρχει έλεγχος, ούτως ώστε τα μηνύματα αυτά δεν θα υπερχειλίσουν το δίκτυο, αλλά ένας MN μπορεί να ψάχνει συνεχώς για ένα FA στέλλοντας μηνύματα «δελεασμού». Η ανακάλυψη ενός νέου FA μπορεί να γίνει οποιαδήποτε στιγμή κι όχι μόνο όταν ο MN δεν είναι συνδεδεμένος με κάποιον άλλο FA (για παράδειγμα ένας MN μπορεί να ψάχνει για καλύτερη σύνδεση ενώ έχει σύνδεση με ένα FA) [5].

Μετά από αυτά τα βήματα διαφήμισης και ανακάλυψης πρακτόρων, ένας MN μπορεί να αποκτήσει μια COA, είτε από τον FA του, ή μια co-located COA από ένα Dynamic Host Configuration Protocol (DHCP) εξυπηρετητή [1], δηλαδή ο MN αποκτά προσωρινά μια επιπρόσθετη IP διεύθυνση. Αυτό που ακολουθεί είναι η διαδικασία εγγραφής του MN με το HN του.

Λόγο του ότι τα μηνύματα διαφήμισης βασίζονται στο Internet Control Message Protocol (ICMP) για σταθερά δίκτυα, παρουσιάζονται κάποια προβλήματα. Ένα είναι το ελάχιστο διάστημα των 3 δευτερολέπτων μεταξύ δυο «διαφημίσεων» (αυτό είναι λογικό στα σταθερά δίκτυα, αφού η τοπολογία σπάνια μετακινείται κι αν μετακινηθεί αυτό γίνεται με αργό ρυθμό, όμως στα κινητά δίκτυα, αυτό το διάστημα είναι υπερβολικό). Έτσι ένας MN πρέπει να περιμένει τουλάχιστο 3 δευτερόλεπτα μέχρι να προσέξει ότι ένας FA δεν είναι πλέον διαθέσιμος. Αλλά μπορεί απλά να χάθηκε η «διαφήμιση» αυτού του FA, έτσι ο MN πρέπει να περιμένει ακόμη περισσότερο για να σιγουρευτεί για την επόμενη του κίνηση.

2.5.3 Εγγραφή

Μετά την λήψη μιας COA, ένας MN πρέπει να κάνει εγγραφή στον HA του για να ενημερώσει των HA για την τοποθεσία του, ούτως ώστε τα πακέτα προς τον MN θα προωθούνται σωστά. Η εγγραφή μπορεί να γίνει με δυο τρόπους:

- Αν η COA είναι στον FA, ο MN στέλνει μια αίτηση εγγραφής που περιέχει την COA του στον FA, ο οποίος προωθεί την αίτηση προς τον HA. Στη συνέχεια, ο HA δημιουργεί ένα mobility binding που περιέχει για αυτόν τον MN, την home IP διεύθυνσή του και την COA που έχει λάβει. (Το mobility binding περιέχει ακόμη και την διάρκεια ζωής της εγγραφής, η οποία είναι διαπραγματεύσιμη κατά τη διάρκεια της διαδικασίας εγγραφής. Όταν λήξει η διάρκεια ζωής, αυτόματα το mobility binding διαγράφεται, έτσι ένας MN πρέπει να ξανακάνει εγγραφή πριν να λήξει η προηγούμενη). Αφού δημιουργηθεί το mobility binding, ο HA στέλνει μια απάντηση στον FA, ο οποίος το προωθεί στον MN.
- Αν η COA είναι co-located, απλά ο MN στέλνει την αίτηση απευθείας στον HA και αντίστοιχα, ο HA στέλνει απευθείας την απάντηση.

Για τις αιτήσεις χρησιμοποιούνται πακέτα UDP.

2.5.5 Προβλήματα και βελτιστοποιήσεις

Ένα αρκετά σοβαρό πρόβλημα με το Mobile IP, είναι ότι παρά την απόσταση των δύο MNs (που μπορεί να είναι και λίγα μέτρα), τα πακέτα για να πάνε από τον ένα MN στον άλλο, πρέπει πάντα να πάνε μέσω του HA (που μπορεί να είναι πολύ πιο μακριά από τον MN). Αυτή η συμπεριφορά ονομάζεται (triangular routing). Ένας τρόπος για να βελτιστοποιηθεί η δρομολόγηση είναι να ενημερώνεται ο CN για την τρέχουσα θέση του MN. Ο CN λοιπόν θα μπορεί να φυλάει την θέση του MN σε ένα binding cache. Αυτός που θα ενημερώνει τον CN για την τοποθεσία του MN είναι ο HA του MN [1].

Επίσης, το Mobile IP καθορίζει ότι ένας MN μπορεί να χρησιμοποιήσει τον τοπικό δρομολογητή του ξένου δικτύου σαν ένα default δρομολογητή. Όμως αυτό δεν είναι δυνατό, αφού ο MN δεν είναι ικανός να μάθει την MAC διεύθυνση του δρομολογητή [8].

Ένα σημείο που χρειάζεται προσοχή είναι ότι ο FA στον οποίο είναι εγγραμμένος ένας MN, δεν μπορεί να στείλει πακέτα στον MN, σαν ένας κανονικός CN. Αυτό γίνεται για τον εξής λόγο: Τα πακέτα θα παραλαμβάνονται από τον HA, ο οποίος θα το στείλει πίσω στον FA (όπως προβλέπει το Mobile IP) και σαν εξωτερική διεύθυνση παραλήπτη θα μπει η διεύθυνση του FA. Όμως ο FA, πρέπει να πετά όλα τα πακέτα που φτάνουν

προς αυτόν με εξωτερική διεύθυνση παραλαβής ίση με εσωτερική διεύθυνση αποστολέα για να αποφεύγονται οι βρόγχοι [8].

Γενικά, το Mobile IP σχεδιάστηκε για να λειτουργά στο Διαδίκτυο, όταν εκείνο χρησιμοποιούσε το IPv4. Το IPv6 όμως κάνει τη ζωή πολύ πιο εύκολη. Πολλοί μηχανισμοί που πριν έπρεπε να καθοριστούν ξεχωριστά για υποστήριξη κινητικότητας, ασφάλειας, ανακάλυψης άλλων κόμβων στο δίκτυο (π.χ. ανακάλυψη FA) έρχονται δωρεάν με το IPv6.

2.6 Γιατί IP σε UMTS

Έρευνες υποστηρίζουν ότι 1200 εκατομύρια cellular χρήστες, 600 εκατομύρια σταθεροί σταθμοί και πάνω από 600 εκατομύρια wireless χρήστες δεδομένων θα είναι ενεργοί μέχρι το έτος 2004. Ακόμη, υπάρχει κοινή γνώση ότι οι υπηρεσίες Διαδικτύου θα συνεχίσουν την αστραπιαία αύξησή τους και ότι τα κινητά τερματικά θα είναι ένα σημαντικό μέρος του Διαδικτύου. Τα τρίτης Γενεάς Συστήματα (συμπεριλαμβανομένου και του UMTS) είναι καλό να υιοθετήσουν το πρωτόκολλο που χρησιμοποιεί το Διαδίκτυο. Παρόλο που έχουν καθοριστεί κι άλλα πρωτόκολλα για το Διαδίκτυο, όπως το Anycast Service και το SLP, φαίνεται ότι υπάρχει μικρή εμπορική υποστήριξη αυτών των πρωτοκόλλων και ακόμη λιγότερη γνώση του πως τα πρωτόκολλα αυτά θα υποστηρίξουν τις επιθυμητές υπηρεσίες του Διαδικτύου, σε σχέση με το IP.

Επίσης, τα συστήματα που έχουν περιγραφεί και αναλυθεί στο κεφάλαιο αυτό είναι πάρα πολύ σημαντικά στον τομέα των Mobile και Wireless Networks. Ήδη υπάρχουν πάρα πολλές εφαρμογές τους ανά το παγκόσμιο και με την πάροδο του χρόνου αυτές οι εφαρμογές θα πολλαπλασιαστούν ραγδαία. Με άλλα λόγια τα συστήματα αυτά είναι ότι πιο καινούργιο στον τομέα των WLANS και Mobile Networks. Είναι λοιπόν πάρα πολύ σημαντικό τα συστήματα αυτά καθώς και το UMTS να μπορούν να συνυπάρχουν και να επικοινωνούν αποδοτικά μεταξύ τους. Έτσι, αφού το Διαδίκτυο υιοθέτησε το IPv6 θα ήταν πολύ καλή εισήγηση τα συστήματα αυτά (από τα οποία τα περισσότερα είναι IP compatible) και τα Τρίτης Γενεάς Συστήματα να μπορούσαν να χρησιμοποιούν το Mobile IPv6 για την αποστολή πακέτων δεδομένων. Με αυτά υπόψη, προτείνεται η χρήση του Mobile IPv6 για το UMTS σύστημα.

2.6.1 Τι μπορεί να προσφέρει το Mobile IPv6.

Σχεδόν σε όλες τις παρουσιάσεις για συζητήσεις περί 3G cellular τεχνολογίες δικτύου, για την υποστήριξη του μεγάλου αριθμού των κινητών χρηστών δεδομένων, το Mobile IPv6 είναι από τις πρώτες επιλογές. Αυτό γιατί το Mobile IPv6, όπως και το IPv6, παρέχει αυξημένες διευθύνσεις IP, σε σχέση με άλλα πρωτόκολλα. Υπάρχουν ελπίδες ότι οι διευθύνσεις αυτές θα είναι αρκετές για να καλύψουν τον αυξημένο αριθμό χρηστών του Διαδικτύου και των 3G συστημάτων. Ακόμη, το Mobile IPv6, έχει λίγο overhead επεξεργασίας και λειτουργεί αποτελεσματικά και με μικρές, λίγων δυνατοτήτων συσκευές.

Η υιοθέτηση του Mobile IPv6 θα βοηθήσει στην υποστήριξη του roaming. Η λειτουργία του autoconfiguration για το “care – of – address” βελτιώνει το robustness και την αποδοτικότητα. Επιπλέον, το MTU μπορεί να προσαρμοστεί πιο εύκολα όταν ένας router προωθεί πακέτα σε καινούργια “care-of-address”. Τα θέματα μετάβασης από το Mobile IPv4 στο Mobile IPv6, εξετάζονται από την επιτροπή IETF Next Generation Transition.

Σε συντομία μερικά από τα κυριότερα χαρακτηριστικά του Mobile IPv6 που είναι χρήσιμα σε 3G συστήματα, όπως και το UMTS είναι [4] [10]:

- Σχεδόν απεριόριστος αριθμός από διευθύνσεις
- Ενσωματωμένη υποστήριξη ασφάλειας (built-in security support)
- Ενσωματωμένη υποστήριξη κινητικότητας (built-in mobility support)
- Αποτελεσματική δρομολόγηση.
- Λειτουργίες για απλοποιημένη διαχείριση δικτύου
- Παρέχει autoconfiguration διευθύνσεων
- Ίδιο επίπεδο QoS υποστήριξης όπως και το IPv4, με δυνατότητες βελτίωσης.
- Επιλογή παροχέα Διαδικτύου (Internet provider selection)
- Αποτελεσματική επεξεργασία πακέτων στους δρομολογητές
- Γενικά, είναι το πρωτόκολλο για μεγαλύτερα και καλύτερης ποιότητας δίκτυα.

Υπάρχουν όμως φυσικά και μερικά προβλήματα μέχρι την πλήρη λειτουργία του Mobile IPv6 σε UMTS και διάφορα σενάρια έχουν δημιουργηθεί. Αυτά θα μελετηθούν σε ακόλουθα κεφάλαια.

Με τη χρήση IP πρωτοκόλλου στα συστήματα τρίτης γενεάς, σε WLAN συστήματα και στο Διαδίκτυο, γίνεται δυνατή η δημιουργία ενός πραγματικά παγκόσμιου ιστού με βάση το IP.

Κεφάλαιο 3

Περιγραφή Mobile IPv6

3.1	Εισαγωγή	30
3.2	Βασικές Ορολογίες	31
3.3	Σύντομο Overview του Mobile IPv6	32
3.4	Λειτουργία Mobile IPv6	34
3.5	QoS για Mobile IPv6	39
3.6	Μηχανισμοί Μετάβασης	40
3.7	Πλεονεκτήματα του Mobile IPv6	43

Όπως έχει αναφερθεί στο δεύτερο κεφάλαιο, είναι πολύ σημαντικό, ή ακόμη και αναγκαίο, τα Συστήματα Τρίτης Γενεάς Κινητών Δικτύων – συμπεριλαμβανομένου και του UMTS – να αλληλεπιδρούν και να συνυπάρχουν με συστήματα για WLANS, με IP συστήματα και το Διαδίκτυο. Ένας από τους σκοπούς εξάλλου του UMTS είναι εκτός από τις φωνητικές κλήσεις και η δυνατότητα αποστολής δεδομένων σε δίκτυο. Πρέπει λοιπόν να υιοθετηθεί ένα κοινό πρωτόκολλο επικοινωνίας μεταξύ των συστημάτων αυτών και το Διαδίκτυο. Κατά συνέπεια, θα ήταν καλή η μελέτη χρήσης του Mobile IPv6 στο UMTS, καθώς γίνονται σενάρια χρήσης του IPv6 στο Διαδίκτυο. Για να μπορούμε όμως να μελετήσουμε την πιθανή αυτή εφαρμογή, πρέπει να ξεκαθαρίσουμε τι είναι ακριβώς το Mobile IPv6, πως λειτουργεί και τι προσφέρει. Αυτό είναι και το θέμα του τρίτου κεφαλαίου.

3.1 Εισαγωγή

Καθώς το Διαδίκτυο μεγαλώνει και επεκτείνεται, γίνεται θύμα της ίδιας της επιτυχίας, λόγω των περιορισμών και προβλημάτων του IPv4. Ανάμεσα στα προβλήματα που είχε να αντιμετωπίσει το IPv4 είναι ότι οι διευθύνσεις του πρωτοκόλλου θα εξαντληθούν στο βραχυπρόθεσμο μέλλον – σύμφωνα με τους ρυθμούς ανάπτυξης του Διαδικτύου. Αυτή ήταν και μια από τις αφορμές που το Internet Engineering Task Force (IETF) άρχισε τις μελέτες για ένα νέο πρωτόκολλο, το IP version 6 (IPv6) γνωστό και σαν IP next generation (IPng). Το τεράστιο διάστημα

διευθύνσεων του IPv6, θα καλύπτει τις ανάγκες του συνεχώς αυξανόμενου Διαδικτύου. Η πρόνοια για κίνηση, η ασφάλεια και τα QoS είναι ενσωματωμένα στο IPv6.

Το IPv6 είναι ένα καθοριστικό ορόσημο για τα κινητά δίκτυα. Τα κύρια χαρακτηριστικά του IPv6 που είναι σημαντικά για τα κινητά και ασύρματα δίκτυα είναι: ικανοποιητικός αριθμός IP διευθύνσεων, υλοποίηση header ασφαλείας, επιλογές προορισμού για ικανοποιητικό rerouting, autoconfiguration διευθύνσεων, ανάκαμψη από λάθη χωρίς στην κατάσταση soft – state bottleneck και άλλα.

Το Mobile IPv6 σχεδιάστηκε για να είναι ένα φυσικό συνεπακόλουθο του Mobile IPv4 (όπως και το IPv6 είναι ένα συνεπακόλουθο του IPv4) και μαζί με διάφορες ευκαιρίες που παρουσιάζονται από τη δημιουργία ενός νέου πρωτοκόλλου.

Η σχεδίαση του Mobile IPv6 είναι τέτοια, έτσι ώστε μια συσκευή που χρησιμοποιεί το πρωτόκολλο αυτό μπορεί να φύγει από το home subnet του και να διατηρήσει όλες τις συνδέσεις του καθώς και να παραμένει προσιτή από άλλες συσκευές στο Διαδίκτυο. Αυτό πετυχαίνεται με την αναγνώριση του κάθε κόμβου με την στατική του Home Address (HA), ανεξαιρέτως της θέσης του και του σημείου σύνδεσής του με το Διαδίκτυο. Ο μηχανισμός με τον οποίο επιτυγχάνεται αυτό είναι εντελώς αόρατος για όλα τα επίπεδα πιο ψηλά από το IP, όπως για παράδειγμα το TCP και UDP – και φυσικά όλες τους τις εφαρμογές. Έτσι τα DNS entries για ένα κόμβο αναφέρονται στο HA του και δεν αλλάζουν με την μετακίνηση του κόμβου. Κατ' ακρίβεια, το Mobile IPv6 επηρεάζει την δρομολόγηση των πακέτων, αλλά είναι ανεξάρτητο από το πρωτόκολλο δρομολόγησης (RIP, OSPF και τα λοιπά) [11]. Αυτό το θέμα, καθώς κι άλλες λειτουργίες του Mobile IPv6, αναλύονται αργότερα σε αυτό το κεφάλαιο.

3.2 Βασικές Ορολογίες

Ακολουθούν κάποιες επεξηγήσεις ορολογιών που θα χρησιμοποιούνται στο κεφάλαιο αυτό [11]:

- Care-of address: Μια IP διεύθυνση που συσχετίζεται με ένα κινητό κόμβο όταν αυτός βρίσκεται σε ένα ξένο subnet και κατ' επέκταση σε μια ξένη σύνδεση. Το subnet prefix της διεύθυνσης αυτής είναι subnet prefix του ξένου δικτύου. Ανάμεσα στις διάφορες care-of addresses που μπορεί να έχει ένας κινητός κόμβος, αυτή που συσχετίζεται με τον Home Agent του κόμβου λέγεται primary

care-of address. Ο κινητός κόμβος συνήθως «λαμβάνει» μια care-of address μέσω stateless ή stateful Address Autoconfiguration, ανάλογα με τις μεθόδους του IPv6 Neighbor Discovery ή με κάποιες άλλες μεθόδους όπως την σταθερή προκαθορισμένη διεύθυνση (static pre-assignment) από τον διαχειριστή μιας ξένης σύνδεσης.

- Δέσιμο (Binding): Η συσχέτιση του Home Agent (HA) ενός κινητού κόμβου με μια care-of address (COA), μαζί με την εναπομείναντα διάρκεια ζωής της σύνδεσης αυτής.
- Correspondent Node (CN): Ένας κόμβος με τον οποίο ο κινητός κόμβος επικοινωνεί. Ο CN μπορεί να είναι είτε κινητός είτε σταθερός.
- Foreign Link (FL): Οποιαδήποτε άλλη σύνδεση εκτός από το Home Link του κόμβου.
- Foreign Subnet Prefix (FSP): Οποιοδήποτε άλλο IP subnet prefix εκτός από το home subnet prefix του δικτύου.
- Home Agent (HA): Ένας δρομολογητής στο home link του κινητού κόμβου στον οποίο έχει εγγράψει ο κινητός κόμβος την COA του. Καθώς ο κινητός κόμβος είναι εκτός του home network του, ο HA δέχεται πακέτα που προορίζονται για την home address του κόμβου αυτού, τα κάνει encapsulate και τα στέλνει στην εγγεγραμμένη COA του κόμβου.
- Home Link (HL): Η σύνδεση στην οποία καθορίζεται το Home Subnet Prefix ενός κινητού κόμβου. Οι τυπικοί μηχανισμοί δρομολόγησης, θα παραδώσουν πακέτα που προορίζονται για κάποιο κόμβο στο HL του.
- Home Registration: Εγγραφή ενός κινητού κόμβου σε μια COA.
- Home Subnet Prefix: Το IP subnet prefix που αντιστοιχεί στο home address ενός κινητού κόμβου.

3.3 Σύντομο Overview του Mobile IPv6

Ο κύριος σκοπός του Mobile IPv6 είναι: ένας κινητός κόμβος να είναι πάντα προσιτός στο Home Address του, είτε βρίσκεται στο Home Link του, είτε κάπου αλλού [12].

3.3.1 Mobile IPv6 Μηνύματα

Το Mobile IPv6 απαιτεί την ανταλλαγή επιπρόσθετων πληροφοριών. Όλα τα νέα μηνύματα που χρησιμοποιούνται στο Mobile IPv6 καθορίζονται σαν IPv6 Επιλογές

Προορισμού (Destination Options). Αυτές οι επιλογές χρησιμοποιούνται στο IPv6 για την παροχή των επιπρόσθετων πληροφοριών που χρειάζονται να εξεταστούν μόνο από τον παραλήπτη ενός πακέτου.

Οι ακόλουθες νέες Επιλογές Προορισμού καθορίζονται στο Mobile IPv6 [11]:

- Binding Update: Η επιλογή αυτή χρησιμοποιείται από ένα κινητό κόμβο, για να πληροφορήσει τον HA του ή οποιοδήποτε άλλο CN για την τρέχουσα COA του.
- Binding Acknowledgement: Αυτή η επιλογή χρησιμοποιείται για αναγνώριση της παραλαβής ενός Binding Update, αν ζητείται αναγνώριση.
- Binding Request: Η επιλογή αυτή χρησιμοποιείται από οποιοδήποτε κόμβο, όταν επιθυμεί ένας κινητός κόμβος να του στείλει ένα Binding Update.
- Home Address: Χρησιμοποιείται σε ένα πακέτο το οποίο έχει αποστείλει ένας κινητός κόμβος για να ενημερώσει τον παραλήπτη του πακέτου για το ποιό είναι η HA του.

3.3.2 Δομές Δεδομένων

Οι προδιαγραφές του Mobile IPv6 περιγράφουν ένα πρωτόκολλο χρησιμοποιώντας τις ακόλουθες τρεις δομές δεδομένων [11]:

Binding Cache

Κάθε Mobile IPv6 κόμβος έχει μια Binding Cache μνήμη η οποία χρησιμοποιείται για να φυλάει τα bindings για άλλους κόμβους. Για παράδειγμα όταν ένας κόμβος λάβει ένα Binding Update, θα το φυλάξει στην Binding Cache του. Κάθε φορά που ένα πακέτο θα αποσταλεί, γίνεται μια αναζήτηση στη Binding Cache για μια εγγραφή που αφορά τον παραλήπτη. Αν βρεθεί μια εγγραφή, το πακέτο αποστέλλεται στη COA του παραλήπτη κι όχι στην HA του.

Binding Λίστα Ενημέρωσης

Κάθε κινητός κόμβος έχει μια binding λίστα ενημέρωσης η οποία χρησιμοποιείται για να αποθηκεύονται πληροφορίες σχετικά με κάθε Binding Update που έχει σταλεί από αυτόν τον κινητό κόμβο και του οποίου δεν έχει λήξη ακόμη η διάρκεια ζωής του. Περιέχει όλα τα Binding Updates που έχουν σταλεί σε οποιοδήποτε CN, είτε σταθερό είτε κινητό και στον HA του.

Home Agents List

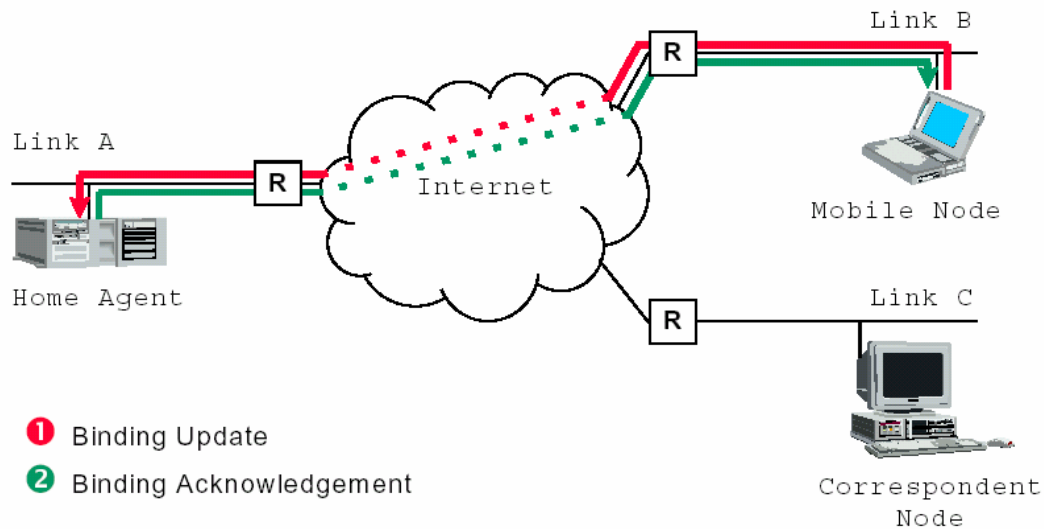
Για κάθε HL όπου ένας κόμβος λειτουργεί σαν HA, δημιουργεί μια λίστα η οποία περιέχει πληροφορίες για όλους τους άλλους HA σε αυτή τη σύνδεση (link). Οι πληροφορίες λαμβάνονται από τις διαφημίσεις των δρομολογητών που στέλνουν οι HAs. Στις διαφημίσεις αυτές, είναι ενεργοποιημένο το home agent bit, αν ο αποστολέας είναι HA σε αυτή τη σύνδεση. Οι πληροφορίες για τους άλλους HAs χρησιμοποιούνται από τον μηχανισμό Dynamic Home Agent Discovery. Ο μηχανισμός αυτός επιτρέπει σε ένα κινητό κόμβο να ανακαλύπτει δυναμικά την IP διεύθυνση ενός HA στο HL του, στον οποίο μπορεί να εγγράψει την primary care-of address του κατά την διάρκεια που βρίσκεται μακριά από το home network του.

3.4 Λειτουργία Mobile IPv6

Για περιγραφή της βασικής λειτουργίας του Mobile IPv6, υποθέτουμε ένα δίκτυο με τρεις συνδέσεις. Στην πρώτη σύνδεση (έστω σύνδεση A) υπάρχει ένας δρομολογητής ο οποίος λειτουργεί σαν HA. Αυτή η σύνδεση είναι επίσης το HL κάποιο κινητού κόμβου ο οποίος έχει μετακινηθεί από την σύνδεση A σε κάποια άλλη σύνδεση (έστω σύνδεση B). Ακόμη, υπάρχει ένας CN (κινητός ή σταθερός) στην τρίτη σύνδεση (έστω σύνδεση Γ).

3.4.1 Εγγραφή Home Agent (Home Agent Registration)

Μόλις ένας κινητός κόμβος αναγνωρίσει ότι έχει μετακινηθεί από μια σύνδεση σε άλλη και ανακαλύπτει ένα καινούργιο default δρομολογητή, κάνει την λειτουργία του address autoconfiguration. Χρησιμοποιεί αυτή την νέα διεύθυνση σαν την COA του. Το prefix της COA είναι το prefix της σύνδεσης στην οποία είναι τώρα ο κινητός κόμβος. Έτσι όλα τα πακέτα που προορίζονται για τον κόμβο αυτό, αποστέλλονται στην σύνδεση στην οποία βρίσκεται. Ο κινητός κόμβος εγγράφει την COA του στον HA του, μέσω της HL [11]. Η διαδικασία Home Agent Registration παρουσιάζεται στο σχήμα 3.1



Σχήμα 3.1 [11]

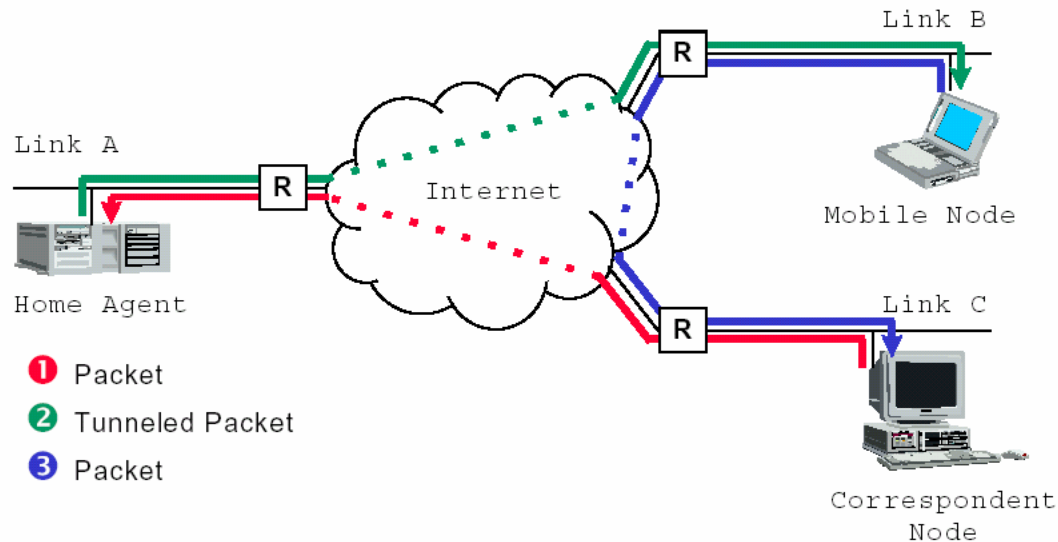
Ο κινητός κόμβος στην σύνδεση Β στέλνει ένα πακέτο στον HA του που περιέχει μια Binding Update επιλογή προορισμού. Ο HA με την σειρά του εγγράφει αυτό το Binding και επιστρέφει ένα πακέτο με μια Binding Acknowledgement επιλογή προορισμού.

3.4.2 Βελτιστοποίηση Διαδρομής (Route Optimization)

Αφού ο HA έχει εγγράψει την COA του κινητού κόμβου, αναλαμβάνει πακέτα που προορίζονται στο home address του κινητού δικτύου. Έτσι χρησιμοποιεί την μέθοδο Proxy Neighbor Discovery. Με την μέθοδο αυτή, ο HA στέλνει μια διαφήμιση γείτονα (Neighbor Advertisement) στο HL εκ μέρους του κινητού κόμβου. Ο HA απαντά και σε γειτονικούς ερεθισμούς (Neighbor Solicitations) εκ μέρους του κινητού κόμβου. Κάθε πακέτο που αποστέλλεται στο home address του κινητού κόμβου, παραλαμβάνεται από τον HA και αποστέλλεται στην COA του κόμβου, με IPv6 encapsulation [11].

Αν ο κινητός κόμβος στείλει πακέτα σε ένα οποιοδήποτε άλλο κόμβο, τα στέλνει απευθείας στον προορισμό τους. Ο κινητός κόμβος θέτει την διεύθυνση αποστολέα στα πακέτα που στέλνει την COA του και συμπεριλαμβάνει μια Home Address επιλογή προορισμού. Επειδή η home address είναι στατική, σε αντίθεση με την COA, επιτρέπει κάθε σε κάθε CN τη «διαφανή» χρήση της COA για στρώματα πάνω από την

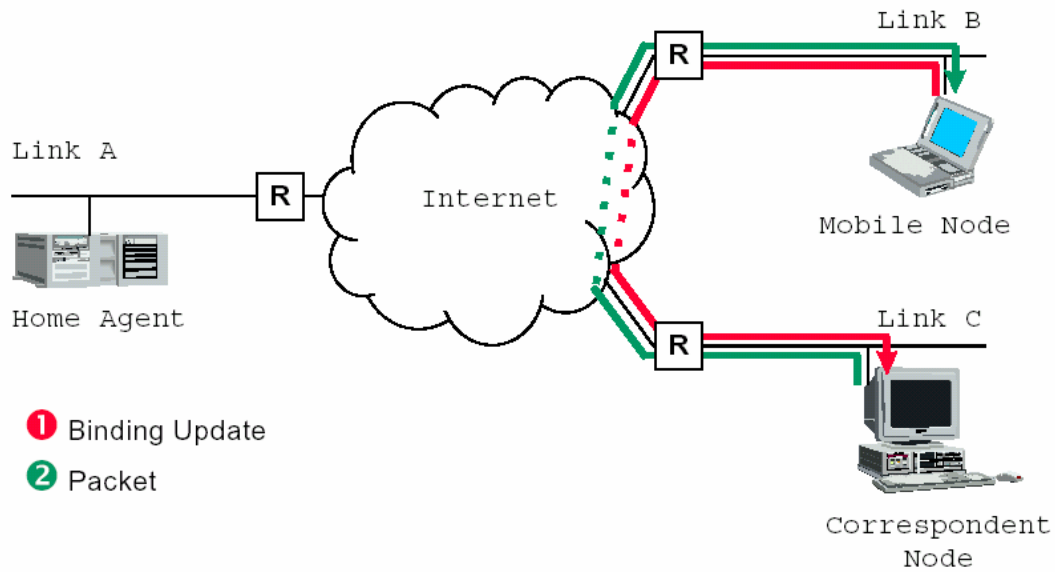
υποστήριξη του IPv6. Τα πιο ψηλά επίπεδα, συμπεριλαμβανομένου και των προγραμμάτων εφαρμογών δεν προσέχουν την COA, μόνο την home address.



Σχήμα 3.2 [11]

Αν ένας κινητός κόμβος επικοινωνεί με ένα CN καθώς είναι μακριά από το home subnet του, τα πακέτα δρομολογούνται από τον CN στον HA, από τον HA στον κινητό κόμβο και από τον κινητό κόμβο στον CN. Αυτή η «ανωμαλία» δρομολόγησης λέγεται Τριγωνική Δρομολόγηση η οποία παρουσιάζεται στο σχήμα 3.2.

Για την αποφυγή της Τριγωνικής Δρομολόγησης, ένας κινητός κόμβος μπορεί να στείλει Binding Updates σε οποιοδήποτε CN, είτε κινητό είτε σταθερό. Αυτό επιτρέπει σε IPv6 CN να φυλάξουν την τρέχουσα COA του κόμβου αυτού και να στέλνουν πακέτα απευθείας [1]. Η διαδικασία αυτή φαίνεται στο σχήμα 2.3



Σχήμα 3.3 [11]

Οποιοσδήποτε IPv6 κόμβος που στέλνει ένα πακέτο, ελέγχει πρώτα την Binding Cache του για την συγκεκριμένη διεύθυνση προορισμού. Αν υπάρχει μια εγγραφή, θα στείλει το πακέτο στον κινητό κόμβο χρησιμοποιώντας ένα routing header. Η διαδρομή που καθορίζεται από αυτό το routing header έχει δυο hops. Το πρώτο hop είναι το COA και το δεύτερο το home address του κινητού κόμβου. Έτσι το πακέτο πηγαίνει απευθείας στην COA του κόμβου. Στην συνέχεια, αφού ο κινητός κόμβος λάβει το πακέτο, το προωθεί στο επόμενο hop που καθορίζεται στο routing header. Αφού το τελευταίο hop είναι η home address του κινητού κόμβου, το πακέτο θα σταλεί στο home address. Το πακέτο θα επεξεργαστεί με τον ίδιο τρόπο λες και ο κόμβος είναι στο home subnet [11].

Αν η Binding Cache δεν έχει καμία εγγραφή, το πακέτο θα σταλεί κανονικά. Μετά θα δρομολογηθεί στο συγκεκριμένο δίκτυο και θα παραληφθεί από το κόμβο προορισμού. Στην περίπτωση που ο προορισμός είναι ένας κινητός κόμβος μακριά από το home subnet του, το πακέτο θα παραληφθεί από τον HA του στο HL και θα σταλεί στον κινητό κόμβο. Με την παραλαβή του πακέτου αυτού, ο κινητός κόμβος θα στείλει στον CN ένα Binding Update με την COA του.

3.4.3 Διαχείριση Binding Μηνυμάτων

Ένας κινητός κόμβος ο οποίος έχει κάνει configure ένα νέο COA σαν την πρωτεύων COA του, πρέπει να εγγράψει αυτή τη διεύθυνση στον HA του και στους CN που έχουν ήδη ενημερωθεί για το binding του κινητού κόμβου. Για αυτό τον σκοπό ο κινητός κόμβος στέλνει ένα Binding Update που περιέχει την νέα του διεύθυνση. Για επιβεβαίωση ότι ο παραλήπτης πράγματι παρέλαβε το Binding Update, ο κινητός κόμβος μπορεί να ζητήσει αναγνώριση ενεργοποιώντας το Acknowledgment bit στο Binding Update (μέχρι την παραλαβή της επιβεβαίωσης, ο κινητός κόμβος θα στέλνει περιοδικά το Binding Update). Ένας κινητός κόμβος πρέπει να ενεργοποιεί το Acknowledgment bit σε Binding Updates που προορίζονται προς τον HA του. Μπορεί ακόμη να ενεργοποιήσει το Acknowledgment bit όταν στέλνει σε CNs αλλά δεν είναι αναγκαίο γιατί αν το Binding Update δεν παραληφθεί για οποιοδήποτε λόγο από τον CN, ο κινητός κόμβος το καταλαβαίνει όταν εξακολουθεί να λαμβάνει πακέτα από CNs, μέσω του HA του [11].

Πριν τη λήξη μιας καταχώρησης στην Binding Cache για ένα κινητό κόμβο, ο CN μπορεί να ανανεώσει την καταχώρηση στέλνοντας ένα Binding Request στον κινητό κόμβο. Κατά συνέπεια, ο κινητός κόμβος θα απαντήσει με ένα Binding Update.

3.4.4 Ανίχνευση Κίνησης

Κατά την διάρκεια που ένας κινητός κόμβος είναι μακριά από το home subnet του, επιλέγει ένα δρομολογητή σαν τον default δρομολογητή και ένα subnet prefix που διαφημίζεται από αυτόν τον δρομολογητή για να το χρησιμοποιήσει στην πρωτεύουσα COA του.

Στην συνέχεια, ο κινητός κόμβος μπορεί να χρησιμοποιήσει οποιοδήποτε συνδυασμό από διαθέσιμους μηχανισμούς για να ανιχνεύσει πότε έχει κινηθεί από μια σύνδεση σε μια άλλη. Μια δυνατότητα είναι ο κόμβος να περιμένει για τα Router Advertisements που στέλνονται περιοδικά. Αν δεν παραλάβει διαφήμιση για ένα συγκεκριμένο χρονικό διάστημα θα υποθέσει ότι ο default δρομολογητής δεν είναι πλέον διαθέσιμος και συνδέεται με άλλον δρομολογητή από τον οποίο είχε λάβει διαφήμιση αυτό το διάστημα [11].

Όταν ο κινητός κόμβος καταλάβει ότι έχει κινηθεί σε άλλη σύνδεση, στέλνει ένα Binding Update στον HA του και στους CN τους οποίους έχει καταχωρημένους στην Binding Λίστα Ενημέρωσής του. Έτσι ο κινητός κόμβος τους ενημερώνει για την νέα COA του και κατά συνέπεια για την μετακίνησή του.

3.4.5 Μηχανισμός Εξεύρεσης Home Agent

Υποθέτοντας ότι ο κινητός κόμβος δεν γνωρίζει το IP του HA του, το πρωτόκολλο Mobile IPv6 προσφέρει ένα μηχανισμό που επιτρέπει στον κινητό κόμβο να ανακαλύπτει δυναμικά την IP διεύθυνση κάποιου HA στο HL του, στον οποίο θα μπορεί να εγγράψει την COA του όταν θα είναι μακριά το home subnet του.

Ο κινητός κόμβος στέλνει ένα Binding Update στο “Home Agents’ anycast address” για το δικό του home subnet prefix και κατά συνέπεια καταφέρνει να επικοινωνήσει με ένα από τους δρομολογητές στο HL του, που εκείνη τη στιγμή λειτουργεί σαν HA. Αν ο HA απορρίψει το Binding Update, θα επιστρέψει μια λίστα με όλους τους HA στο HL. Αυτή η λίστα διατηρείται από κάθε HA και δημιουργείται μέσω των περιοδικών αποστολών Routing Advertisements. Ο κινητός κόμβος στέλνει ένα Binding Update σε μια από τις διευθύνσεις στην λίστα και περιμένει για το ανάλογο Binding Acknowledgement. Αν δεν το λάβει, ή αν απορριφθεί, δοκιμάζει να εγγραφεί σε ένα άλλο HA της λίστας. Η επιλογή των HAs στην λίστα, γίνεται με την σειρά που καταγράφονται στην λίστα, γιατί η πρώτη διεύθυνση είναι του πιο διαθέσιμου HA και η τελευταία του λιγότερου διαθέσιμου [11].

3.5 QoS για Mobile IPv6

Λόγο του ότι τα πακέτα που αποστέλλονται και λαμβάνονται από ένα κινητό κόμβο περνούν από πολλά ενδιάμεσα network domains, χρειάζεται κατάλληλη QoS υποστήριξη στα πακέτα, ούτως ώστε η απόδοση διάφορων εφαρμογών που είναι ευαίσθητες σε QoS να διατηρείται σε επιθυμητά επίπεδα.

Μια καινούργια IPv6 επιλογή το QoS Object, εισάγεται ανάλογα με το περιεχόμενο είτε σαν Επιλογή Προορισμού, ή σαν Hop – by – hop Επιλογή μαζί με τα πακέτα που έχουν Binding Update ή Binding Acknowledgment επιλογές. Η βασική ιδέα είναι να συμπεριλαμβάνεται το QoS Object σαν μια Hop-By-Hop επιλογή μαζί με το Binding μήνυμα που ταξιδεύει στην ίδια κατεύθυνση με την QoS ευαίσθητη ροή πακέτων του

κινητού κόμβου. Καθώς αυτό το πακέτο ταξιδεύει από διαφορετικά δίκτυα, εξετάζεται το QoS Object για να προγραμματιστεί η κατάλληλη QoS υποστήριξη για τα πακέτα δεδομένων του κινητού κόμβου [12].

Υπάρχουν δυο ήδη QoS:

- Κράτηση Πόρων – Resource Reservation (συνενωμένες υπηρεσίες - integrated services): οι πόροι ενός δικτύου διαχωρίζονται ανάλογα με την αίτηση για QoS της κάθε εφαρμογής και είναι υποκείμενες στην πολιτική διαχείρισης του bandwidth.
- Με Προτεραιότητα – Prioritization (διαφοροποιημένες υπηρεσίες – differentiated services): η κίνηση του δικτύου ταξινομείται και διαχωρίζονται οι πόροι ανάλογα με κριτήρια της πολιτικής διαχείρισης του bandwidth. Για να καταστούν δυνατά τα QoS, λόγω των ταξινομήσεων γίνεται διαφορετική αντιμετώπιση σε εφαρμογές με περισσότερες απαιτήσεις.

Αυτά τα είδη QoS μπορούν να εφαρμοστούν αποκλειστικά στη ροή κάθε εφαρμογής είτε σε σύνολο ροών κι έτσι υπάρχουν ακόμη δυο τρόποι με τους οποίους μπορούν να χαρακτηριστούν τα QoS: ανά ροή (per flow) και ανά σύνολο (per aggregate).

Μελετάται επίσης η δημιουργία ενός response μοντέλου για Mobile IPv6 σε DiffServ περιβάλλον. Το μοντέλο αυτό βασίζεται στην προέκταση των υπάρχων σημάτων του Mobile IPv6, σαν Binding Update, Binding Acknowledgment, Binding Request και τα λοιπά. Γίνονται επίσης και βλέψεις για «DiffServ for Mobile IPv6» του οποίου η αρχιτεκτονική θα βασίζεται σε διαφοροποιημένες υπηρεσίες [12].

3.6 Μηχανισμοί μετάβασης

Για να διατηρηθούν οι τρέχουσες επενδύσεις και υπηρεσίες, το IETF έχει προτυποποιήσει διάφορους μηχανισμούς μετάβασης για να υποστηρίζεται η παράλληλη λειτουργία και συνύπαρξη των IPv4 και IPv6. Τα τρία είδη μηχανισμών μετάβασης είναι: διπλή στοίβα (dual stack), δημιουργία τούνελ (tunnelling) και μετάφραση (translation).

3.6.1 Διπλή στοίβα

Η μέθοδος της διπλής στοίβας απαιτεί ένας host ή ένας δρομολογητής να υποστηρίζουν και την στοίβα πρωτοκόλλου του IPv4 και του IPv6. Έτσι ο host ή ο δρομολογητής μπορεί να εξυπηρετήσει τόσο IPv4 όσο και IPv6 κίνηση και εφαρμογές. Ο σκοπός ενός δικτύου διπλής στοίβας είναι να παρέχει συνεχή πρόσβαση σε παραδοσιακά IPv4 based δίκτυα και υπηρεσίες μαζί με τοπική πρόσβαση σε IPv6 υπηρεσίες. Η μέθοδος αυτή παρέχει καλή σταδιακή μετακίνηση προς το IPv6. Επιτρέπει υποστήριξη και για IPv4 και για IPv6 εφαρμογές και υπηρεσίες κατά την διάρκεια της περιόδου που οι IPv4 υπηρεσίες θα αντικαθιστώνται από IPv6 εκδόσεις και θα παρουσιάζονται καινούργιες IPv6 υπηρεσίες. Ένας μηχανισμός διπλής στοίβας που έχει καθοριστεί είναι ο DSTM (Dual Stack Transition Mechanism) [7].

Mobile IPv6 σε συνδυασμό με DSTM

Για ένα τερματικό διπλής στοίβας που υποστηρίζει Mobile IPv6, είναι δυνατή η διακίνηση σε διάφορα δίκτυα ακόμη κι όταν έχει ήδη μια ανοικτή επικοινωνία με CNs (corresponding nodes), με την χρήση του DTSM μηχανισμού. Όπως ήδη γνωρίζουμε, όταν ο κινητός κόμβος είναι μακριά από το Home Network του, μπορεί να στείλει Binding Updates προς τον Home Agent του για να τον ενημερώσει για την καινούργια του τοποθεσία. Αν υπάρχει επικοινωνία με IPv4 host, τότε η κίνηση από τον Home Agent προς τον host αυτό γίνεται δια μέσω ενός DSTM εξυπηρετητή. Αυτή η διαδικασία όμως προσθέτει ένα επιπλέον IPv6 header στα IPv4 πακέτα κι έτσι υπάρχει επιπρόσθετη επιβάρυνση στην ραδιο – σύνδεση. Για να μειωθεί το κόστος αυτό, είναι προτιμότερο ο κινητός κόμβος να στέλνει τα Binding Updates απευθείας στον DSTM εξυπηρετητή (αν ο εξυπηρετητής υποστηρίζει Binding Updates). Ο εξυπηρετητής θα αποθηκεύσει μια νέα συσχέτιση (binding) μεταξύ της IPv4 διεύθυνσης του IPv4 host και της IPv6 COA κι έτσι μπορεί τώρα να αποστέλλει πακέτα απευθείας στον κινητό κόμβο, χωρίς να χρειάζεται η μεσολάβηση του Home Agent [7].

3.6.2 Δημιουργία Τούνελ

Η δημιουργία τούνελ παρέχει ένα μηχανισμό μετάβασης για την περίπτωση που τα IPv6 δίκτυα αρχίζουν να εμφανίζονται γύρω από την περιφέρεια του IPv4 Διαδικτύου. Όπου τα IPv6 δίκτυα δεν έχουν άμεση τοπική σύνδεση μεταξύ τους, ένα τούνελ μπορεί να γίνει configured. Η κίνηση του IPv6 θα περνά από το τούνελ στο IPv4 δίκτυο με το encapsulation των IPv6 πακέτων μέσα στα IPv4 πακέτα και την δρομολόγησή τους στο

IPv4 δίκτυο. Το μεγάλο πλεονέκτημα της μεθόδου αυτής, είναι ότι διατηρείται η ακεραιότητα των IPv6 πακέτων από σημείο σε σημείο. Οι μηχανισμοί δημιουργίας τούνελ που καθορίζονται από το IETF είναι το 6to4, 6over4 και το tunnel broker [7].

Mobile IPv6 σε συνδυασμό με την δημιουργία τούνελ

Το Mobile IPv6 παρουσιάζεται ιδιαίτερα κατάλληλο για χρήση με το μηχανισμό αυτό. Είναι πράγματι πολύ απλό: κάθε φορά που ένας κινητός κόμβος αλλάζει την τοποθεσία του, μπορεί να στείλει ένα Binding Update στον Home Agent του ή και στον CN, μέσω ενός τούνελ που έχει δημιουργηθεί με κάποιο μηχανισμό δημιουργίας τούνελ [7] (θεωρούμε ότι ο κινητός κόμβος, Home Agent και CN είναι IPv6 συμβατοί και η αποστολή πακέτων περνά δια μέσω ενός ή και διάφορων IPv4 δικτύων).

3.6.3 Μετάφραση

Ο μηχανισμός αυτός μπορεί να χρησιμοποιηθεί όταν ένας IPv6 host ή εφαρμογή χρειάζεται να επικοινωνήσει με ένα IPv4 host ή μια IPv4 version της εφαρμογής. Ο μεταφραστής χρησιμοποιείται για να μετατρέψει ένα IPv6 header σε ένα IPv4 header και αντίστροφα, καθώς επίσης να μετατρέψει τις 128 bit IPv6 διευθύνσεις σε 32 bit IPv4 διευθύνσεις. Ο μεταφραστής μπορεί να χρειαστεί μια συλλογή από IPv4 διευθύνσεις για να μπορεί να προμηθεύει μια διεύθυνση σε ένα IPv6 host που θέλει να επικοινωνήσει με ένα IPv4 host. Ο μεταφραστής μπορεί να τοποθετηθεί στα σύνορα των IPv4 – IPv6 δικτύων ή αν μια IPv6 εφαρμογή βρίσκεται σε ένα IPv4 capable host, μπορεί να τοποθετηθεί στον end host [7]. Μερικοί μηχανισμοί μετάφρασης είναι οι NAT-PT, BIS και SOCKS.

Mobile IPv6 σε συνδυασμό με NAT-PT

Ο NAT-PT μηχανισμός αρχικοποιεί μια σύνδεση μεταξύ ενός IPv4 και ενός IPv6 host. Κατά την διάρκεια της σύνδεσης, όλη η κίνηση μεταξύ των δυο hosts πρέπει να περνά δια μέσω του ίδιου NAT-PT εξυπηρετητή. Με την κίνηση ενός κόμβου, είναι δυνατή η αποστολή Binding Updates προς τον Home Agent του, αλλά δεν μπορεί να στείλει Binding Updates στον CN. Αυτό συμβαίνει για τον λόγο ότι ο NAT-PT εξυπηρετητής δεν μπορεί να μεταφράσει το Binding Update για να το προωθήσει στον IPv4 host, γιατί θα χρειαστεί να «σπάσει» το Authentication Header του Binding Update. Για αυτό τον λόγο, δεν μπορεί να υπάρξει απ' ευθείας επικοινωνία μεταξύ των δυο hosts. Η επικοινωνία μπορεί να γίνει με δυο τρόπους [7]:

- Ο κινητός κόμβος στέλνει τα Binding Updates στον NA-PT εξυπηρετητή κι αυτός φυλάει νέα συσχέτιση μεταξύ της καινούργιας IPv6 COA του κινητού κόμβου και της IPv4 διεύθυνσης του CN, οπότε γίνεται δυνατή η επικοινωνία μεταξύ τους.
- Ο NAT-PT για κάποιο λόγο δεν μπορεί να φυλάξει νέα συσχέτιση κι έτσι ο NAT-PT στέλνει τα πακέτα προς τον Home Agent του κινητού κόμβου, ο οποίος αναλαμβάνει κανονικά από εδώ και πέρα.

3.7 Πλεονεκτήματα του Mobile IPv6

Η υποστήριξη κινητικότητας για συσκευές Διαδικτύου είναι δυνατή και τυποποιείται τόσο για το IPv4 και το IPv6. Όμως, λόγω της εμπλουτισμένης λειτουργικότητας και της πιο πρόσφατης σχεδίασης του IPv6, κάποια χαρακτηριστικά που αφορούν την υποστήριξη κινητικότητας είναι πιο αποτελεσματικά σε σύγκριση με το Mobile IPv4. Σύντομα, κάποια προτερήματα του Mobile IPv6 [11]:

- Το Mobile IP πρέπει να αναθέσει παγκόσμιες IP διευθύνσεις σε ένα κινητό κόμβο, σε οποιονδήποτε σημείο συνδέεται με το Διαδίκτυο. Σε συνδέσεις όπου βρίσκονται κινητοί κόμβοι, ένα μέρος των IP διευθύνσεων θα ανατεθεί σαν COA στους κόμβους αυτούς. Λόγο της έλλειψης διευθύνσεων στο IPv4, μπορεί να υπάρξουν προβλήματα σε μερικές συνδέσεις, ενώ στο IPv6 υπάρχουν αρκετές διαθέσιμες διευθύνσεις.
- Χρησιμοποιώντας τις anycast διευθύνσεις του IPv6, ένας κόμβος μπορεί να στείλει ένα πακέτο σε πολλά συστήματα που έχουν αυτή την anycast διεύθυνση σε ένα από τα interfaces τους. Το Mobile IPv6 κάνει αποτελεσματική χρήση αυτού του μηχανισμού για το Dynamic Home Agent Discovery, στέλνοντας ένα Binding Update στην anycast διεύθυνση του HA και παίρνοντας απάντηση από τους υπόλοιπους HAs. Το Mobile IPv4 δεν παρέχει τέτοια έξυπνη λύση.
- Το stateless autoconfiguration διευθύνσεων και οι μηχανισμοί ανακάλυψης γειτόνων του Mobile IPv6, δεν χρειάζονται DHCP εξυπηρετητές για να γίνονται configure οι COAs των κινητών κόμβων.

- Το Mobile IPv6 μπορεί να χρησιμοποιήσει το IPSec¹ για όλες τις απαιτήσεις ασφαλείας, όπως πιστοποίηση, προστασία της ακεραιότητας των δεδομένων και τα λοιπά.
- Η Βελτιστοποίηση Διαδρομής (Route Optimization) που χρησιμοποιείται για αποφυγή της τριγωνικής δρομολόγησης (με αποτέλεσμα καλύτερη χρήση των πόρων του δικτύου – συνδέσμους, bandwidth και τα λοιπά), είναι μια επιπρόσθετη λειτουργία για το Mobile IPv4, ενώ είναι ένα αναπόσπαστο κομμάτι για το Mobile IPv6.
- Για να μην δημιουργούνται προβλήματα από δρομολογητές που χρησιμοποιούν ingress filtering², στην αποστολή πακέτων από ένα κινητό κόμβο θέτεται η διεύθυνση αποστολέα η COA διεύθυνση (που είναι προσιτή από το interface του δρομολογητή στο οποίο φτάνει το πακέτο) και η διεύθυνση του Home Agent θέτεται στην Home Agent επιλογή προορισμού.

Έχει γίνει πλέον αποδεκτό ότι όπως το IPv6 θα αντικαταστήσει το IPv4, έτσι και το Mobile IPv6 θα αντικαταστήσει το Mobile IPv4. Κατ' ακρίβεια έχει ήδη αρχίσει η υλοποίηση των IPv6 και Mobile IPv6 σε διάφορα δίκτυα. Εκτός από τα πολλά πλεονεκτήματα του Mobile IPv6, έχουμε δείξει ότι είναι και προσιτή η ομαλή μετάβαση από το Mobile IPv4 σε Mobile IPv6 με την χρήση των κατάλληλων μηχανισμών μετάβασης. Όλα λοιπόν δείχνουν να είναι θετικά ως προς την χρήση του Mobile IPv6 και στα συστήματα Τρίτης Γενεάς, συμπεριλαμβανομένου και του UMTS, αλλά χρειάζεται να γίνει και κάποια μελέτη διάφορων πιθανών σεναρίων που να διαγράφουν την λειτουργία του UMTS με Mobile IPv6 και την διαδικασία επικοινωνίας του UMTS IPv6 compatible δικτύου με άλλα δίκτυα.

¹ Το IPSec (IP security protocol) είναι ένα πρωτόκολλο για ασφάλεια στο Διαδίκτυο που παρέχει συν τοις άλλοις, per-packet πιστοποίηση / εμπιστευτικότητα authenticity/confidentiality guarantees between peers communicate using IPsec. IPsec is available for both IPv6 and IPv4.

² Το ingress filtering είναι μια διαδικασία που εφαρμόζεται στους δρομολογητές κάποιου δικτύου, κατά την οποία πετάγονται πακέτα των οποίων το network prefix τους δεν είναι προσιτό από το interface στο οποίο καταφθάνουν τα πακέτα.

Κεφάλαιο 4

Περιγραφή Συστήματος UMTS

4.1	Σύντομο Overview του UMTS	46
4.2	UMTS Έκδοση 99	47
4.3	UMTS Έκδοση 2000 (Έκδοση 4 και Έκδοση 5)	50
4.4	All - IP UMTS	52
4.5	IP Έκδοση στο UMTS	57

Παρά το γεγονός ότι το IPv6 θεωρείται από πολλούς αναγκαίο για τις μελλοντικές συσκευές και συστήματα δικτύων, η χρήση του είναι προς το παρόν κάπως περιορισμένη. Αρκετοί πιστεύουν ότι στα δίκτυα της επόμενης γενεάς, όπως το UMTS, θα είναι όπου θα χρησιμοποιηθεί το IPv6 σε μεγάλη κλίμακα.

Έχουν ήδη γίνει πολλά σχέδια για συμπίληψη υπηρεσιών UMTS σε τρίτης και τέταρτης γενεάς δίκτυα. Είναι αναμενόμενο ότι με την πρόσβαση των κινητών τηλεφώνων σε υπηρεσίες Διαδικτύου, θα υπάρχει μια πρωτοφανής αύξηση σε απαιτήσεις για νέες διευθύνσεις, ευκολότερη διαχείριση και περισσότερη ασφάλεια. Το IPv6 θα είναι ένας σημαντικός παράγοντας στην επιτυχία της υλοποίησης υπηρεσιών Διαδικτύου μέσω του UMTS. Όπως έχει αναφερθεί σε προηγούμενο κεφάλαιο, το IPv6 παρέχει πληθώρα διευθύνσεων Διαδικτύου, γεγονός το οποίο καθιστά δυνατή την ανάθεση διεύθυνσης, σχεδόν σε κάθε ηλεκτρονική συσκευή στην γη – καθαρό πλεονέκτημα πάνω στο IPv4. Επιπρόσθετα, η τεχνολογία του IPv6, «κουβαλά» μαζί της την αναγκαία ασφάλεια και ποιότητα που είναι απών από το Διαδίκτυο όπως το γνωρίζουμε σήμερα.

Είναι δύσκολο να πει κανείς πώς τα διαφορετικά σενάρια του UMTS/IPv6 θα πραγματοποιηθούν. Αυτό εξαρτάται από πολλούς παράγοντες όπως τον αριθμό των διαθέσιμων IPv4 διευθύνσεων, την στρατηγική του UMTS διαχειριστή (operator) και τα λοιπά. Είναι επίσης ακαθόριστο το πότε και πως θα εισαχθούν οι IPv6 υπηρεσίες. Ένα άλλο σημαντικό θέμα είναι ο καθορισμός σεναρίων συνύπαρξης του IPv4 και

IPv6, αφού αυτό είναι σίγουρο ότι θα συμβεί και για αρκετό χρονικό διάστημα. Προτού όμως μελετηθούν τα διάφορα σενάρια, πρέπει να αναλυθούν οι βασικές έννοιες και η αρχιτεκτονική του συστήματος UMTS που είναι και το θέμα του κεφαλαίου αυτού.

4.1 Σύντομο overview του UMTS

Όπως έχει προαναφερθεί, το UMTS είναι ένα τρίτης γενεάς ασύρματο σύστημα που σχεδιάστηκε για να προσφέρει ψηλότερα bit rates και ανεπτυγμένες υπηρεσίες σε συνδρομητές. Είναι επίσης γνωστό ότι ένα από τα επικρατέστερα συστήματα δεύτερης γενεάς είναι το GSM, αλλά αφού είναι σχεδιασμένα για circuit switched υπηρεσίες φωνής και προσφέρουν χαμηλά data rates, δεν είναι τόσο κατάλληλο για την υποστήριξη packet switched υπηρεσιών Διαδικτύου. Αυτός ήταν και ο κύριος λόγος της προσθήκης του GPRS δικτύου στο GSM, για την επαρκή υποστήριξη packet switched υπηρεσιών. Τα GSM/GPRS δίκτυα συχνά αναφέρονται και σαν 2.5 γενεάς δίκτυα. Ακόμη και με το GPRS, τα bit rates περιορίζονται στα 64 kbps ανά συνδρομητή και υποστηρίζονται μόνο packet switched υπηρεσίες μη πραγματικού χρόνου. Το UMTS, σαν η εξέλιξη του GSM/GPRS, προσφέρει data rates μέχρι και 2 Mbps και υποστηρίζει ανεπτυγμένες υπηρεσίες σαν streaming video και audio και υπηρεσίες που βασίζονται στην τοποθεσία (location based services) [16].

Η προτυποποίηση του UMTS έχει περάσει από μέχρι τώρα από δυο φάσεις. Η πρώτη φάση είναι γνωστή σαν Έκδοση 99 (Release 99). Το επόμενο βήμα της προτυποποίησης είναι η Έκδοση 00 (Release 00). Όμως λόγω του μεγάλου αριθμού των αλλαγών που είχαν προταθεί, είχε αργότερα χωριστεί σε δυο ξεχωριστές εκδόσεις: Έκδοση 4 (Release 4) και Έκδοση 5 (Release 5) [16].

Οι εργασίες προς τις επόμενες εκδόσεις συγκεντρώνονται περισσότερο στο πως να αναμείξουν IP και στο core δίκτυο καθώς και στο δίκτυο ραδιο - πρόσβασης. Αυτό σημαίνει ότι μπορούμε να αναμένουμε τις καινούργιες αρχιτεκτονικές να είναι πιο πολύ ταυτισμένες με την IP αρχιτεκτονική. Μια από τις αναμενόμενες εκδοχές του UMTS είναι και η ALL – IP η οποία θα είναι και η βάση της πρώτης ανάπτυξης του UMTS. Ο σκοπός της ALL – IP αρχιτεκτονικής είναι να επιτρέπεται στους διαχειριστές η χρήση IP τεχνολογίας για την πραγματοποίηση τρίτης γενεάς υπηρεσιών [2]. Με άλλα λόγια, μια αρχιτεκτονική βασισμένη σε τεχνολογίες πακέτου και IP τηλεφωνία για ταυτόχρονες υπηρεσίες πραγματικού και μη πραγματικού χρόνου. Αυτή

η εκδοχή είναι ιδιαίτερα ενδιαφέρουσα, αφού προσθέτει την έννοια της διαχείρισης κινητικότητας, βάσει του IP.

Στην συνέχεια θα αναλυθεί περισσότερο η Έκδοση 99, αφού είναι και η βασική αρχιτεκτονική των UMTS και θα γίνει αναφορά στις Εκδόσεις 4 και 5. Ακολουθεί επίσης περισσότερη ανάλυση της ALL – IP αρχιτεκτονικής.

4.2 UMTS Έκδοση 99

Οι πρώτες εμπορικές υπηρεσίες UMTS, θα βασίζονται στο UMTS Έκδοση 99. Οι προδιαγραφές της Έκδοσης 99 καθορίζουν την βασική αρχιτεκτονική που αποτελείτε από το ραδιο - δίκτυο πρόσβασης (radio access network) UMTS Terrestrial (UTRAN) το οποίο έχει καθοριστεί με τα ικανότερα στοιχεία και πρωτόκολλα και το κυρίως δίκτυο που χωρίζεται στο Circuit Switched Core Network (CS – CN) και το Packet Switched Core Network (PS – CN) [16]. Η Έκδοση 99 προσφέρει τις «παραδοσιακές» circuit και packet switched υπηρεσίες. Δίνεται πολλή έμφαση στην δυνατότητα ομαλής εξέλιξης από τα GSM στα UMTS δίκτυα. Το UMTS δίκτυο πρέπει να είναι προς τα πίσω συμβατό (backward compatible) με GSM δίκτυα, να μπορεί να λειτουργεί μαζί με το GSM [2] και βασίζεται πάρα πολύ στο GPRS στο packet mode [7].

4.2.1 Καινοτομίες και νέα στοιχεία στην Έκδοση 99

Οι πιο σημαντικές καινοτομίες που εισάγονται (συγκρίνοντας με το GSM) είναι μια νέα ράδιο- διαπροσωπία (radio interface), μια σημαντική αύξηση στο bandwidth, προνοώντας τόσο για circuit switched όσο και packet switched συμφόρηση, καθώς και την εισαγωγή της ATM τεχνολογίας στην διαπροσωπία μεταξύ του ραδιο - δικτύου πρόσβασης και του κυρίως δικτύου (core network). Έχει επίσης την αποδοτικότερη (με γενικά καλύτερη φασματική αποδοτικότητα) ραδιο - μέθοδο προσπέλασης WCDMA [2].

Τα νέα στοιχεία στα συνυπάρχοντα δίκτυα GSM/UMTS, όπως φαίνονται σε ακόλουθο σχήμα είναι: Κόμβος B (node B), Radio Network Subsystems (RNC), και δομοστοιχεία διαπροσωπιών (interface modules - IS).

- Κόμβος B: Είναι υπεύθυνος για την παροχή του ραδιο – συνδέσμου μεταξύ του κινητού κόμβου και του UMTS δικτύου. Μαζί με την παραλαβή και μετάδοση των δεδομένων στην ραδιο – διαπροσωπία, ο Κόμβος – B εφαρμόζει και τους

αναγκαίους κωδικούς για την περιγραφή των καναλιών σε ένα Code Division Multiple Access (CDMA) σύστημα [14].

- RNC: Μαζί αποτελούν το UTRAN. Είναι υπεύθυνα για κρυπτογράφηση και αποκρυπτογράφηση των ραδιο – καναλιών, έλεγχο handover, διαχείριση ραδιο – πόρων και τα λοιπά [1].
- Δομοστοιχεία Διαπροσωπιών: Χρειάζονται στους κινητούς κόμβους για να μπορούν να χρησιμοποιούν την UMTS τεχνολογία.

Τα άλλα στοιχεία του δικτύου χρειάζονται μόνο μια μερική βελτίωση λογισμικού ή υλικού [2]. Έτσι η Έκδοση 99 μπορεί να γίνει σαν η επέκταση του ήδη υπάρχοντος GSM/GPRS δικτύου μετάδοσης (αν είναι αρκετά «μεγάλο» για να υποστηρίξει τις νέες υπηρεσίες και τα ψηλότερα bit rates). Αυτό έχει άμεση και δυνατή επίδραση στους διαχειριστές, καθώς μειώνονται τα έξοδα και δίνεται η δυνατότητα προσαρμογής της κινητής εφαρμογής ανάλογα με τις ανάγκες της αγοράς, χρησιμοποιώντας τον ίδιο εξοπλισμό [2].

4.2.2 Αρχιτεκτονική Έκδοσης 99

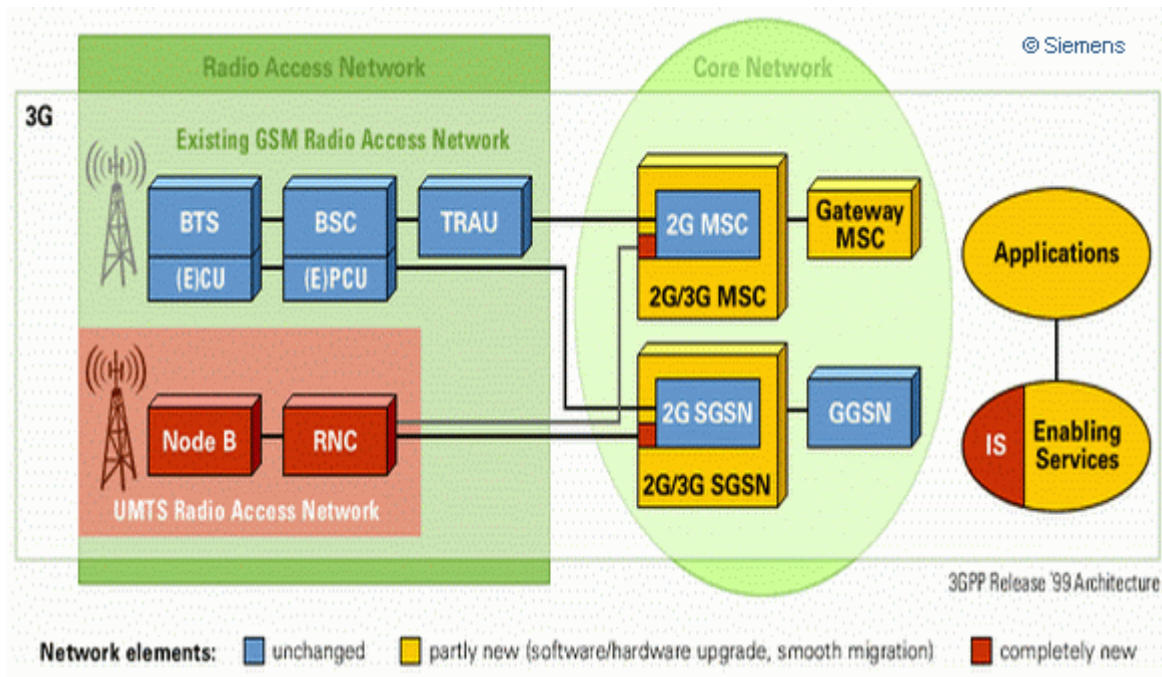
Όπως έχει προαναφερθεί, η αρχιτεκτονική της Έκδοσης 99 αποτελείται από τρία σημαντικά συστατικά: UTRAN, CS-CN και PS-CN.

- Το UTRAN είναι αρμόδιο για το χειρισμό της πλήρους ραδιο-λειτουργίας (radio functionality). Στην πραγματικότητα, το UMTS φροντίζει τα κεντρικά δίκτυα να είναι εντελώς απομονωμένα από ραδιο - λειτουργία έτσι ώστε να μπορούν να λειτουργήσουν με διαφορετικούς τύπους ραδιο - δικτύων όπως UTRAN και WLANs. Το UTRAN χρησιμοποιεί το Asynchronous Transfer Mode (ATM) σαν την επιλογή μεταφοράς δικτύου (transport network option). Οι μελλοντικές εκδόσεις του UMTS αναμένονται να παρέχουν το IP ως επιλογή για το δίκτυο μεταφορών [16]. Οι λειτουργίες του UTRAN συμπεριλαμβάνουν soft handover, έλεγχο συμφόρησης, έλεγχο διαχείρισης ραδιο – πόρων και άλλα [7].
- Το UMTS CS-CN είναι η εξέλιξη του SS7 κεντρικού δικτύου, το οποίο βασίζεται στο GSM. Υποστηρίζει συνδέσεις στο Public Switched Telephony Network (PSTN) – με απλά λόγια συνδέσεις τηλεφώνου – και στο Integrated Digital Services Network (ISDN) για circuit switched υπηρεσίες. Παρέχει παραδοσιακές υπηρεσίες τηλεφωνίας, όπως φωνητική επικοινωνία και

υπηρεσία φαξ, αλλά και ανεπτυγμένες υπηρεσίες όπως την Short Message Service (SMS) και άλλες circuit – switched υπηρεσίες [16].

- Το UMTS PS-CN εξελίχθηκε από IP based GPRS δίκτυα. Υποστηρίζει συνδέσεις στο Διαδίκτυο για packet switched υπηρεσίες. Εκτός από την πρόσβαση στο Διαδίκτυο, υποστηρίζει υπηρεσίες σαν τα Virtual Private Networks (VPN) και SMS. Τα σημαντικά κομμάτια του PS-CN είναι το Service GPRS Support Node (SGSN), που είναι υπεύθυνο για διαχείριση κινητικότητας και λειτουργίες ασφάλειας και πιστοποίησης και το Gateway GPRS Support Node (GGSN), που είναι υπεύθυνο για διαχείριση IP διευθύνσεων, διαχείριση QoS και για διάφορες εξωτερικές λειτουργίες που έχει σαν gateway [16].

Στο σχήμα που ακολουθεί παρουσιάζεται η βασική αρχιτεκτονική της Έκδοσης 99.



Σχήμα 4.1 [2]

Όπως φαίνεται και στο Σχήμα 4.1, UTRAN χρησιμοποιείται αναλλοίωτο το GSM δίκτυο μαζί με την προσθήκη των Κόμβος – B και RNC. Στο CS-CN υπάρχει αναλλοίωτο το Mobile Switching Center (MSC) που χρησιμοποιούταν στο GSM δίκτυο, ενώ έχει βελτιωθεί το Gateway για το MSC. Στο PS-CN είναι αναλλοίωτο το SGSN ενώ έχει βελτιωθεί το GGSN. Φαίνεται ακόμη και η χρήση των δομοστοιχείων διαπροσωπίας στις εφαρμογές των κινητών κόμβων.

Οι συνδέσεις μετάδοσης μέσα στο ραδιο-δίκτυο πρόσβασης, χρησιμοποιούν το πρωτόκολλο του ATM, και το δίκτυο είναι καταλληλότερο για την υποστήριξη πακέτων δεδομένων. Η χρήση των Προσαρμοσμένων Εφαρμογών για Ενισχυμένη Λογική Κινητών δικτύων (Customized Applications for Mobile network Enhanced Logic – CAMEL) έχει εφαρμοστεί για να βεβαιωθεί η δυνατότητα μεταφοράς πληροφοριών υπηρεσιών μεταξύ διαφορετικών δικτύων. Στο μέλλον το CAMEL θα περιληφθεί σχεδόν σε όλες τις συναλλαγές μεταξύ των δικτύων [2].

Αυτά τα σημεία που έχουν προαναφερθεί, παρουσιάζουν μόνο ένα μικρό μέρος των βασικών καινοτομιών και διευκολύνσεων που παρέχονται από την Έκδοση 99. Καθώς η έκδοση αυτή είναι μόνο η αρχική των UMTS, οι διάφορες εκδόσεις που ακολουθούν, προσφέρουν ακόμη πιο ανεπτυγμένες υπηρεσίες και περισσότερες εξυπηρετήσεις. Θα ακολουθήσει μια πολύ σύντομη ματιά στις εκδόσεις 4 και 5.

4.3 UMTS Έκδοση 2000 (Έκδοση 4 και Έκδοση 5)

Η επόμενη φάση στην ανάπτυξη των UMTS ήταν η Έκδοση 2000, η οποία κυκλοφόρησε σαν δυο εκδόσεις, η Έκδοση 4 και Έκδοση 5. Ακολουθούν οι βασικές αλλαγές και καινοτομίες κάθε έκδοσης.

4.3.1 UMTS Έκδοση 4

Σαν επόμενο βήμα, έχει διασπαστεί η σύνδεση και ο έλεγχος την σύνδεσης από το CS – CN. Τα δεδομένα του χρήστη μεταφέρονται μέσω Media Gateways (MGW), ένα νέο στοιχείο που εισαγάγεται στο CS-CN, και ο έλεγχος των συνδέσεων θα διαχειρίζεται από τον MSC Εξυπηρετητή, ξεχωριστό στοιχείο που αναπτύχθηκε από το MSC/VLR. Το MGW τότε θα είναι υπεύθυνο για την διατήρηση της σύνδεσης και το switching, ενώ ο MSC Εξυπηρετητής θα ελέγχει την σύνδεση. Χάρη σε αυτό, το CS – CN θα είναι πιο κλιμακωτό (αυξομειώσιμο): αν χρειάζεται περισσότερη δυνατότητα switching, προσθέτονται MGWs · αν χρειάζεται περισσότερη δυνατότητα ελέγχου, προστίθεται ένα MSC εξυπηρετητής [2].

Το MGW μπορεί να αλλάζει circuit switched συνδέσεις σε packet switched συνδέσεις (voice over IP). Για να γίνουν δυνατές αυτού του είδους οι συνδέσεις, έχει προστεθεί επίσης και το IP Multimedia System (IMS) στο δίκτυο. Η λειτουργία του είναι

ενδιάμεση των CS – CN και PS – CN για μεγαλύτερη ομοιομορφία δικτύου. Το IMS θα χρησιμοποιείται επίσης και για IP based υπηρεσίες πολυμέσων [2].

Τέλος, στην Έκδοση 4 το CAMEL έχει μια σύνδεση στα PS – CN στοιχεία και η παρέχετε επίσης η δυνατότητα εισαγωγής του GSM/EDGE¹ Δίκτυο Ράδιο Πρόσβασης (Radio Access Network – GERAN) σαν μέρος του UTRAN [2].

4.3.2 UMTS Έκδοση 5

Καθώς οι εξελίξεις συνεχίζονται, όλη η κίνηση που έρχεται από τον κινητό κόμβο πρέπει να γίνει IP based. Αυτό χρειάζεται κι άλλες βελτιώσεις (κυρίως σε λογισμικό, αφού νέοι τύποι στοιχείων δικτύων δεν είναι αναγκαίοι) και απαιτούνται εντελώς καινούργια τοπικά IP τερματικά (native IP terminals). Η σημαντική καινοτομία της Έκδοσης 5 με λίγα λόγια, είναι η διαμόρφωση του δικτύου σε ένα σημείο προς σημείο packet switch cellular δίκτυο [2]. Για παράδειγμα, γίνεται χρήση του SIP (Session Initiation Protocol) πρωτοκόλλου για την δημιουργία φωνητικών κλήσεων από κινητούς χρήστες που λειτουργούν σε packet mode κι έτσι οι φωνητικές κλήσεις δεν είναι υπευθυνότητα του CS-CN πλέον. Παρουσιάζονται δυο κύριες λειτουργίες που εισήχθησαν στην Έκδοση 5, η Call Session Control Function (CSCF) και η Media Gateway Control Function (MGCF).

CSCF:

Η λειτουργία αυτή κυρίως επεξεργάζεται μηνύματα σήμανσης (signaling) για έλεγχο του session πολυμέσων ενός χρήστη ο οποίος εξελίχθηκε από την λειτουργία ελέγχου κλήσης του MSC. Για ένα συγκεκριμένο session, χρησιμοποιείται η CSCF για την δημιουργία του και παροχή των διάφορων features του session, ενώ το PS-CN χρησιμοποιείται για υποστήριξη του μονοπατιού φορέα (bearer path) [16].

MGCF:

Χρησιμοποιείται για τον έλεγχο ενός ή περισσότερων MGWs. Χρησιμοποιείται για διαχείριση της σύνδεσης μεταξύ του PSTN και του IP stream. Η MGCF σε συνδυασμό με SIP μηνύματα που δημιουργούνται από την CSCF, καθορίζει πως θα χρησιμοποιηθούν τα MGWs [16].

¹ GSM/EDGE (Enhanced Data rate for GSM Evolution): Σύστημα GSM με αυξημένες ταχύτητες μετάδοσης δεδομένων.

4.4 All IP UMTS

Το τρίτης γενεάς δίκτυο για το οποίο στοχεύει το IETF, σύμφωνα με τις περιγραφές στις προδιαγραφές, είναι ένα και μοναδικό συνενωμένο δίκτυο το οποίο είναι 100% IP. Δεν υπάρχουν ακόμη οι ακριβείς προδιαγραφές για την αρχιτεκτονική αυτή, όμως πολλές εναλλακτικές λύσεις έχουν προταθεί και μελετηθεί. Πιο κάτω θα παρουσιαστεί εν συντομία μια εναλλακτική λύση.

4.4.1 All IP UMTS πλεονεκτήματα και μειονεκτήματα

Η εξέλιξη στο IP based δίκτυο έχει τέσσερα σημαντικά πλεονεκτήματα [2]:

- Ένα IP based δίκτυο υπόσχεται χαμηλότερη χρέωση επικοινωνίας και μειωμένο κόστος κατασκευής συστήματος. Ο εξοπλισμός ενός IP συστήματος που χρησιμοποιείται για υποστήριξη τόσο της υπηρεσίας φωνητικής επικοινωνίας, όσο και της υπηρεσίας επικοινωνίας με πακέτα, κοστίζει πολύ λιγότερα παρά τον ειδικό εξοπλισμό που χρησιμοποιείται στα παλαιότερα δίκτυα, που προσφέρουν αυτές τις υπηρεσίες.
- Γίνεται πιο εύκολη η ανάπτυξη εφαρμογών που θα συνδυάζουν επικοινωνία φωνής και δεδομένων. Αν χρησιμοποιείται το IP σημείο προς σημείο, τότε οι ISPs θα εξαρτώνται λιγότερο από cellular διαχειριστές και θα μπορούν να αναπτύξουν εφαρμογές πιο ελεύθερα.
- Αφού είναι δυνατή η διαχείριση φωνής και δεδομένων σε ένα μοναδικό all –IP κυρίως δίκτυο, τα κόστη συντήρησης και διατήρησης σε ενεργεία του δικτύου μειώνονται σημαντικά.
- Οι περισσότεροι από τους πωλητές δικτυακής υποδομής γνωρίζουν την all IP τάση στα τρίτης γενεάς δίκτυα. Έτσι, οι υποδομές που οι πωλητές παρέχουν κατασκευάζονται με τέτοιο τρόπο, έτσι ώστε να μπορούν εύκολα να αναβαθμιστούν σε IP based διαχείριση. Γι' αυτό το λόγο, στις πιο πολλές περιπτώσεις δεν χρειάζονται καινούργια στοιχεία δικτύου για την εξέλιξη σε μια all IP αρχιτεκτονική

Ωστόσο, η υλοποίηση του IP μπορεί να παρουσιάσει μερικά αρχικά προβλήματα. Επειδή το IP από μόνο του δεν ικανοποιεί μερικές απαιτήσεις για QoS, κινητικότητα και bandwidth αποδοτικότητα σε narrowband συνδέσεις, νέα πρωτόκολλα πρέπει να προστεθούν στο σύστημα. Η χρήση οποιασδήποτε τεχνικής προσαρμογής – συμπίεση

header², MPLS³, ή PPP⁴ επεκτάσεις – για την αύξηση του IP σε narrowband συνδέσεις, έχει ως αποτέλεσμα υψηλό επίπεδο πολυπλοκότητας. Για να αντιμετωπιστεί αυτή η κατάσταση, μερικοί εισηγούνται broadband ή κατανεμημένες αρχιτεκτονικές [2].

4.4.2 Συνενωμένο Δίκτυο

Η εγκατάσταση και οργάνωση δυο ξεχωριστών δικτύων για τηλεφωνία και υπηρεσίες δεδομένων, εισαγάγει σοβαρούς περιορισμούς όσον αφορά υπηρεσίες πολυμέσων και την διαχείριση των δικτύων αυτών. Γίνονται σκέψεις λοιπόν για την συνένωση αυτών των δυο δικτύων. Μερικά από τα προτερήματα ενός συνενωμένου ασύρματου δικτύου είναι [16]:

- Χαμηλό κόστος υποδομής: Το συνενωμένο δίκτυο προϋποθέτει ότι το CS – CN δεν θα είναι πλέον αναγκαίο. Κατά συνέπεια, μειώνεται το κόστος για τους διαχειριστές. Μερικοί όμως επιχειρηματολογούν ότι θα χρειαστεί να αναπτυχθούν καινούργια συστατικά για το νέο συνενωμένο δίκτυο, για να μπορεί να υποστηρίξει CS – CN λειτουργίες. Ωστόσο, αυτά τα συστατικά θα βασίζονται σε IP τεχνολογίες και κατά κανόνα κοστίζουν λιγότερο σε σχέση με συστατικά τηλεφωνίας – λόγω ανταγωνισμού και ανοιχτών προτύπων. Σε τελική ανάλυση, οι διαχειριστές μπορούν να αφαιρέσουν από το δίκτυο περιττά συστατικά τα οποία κάνουν την ίδια λειτουργία και στα δυο δίκτυα. Για παράδειγμα, μια μόνο συνενωμένη πλατφόρμα διαχείρισης δικτύου (integrated network management platform), μπορεί τώρα να διαχειρίζεται ολόκληρο το δίκτυο, αντί δυο ξεχωριστές πλατφόρμες για το CS – CN και το PS – CN.
- Χαμηλότερο κόστος συντήρησης: Ένα συνενωμένο δίκτυο που βασίζεται σε IP, έχει μειωμένα κόστη συντήρησης και διαχείρισης. Όπως έχει προαναφερθεί, η διαχείριση IP συστατικών δικτύου είναι λιγότερο δαπανηρή σε σχέση με συστατικά τηλεφωνίας. Επίσης οι διαχειριστές μπορούν να διευθύνουν το συνενωμένο δίκτυο εργοδοτώντας λιγότερα στελέχη. Με λίγα λόγια, οι διαχειριστές δεν θα χρειάζεται να επενδύουν εκπαίδευση ειδικών σε πολλαπλές τεχνολογίες, αφού το συνενωμένο δίκτυο θα βασίζεται σε ένα bearer δίκτυο σήμανσης.

² Μηχανισμός συμπίεσης header πακέτου για μείωση του header overhead και κατά συνέπεια καλύτερη χρήση των πόρων δικτύου.

³ MPLS (MultiProtocol Label Switching): Label Switching μηχανισμός που σχεδιάστηκε για αύξηση απόδοσης προώθησης (forwarding).

⁴ PPP (Point to Point Protocol): Παρέχει μια μέθοδο μεταφοράς πακέτων διαφόρων πρωτοκόλλων (multi – protocol datagrams) σε σημείο προς σημείο συνδέσεις (point-to-point links).

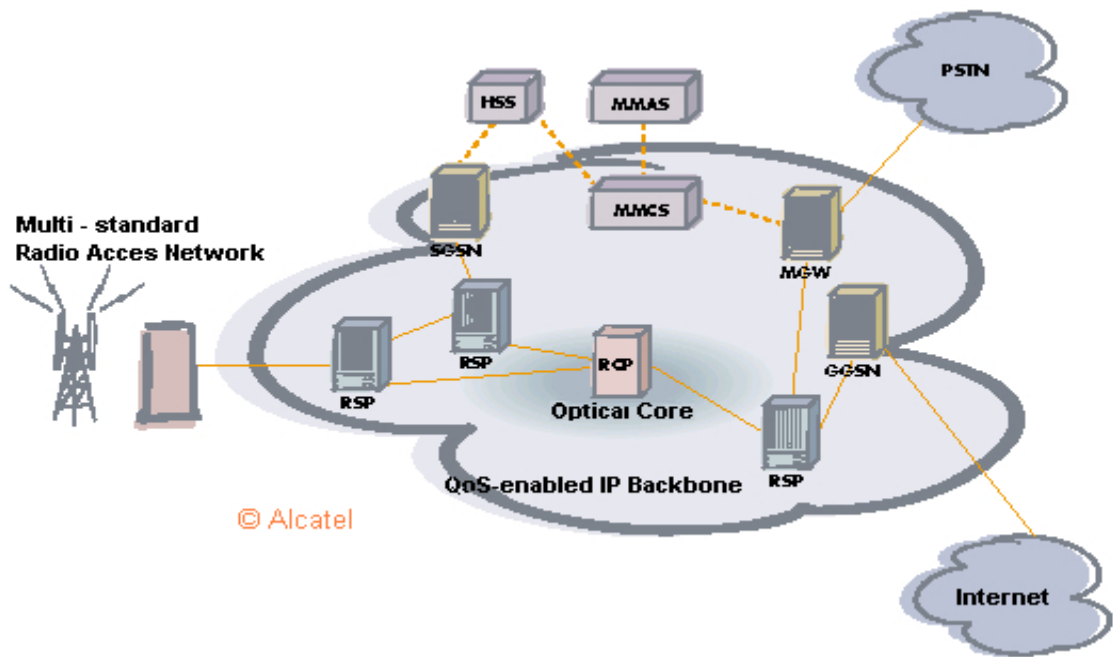
- **Ανεπτυγμένες Υπηρεσίες:** Η ανάμιξη δικτύων φωνής και δεδομένων προσφέρει ευκαιρίες για ανάπτυξη ανεπτυγμένων υπηρεσιών πολυμέσων. Σχεδόν κάθε υπηρεσία, εκτός από τις τηλεφωνικές υπηρεσίες, είναι διαθέσιμη στο Διαδίκτυο σήμερα. Ο συνδυασμός του Διαδικτύου και των τηλεφωνικών υπηρεσιών δημιουργεί πολλές καινούριες ευκαιρίες αποκόμισης κέρδους για τους παροχείς υπηρεσιών.
- **Ανάπτυξη Ταχείας Υπηρεσίας (Rapid Service Deployment):** Η ανάπτυξη ενός συνενωμένου δικτύου που θα βασίζεται σε ένα μόνο πρότυπο επιτρέπει την ταχεία ανάπτυξη καινούργιων υπηρεσιών. Πολλά από τα αναγκαία που χρειάζονται για την εισαγωγή καινούργιων υπηρεσιών μειώνονται λόγω της ανάμιξης της διαχείρισης των ασύρματων δικτύων.

4.4.3 All IP UMTS αρχιτεκτονική

Είναι πιθανό ότι η εξέλιξη μιας All – IP αρχιτεκτονικής θα περάσει από διάφορα στάδια και δεν είναι καθαρό κατά πόσο η All – IP λύση «κτίζει» μόνο στο packet domain ή αν τόσο το packet και το circuit switched mode λειτουργίας θα υποστηρίζονται [7].

Όπως έχει ήδη αναφερθεί, τα κυριότερα πλεονεκτήματα μιας all IP αρχιτεκτονικής είναι: ευκαμψία, αυξομειωσιμότητα και η μείωση του κόστους. Μερικά προβλήματα που παρουσιάστηκαν (QoS, κινητικότητα και bandwidth αποδοτικότητα) ακόμη επιλύονται. Η διαδικασία προτυποποίησης της all IP αρχιτεκτονικής στο UMTS έχει ήδη αρχίσει και αναμένεται να τελειώσει μέχρι την Έκδοση 5 των 3GPP προτύπων.

Ακολουθεί ένα σχήμα της προτεινόμενης All – IP UMTS αρχιτεκτονικής από την όπως την έχει αντιληφθεί η εταιρία Alcatel.



Σχήμα 4.2 [2]

Όπως φαίνεται στο σχήμα, τα PS-CN και CS-CN έχουν αντικατασταθεί από το συνενωμένο δίκτυο.

Επεξήγηση συστατικών μερών σχήματος:

- RSP (Routing Switch Platform) – λειτουργεί σαν ένα backbone front – end για circuit - switch και packet - switch domains.
- RCP (Routing Core Platform) – ένας backbone δρομολογητής τύπου μεταφορέα. Υποβοηθά την δημιουργία μεγάλων πολύ – υπηρεσιακών (multi – service) IP based οπτικών δικτύων.
- GGSN (Gateway GPRS Support Node) – παρέχει πρόσβαση σε υπηρεσίες Διαδικτύου.
- SGSN (Serving GPRS Support Node) – παρέχει τις λειτουργίες πρόσβασης κόμβου δικτύου (network access node) και διαχείριση κινητικότητας.
- MGW (Media Gateway) – παρέχει interworking αλληλεπίδραση μεταξύ των δικτύων πρόσβασης και μεταφοράς, για να ελέγχεται η ροή μέσω στο PSTN.
- MMCS (Multimedia Call Server) – υποστηρίζει και ελέγχει το VoIP (Voice IP) και sessions πολυμέσων παρέχοντας την ευελιξία να προστεθούν, τροποποιηθούν ή να διαγραφούν κομιστές που χρησιμοποιούνται από υπηρεσίες χρηστών.

- HSS (Home Subscriber Server) – μια εξέλιξη του Home Location Register. Παρέχει αποθήκευση για πληροφορίες σχετικές με τους GSM και UMTS συνδρομητές. Ο HSS συμπεριλαμβάνει επίσης την λειτουργία IP AAA και διαχειρίζεται επικοινωνία με DNS εξυπηρετητές [7].

4.4.5 Πιο συγκεκριμένη ανάλυση αρχιτεκτονικής με παρουσίαση τριών σταδίων εισαγωγής της All – IP

Η γενική UMTS All – IP αρχιτεκτονική έχει πολλά κοινά με την Έκδοση 99. Όπως και στην Έκδοση 99, αποτελείται από terminal equipment (TE) και κινητούς κόμβους που συνδέονται μέσω ενός ράδιο συστήματος (UTRAN) σε ένα Serving GPRS Support Node (SGSN). Το SGSN επικοινωνεί με άλλα SGSN ή με άλλα GGSN (Gateway GPRS Support Node). Η λειτουργία καταγραφής τοποθεσίας στο SGSN φυλάει δυο ειδών δεδομένα συνδρομητή, τις πληροφορίες του συνδρομητή και πληροφορίες τοποθεσίας [7].

Το πρώτο βήμα πιθανό να συμπεριλάβει το Mobile IP, σαν μια υπηρεσία που θα προσφέρει κινητικότητα στους UMTS κόμβους. Επιπρόσθετα, θα μπορεί να χρησιμοποιείται σαν ενδιάμεσο GPRS – Mobile IP σύστημα και για Intra System Mobility (τοπική κίνηση, μέσα στην εμβέλεια του συγκεκριμένου UMTS συστήματος). Αυτό απαιτεί Foreign Agent λειτουργίες στο GGSN και υποστήριξη Mobile IP στα κινητά τερματικά. Δεν υπάρχουν αλλαγές στην κυρίως αρχιτεκτονική και τα κινητά τερματικά δεν είναι αναγκαίο να αλλάξουν [7].

Το δεύτερο βήμα μπορεί να είναι η χρήση του Mobile IP για προσφορά GGSN handover κατά την διάρκεια ενός session. Αυτό επίσης απαιτεί υποστήριξη Mobile IP στα κινητά τερματικά αλλά θεωρούμε ότι αυτό έχει τακτοποιηθεί στο πρώτο βήμα [7].

Το τρίτο βήμα προσφέρει μια πιο δραστική αλλαγή από την τρέχουσα έκδοση και υπάρχει περισσότερη αβεβαιότητα σχετικά με μια εξέλιξη εκείνη τη στιγμή. Η λύση που παρουσιάζεται εδώ είναι η χρήση του GTP⁵ πρωτοκόλλου μόνο για έλεγχο μέσα στο κυρίως δίκτυο, καθώς για τον χρήστη θα χρησιμοποιείται καθαρό IP. Τα SGSN και GGSN θα συνενωθούν στο IGSN (Internet GPRS Support Node). Η διαχείριση της κινητικότητας, σε μακροχρόνιο επίπεδο, βασίζεται στο ότι το Mobile IP θα απαιτεί

⁵ GTP (GPRS Tunneling Protocol): Πρωτόκολλο που χρησιμοποιείται για την μεταφορά IP πακέτων μεταξύ ενός SGSN και ενός GGSN.

υποστήριξη για Mobile IP σε όλα τα κινητά τερματικά. Δεν υπάρχει καθαρή εξέλιξη από πλευράς προτυποποίησης προς αυτή την εναλλακτική λύση που παρουσιάζεται, αλλά οι πωλητές εξοπλισμού και η κοινωνία Διαδικτύου υποστηρίζουν αυτή την εξέλιξη αφού θα μειώσει το κόστος εξοπλισμού – λόγο συνένωσης των SGSN και GGSN. Υποστηρίζεται ακόμη σε αυτή την λύση, μια πιο κοντινή συνένωση των UMTS και του Διαδικτύου, λόγο χρήσης καθαρού IP [7].

4.5 IP έκδοση στο UMTS

Σύμφωνα με πηγές από το EURESCOM, η επιλογή της έκδοσης του IP δεν ήταν η πρωτεύουσα ανησυχία στην διαδικασία προτυποποίησης του UMTS. Τελευταίως όμως, το θέμα αυτό έχει γίνει περισσότερο αντικείμενο συζήτησης και είναι πολύ πιθανό ότι θα είναι αναγκαία η υποστήριξη των UMTS τερματικών τόσο του IPv4, όσο και του IPv6.

Η επιλογή της έκδοσης του πρωτοκόλλου που θα υποστηρίζεται από το UMTS δίκτυο, ίσως να αφεθεί στην κρίση του διαχειριστή του δικτύου. Είναι λογικό τότε, ότι η κρίση των διαχειριστών θα επηρεαστεί από την διαθεσιμότητα των IP διευθύνσεων, την υποστήριξη που θα παρέχεται από την βιομηχανία, από την πληρότητα του κάθε πρωτοκόλλου και τα λοιπά. Όμως, η άποψη τους θα διαμορφωθεί και από την γνώμη άλλων διαχειριστών: δηλαδή αν πολλοί διαχειριστές αποφασίσουν να τραβήξουν προς το IPv6, αυτό θα δημιουργήσει προώθηση προς καθαρά IPv6 δίκτυα [7].

Επομένως, με την πάροδο του χρόνου είναι πολύ πιθανό να: σε αρχικό στάδιο τα περισσότερα UMTS δίκτυα να βασίζονται σε διπλή στοίβα (IPv4 και IPv6) και σε μετέπειτα στάδιο να αναπτυχθούν πλήρη IPv6 δίκτυα [7].

Κεφάλαιο 5

Ανάλυση Δυνατών Σεναρίων Χρήσης UMTS με IPv6

5.1	Απαιτήσεις και Υποθέσεις	58
5.2	Σενάριο 1	59
5.3	Σενάριο 2	64
5.4	Σενάριο 3	70
5.5	Σενάριο 4	74
5.6	Σενάριο 5	77
5.7	Σενάριο 6	80
5.8	Συνοπτικός Πίνακας των Σεναρίων	85

Τώρα που έχει πλέον περιγραφεί η λειτουργία του Mobile IPv6 και οι αρχιτεκτονικές των διάφορων εκδόσεων των UMTS, χρειάζεται να δούμε πως μπορούν να δουλέψουν μαζί. Έχω εντοπίσει μετά από έρευνα έξι δυνατά σενάρια που βασίζονται στην UMTS Έκδοση 99 και Έκδοση All – IP. Τα σενάρια 5.1 και 5.2 βασίζονται στην Έκδοση 99 και τα σενάρια 5.3, 5.4, 5.5 και 5.6 βασίζονται στην Έκδοση All – IP. Τα σενάρια αυτά έχει προτείνει το EURESCOM.

5.1 Απαιτήσεις και υποθέσεις

Για να γίνει η ανάλυση των διαφορετικών σεναρίων εφικτή, έπρεπε να περιοριστεί ο αριθμός των πιθανών συνδυασμών καθορίζοντας τις ακόλουθες απαιτήσεις και υποθέσεις για το UMTS δίκτυο και τα τερματικά [7]:

- Η διασύνδεση μεταξύ UMTS τερματικών στο δίκτυο ενός UMTS διαχειριστή και UMTS δικτύων άλλων διαχειριστών πρέπει να υποστηρίζεται.
- Τα UMTS τερματικά θα ενώνονται και με IPv4 και με IPv6 hosts στο Διαδίκτυο και σε διάφορα Intranets.
- Τα UMTS κυρίως δίκτυα είναι είτε διπλής στοίβας, ή IPv6.

- Μόνο το Mobile IPv6 υποστηρίζεται για διαχείριση κινητικότητας στο UMTS δίκτυο.
- Θα είναι δυνατή η περιπλάνηση (roaming) σε άλλα UMTS δίκτυα και διπλής στοίβας και IPv6.
- Είναι δυνατό το IP handover μεταξύ home και visiting δικτύων.
- Τα τερματικά θα μπορούν να έχουν πρόσβαση και σε IPv4 και σε IPv6 based εφαρμογές.
- Απαντήσεις σε DNS queries αποφασίζουν πιο IP version θα χρησιμοποιηθεί από την εφαρμογή.
- Μόνο οι μηχανισμοί μετάβασης που απαιτούνται στο UMTS τερματικό, μέσα στο UMTS δίκτυο ή στο GGSN λαμβάνονται υπόψη, δηλαδή επιπλέον μηχανισμοί που χρησιμοποιούνται μέσα στο Διαδίκτυο δεν μελετούνται σε αυτές τις αναλύσεις.
- Μόνο υλοποιήσεις που επηρεάζουν τα στοιχεία του UMTS δικτύου και τα τερματικά θα αναλυθούν σε λεπτομέρεια.

Για κάθε περίπτωση, οι ακόλουθοι τομείς έχουν αναλυθεί σε σχέση με τα στοιχεία UMTS δικτύου και τερματικών:

- Από σημείο σε σημείο ασφάλεια
- Κινητικότητα
- DNS
- AAA (Authentication, Authorization και Accounting) υπηρεσίες
- Signaling για VoIP υπηρεσίες
- QoS

5.2 Σενάριο 1 [7]

Σε αυτό το σενάριο το UMTS δίκτυο είναι ένα non-IP aware δίκτυο και βασίζεται στην UMTS Έκδοση 99. Έτσι όλη η IP κίνηση μέσα στο UMTS δίκτυο θα γίνεται tunneled με την χρήση του GTP πρωτοκόλλου. Αυτό σημαίνει ότι τα UMTS τερματικά βλέπουν το UMTS δίκτυο σαν ένα ενδιάμεσο δίκτυο το οποίο δεν επεμβαίνει στην IP κίνηση.

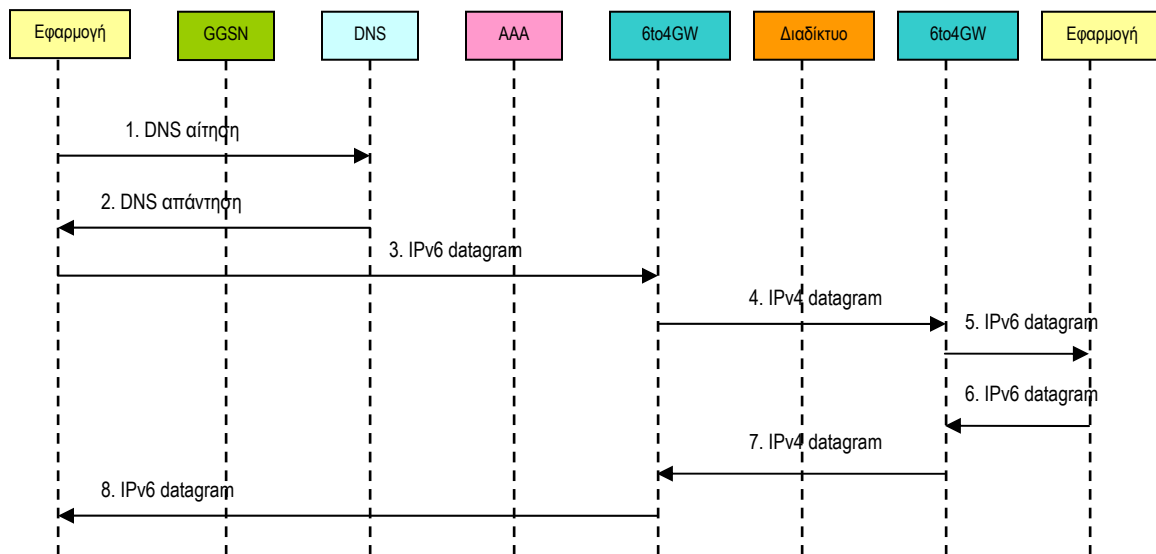
Αυτό το σενάριο είναι πιθανό να συμβεί στις αρχικές εκδόσεις των UMTS. Λόγω της έλλειψης των IPv4 διευθύνσεων, τα UMTS τερματικά και το GGSN θα δημιουργηθούν με υποστήριξη IPv6 τεχνολογίας, έτσι πολλά τερματικά θα μπορούν να τρέξουν εφαρμογές διπλής στοίβας, συνδέοντας με ένα ISP και να έχουν ένα IPv6 δίκτυο. Παρόλα αυτά, το Διαδίκτυο θα είναι ακόμη κυρίως IPv4, με IPv4 εφαρμογές καθώς θα υλοποιούνται IPv6 εφαρμογές, συστήματα και συσκευές.

Στο Σενάριο 1 χρειάζεται ένας μηχανισμός μετάβασης για να βεβαιωθεί η διασύνδεση των IPv6 τερματικών και του IPv4 Διαδικτύου. Αφού το UMTS μέρος της υποδομής έχει διπλή στοίβα, το IPv6 μπορεί λίγο πολύ να μεταδίδεται μέσα στο UMTS μέρος του δικτύου. Το κρίσιμο μέρος στο σενάριο είναι η γεφύρωση του IPv4 Διαδικτύου από το GGSN στον IPv6 εξυπηρετητή που τρέχει μια IPv6 εφαρμογή. Θεωρούμε κίνηση μεταξύ μιας IPv6 εφαρμογής που τρέχει σε ένα UMTS τερματικό διπλής στοίβας και μιας IPv6 εφαρμογής που τρέχει σε host του Διαδικτύου, διαμέσω του UMTS δικτύου και του IPv4 Διαδικτύου.

Εισηγήσεις για αυτό το σενάριο είναι η χρήση τούνελ, για παράδειγμα ένα στατικό τούνελ, το 6over4, το 6to4 κτλ. Αφού ο μηχανισμός τούνελ απαιτεί τη δημιουργία ενός τούνελ με την βοήθεια του παροχέα, αυτή δεν είναι λύση για αυτόματη διασύνδεση. Αυτό μπορεί να χρησιμοποιηθεί αν χρειάζεται, για συχνά επισκέψιμα sites, αλλά όχι για μικρά ή άγνωστα sites, αφού το κόστος διαχείρισης είναι πολύ μεγάλο. Το 6over4 χρειάζεται να υπάρχει διαθέσιμη συνέχεια μια multicast υποδομή και δεν μπορούμε να θεωρήσουμε ότι αυτό ισχύει για όλο το Διαδίκτυο, γιατί μπορεί να υπάρχουν κάποια άλλα μικρότερα δίκτυα μέσα στο Διαδίκτυο που να μην έχουν την υποδομή αυτή. Αυτή η απαίτηση δεν ισχύει για το 6to4 όπως αυτό καθορίζεται από το IETF, έτσι η πιο κατάλληλη λύση είναι η χρήση του 6to4.

5.2.1 Λειτουργία

Ακολουθεί μια περιγραφή της απαραίτητης λειτουργίας για την αρχικοποίηση και μεταφορά δεδομένων μεταξύ της IPv6 εφαρμογής και του IPv4 Διαδικτύου με την χρήση του 6to4 μηχανισμού μετάβασης.



Σημειώσεις:

- Τα τόξα που περνούν πάνω από τον GGSN αντιπροσωπεύουν κίνηση πακέτων που διοχετεύεται προς και από την UMTS εφαρμογή δια μέσω του GGSN.
- Τα τόξα που περνούν πάνω από το Διαδίκτυο αντιπροσωπεύουν κίνηση πακέτων που περνούν δια μέσω του Διαδικτύου.
- Τα τόξα που περνούν πάνω από το AAA αντιπροσωπεύουν κίνηση πακέτων που περνούν δια μέσω ενός AAA εξυπηρετητή.

Επεξήγηση Ροής Επικοινωνίας:

1. Η IPv6 εφαρμογή αρχικοποιεί ένα AAAA αίτημα προς τον DNS εξυπηρετητή του.
2. Ο DNS εξυπηρετητής απαντά είτε με μια τοπική IPv6 διεύθυνση ή με μια 6to4 διεύθυνση.
3. Η IPv6 εφαρμογή δρομολογεί το πακέτο με την IPv6 διεύθυνση προορισμού πάνω από μια τοπική IPv6 σύνδεση στο 6to4 gateway.
4. Το 6to4 gateway δρομολογεί το πακέτο πάνω από IPv4 είτε προς το 6to4 gateway προορισμού το οποίο το προωθεί στον IPv6 προορισμό, ή δρομολογεί το πακέτο σε ένα τυχαίο 6to4 gateway που γνωρίζει ότι είναι μέρος μιας μεγαλύτερης IPv6 υποδομής και θεωρεί ότι το πακέτο θα δρομολογηθεί σωστά στον IPv6 προορισμό του. Εισάγεται η τοπική IPv4 διεύθυνση σαν την διεύθυνση αποστολέα και μια εγγραφή στον εσωτερικό του πίνακα.

5. Το 6to4 gateway δρομολογεί το πακέτο είτε στην τοπική IPv6 διεύθυνση ή στην 6to4 διεύθυνση που διατηρεί για τον συγκεκριμένο IPv6 προορισμό.
6. Η IPv6 εφαρμογή εξυπηρετητή απαντά στην 6to4 IPv6 διεύθυνση αποστολέα που έλαβε από το 6to4 gateway αποστολέα. Δρομολογεί το πακέτο στο ανάλογο 6to4 gateway.
7. Το 6to4 gateway δρομολογεί το πακέτο πάνω από IPv4 στο 6to4 gateway του αποστολέα.
8. Το 6to4 gateway του αποστολέα προωθεί το πακέτο πάνω IPv6 στην UMTS υποδομή προς την διεύθυνση αποστολέα που έχει προηγουμένως εγγραφεί.

5.2.2 Μηχανισμοί μετάβασης που υποστηρίζονται

Όπως έχει προαναφερθεί, η δημιουργία τούνελ μπορεί να χρησιμοποιηθεί σε αυτό το σενάριο για να λυθεί το πρόβλημα επικοινωνίας ενός IPv6 τερματικού στο UMTS δίκτυο με ένα άλλο IPv6 τερματικό – ή με ένα εξυπηρετητή – μέσω μιας IPv4 υποδομής. Υπάρχουν όμως δυο ειδών τούνελ, τα stateful, που πρέπει να γίνουν configured και τα stateless, σαν το 6to4 και 6over4. Τα stateless τούνελ έχουν πλεονέκτημα ως προς τα stateful γιατί δεν χρειάζεται για γίνουν configured κάθε φορά από τον χρήστη. Ακολουθώντας, το 6to4 έχει πλεονέκτημα ως προς το 6over4 γιατί το δεύτερο χρειάζεται multicast υποδομή, η οποία δεν είναι διαθέσιμη στο Διαδίκτυο σήμερα. Γι' αυτό και γίνεται αναφορά στον μηχανισμό 6to4 στο σενάριο αυτό.

5.2.3 DNS και AAA

Αν ο ISP υποστηρίζει IPv6 AAA και υπάρχουν IPv6 capable DNS εξυπηρετητές δεν υπάρχει κανένα πρόβλημα στην υλοποίηση της υπηρεσίας αυτής.

5.2.4 Κινητικότητα

Έχει γίνει η υπόθεση ότι δεν υποστηρίζεται IP κινητικότητα στο σενάριο αυτό, λόγω του ότι το UMTS δίκτυο είναι Non – IP aware. Μπορεί να θεωρηθεί ότι στο packet switched mode of operation της UMTS αρχιτεκτονικής, η κινητικότητα υποστηρίζεται με την χρήση GPRS standards.

5.2.5 Ασφάλεια

Αφού το 6to4 παρέχει end-to-end επικοινωνία στο IPv4, οι IPsec μηχανισμοί μπορούν να χρησιμοποιηθούν.

5.2.6 Σήμανση (Signaling)

Στο σενάριο αυτό το UMTS δίκτυο δεν υποστηρίζει IP σήμανση. Όμως μπορεί να χρησιμοποιηθεί το SIP με το 6to4, αφού η σήμανση γίνεται σε IPv6, το οποίο παρέχεται end-to-end.

5.2.7 Υποστήριξη QoS

Το QoS μπορεί να χρησιμοποιηθεί με το 6to4, αν τόσο το IPv4 όσο και το IPv6 δίκτυο υποστηρίζουν τις ίδιες κλάσεις υπηρεσιών. Ο 6to4 δρομολογητής θα πρέπει να κάνει το mapping για το IPv4 μέρος της αλληλεπίδρασης. Για να γίνει αυτό, ο δρομολογητής χρειάζεται να μελετήσει την κίνηση που περνά από τούνελ για τα RSVP μηνύματα σήμανσης. Αφού δεν είναι γνωστό το κόστος αυτής της διαδικασίας με πραγματικό εξοπλισμό δικτύου, η μεγαλύτερη πιθανότητα είναι ότι θα μειώσει την QoS απόδοση.

5.2.8 Συμπεράσματα

Το σενάριο αυτό μπορεί εύκολα να υποστηρικτεί, γιατί χρησιμοποιούνται πολύ απλοί μηχανισμοί μετάβασης και προσιτή υποδομή και αναμένεται να είναι ένα από τα πρώτα σενάρια που θα υλοποιηθούν παράλληλα την υλοποίηση του IPv6. Θα βοηθήσει καινούργιες IPv6 εφαρμογές να επικοινωνούν με τον IPv4 δικτυακό κόσμο. Η χρήση του 6to4 είναι απαραίτητη σε περιπτώσεις που όπου πρόσβαση προς τον παραλήπτη host ή δίκτυο είναι εφικτή μόνο με IPv4 υποδομή. Παρόλα αυτά, ο αριθμός των hosts και συγκεκριμένα των sites εξυπηρετητών, που χρησιμοποιούν IPv6 αλλά δεν είναι ενωμένα ακόμη με την παγκόσμια IPv6 υποδομή, είναι κατά πάσα πιθανότητα ελάχιστος. Έτσι φαίνεται ότι είναι καλύτερη η σύνδεση της UMTS υποδομής απευθείας με την παγκόσμια IPv6 υποδομή και να γίνεται χρήση των παγκόσμια αποδεκτών unicast IPv6 διευθύνσεων. Η υποστήριξη από το 6to4 μπορεί να είναι μια προσωρινή λύση αρχικά για ορισμένα sites.

5.3 Σενάριο 2 [7]

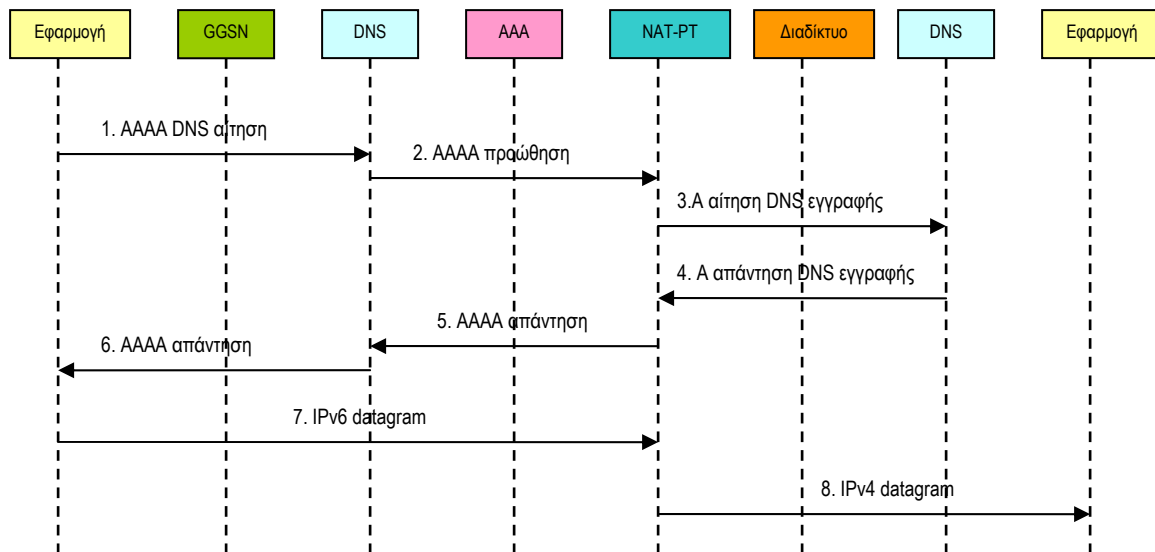
Και σε αυτό το σενάριο το UMTS δίκτυο είναι ένα non-IP aware δίκτυο και βασίζεται στην UMTS Έκδοση 99. Έτσι ξανά, όλη η IP κίνηση μέσα στο UMTS δίκτυο θα γίνεται tunneled με την χρήση του GTP πρωτοκόλλου και όπως και πριν τα UMTS τερματικά βλέπουν το UMTS δίκτυο σαν ένα ενδιάμεσο δίκτυο το οποίο δεν επεμβαίνει στην IP κίνηση.

Κι αυτό το σενάριο είναι πιθανό να συμβεί στις αρχικές εκδόσεις των UMTS και πάλι λόγω έλλειψης των IPv4 διευθύνσεων, τα UMTS τερματικά και το GGSN θα δημιουργηθούν με υποστήριξη IPv6 τεχνολογίας. Όμως όπως έχει προαναφερθεί, το Διαδίκτυο θα είναι ακόμη κυρίως IPv4, με IPv4 εφαρμογές καθώς θα υλοποιούνται IPv6 εφαρμογές, συστήματα και συσκευές. Θεωρούμε κίνηση μεταξύ μιας είτε IPv6 εφαρμογής ή εφαρμογή διπλής στοίβας που τρέχει σε ένα UMTS τερματικό διπλής στοίβας και μιας IPv4 εφαρμογής που τρέχει σε host του Διαδικτύου, διαμέσω του UMTS δικτύου, ενός IPv6 ISP και του IPv4 Διαδικτύου.

Κι εδώ χρειάζονται κάποιοι μηχανισμοί μετάβασης για να βεβαιωθεί η διασύνδεση του UMTS τερματικού με το IPv4 Διαδίκτυο. Σε αυτό το σενάριο θα μελετηθούν οι μηχανισμοί NAT-PT και DSTM. Θα μελετηθεί επίσης πως ο DNS εξυπηρετητής δουλεύει με αυτές τις δυο περιπτώσεις καθώς και άλλα θέματα όπως ασφάλεια, QoS, σήμανση κτλ.

5.3.1 Λειτουργία

Πιο κάτω περιγράφετε η λειτουργία που χρειάζεται για να αρχικοποιηθούν και να μεταφερθούν δεδομένα μεταξύ της IPv6 εφαρμογής και του IPv4 Διαδικτύου όταν χρησιμοποιείται το NAT-PT σαν ο μηχανισμός μετάβασης. Το NAT-PT μπορεί να χρησιμοποιηθεί ακόμη κι αν η εφαρμογή του UMTS host είναι μια εφαρμογή διπλής στοίβας ή είναι μια καθαρά IPv6 εφαρμογή.



Σημειώσεις:

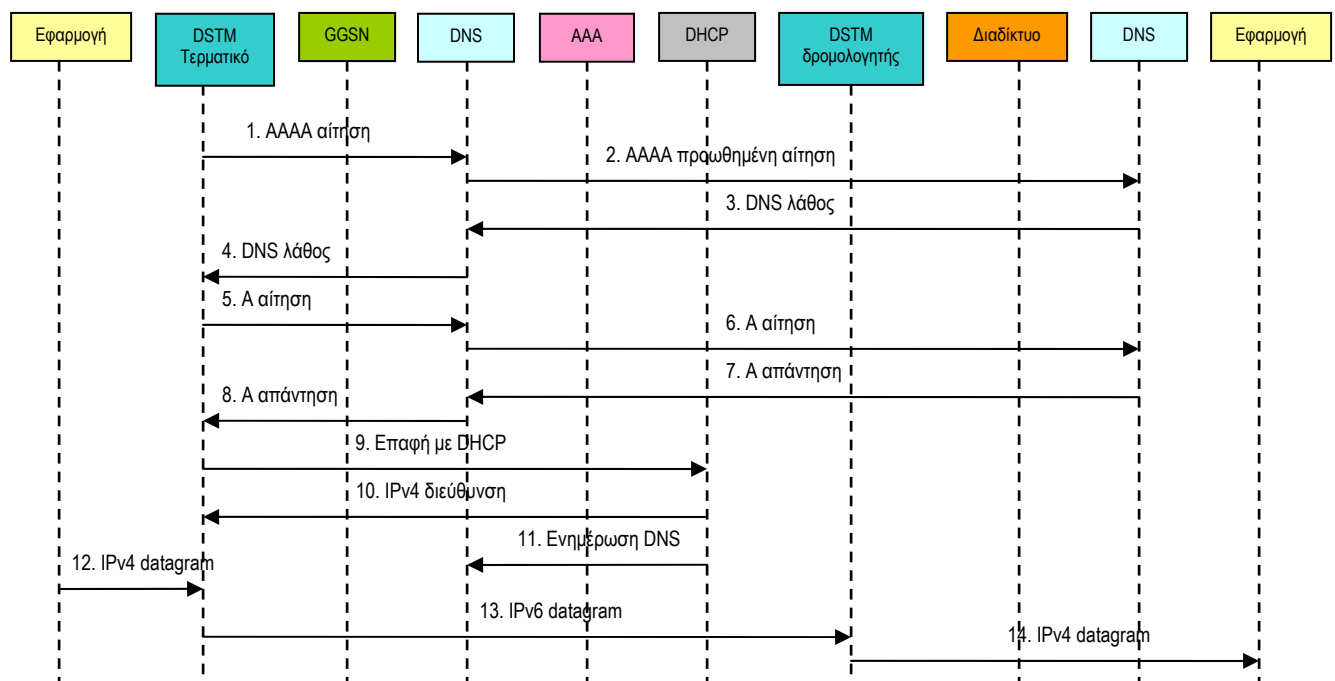
- Τα τόξα που περνούν πάνω από τον GGSN αντιπροσωπεύουν κίνηση πακέτων που διοχετεύεται προς και από την UMTS εφαρμογή δια μέσω του GGSN.
- Τα τόξα που περνούν πάνω από το Διαδίκτυο αντιπροσωπεύουν κίνηση πακέτων που περνούν δια μέσω του Διαδικτύου.
- Τα τόξα που περνούν πάνω από το AAA αντιπροσωπεύουν κίνηση πακέτων που περνούν δια μέσω ενός AAA εξυπηρετητή.

Επεξήγηση Ροής Επικοινωνίας:

1. Η IPv6 εφαρμογή αρχικοποιεί μία AAAA αίτηση προς τον DNS εξυπηρετητή της.
2. Ο DNS εξυπηρετητής έχει μια διεύθυνση συσχετισμένη με την αίτηση της IPv6 εφαρμογής και την προωθεί προς τον NAT-PT.
3. Ο NAT-PT μεταφράζει την AAAA αίτηση σε μια Α αίτηση με μια IPv4 διεύθυνση που έχει στο pool του και μετά την προωθεί σε ένα IPv4 DNS εξυπηρετητή.
4. Ο DNS εξυπηρετητής απαντά με μια Α εγγραφή και μια IPv4 διεύθυνση που είναι συσχετισμένη με την εγγραφή αυτή.
5. Ο NAT-PT μεταφράζει την εγγραφή σε μια AAAA εγγραφή και μεταφράζει την IPv4 διεύθυνση σε μια IPv6 διεύθυνση.
6. Η AAAA εγγραφή και η IPv6 διεύθυνση προωθούνται στην IPv6 εφαρμογή.

7. Το IPv6 πακέτο στέλνεται στο NAT-PT, όπου και μεταφράζεται κατάλληλα.
8. Το μεταφρασμένο IPv4 πακέτο φτάνει στην IPv4 εφαρμογή.

Το DSTM μπορεί να χρησιμοποιηθεί μόνο αν η εφαρμογή του UMTS host είναι μια εφαρμογή διπλής στοίβας. Όταν το DSTM χρησιμοποιηθεί σαν ο μηχανισμός μετάβασης μεταξύ του UMTS δικτύου και του IPv4 Διαδικτύου τότε η ακόλουθη λειτουργία μπορεί να αρχικοποιηθεί για το IPv6 δίκτυο για να επικοινωνεί με το IPv4 Διαδίκτυο.



Σημειώσεις:

- Τα τόξα που περνούν πάνω από τον GGSN αντιπροσωπεύουν κίνηση πακέτων που διοχετεύεται προς και από την UMTS εφαρμογή δια μέσω του GGSN.
- Τα τόξα που περνούν πάνω από το Διαδίκτυο αντιπροσωπεύουν κίνηση πακέτων που περνούν δια μέσω του Διαδικτύου.
- Τα τόξα που περνούν πάνω από το AAA αντιπροσωπεύουν κίνηση πακέτων που περνούν δια μέσω ενός AAA εξυπηρετητή.

Επεξήγηση Ροής Επικοινωνίας:

1. Το τερματικό στέλνει μια AAAA αίτηση στον DNS εξυπηρετητή.
2. Ο DNS εξυπηρετητής προωθεί την AAAA αίτηση στον πρωτεύων DNS εξυπηρετητή.
3. (3 και 4) Ο DNS επιστρέφει λάθος γιατί η εφαρμογή παραλήπτης δεν υποστηρίζει IPv6.
5. Το τερματικό στέλνει μια A εγγραφή στον DNS εξυπηρετητή.
6. (6, 7 και 8) Η DNS απάντηση είναι μια A αίτηση που συσχετίζεται μια IPv4 διεύθυνση.
9. Το DSTM τερματικό επικοινωνεί με τον DHCP εξυπηρετητή για να του ανατεθεί μια IPv4 διεύθυνση.
10. Ο DHCP εξυπηρετητής αναθέτει στο τερματικό μια IPv4 διεύθυνση.
11. Ο DHCP εξυπηρετητής επικοινωνεί με τον DNS εξυπηρετητή για να ενημερώσει την DNS εγγραφή με την καινούργια IPv4 διεύθυνση που έχει ανατεθεί στο τερματικό.
12. Η εφαρμογή στέλνει ένα IPv4 datagram στο DSTM τερματικό.
13. Το DSTM τερματικό encapsulates το IPv4 datagram σε ένα IPv6 datagram και το μεταφέρει στον DSTM δρομολογητή.
14. Ο DSTM δρομολογητής decapsulates το datagram και το προωθεί προς την IPv4 εφαρμογή.

5.3.2 Μηχανισμοί Μετάβασης που υποστηρίζονται

Σε αυτό το σενάριο μπορούν να χρησιμοποιηθούν δύο μηχανισμοί μετάβασης: το NAT-PT και το DSTM. Με το NAT-PT δεν έχει σημασία αν η εφαρμογή του UMTS host είναι διπλής στοίβας ή καθαρά IPv6, ενώ το DSTM μπορεί να χρησιμοποιηθεί μόνο σε εφαρμογές που χρησιμοποιούν διπλή στοίβα. Το NAT-PT επιτρέπει σε τοπικούς IPv6 hosts και εφαρμογές να επικοινωνούν με IPv4 hosts και εφαρμογές και αντίστροφα.

Μια NAT-PT συσκευή βρίσκεται στα σύνορα των IPv4 και IPv6 δικτύων. Άρα το NAT-PT κουτί θα βρίσκεται μεταξύ του καθαρά IPv6 δικτύου και του IPv4

Διαδικτύου. Τα πλεονεκτήματα του NAT-PT σε αυτό το σενάριο είναι ότι: είναι μια απλή λύση από μεριά υλοποίησης και διαχείρισης και παρέχει πρόσβαση στο IPv4 Διαδίκτυο. Χρησιμοποιείται μόνο στο backbone δίκτυο κι έτσι καμία τροποποίηση δεν χρειάζεται στα κινητά τερματικά. Ακόμη, δεν υπάρχει επιπλέον κόστος για encapsulation των πακέτων δια μέσου της ράδιο διαπροσωπίας γιατί το NAT-PT δεν χρησιμοποιεί καμία τεχνική δημιουργίας τούνελ. Όμως το NAT-PT έχει και αρκετά μειονεκτήματα. Το κυριότερο είναι ότι το NAT-PT καθιστά την end-to-end ασφάλεια πολύ δύσκολη, αν όχι αδύνατη, να υλοποιηθεί μέσα στο δίκτυο. Επιπλέον, η μετάφραση μπορεί να γίνει σε μια “best effort” προσέγγιση, λόγω στις σημαντικές διαφορές μεταξύ των IPv4 και IPv6 headers που προκαλούν καθυστερήσεις στην μετάφραση.

Το DSTM μπορεί επίσης να χρησιμοποιηθεί σαν μηχανισμό μετάβασης. Για να γίνει αυτό όμως, είναι αναγκαίος ένας DHCPv6 εξυπηρετητής. Ο εξυπηρετητής μπορεί να χρησιμοποιηθεί σε συνύπαρξη με τον DNS για να παρέχει IPv4 διευθύνσεις στον DSTM client και το UMTS τερματικό στο σενάριο αυτό. Τα πλεονεκτήματα του DSTM είναι ότι η end-to-end ασφάλεια στα network και transport layer μπορεί να διατηρηθεί και ότι μέρη της IPv4/ IPv6 μετάφρασης μπορεί να διανεμηθεί ανάμεσα στα UMTS τερματικά. Τα μειονεκτήματα του DSTM είναι ότι τα UMTS τερματικά πρέπει να υποστηρίζουν DSTM και παρουσιάζεται επιπλέον κόστος στην ράδιο διαπροσωπία αφού τα IPv4 πακέτα γίνονται encapsulated σε IPv6.

5.3.3 DNS και AAA

Αν ο ISP υποστηρίζει IPv6 AAA και IPv6 capable DNS εξυπηρετητές δεν υπάρχει πρόβλημα άσχετα από τον μηχανισμό μετάβασης που χρησιμοποιείται για την υλοποίηση της υπηρεσίας.

5.3.4 Κινητικότητα

Δεν υποστηρίζεται IP κινητικότητα στο σενάριο αυτό, για τους ίδιους λόγους που δεν υποστηρίζεται και στο Σενάριο 1.

5.3.5 Ασφάλεια

Με το NAT-PT η end-to-end ασφάλεια στα network και transport layers δεν είναι δυνατή, έτσι δεν μπορεί να υλοποιηθεί ασφάλεια στο δίκτυο. Αντίθετα, με το DSTM μπορούν να χρησιμοποιηθούν διάφοροι μηχανισμοί για παροχή ασφαλείας, σαν το IPsec, αφού το DSTM δεν σπάζει την ασφαλή end-to-end επικοινωνία σε καμία στιγμή.

5.3.6 Σήμανση

Σε αυτό το σενάριο το UMTS δεν υποστηρίζει IP σήμανση. Το SIP όμως μπορεί να χρησιμοποιηθεί με το DSTM αφού τα IPv4 πακέτα μπορούν να περάσουν μέσω τούνελ πάνω από το IPv6 δίκτυο. Έτσι οι IPv4 εφαρμογές μπορούν να συνδεθούν με ένα IPv4 SIP εξυπηρετητή και να δημιουργήσουν μια σύνδεση με ένα IPv4 host. Με το NAT-PT μπορεί επίσης να χρησιμοποιηθεί το SIP, αλλά θα χρειαστεί και κάποιες επιπρόσθετες λειτουργικές μονάδες για να χειρίζεται τα SIP μηνύματα.

5.3.7 Υποστήριξη QoS

Το QoS θα μπορούσε να χρησιμοποιηθεί με το DSTM αν και το IPv4 και το IPv6 δίκτυο υποστηρίζουν τις ίδιες κλάσεις υπηρεσιών. Με το NAT-PT είναι ακόμη ένα ανοικτό θέμα αφού οι πληροφορίες για τα πεδία του QoS δεν έχουν ακόμη προτυποποιηθεί. Αν τα πεδία του QoS είναι ακόμη τα ίδια μετά από την μετάφραση από IPv4 σε IPv6 ή από IPv6 σε IPv4, τότε δεν θα δημιουργηθούν προβλήματα.

5.3.8 Συμπεράσματα

Όπως και με το προηγούμενο σενάριο και το σενάριο 2 μπορεί εύκολα να υποστηρικτεί για τους ίδιους λόγους και θα είναι ένα από τα πρώτα σενάρια που θα υλοποιηθούν και θα βοηθήσει καινούργιες IPv6 εφαρμογές να επικοινωνούν με τον IPv4 δικτυακό κόσμο. Η λύση με το NAT-PT έχει το πλεονέκτημα ότι ο μηχανισμός αυτός είναι κεντρικός και κατά συνέπεια εύκολος στην υλοποίηση και διαχείρισή του. Ακόμη, είναι εντελώς διαφανής προς τους χρήστες. Το κυριότερο πρόβλημα με αυτή τη λύση είναι ότι δεν προσφέρεται ασφάλεια στο δίκτυο. Με την DSTM λύση, μπορεί να υπάρξει ασφάλεια δια μέσω του δικτύου αλλά είναι πολύπλοκη για υλοποίηση και κάθε UMTS τερματικό θα πρέπει να υποστηρίζει διπλή στοίβα. Πρέπει επίσης να

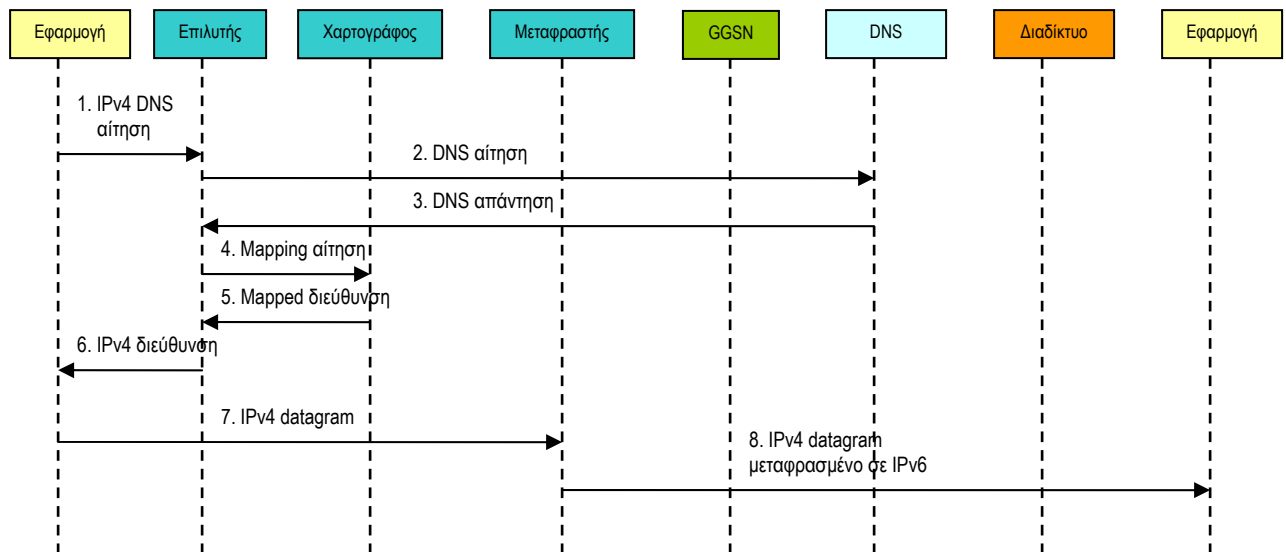
παρατηρηθεί η διαφορά στον αριθμό των μηνυμάτων σήμανσης πριν την εγκαθίδρυση σύνδεσης, με την χρήση των δύο μηχανισμών μετάβασης (με το NAT-PT είναι 6, με το DSTM είναι 11) καθώς αυτή η καθυστέρηση μπορεί να είναι σημαντική. Το NAT-PT μπορεί να είναι η καλύτερη λύση αρχικά γιατί είναι πιο εύκολο να υλοποιηθεί και αργότερα να εφαρμοστεί το DSTM αφού δεν χρειάζεται επιπρόσθετες λειτουργικές μονάδες για την σήμανση και παρέχεται ασφάλεια δια μέσω του δικτύου.

5.4 Σενάριο 3 [7]

Σε αυτό το σενάριο το UMTS δίκτυο είναι IP aware. Αυτό σημαίνει ότι το UMTS δίκτυο υποστηρίζει SIP σήμανση, αλλά τα IP δεδομένα μέσα στο κυρίως δίκτυο ακόμα περνούν μέσω ενός τούνελ με το GTP πρωτόκολλο. Το σενάριο αυτό συσχετίζεται με την Έκδοση 00 των UMTS. IP κινητικότητα δεν υποστηρίζεται σαν μέρος του UMTS δικτύου αλλά μπορεί να χρησιμοποιηθεί για μετακίνηση μεταξύ δύο GGSNs. Το σενάριο αντικατοπτρίζει την κατάσταση όπου τα UMTS τερματικά θα τρέχουν IPv4 εφαρμογές παρά το γεγονός ότι το UMTS δίκτυο και το Διαδίκτυο θα χρησιμοποιούν πλέον IPv6. Θεωρούμε κίνηση μεταξύ μιας IPv4 εφαρμογής που τρέχει σε ένα UMTS IPv6 τερματικό και μιας IPv6 εφαρμογής που τρέχει σε host του Διαδικτύου, διαμέσω του IPv6 UMTS δικτύου και του IPv6 Διαδικτύου. Αυτό είναι πιθανό να συμβεί και όταν δύο UMTS τερματικά επικοινωνούν μεταξύ τους και μόνο το ένα από τα δύο χρησιμοποιεί μια IPv6 based εφαρμογή.

5.4.1 Λειτουργία

Αφού το UMTS δίκτυο είναι πλέον IPv6, η μετάφραση από IPv4 σε IPv6 πρέπει να υποστηρίζεται από το τερματικό και η προτυποποιημένη μέθοδος για αυτή τη διαδικασία είναι η bump-in-the-stack. Η ακολουθία για επικοινωνία είναι τότε η εξής:



Σημειώσεις:

- Τα τόξα που περνούν πάνω από τον GGSN αντιπροσωπεύουν κίνηση πακέτων που διοχετεύεται προς και από την UMTS εφαρμογή δια μέσω του GGSN.
- Τα τόξα που περνούν πάνω από το Διαδίκτυο αντιπροσωπεύουν κίνηση πακέτων που περνούν δια μέσω του Διαδικτύου.

Επεξήγηση Ροής Επικοινωνίας:

1. Η εφαρμογή ζητά μια IPv4 διεύθυνση.
2. Ο BIS (Bump In the Stack) επιλυτής διευθύνσεων στέλνει μια DNS αίτηση.
3. Ο DNS επιστρέφει μια IPv6 διεύθυνση στον επιλυτή.
4. Ο επιλυτής ζητά από τον χαρτογράφο διευθύνσεων να του παρέχει μια IPv4 διεύθυνση.
5. Ο επιλυτής παραλαμβάνει μια IPv4 διεύθυνση.
6. Η χαρτογραφημένη IPv4 διεύθυνση δίνεται στην εφαρμογή.
7. Το IPv4 πακέτο στέλνεται στον BIS μεταφραστή ο οποίος το μεταφράζει σε ένα IPv6 πακέτο.
8. Το IPv6 πακέτο στέλνεται στον ανάλογο host.

5.4.2 Μηχανισμοί μετάβασης που υποστηρίζονται

Ο μοναδικός μηχανισμό μετάβασης σε αυτό το σενάριο είναι ο BIS. Ο BIS παρέχει τόσο χαρτογράφηση διεύθυνσης, όσο και λειτουργία μετάφρασης μεταξύ IPv4 και

IPv6. Αυτός ο μηχανισμός μπορεί να είναι ιδιαίτερα χρήσιμος στο αρχικό στάδιο της υλοποίησης του IPv6, όταν μερικές εφαρμογές δεν θα αλλάξουν σε IPv6. Αυτή η τεχνική γίνεται για να επιτρέπεται σε εφαρμογές που τρέχουν σε ένα host να επικοινωνούν και με IPv4 και με IPv6 hosts. Το BIS μπορεί να συνδυαστεί με άλλες τεχνικές μετάβασης. Είναι επίσης δυνατό να χρησιμοποιηθεί ένας ιδιωτικός χώρος διευθύνσεων για τις προσωρινές IPv4 διευθύνσεις, αφού ένας BIS host τις χρησιμοποιεί μόνο τοπικά.

Με τον BIS δεν χρειάζεται να γίνουν καθόλου αλλαγές στο δίκτυο και μόνο στα τερματικά που τρέχουν και IPv4 και IPv6 εφαρμογές θα πρέπει να εφαρμοστεί το BIS. Ακόμη, αφού το BIS υλοποιείται μόνο στα τερματικά είναι πολύ αυξομειώσιμο, αλλά η δυσκολία διαχείρισης μπορεί να είναι σημαντική ανάλογα με τον αριθμό των BIS hosts.

Το BIS είναι έγκυρο μόνο για unicast κίνηση και δεν θα δουλέψει όταν IPv4 ή IPv6 επιλογές χρησιμοποιούνται. Αυτό συμβαίνει γιατί είναι αδύνατη η μετάφραση μεταξύ των διαφορετικών επιλογών. Όπως και με άλλες NAT λύσεις, η IP μετατροπή δεν μπορεί να μεταφράσει διευθύνσεις, που είναι εμπεδωμένες σε πρωτόκολλα του application layer που συναντιόνται συνήθως στο FTP. Αυτό αντιμετωπίζεται με συγκεκριμένα Application Layer Gateways (ALGs) για κάθε εφαρμογή, τα οποία πρέπει να υλοποιηθούν σε κάθε BIS host.

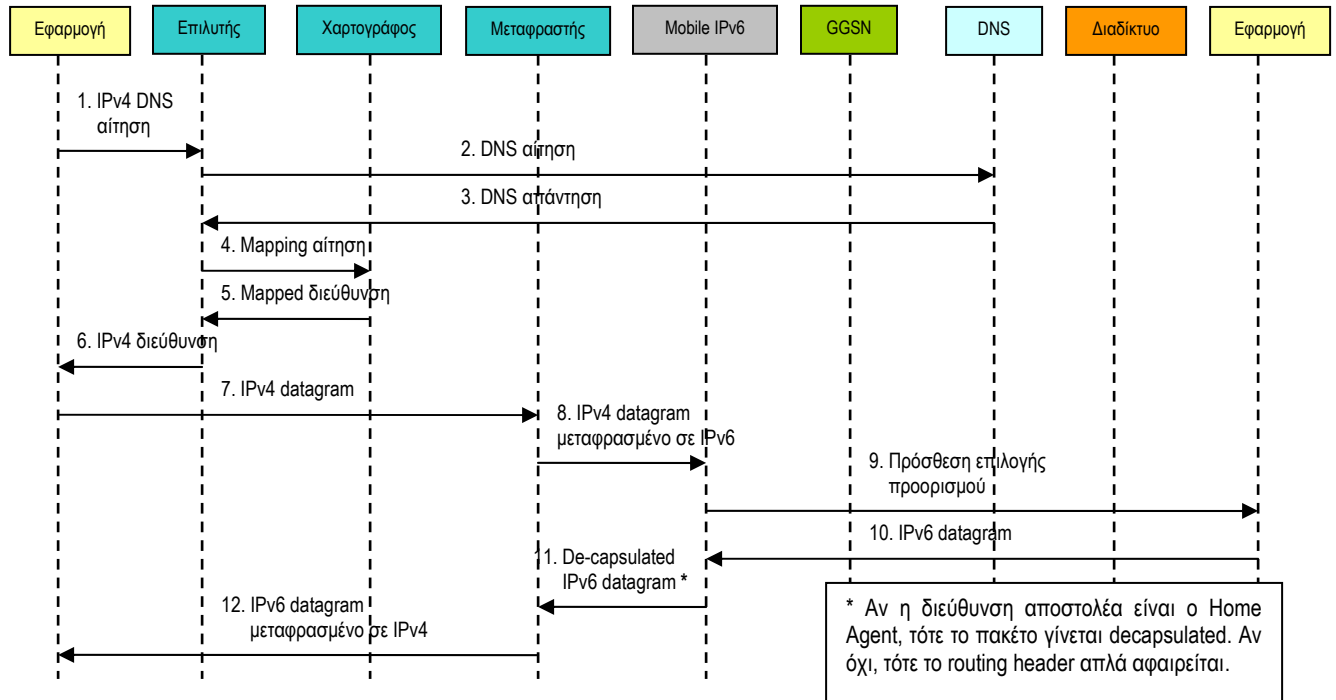
Ο BIS μηχανισμός μετάβασης μπορεί να παίξει σημαντικό ρόλο στην μετάβαση από IPv4 σε IPv6, ειδικά στην αρχική φάση - που θα υπάρχει έλλειψη τοπικών IPv6 εφαρμογών - και στην τελική φάση - που θα υπάρχει έλλειψη τοπικών IPv4 εφαρμογών.

5.4.3 DNS και AAA

Το δίκτυο θεωρείται ένα IPv6 δίκτυο με την μόνη διαφορά ότι τα τερματικά έχουν IPv4 διευθύνσεις. Έτσι τα AAA και DNS δεν αποτελούν κανένα πρόβλημα.

5.4.4 Κινητικότητα

Το Mobile IPv6 θα μπορεί να χρησιμοποιηθεί σε συνδυασμό με το BIS, αφού οι IPv4 διευθύνσεις είναι τοπικές προς τον IPv6 host και δεν επηρεάζουν την φάση του handover. Αυτό παρουσιάζεται στο πιο κάτω διάγραμμα:



5.4.5 Ασφάλεια

Οι hosts μπορούν να χρησιμοποιήσουν την ασφάλεια σε όλα τα layers, σαν την συνηθισμένη IPv4 επικοινωνία, όταν επικοινωνούν με IPv4 hosts χρησιμοποιώντας IPv4 εφαρμογές με την χρήση του BIS μηχανισμού. Παρόμοια, μπορούν να χρησιμοποιήσουν την ασφάλεια όλων των layers σαν την συνηθισμένη IPv6 επικοινωνία, όταν επικοινωνούν με IPv6 hosts χρησιμοποιώντας IPv6 εφαρμογές μέσω της πλήρης IPv6 στοίβας. Όμως, δεν μπορούν να υλοποιήσουν την ασφάλεια πάνω από το network layer όταν επικοινωνούν με IPv6 hosts χρησιμοποιώντας IPv4 εφαρμογές μέσω του μηχανισμού μετάβασης. Ο λόγος είναι γιατί όταν κωδικοποιούνται τα δεδομένα πρωτοκόλλου με τα οποία εμπεδώνονται οι IP διευθύνσεις, ή όταν κωδικοποιούνται χρησιμοποιώντας IP διευθύνσεις σαν κλειδιά, είναι αδύνατο για τον μηχανισμό να μεταφράσει τα IPv4 δεδομένα σε IPv6 και αντίστροφα.

5.4.6 Σήμανση

Σε αυτό το σενάριο το UMTS δίκτυο χρησιμοποιεί το SIP για σήμανση. Έτσι τυπικές IPv6 εφαρμογές μπορούν να χρησιμοποιήσουν το SIP χωρίς πρόβλημα. Αν ο BIS μεταφραστής μπορεί να μεταφράσει τα πεδία της IP διεύθυνσης τα οποία εμπεδώνονται στο SIP μήνυμα, οι IPv4 εφαρμογές μπορούν να χρησιμοποιήσουν το SIP για να στέλνουν σήμα σε IPv6 hosts για session set-up. Αυτό απαιτεί ο BIS μηχανισμός να μπορεί να κοιτάζει μέσα στο ωφέλιμο φορτίο (payload).

5.4.7 Υποστήριξη QoS

Το QoS βασίζεται σε Διαφοροποιημένες Υπηρεσίες (Differentiated Services) οι οποίες μπορούν να υποστηριχτούν αν ο BIS μηχανισμός μετάφρασης αντιγράφει το DSCP¹ πεδίο από το header του IPv4 πακέτου στο header του IPv6 πακέτου. Η χρήση των Συνενωμένων Υπηρεσιών (Integrated Services) μπορεί επίσης να υποστηρικτεί, αλλά απαιτεί μετάφραση των RSVP μηνυμάτων.

5.4.8 Συμπεράσματα

Αυτό το σενάριο είναι πιθανό να χρησιμοποιηθεί στην δεύτερη φάση υλοποίησης των UMTS, όπου υπάρχοντα UMTS τερματικά θα υποστηρίζουν IPv4 εφαρμογές, αλλά οι περισσότερες UMTS εφαρμογές θα χρησιμοποιούν IPv6. Υπάρχουν μερικά προβλήματα με την χρήση του BIS, αφού κάθε τερματικό πρέπει να περιέχει το BIS λογισμικό και επιπλέον μεταφραστές για FTP, SIP κτλ. Παρόλα αυτά, το BIS είναι μια καλή λύση και ένα πολύτιμο εργαλείο για χρήση παλαιών IPv4 εφαρμογών σε IPv6 περιβάλλοντα.

5.5 Σενάριο 4 [7]

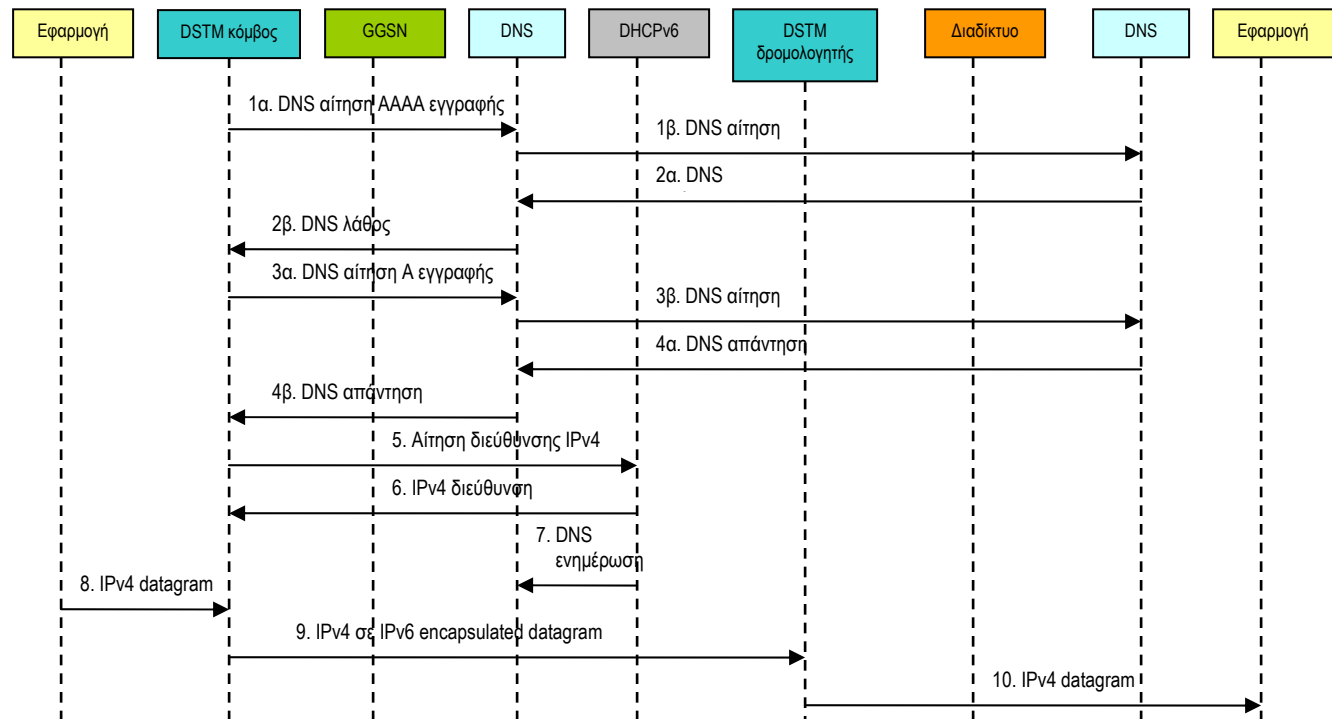
Σε αυτό το σενάριο, το UMTS δίκτυο είναι IPv6 based αλλά το Διαδίκτυο είναι ακόμη IPv4 based. Το UMTS υποστηρίζει SIP σήμανση, αλλά τα IP δεδομένα ακόμη περνούν από τούνελ μέσω του GTP πρωτοκόλλου. Αυτό συσχετίζεται με την δεύτερη φάση εισαγωγής των UMTS και βασίζεται στην Έκδοση 00. Η IP κινητικότητα δεν υποστηρίζεται σαν μέρος του UMTS δικτύου, αλλά μπορεί να χρησιμοποιηθεί για

¹ DSCP (Differentiated Services CodePoint): Καθορίζει την per-hop-behavior ενός πακέτου.

μετακίνηση μεταξύ δύο GGSNs. Τόσο οι IPv4 όσο και οι IPv6 εφαρμογές μπορούν να υποστηριχτούν στο κινητό τερματικό. Ένα τερματικό διπλής στοίβας είναι αναγκαίο γιατί το Διαδίκτυο είναι ακόμη κυρίως IPv4, με IPv4 εφαρμογές ακόμη κι αν το UMTS δίκτυο χρησιμοποιεί IPv6. Θεωρούμε κίνηση μεταξύ μιας IPv4 εφαρμογής που τρέχει σε ένα UMTS τερματικό διπλής στοίβας και μιας IPv4 εφαρμογής που τρέχει σε ένα Host του Διαδικτύου, διαμέσω του IPv6 UMTS δικτύου και του IPv4 Διαδικτύου.

5.5.1 Λειτουργία

Πιο κάτω περιγράφονται οι απαραίτητες λειτουργίες για αρχικοποίηση και μεταφορά δεδομένων μεταξύ των δύο IPv4 εφαρμογών.



Σημειώσεις:

- Τα τόξα που περνούν πάνω από τον GGSN αντιπροσωπεύουν κίνηση πακέτων που διοχετεύεται προς και από την UMTS εφαρμογή δια μέσω του GGSN.
- Τα τόξα που περνούν πάνω από το Διαδίκτυο αντιπροσωπεύουν κίνηση πακέτων που περνούν δια μέσω του Διαδικτύου.

Επεξήγηση Ροής Επικοινωνίας:

1. Ο host ζητάει την IPv6 διεύθυνση του αντίστοιχου κόμβου.
2. Ο DNS επιστρέφει λάθος γιατί ο αντίστοιχος κόμβος δεν υποστηρίζει IPv6.
3. Ο DSTM host ζητάει μια IPv4 διεύθυνση.
4. Η IPv4 διεύθυνση του αντίστοιχου κόμβου επιστρέφεται.
5. Ο DSTM host ζητάει από τον DHCP εξυπηρετητή για μια δυναμική IPv4 διεύθυνση.
6. Επιστρέφεται η IPv4 διεύθυνση.
7. Ο DHCP εξυπηρετητής ενημερώνει την DNS εγγραφή για την καινούργια IPv4 διεύθυνση του DSTM host.
8. Η εφαρμογή φτιάχνει ένα IPv4 datagram.
9. Ο DSTM κόμβος κάνει encapsulate το IPv4 datagram σε IPv6 και το μεταδίδει στον DSTM δρομολογητή.
10. Ο DSTM δρομολογητής de-encapsulates το πακέτο και το προωθεί προς τον αντίστοιχο IPv4 κόμβο.

5.5.2 Μηχανισμοί Μετάβασης που Υποστηρίζονται

Υπάρχουν δύο πιθανοί τρόποι επικοινωνίας που μπορούν να χρησιμοποιηθούν για επικοινωνία του IPv6 UMTS με IPv4 εφαρμογές. Ένας είναι ο BIS στο κινητό τερματικό και το NAT-PT στο GGSN. Άλλος τρόπος είναι η χρήση DSTM για εγκαθίδρυση μιας end-to-end IPv4 επικοινωνίας μεταξύ του κινητού εξυπηρετητή με διπλή στοίβα και του IPv4 εξυπηρετητή.

5.5.3 DNS και AAA

Όπως και στο Σενάριο 2, ο DSTM μηχανισμός είναι διαφανής ως προς το DNS και AAA. Έτσι το θέμα του DNS και των AAA αφορά τον ISP.

5.5.4 Κινητικότητα

Η κίνηση ενός UMTS κόμβου με χρήση IPv6 και DSTM έχει περιγραφεί στο κεφάλαιο 3, στο μέρος που αφορά τους διάφορους μηχανισμούς μετάβασης. Όταν ο κινητός κόμβος αλλάζει default δρομολογητή, απλά στέλνει ένα Binding Update στο τελικό

σημείο του τούνελ (Tunnel End Point – TEP) του DSTM εξυπηρετητή. Πρέπει να ληφθεί υπόψη όμως ότι η διακίνηση (roaming) μεταξύ UMTS διαχειριστών απαιτεί οι AAA εξυπηρετητές να συμπεριλαμβάνονται στην διαδικασία διακίνησης.

5.5.5 QoS υποστήριξη

Τα QoS που βασίζονται στις Διαφοροποιημένες Υπηρεσίες μπορούν να υποστηριχθούν αν ο DSRM δρομολογητής αντιγράφει τα DSCP πεδία από το header του IPv6 πακέτου στο header του IPv4 πακέτου και αν τα διάφορα δίκτυα υποστηρίζουν τις ίδιες κλάσεις υπηρεσιών.

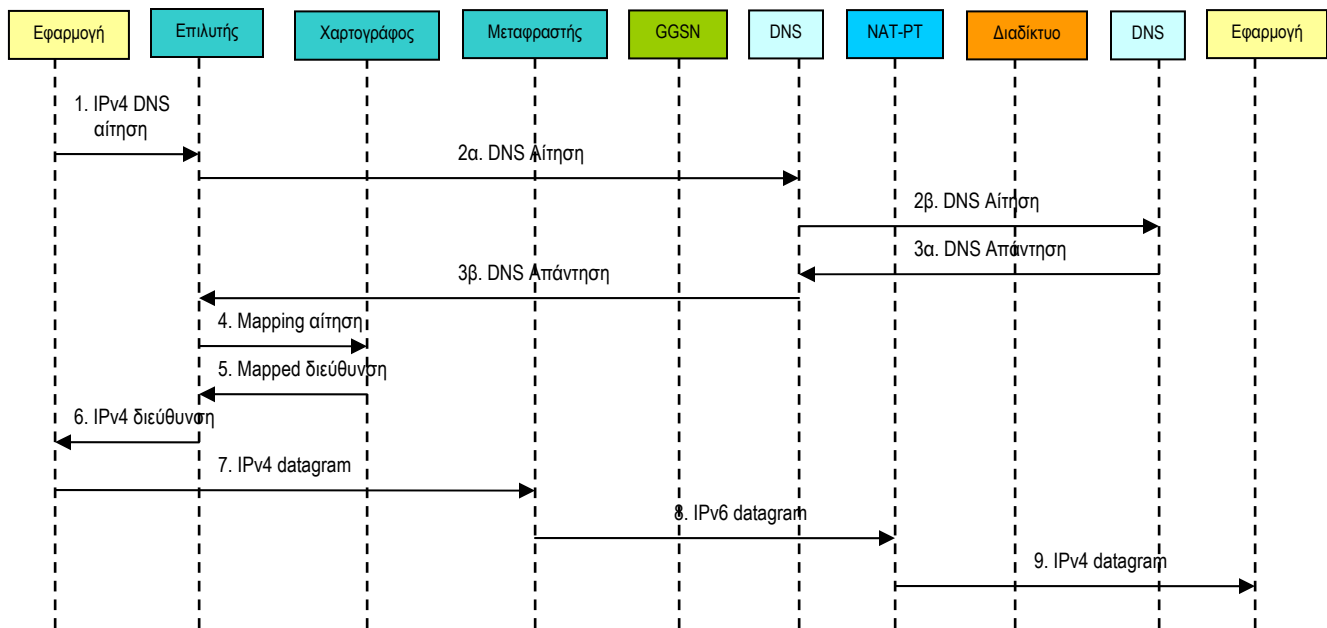
5.6 Σενάριο 5 [7]

Σε αυτό το σενάριο, τόσο τα UMTS τερματικά όσο και το δίκτυο είναι μόνο IPv6 – δηλαδή χρησιμοποιούν μόνο μια IPv6 στοίβα και το UMTS δίκτυο είναι ενωμένο με το IPv4 Διαδίκτυο. Έτσι μια IPv4 εφαρμογή που είναι τρέχει σε ένα IPv6 τερματικό, χρειάζεται να επικοινωνεί με ένα IPv4 εξυπηρετητή στο Διαδίκτυο. Το σενάριο περιγράφει μια κατάσταση μερικά χρόνια μπροστά, όπου το UMTS έχει αναπτυχθεί προς την All IP Έκδοση και λόγω της έλλειψης των IPv4 διευθύνσεων, το UMTS δίκτυο είναι ένα καθαρά IPv6 δίκτυο, αλλά το Διαδίκτυο καθυστερεί στην υλοποίηση του IPv6 κι έτσι πολλές εφαρμογές Διαδικτύου είναι μόνο IPv4. Θεωρούμε κίνηση μεταξύ μιας IPv4 εφαρμογής που τρέχει σε ένα UMTS IPv6 τερματικό και μιας IPv4 εφαρμογής που τρέχει σε host του Διαδικτύου, διαμέσω του IPv6 UMTS δικτύου και του IPv4 Διαδικτύου.

Το σενάριο 5 είναι σημαντικό στην περίπτωση όπου IPv4 εφαρμογές πελάτη / εξυπηρετητή (client / server) θέλουν να επικοινωνήσουν δια μέσω των 3G κινητών συστημάτων.

5.6.1 Λειτουργία

Πιο κάτω περιγράφονται οι απαραίτητες λειτουργίες για αρχικοποίηση και μεταφορά δεδομένων μεταξύ δύο IPv4 εφαρμογών:



Σημειώσεις:

- Τα τόξα που περνούν πάνω από τον GGSN αντιπροσωπεύουν κίνηση πακέτων που διοχετεύεται προς και από την UMTS εφαρμογή δια μέσω του GGSN.
- Τα τόξα που περνούν πάνω από το Διαδίκτυο αντιπροσωπεύουν κίνηση πακέτων που περνούν δια μέσω του Διαδικτύου.

Επεξήγηση Ροής Επικοινωνίας:

1. Η εφαρμογή ζητά μια IPv4 διεύθυνση.
2. Ο BIS επιλυτής στέλνει μια DNS αίτηση.
3. Ο DNS επιστρέφει μια IPv6 διεύθυνση στον επιλυτή.
4. Ο επιλυτής ζητά από τον χαρτογράφο να του παρέχει μια IPv4 διεύθυνση.
5. Ο επιλυτής λαμβάνει μια IPv4 διεύθυνση.
6. Η εφαρμογή λαμβάνει την IPv4 χαρτογραφημένη διεύθυνση του αντίστοιχου κόμβου.
7. Το IPv4 πακέτο αποστέλλεται στον BIS μεταφραστή, ο οποίος το μεταφράζει σε ένα IPv6 πακέτο.
8. Το IPv6 πακέτο στέλλεται στον NAT-PT δρομολογητή, ο οποίος μεταφράζει το πακέτο και το στέλνει στον αντίστοιχο host.

5.6.2 Μηχανισμοί μετάβασης που υποστηρίζονται

Τα UMTS τερματικά δεν έχουν μια IPv4 στοίβα διαθέσιμη, έτσι η IPv4 εφαρμογή που αρχίζει την επικοινωνία πρέπει να χρησιμοποιήσει ένα μηχανισμό μετάβασης. Η λύση θα επιτρέπει σε IPv4 εφαρμογές πελάτη / εξυπηρετητή να επικοινωνούν διαμέσου της UMTS υπηρεσίας. Η λύση αυτή χρησιμοποιεί BIS στον IPv4 πελάτη και NAT-PT στα σύνορα του IPv6 UMTS δικτύου. Παρόμοια είναι και η πρώτη λύση που παρουσιάζεται στο σενάριο 4.

5.6.3 DNS και AAA

Το NAT-PT κουτί στα σύνορα του UMTS δικτύου πρέπει να καθιστά δυνατά ένα DNS ALG και ένα AAA ALG. Όμως, ο BIS μηχανισμός πρέπει επίσης να υλοποιεί μια προέκταση του name resolver που να λειτουργεί σαν ένας DNS ALG. Ο BIS δεν μπορεί να συνδυαστεί με AAA, ή με ασφαλή DNS αφού η προέκταση του name resolver δεν μπορεί να χειριστεί το πρωτόκολλο.

5.6.4 Κινητικότητα

Το Mobile IPv6 θα δουλέψει με την χρήση του BIS αφού η IPv4 διεύθυνση είναι τοπική στον BIS host κι έτσι δεν επηρεάζεται στην διάρκεια της handover φάσης. Η εισαγωγή του NAT-PT σαν τον δεύτερο μηχανισμό μετάβασης απαιτεί η κίνηση μεταξύ του BIS host και του αντίστοιχου κόμβου, να περνά δια μέσω του ίδιου NAT-PT. Ο κινητός κόμβος (BIS host) μπορεί να στείλει ένα BU στον NAT-PT δρομολογητή και κατά συνέπεια να δημιουργήσει ένα binding στην καινούργια care-of-address. Όπως και στο προηγούμενο σενάριο κι εδώ το σημείο αυτό αναφέρεται στο κεφάλαιο 3. Επίσης, για να είναι δυνατή η επικοινωνία μεταξύ δυο κόμβων που ανήκουν σε διαφορετικά UMTS δίκτυα, είναι αναγκαία η χρησιμοποίηση ενός AAA εξυπηρετητή στη διαδικασία διακίνησης.

5.6.5 Ασφάλεια

Το κυριότερο θέμα σχετικά με την ασφάλεια είναι η χρήση του NAT-PT κουτιού που δεν επιτρέπει κανένα end – to – end ασφαλή session. Πάραυτα, μηχανισμοί ασφάλειας μπορούν να χρησιμοποιηθούν μεταξύ δύο ξεχωριστών UMTS δικτύων.

5.6.6 Σήμανση

Σε αυτό το σενάριο το UMTS δίκτυο χρησιμοποιεί SIP για σήμανση. Ο BIS μηχανισμός δεν προτυποποιεί καμία λειτουργία μετάφρασης εκτός από την μετάφραση του header. Αν ο BIS μπορεί να «κοιτάξει» στο payload ενός πακέτου, τα πεδία της IP διεύθυνσης που μπορούν να συμπεριληφθούν στο SIP μήνυμα, μπορούν να μεταφραστούν. Οι IPv4 εφαρμογές μπορούν έτσι να χρησιμοποιήσουν το SIP στέλνουν σήμα σε άλλους hosts για session set-up. Αφού το σενάριο αυτό συμπεριλαμβάνει δυο μηχανισμούς μετάβασης, ο NAT-PT δρομολογητής πρέπει ακόμη να μεταφράζει την IP διεύθυνση που συμπεριλαμβάνεται στο payload.

5.6.7 Υποστήριξη QoS

Το QoS που βασίζεται στις Διαφοροποιημένες Υπηρεσίες μπορεί να υποστηριχτεί αν ο BIS μηχανισμός αντιγράφει τα DSCP πεδία από το header του IPv6 πακέτου στο header του IPv4 πακέτου και αν τα διάφορα δίκτυα υποστηρίζουν τις ίδιες κλάσεις υπηρεσιών. Πρέπει και ο NAT-PT να μπορεί να μεταφράζει το DSCP πεδίο από IPv6 σε IPv4 και αντίστροφα. Τα δύο δίκτυα πρέπει επίσης να υποστηρίζουν την ίδια κλάση υπηρεσιών.

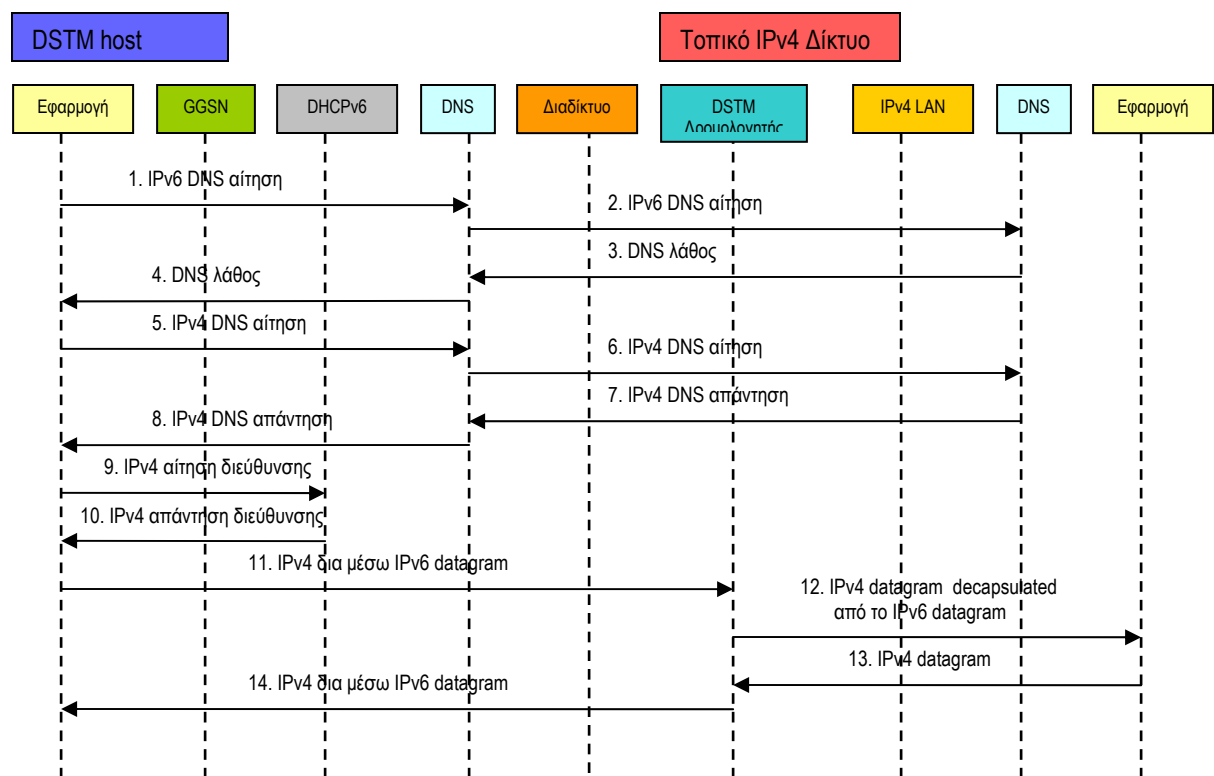
5.7 Σενάριο 6 [7]

Σε αυτό το σενάριο, και οι IPv6 και οι IPv4 εφαρμογές μπορούν να υποστηρίζονται στο κινητό τερματικό. Για τις IPv6 εφαρμογές θα υπάρχει ένα πλήρη τοπικό IPv6 δίκτυο, δηλαδή όλη η δρομολόγηση θα γίνεται στο IPv6 domain και δεν θα χρειάζεται κάποιος μηχανισμός μετάβασης. Για να τρέξει μια IPv4 εφαρμογή όμως, θα χρειάζεται ένας μηχανισμός μετάβασης κάπου μέσα στο δίκτυο. Μια πιθανότητα είναι τα IPv4 πακέτα να περνούν από τούνελ σε ένα δρομολογητή στην άκρη του δικτύου που θα τα μεταφράζει σε IPv6 πακέτα. Άλλη πιθανότητα είναι η μετάφραση των IPv4 πακέτων σε IPv6 κοντά στο IPv4 τερματικό. Σε αυτή την περίπτωση, το UMTS δίκτυο θα είναι τοπικά IPv6. Θεωρούμε κίνηση μεταξύ είτε μιας IPv4 ή IPv6 εφαρμογής που τρέχει σε ένα UMTS τερματικό διπλής στοίβας και είτε μιας IPv4 ή IPv6 εφαρμογής που τρέχει σε host του Διαδικτύου, διαμέσω του UMTS δικτύου διπλής στοίβας και του IPv6 Διαδικτύου.

Το σενάριο 6 αντανακλά την περίπτωση που τα UMTS τερματικά θα τρέχουν ακόμη IPv4 εφαρμογές παρά το γεγονός ότι και το UMTS δίκτυο και το Διαδίκτυο θα χρησιμοποιούν IPv6. Έτσι όμως, έχουν εξεταστεί μόνο οι πιθανές λύσεις που έχουν IPv4 εφαρμογές τόσο σε hosts του UMTS δικτύου, όσο και σε hosts του Διαδικτύου.

5.7.1 Λειτουργία

Πιο κάτω περιγράφεται η λειτουργία που χρειάζεται για αρχικοποίηση και μεταφορά δεδομένων μεταξύ δυο IPv4 εφαρμογών.



Σημειώσεις:

- Τα τόξα που περνούν πάνω από τον GGSN αντιπροσωπεύουν κίνηση πακέτων που διοχετεύεται προς και από την UMTS εφαρμογή δια μέσω του GGSN.
- Τα τόξα που περνούν πάνω από το Διαδίκτυο αντιπροσωπεύουν κίνηση πακέτων που περνούν δια μέσω του Διαδικτύου.
- Τα τόξα που περνούν πάνω από το IPv4 LAN αντιπροσωπεύουν κίνηση πακέτων που περνούν δια μέσω του LAN εκείνου.

Επεξήγηση Ροής Επικοινωνίας:

1. Ο DSTM host ζητά την IPv6 διεύθυνση του άλλου host (IPv4) από τον DNS εξυπηρετητή του.
2. Ο DNS εξυπηρετητής ζητά μια IPv6 διεύθυνση μέσω της αλυσίδας DNS εξυπηρετητών, μέχρι να φτάσει τον DNS εξυπηρετητή του άλλου host.
3. Ο DNS εξυπηρετητής που βρίσκεται σε IPv4 δίκτυο, επιστρέφει λάθος αφού δεν υπάρχει IPv6 διεύθυνση για αυτό τον host.
4. Ο τοπικός DNS εξυπηρετητής απαντά με λάθος.
5. Ο DSTM host ζητά μια IPv4 διεύθυνση για τον άλλο host.
6. Ο DNS εξυπηρετητής προωθεί το αίτημα.
7. Επιστρέφεται μια IPv4 διεύθυνση.
8. Η διεύθυνση προωθείται πίσω στον DSTM host.
9. Ο DSTM host ζητά από τον DHCPv6 να του αναθέσει μια IPv4 διεύθυνση.
10. Ο DHCP απαντά με την IPv4 διεύθυνση.
11. Ο DSTM host πετυχαίνει ένα τούνελ IPv4 δια μέσω IPv6 προς τον DSTM δρομολογητή και στέλνει μέσω αυτού IPv4 πακέτα.
12. Ο DSTM δρομολογητής εξάγει τα IPv4 πακέτα και το προωθεί προς τον IPv4 host.
13. Ο IPv4 host απαντά και στέλνει IPv4 πακέτα στον DSTM host.
14. Ο DSTM δρομολογητής encapsulates αυτά τα πακέτα σε IPv6 πακέτα και τα προωθεί στον DSTM host.

5.7.2 Μηχανισμοί μετάβασης που υποστηρίζονται

Υπάρχουν διάφοροι μηχανισμοί που μπορούν να παρέχουν σύνδεση μεταξύ των δύο IPv4 εφαρμογών. Είναι τεχνικά εφικτό η χρήση ενός μηχανισμού μετάφρασης δύο φορές, σαν το NAT-PT ή το BIS ή ένας συνδυασμός των δύο. Αυτό θα χρειάζεται μια μετάφραση από IPv4 σε IPv6 και πάλι πίσω σε IPv4.

Είδαμε στο πιο πάνω σχήμα την περιγραφή της κατάστασης όπου ένας DSTM δρομολογητής χρησιμοποιείται στο IPv6 Διαδίκτυο. Οι UMTS hosts πρέπει να έχουν τον DSTM μηχανισμό. Όλη η IPv4 κίνηση από τον IPv4 host αποστέλλεται μέσω

τούνελ στο IPv6 δίκτυο (και Διαδίκτυο και UMTS) μέχρι να φτάσει τον DSTM host στην άκρη του UMTS δικτύου. Υπάρχει ακόμη ένα πιθανό σενάριο, όπου ο DSTM host είναι στο IPv6 Διαδίκτυο, ο DSTM δρομολογητής στα σύνορα μεταξύ του UMTS και του IPv6 Διαδικτύου και ο IPv4 host θα είναι ένα UMTS τερματικό. Όμως αυτό δεν είναι πολύ πιθανό να συμβεί στο μέλλον. Ακόμη μια άλλη λύση θα είναι, αντί να γίνει η χρήση του DSTM, να δημιουργηθεί ένα pre-configured τούνελ που θα κάνει το encapsulation από IPv4 σε IPv6.

5.7.3 DNS και AAA

Δεν υπάρχει κανένα πρόβλημα με το DNS resolution, ενώ το AAA χρησιμοποιείται κανονικά σε επίπεδο IPv4.

5.7.4 Κινητικότητα

Σε αυτό το σενάριο, η IPv6 κινητικότητα υποστηρίζεται αν ο DSTM host και ο DSTM δρομολογητής υποστηρίζουν IPv6 χαρακτηριστικά κινητικότητας όπως την διαχείριση Binding Updates.

5.7.5 Ασφάλεια

Το DSTM δεν σπάζει την ασφαλή end-to-end επικοινωνία σε καμία στιγμή, έτσι με την χρήση του μηχανισμού αυτού δεν υπάρχουν εκκρεμή θέματα ασφάλειας.

5.7.6 Σήμανση

Το UMTS δίκτυο σε αυτό το σενάριο, υποστηρίζει SIP. Αυτό σημαίνει ότι όλες οι IPv6 εφαρμογές θα μπορούν να χρησιμοποιούν την SIP υπηρεσία που θα παρέχεται από το δίκτυο χωρίς ιδιαίτερα προβλήματα φτάνει η επικοινωνία να γίνεται με επίσης IPv6 host. Αν μια IPv4 εφαρμογή θέλει να χρησιμοποιήσει την SIP σήμανση, πρέπει να υπάρχει ένας IPv4 SIP εξυπηρετητής.

5.7.7 Υποστήριξη QoS

Το QoS που βασίζεται στις Διαφοροποιημένες Υπηρεσίες μπορεί να υποστηριχτεί αν ο BIS μηχανισμός μετάφρασης ή ο NAT-PT μηχανισμός αντιγράφει τα DSCP πεδία από

το header του IPv4 πακέτου στο header του IPv6 πακέτου. Η χρήση των Ενσωματωμένων Υπηρεσιών (Integrated Services) μπορεί επίσης να υποστηρικτεί, αλλά χρειάζεται μετάφραση των RSVP μηνυμάτων. Θεωρητικά, το DSTM δεν έχει καθόλου περιορισμούς.

5.7.8 Συμπεράσματα

Αυτό το σενάριο πιθανό να μην συμβεί ποτέ. Αναμένεται ότι τα UMTS τερματικά θα χρησιμοποιούν IPv4 εφαρμογές. Όπως έχει παρατηρηθεί, σήμερα τα κινητά τερματικά είναι σχεδόν πάντα πολύ πιο ανεπτυγμένα από μεριά τεχνολογικής ανάπτυξης σε σχέση με τα σταθερά τερματικά. Έτσι δεν είναι αναμενόμενο ότι θα υπάρχουν IPv4 τερματικά στο UMTS δίκτυο όταν όλο το Διαδίκτυο θα χρησιμοποιεί IPv6. Χρησιμοποιώντας DTSM γίνεται δυνατή η σύνδεση με ένα μοναδικό μηχανισμό μετάφρασης. Αυτό, σε συνδυασμό με ένα εύκολο DNS resolution είναι το κυριότερο πλεονέκτημα της χρήσης του DSTM.

5.8 Συνοπτικός πίνακας των σεναρίων

	Σενάριο 1	Σενάριο 2	Σενάριο 3	Σενάριο 4	Σενάριο 5	Σενάριο 6
Έκδοση UMTS που υποστηρίζεται	Έκδοση 99	Έκδοση 99	All IP	All IP	All IP	All IP
Είδος τερματικού	IPv6 ή διπλή στοίβα	IPv6 και διπλή στοίβα	IPv6 στοίβα	Διπλή στοίβα	IPv6 στοίβα	Διπλή στοίβα
Μηχανισμός Μετάβασης	δto4	NAT-PT και DSTM	BIS	DSTM	BIS και NAT-PT	DSTM
Είδος σύνδεσης	IPv6-IPv6	IPv6- IPv4	IPv4- IPv4	IPv4- IPv4	IPv4- IPv4	IPv4- IPv4
Ασφάλεια	OK	Περιορίζεται από το NAT-PT	OK	OK	Περιορίζεται από το NAT-PT	OK
Σήμανση	Όχι IP σήμανση	Όχι IP σήμανση	OK	OK	Χρειάζεται ALG	OK
QoS	OK	OK	OK	OK	OK	OK
DNS	OK	OK	OK	OK	OK	OK
Κινητικότητα	Δεν υποστηρίζεται	Δεν υποστηρίζεται	Ναι	OK αλλά οδηγεί σε triangle routing	OK αλλά οδηγεί σε triangle routing	OK
Αριθμός IPv4 διευθύνσεων που χρειάζονται	Μια διεύθυνση	Μια ή περισσότερες	Μπορεί να χρησιμοποιήσει τοπικές διευθύνσεις	Ένα pool με μια ή περισσότερες	Μία ή περισσότερες	Ένα pool με μια ή περισσότερες

Τα σενάρια αυτά δεν έχουν ακόμη εφαρμοστεί πρακτικά. Ο λόγος είναι ότι δεν υπάρχει ακόμη τόσο μεγάλος αριθμός χρηστών που να χρησιμοποιούν UMTS και το IPv6 δεν είναι ακόμη ευρέως διαδεδομένο. Εξάλλου δεν είναι η επίσημη πρόταση του IETF είναι απλά μελέτες του EUROSCOM που έστω και θεωρητικά έχουν αποδείξει ότι υπάρχουν τα μέσα, ο τρόπος και η κατάλληλη υποδομή για να δουλέψει το UMTS με άλλα δίκτυα, ανεξάρτητα από το πιο πρωτόκολλο χρησιμοποιεί το καθένα, IPv4 ή IPv6.

Κεφάλαιο 6

Προσομοιώσεις Handover δικτύου UMTS με χρήση εργαλείου OPNET

6.1	UMTS Handover	86
6.2	Προσομοίωση με την χρήση του εργαλείου OPNET: Παράδειγμα Soft Handover	88
6.3	Προσομοίωση με την χρήση του εργαλείου OPNET: Σύγκριση Soft Handover και Hard Handover	90
6.4	Συμπεράσματα	100

Στο κεφάλαιο αυτό θα παρουσιαστούν κάποιες προσομοιώσεις και τα αποτελέσματά τους που έχουν πραγματοποιηθεί με το εργαλείο OPNET. Οι προσομοιώσεις αφορούν το δίκτυο UMTS και πιο συγκεκριμένα μελετούν διάφορα θέματα handover. Δεν ήταν δυνατή η δημιουργία και μελέτη σεναρίων στο OPNET που να αφορούν την χρήση του Mobile IPv6 σε UMTS περιβάλλον, συμπεριλαμβανομένου και των σεναρίων που μελετήθηκαν στο πέμπτο κεφάλαιο. Αυτό γιατί το εργαλείο OPNET ακόμη δεν παρέχει υποστήριξη για δίκτυα UMTS μαζί με Mobile IPv6 και λόγω πίεσης χρόνου δεν μπορούσα να αναπτύξω από την αρχή τέτοια σενάρια.

6.1 UMTS Handover

Πριν την παρουσίαση των προσομοιώσεων, αναφέρονται κάποιες βασικές έννοιες που αφορούν το UMTS handover. Κατ' αρχάς, handover είναι η διαδικασία κατά την οποία λόγω της κίνησης του κόμβου, ο κόμβος μεταβαίνει σε άλλα κελιά (cells) του δικτύου κι έτσι λαμβάνει και στέλνει δεδομένα από άλλη τοποθεσία (ανατίθεται σε άλλο Κόμβο – B για την περίπτωση ενός UMTS κινητού κόμβου). Η πιο προφανής αιτία που γίνεται η διαδικασία του handover, είναι ότι λόγω της κίνησης του χρήστη μπορεί να εξυπηρετηθεί από ένα άλλο κελί πιο αποδοτικά. Η διαδικασία handover όμως μπορεί να γίνει και για άλλους σκοπούς όπως έλεγχο φόρτωσης συστήματος [1].

6.1.1 Είδη UMTS Handovers

Υπάρχουν τρία είδη UMTS handovers [22]:

- **Hard Handover:** Με την έννοια hard handover, εννοούμε ότι όλοι οι παλιοί ραδιο – σύνδεσμοι αφαιρούνται από τον κινητό κόμβο πριν να γίνουν οι συνδέσεις με τους καινούργιους ραδιο – συνδέσμους. Το hard handover μπορεί να είναι seamless ή non – seamless. Η διαφορά του seamless hard handover με το non – seamless είναι ότι το seamless handover δεν γίνεται αντιληπτό από τον χρήστη. Πρακτικά όμως, ένα handover για το οποίο χρειάζεται αλλαγή της συχνότητας του φορέα (inter – frequency handover) πάντα είναι hard handover.
- **Soft Handover:** Στο soft – handover, οι ραδιο – σύνδεσμοι αφαιρούνται με τέτοιο τρόπο έτσι ώστε ο κινητός κόμβος πάντα κρατά τουλάχιστο ένα προκαθορισμένο αριθμό από ραδιο – συνδέσμους στο UTRAN. Το soft handover λειτουργεί με την χρήση του macro diversity, δηλαδή λαμβάνει υπόψη το γεγονός ότι διάφοροι ραδιο – σύνδεσμοι είναι ενεργοί την ίδια χρονική στιγμή. Υπό κανονικές συνθήκες, το soft handover μπορεί να χρησιμοποιηθεί όταν ο κινητός κόμβος αλλάζει κελιά που λειτουργούν στην ίδια συχνότητα.
- **Softer Handover:** Το Softer Handover είναι μια ειδική περίπτωση του Soft Handover, όπου οι ραδιο – σύνδεσμοι που προσθέτονται και αφαιρούνται από τον κινητό κόμβο, ανήκουν στο ίδιο Node-B.

6.1.2 Βασικές έννοιες

Κάποιες έννοιες που αφορούν τα Soft και Softer Handover είναι:

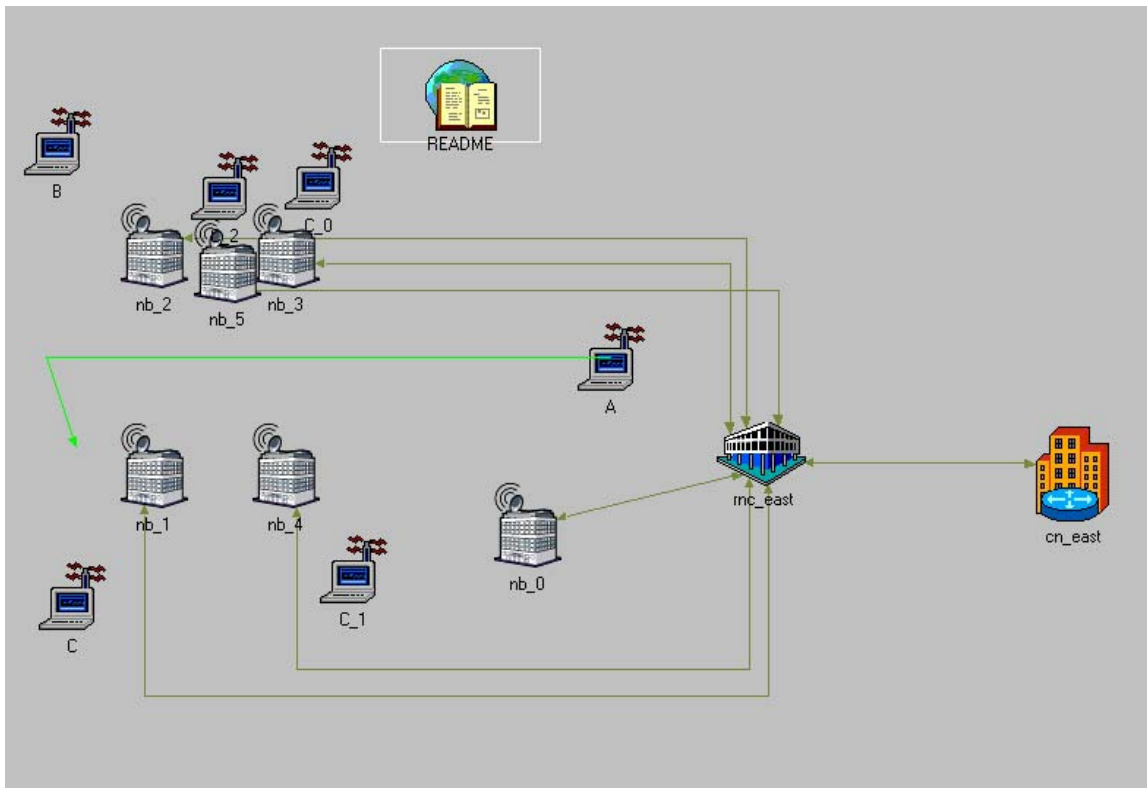
- **Active Set:** Το Active Set καθορίζεται σαν το σετ από τους Node-Bs με τους οποίους ο κινητός κόμβος είναι ταυτόχρονα συνδεδεμένος. Με άλλα λόγια, είναι τα UTRAN κελιά τα οποία έχουν την συγκεκριμένη στιγμή ένα downlink DPCH στον κινητό κόμβο.
- Τα κελιά τα οποία δεν συμπεριλαμβάνονται στο Active Set, αλλά υπάρχουν στο CELL_INFO_LIST ανήκουν στο Monitored Set.
- Τα κελιά που ανιχνεύονται από τον κινητό κόμβο και δεν είναι ούτε στο CELL_INFO_LIST ούτε στο Active Set, ανήκουν στο Detected Set.

6.2 Προσομοίωση με την χρήση του εργαλείου OPNET: Παράδειγμα Soft Handover

Στην προσομοίωση αυτή παρουσιάζεται πως οι soft handover διαδικασίες εφαρμόζονται σε ένα κινητό UMTS κόμβο από τον εξυπηρετητή RNC.

6.2.1 Περιγραφή Σεναρίου

Στο σενάριο αυτό χρησιμοποιήθηκε το δίκτυο που παρουσιάζετε στο σχήμα 6.1



Σχήμα 6.1

Ο κινητός κόμβος A, που είναι αρχικά συνδεδεμένος με τον Node-B-0, έχει μια συγκεκριμένη τροχιά την οποία ακολουθεί κατά την διάρκεια της προσομοίωσης. Λόγο του ότι η τοποθεσία του A αλλάζει κατά την διάρκεια της προσομοίωσης και πλησιάζει σε άλλα συγκεκριμένα Node-Bs σε συγκεκριμένες χρονικές στιγμές, αναμένεται ότι ο RNC θα αναθέσει τον A σε διάφορους Node_Bs που βρίσκονται στην τροχιά του A, ανάλογα με τις αναφορές μετρήσεων που θα λαμβάνει από τον A.

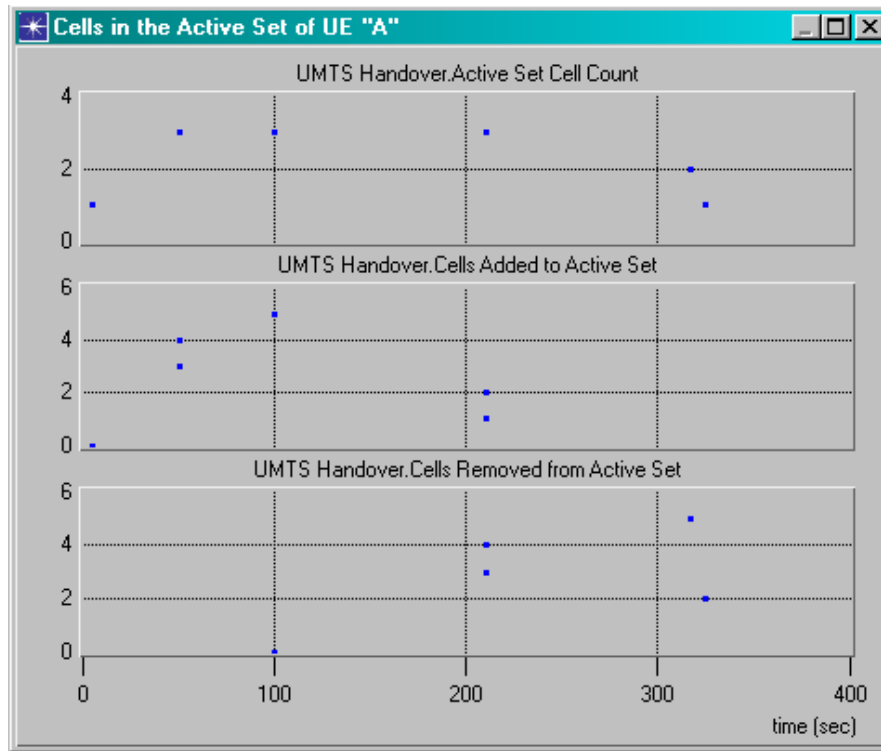
Οι αριθμοί στις ονομασίες των Node-Bs είναι οι ίδιοι με τα Cell IDs τους. Δηλαδή το κελί 2 είναι το κελί του Node-B nb_2.

Το μέγεθος του Active Set των κινητών κόμβων είναι 3.

6.2.2 Αποτελέσματα

Αυτό το σενάριο επικεντρώνεται σε τρεις στατιστικές οι οποίες παρουσιάζουν τον αριθμό των κελιών που υπάρχουν στο Active Set του A και ποια κελιά προστίθενται και αφαιρούνται από το Set κατά την διάρκεια του simulation.

Βλέπουμε στο σχήμα 6.2 το Active Set του κόμβου A και πως προστίθενται και αφαιρούνται τα κελιά.



Σχήμα 6.2

Αρχικά, ο A ξεκινά με ένα μόνο κελί στο Active Set του, το οποίο είναι το κελί 0. Αυτό καταγράφεται στις στατιστικές όταν ο A ολοκληρώνει την διαδικασία GPRS επισύναψης. Στην συνέχεια, ο A προχωρεί προς άλλα Node-Bs και πλησιάζει τα nb_3 και nb_4. Τότε αρχίζει η διαδικασία soft handover για τον κόμβο A και ο RNC με ένα Active Set Update Message προσθέτει στο Active Set του A τα κελιά 3 και 4. Σε χρόνο περίπου 100 δευτερόλεπτα ο nb_5 γίνεται διαθέσιμος στον A, ενώ βρίσκονται στο Active Set τα κελιά 0, 3 και 4. Αφού το μέγεθος του Active Set περιορίζεται σε 3 κελιά,

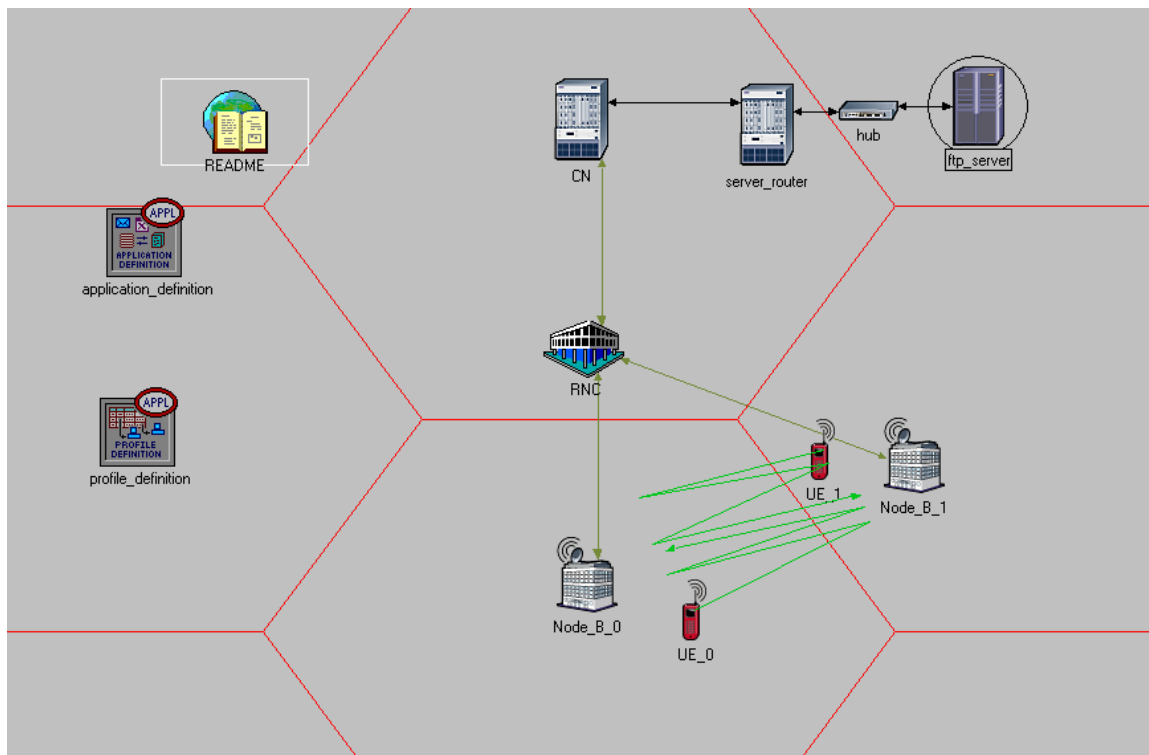
ο RNC με το ίδιο μήνυμα, αντικαθιστά το κελί 0, με το κελί 5. Η αντικατάσταση αυτή παρουσιάζεται στις στατιστικές με την καταγραφή μιας εισαγωγής, αφαίρεσης και την επανάληψη μέτρησης των κελιών στο Active Set την ίδια χρονική στιγμή. Καθώς ο A συνεχίζει την πορεία του, περίπου στα 210 δευτερόλεπτα συμβαίνει μια διπλή αντικατάσταση: τα κελιά 3 και 4 αντικαθιστώνται από τα κελιά 1 και 2 με μια αναφορά μέτρησης από το A στο RNC και με ένα Active Set Update Message από τον RNC στον A. Τέλος, ο A πλησιάζει τον nb_1 και τα κελιά 5 και 2 αφαιρούνται από το Active Set περίπου στα 317 και 325 δευτερόλεπτα αντίστοιχα. Με την αφαίρεση του nb_2 από το Active Set, μένει μόνο το κελί 1 στο Set και τελειώνει η διαδικασία του soft handover.

6.3 Προσομοίωση με την χρήση του εργαλείου OPNET: Σύγκριση Soft Handover και Hard Handover

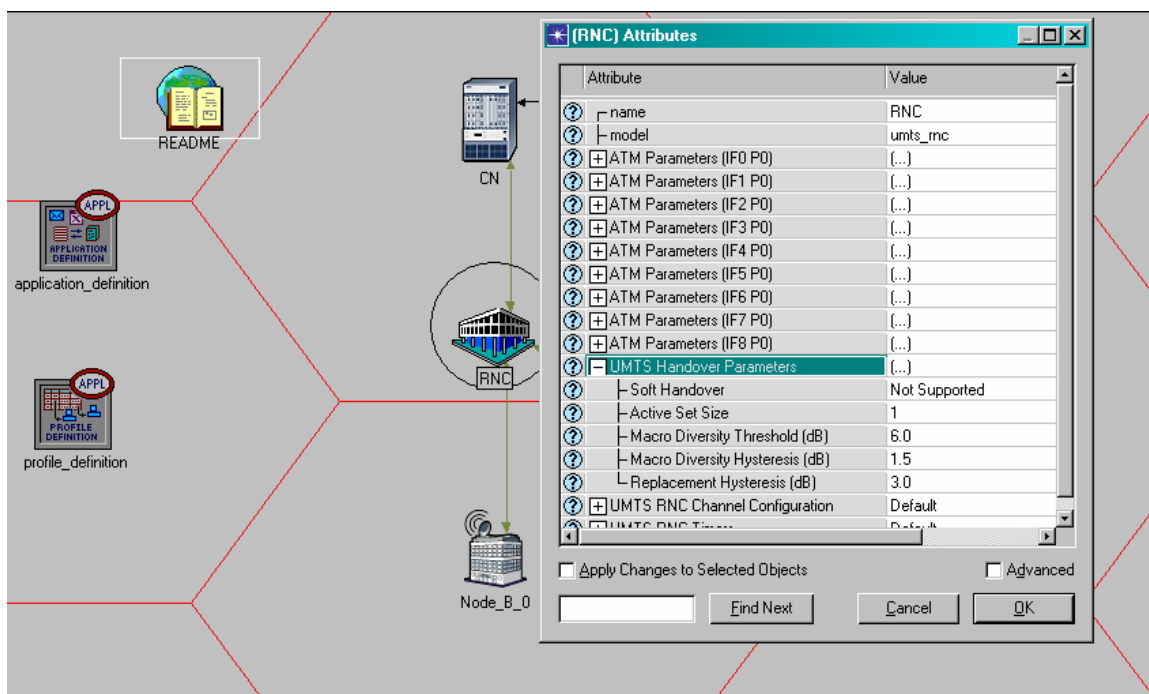
Με την προσομοίωση αυτή γίνεται μια σύγκριση μεταξύ Soft Handover και Hard Handover, χρησιμοποιώντας δυο σενάρια

6.3.1 Περιγραφή σεναρίων

Σε αυτά τα δυο σενάρια, δυο κινητοί κόμβοι ακολουθούν τις τροχιές τους που κάνουν πορεία ζιγκ ζαγκ μεταξύ δύο Node-Bs με αποτέλεσμα την επανάληψη handovers από το ένα κελί στο άλλο. Και οι δυο κινητοί κόμβοι σχεδόν συνέχεια φορτώνουν μεγάλα FTP αρχεία σε ένα εξυπηρετητή ενός κινητού δικτύου, κατά την διάρκεια της προσομοίωσης. Γι' αυτό τον λόγο η περισσότερη κίνηση πηγαίνει προς την uplink κατεύθυνση του UMTS δικτύου. Στο συγκεκριμένο σενάριο για την FTP κίνηση χρησιμοποιείται το UMTS QoS 3. Στο σχήμα 6.2 παρουσιάζεται το UMTS δίκτυο που εφαρμόζει Soft Handover και στο σχήμα 6.3 το UMTS δίκτυο που εφαρμόζει Hard Handover.



Σχήμα 6.2



Σχήμα 6.3

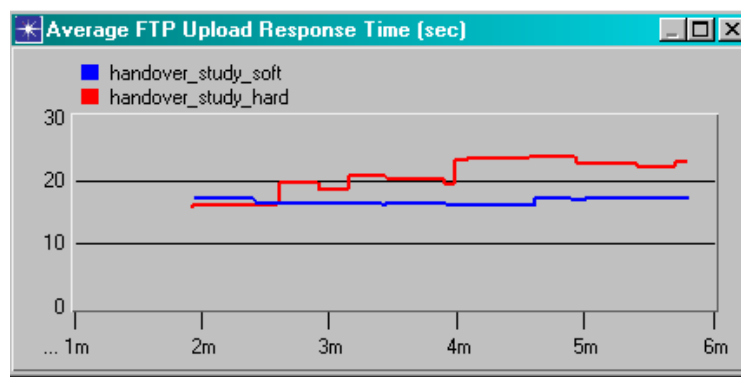
Τα δίκτυα και η διαμόρφωσή τους είναι τα ίδια και στα δυο σενάρια, εκτός από το γεγονός ότι στο σενάριο για Hard Handover, έχουν γίνει disabled τα soft handovers

στον RNC κι έτσι όλα τα handovers είναι hard handovers. Ανάλογα, όλα τα handovers στο Soft Handover σενάριο είναι soft handovers.

6.3.2 Αποτελέσματα:

Έχουν προσομοιωθεί 15 λεπτά και των δύο δικτύων και έχουν συγκεντρωθεί αποτελέσματα για εννέα στατιστικές:

1. FTP upload response time του FTP εξυπηρετητή για τους χρόνους ανταπόκρισης της εφαρμογής και για τα δυο σενάρια.

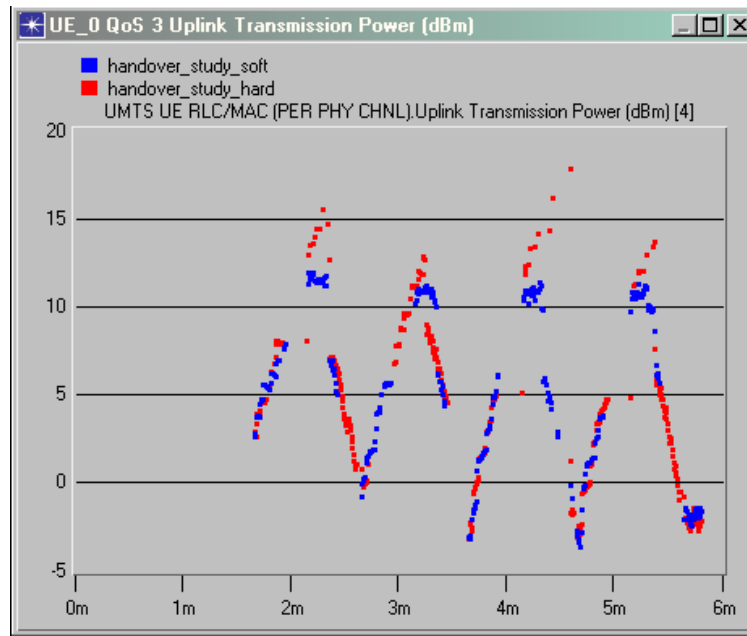


Σχήμα 6.4

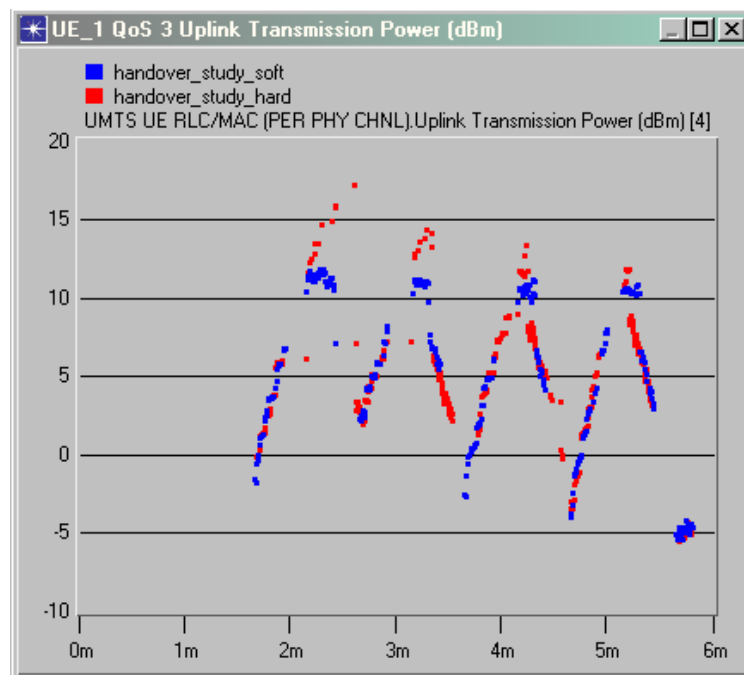
Από ότι φαίνεται ότι δεν υπάρχει σημαντική διαφορά μεταξύ soft και hard handovers, όσον αφορά την επίδρασή τους στον χρόνο ανταπόκρισης. Απλά, το Soft Handover παρουσιάζει ελαφρά γρηγορότερους χρόνους ανταπόκρισης.

2. Uplink Transmission Power και για τα δυο σενάρια που παρουσιάζει την ενέργεια που καταναλώνουν οι κινητοί κόμβοι για uplink μετάδοση.

Στο σχήμα 6.5 παρουσιάζεται το Uplink Transmission Power για τον πρώτο κινητό κόμβο και για τα δυο σενάρια και στο σχήμα 6.6 το Uplink Transmission Power για τον δεύτερο κινητό κόμβο και για τα δυο σενάρια.



Σχήμα 6.5



Σχήμα 6.6

Βλέπουμε, ότι και για τους δυο κινητούς κόμβους το soft handover έχει καλύτερα αποτελέσματα όσον αφορά το Uplink Transmission Power. Στις γραφικές παραστάσεις του Uplink Transmission Power, όπου υπάρχει κορυφή σημαίνει ότι έχει γίνει handover, γιατί πριν τα handovers οι κινητοί κόμβοι απομακρύνονται πολύ από το ανάλογο Node-B – κι έτσι αυξάνουν το transmission power τους – και μετά το

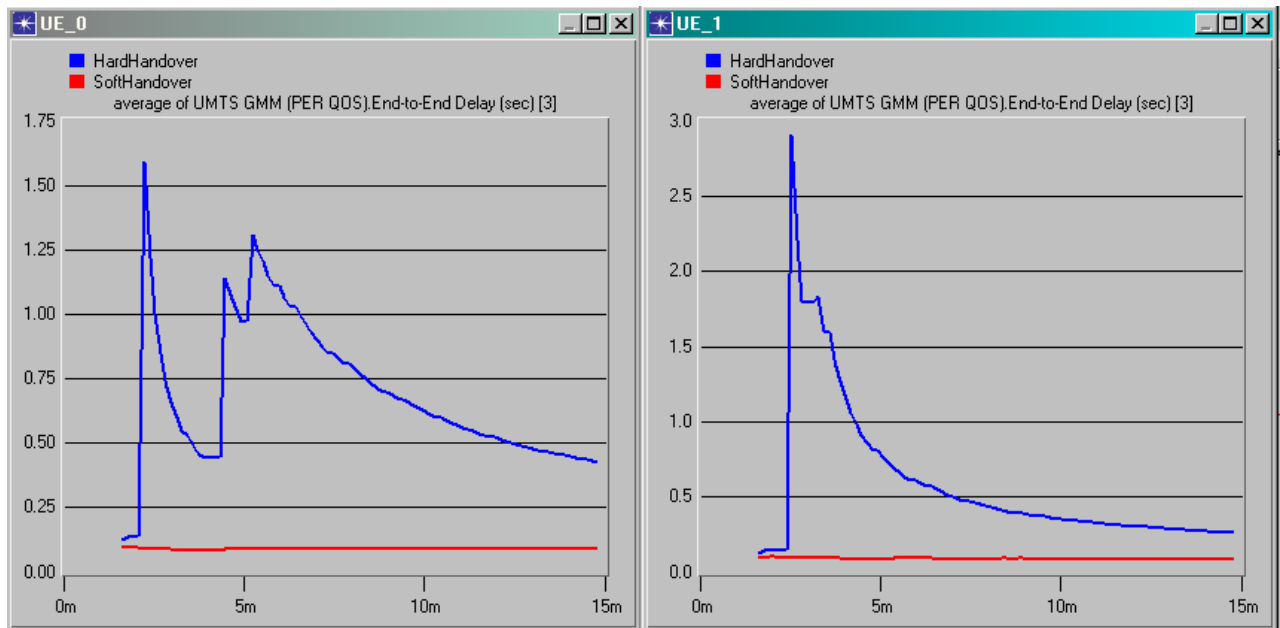
handover συνδέονται με κοντινότερο Node-B – κι έτσι μειώνουν το transmission power. Συγκρίνοντας τις καμπύλες των κορυφών στα δυο σενάρια, το transmission power των κινητών κόμβων φτάνει σε πολύ μεγαλύτερες τιμές κατά την διάρκεια του hard handover παρά στο soft handover το οποίο φανερώνει κι ένα προτέρημα των soft handovers. Δίνεται έτσι η δυνατότητα στους κινητούς κόμβους να κάνουν το handover με λιγότερο ενεργειακό κόστος.

Για να μπορεί να υπάρξει η ίδια απόδοση με λιγότερο ενεργειακό κόστος, η διαδικασία του soft handover χρησιμοποιεί το soft handover gain. Η ιδέα είναι η εξής: αφού ένας κινητός κόμβος υποστηρίζεται από πολλαπλές ραδιο – συνδέσεις κατά την διάρκεια του soft handover, το δίκτυο μπορεί να χαμηλώσει την ποιότητα των συνδέσεων κάτω από το επιθυμητό επίπεδο, φτάνει ο συνδυασμός τους να είναι αρκετός για να παρέχει την αναγκαία ποιότητα σύνδεσης. Σαν αποτέλεσμα της μείωσης της ποιότητας της ραδιο – σύνδεσης, η ενέργεια μετάδοσης μπορεί να κρατηθεί σε χαμηλά επίπεδα κατά την διάρκεια του soft handover, και παράλληλα να παρέχεται η ίδια ποιότητα σε υψηλότερο επίπεδο, όπως φαίνεται και από τα αποτελέσματα του σεναρίου.

3. GMM¹ end-to end delay και για τα δύο σενάρια που αντιπροσωπεύει την καθυστέρηση επικοινωνίας από το GMM στον κάθε κινητό κόμβο.

Βλέπουμε στο σχήμα 6.7 την GMM σημείο προς σημείο καθυστέρηση και για τα δυο σενάρια και για τους δυο κόμβους.

¹ GMM (GPRS Mobility Management): Πολύπλευρο πρωτόκολλο που λειτουργεί για σκοπούς σήμανσης του GPRS και χειρίζεται roaming, προτυποποίηση και επιλογή αλγορίθμων κρυπτογράφησης. thin the signaling plane of GPRS handling such things as: roaming, authentication, and selection of encryption algorithms

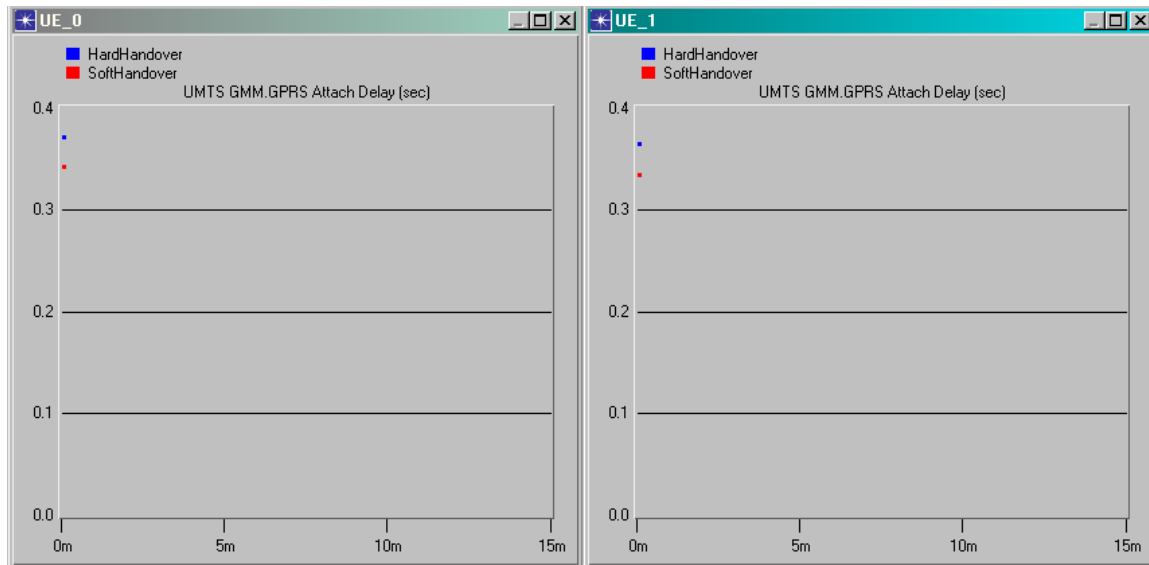


Σχήμα 6.7

Όπως βλέπουμε, στο Soft Handover υπάρχει μια σταθερή και μικρή καθυστέρηση, ενώ στο Hard Handover αρχικά παρουσιάζεται μια σημαντική καθυστέρηση η οποία όμως στην συνέχεια μειώνεται. Αυτό πολύ πιθανό να οφείλεται στο γεγονός ότι στην περίπτωση του Soft Handover, οι κινητοί κόμβοι έχουν ένα αριθμό από Node-Bs (στο Active Set τους) τους οποίους μπορούν να χρησιμοποιήσουν ανάλογα. Στο Hard Handover όμως, πρέπει να περιμένουν οι κινητοί κόμβοι μέχρι να μην μπορούν αν χρησιμοποιήσουν καθόλου τον παλιό Node-B για να συνδεθούν με κάποιο άλλο. Ίσως η μεγάλη αρχική καθυστέρηση στην επικοινωνία με το GMM να οφείλεται λοιπόν στην εξασθένηση της σύνδεσης με τον παλιό Node-B και κατά συνέπεια υπάρχει καθυστέρηση στην επικοινωνία με τον GMM. Με την σύνδεση με καινούργιο Node-B, μειώνεται και η καθυστέρηση.

4. GPRS attach delay που παρουσιάζει την καθυστέρηση GPRS σύνδεσης των κινητών κόμβων.

Βλέπουμε στο σχήμα 6.8 την GPRS καθυστέρηση σύνδεσης και για τα δυο σενάρια και για τους δυο κόμβους.

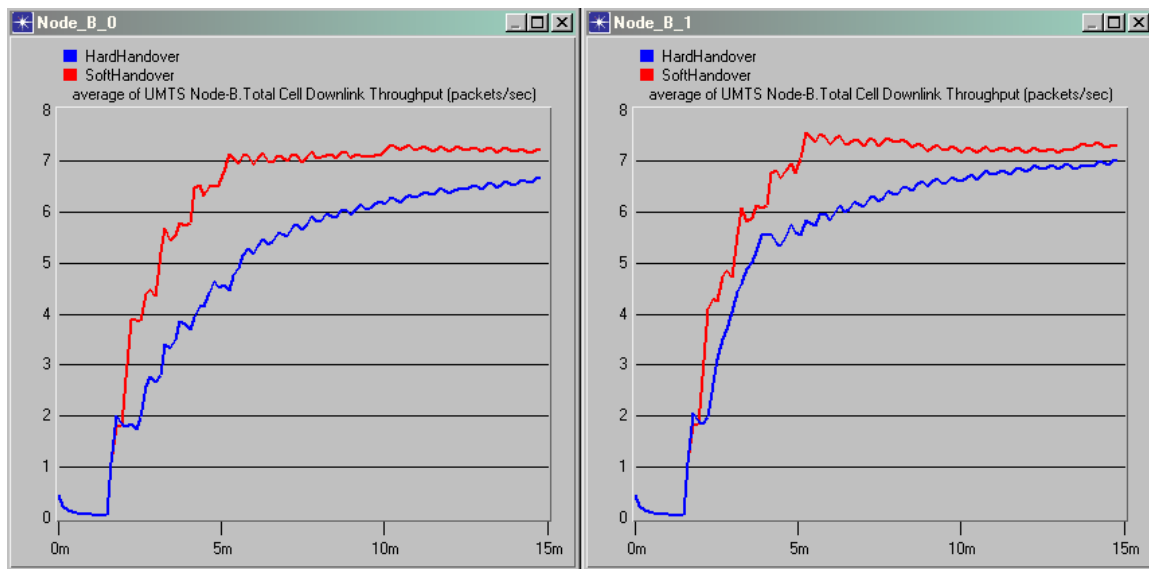


Σχήμα 6.8

Βλέπουμε ότι είναι πολύ μικρή η διαφορά καθυστέρησης μεταξύ του Soft και του Hard Handover σεναρίου.

5. Node-B total cell downlink throughput (packets/sec) που αντιπροσωπεύει την ολική παραγωγή (throughput) του downlink για κάθε Node-B, σε πακέτα ανά δευτερόλεπτο.

Βλέπουμε στο σχήμα 6.9 την ολική παραγωγή downlink για κάθε κόμβο και κάθε σενάριο.

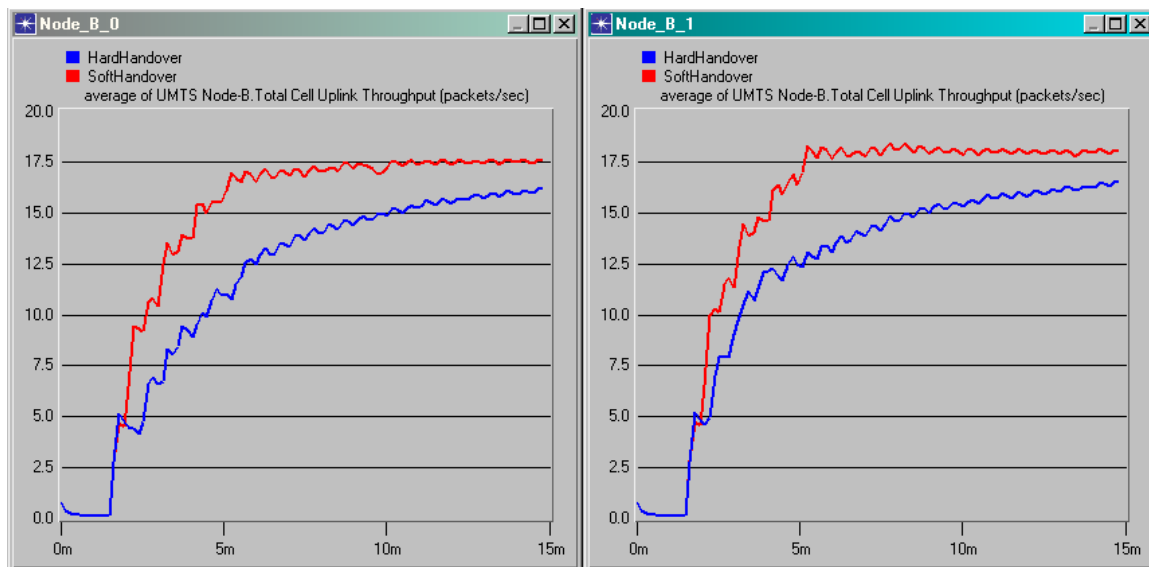


Σχήμα 6.9

Φαίνεται ότι δεν υπάρχει κάποια σημαντική διαφορά μεταξύ του Soft και Hard Handover, αλλά στην περίπτωση του Soft Handover, υπάρχει περισσότερη παραγωγή πακέτων για downlink. Αυτό και πάλι μπορεί να οφείλεται στο ότι υπάρχει μια πιο ομαλή και σταθερή σύνδεση μεταξύ ενός Node-B και των κινητών κόμβων στο Soft Handover. Έτσι αξιοποιείται καλύτερα το downlink παρά στο Hard Handover που καθυστερεί να γίνει η σύνδεση του κόμβου με καινούργιο Node-B.

6. Node-B total cell uplink throughput (packets/sec) που αντιπροσωπεύει την ολική παραγωγή (throughput) του uplink για κάθε Node-B, σε πακέτα ανά δευτερόλεπτο.

Βλέπουμε στο σχήμα 6.10 την ολική παραγωγή του uplink για κάθε κόμβο και κάθε σενάριο.

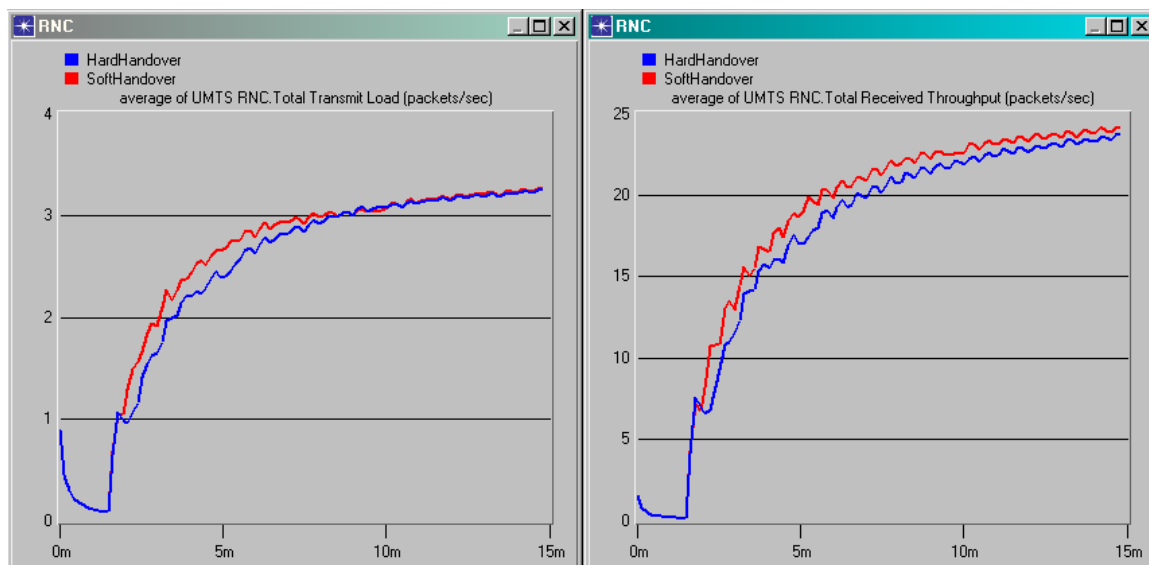


Σχήμα 6.10

Ισχύουν τα ίδια συμπεράσματα όπως και για το total cell downlink throughput.

7. RNC total transmit load (packets/sec) και RNC total received Throughput(packets/sec) που αντιπροσωπεύει το ολικό «φορτίο» που έχει μεταδοθεί και παραληφθεί αντίστοιχα από το RNC.

Βλέπουμε στο σχήμα 6.11 το ολικό φορτίο που έχει μεταδοθεί και παραληφθεί από τον RNC και για τα δυο σενάρια.

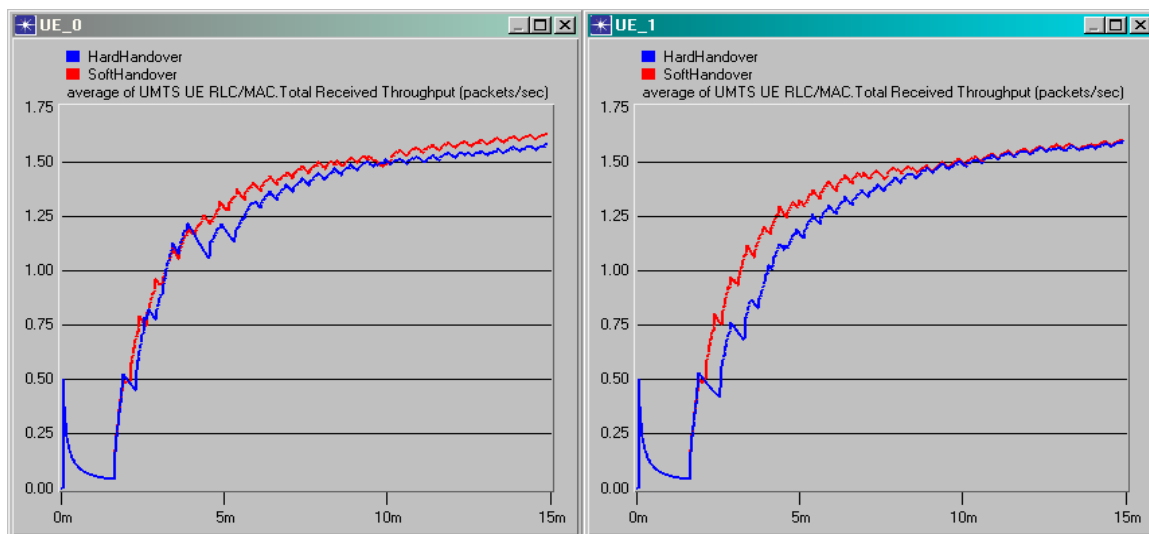


Σχήμα 6.11

Και πάλι βλέπουμε πως δεν υπάρχει ιδιαίτερη διαφορά μεταξύ των δύο σεναρίων, εκτός του ότι το RNC στο Soft Handover σε μερικά σημεία έχει στείλει και παραλάβει ελαφρώς περισσότερα πακέτα. Αυτό και πάλι ίσως να οφείλεται στο γεγονός της πιο ομαλής σύνδεσης των κινητών κόμβων με τα Node-Bs στο Soft Handover.

8. UE Total Received Throughput (packets / sec) που παρουσιάζει την ολική παραγωγή που έχει παραλάβει κάθε κόμβος και στα δύο σενάρια.

Βλέπουμε στο σχήμα 6.12 την ολική παραγωγή που έχει παραλάβει κάθε κόμβος και για τα δυο σενάρια.

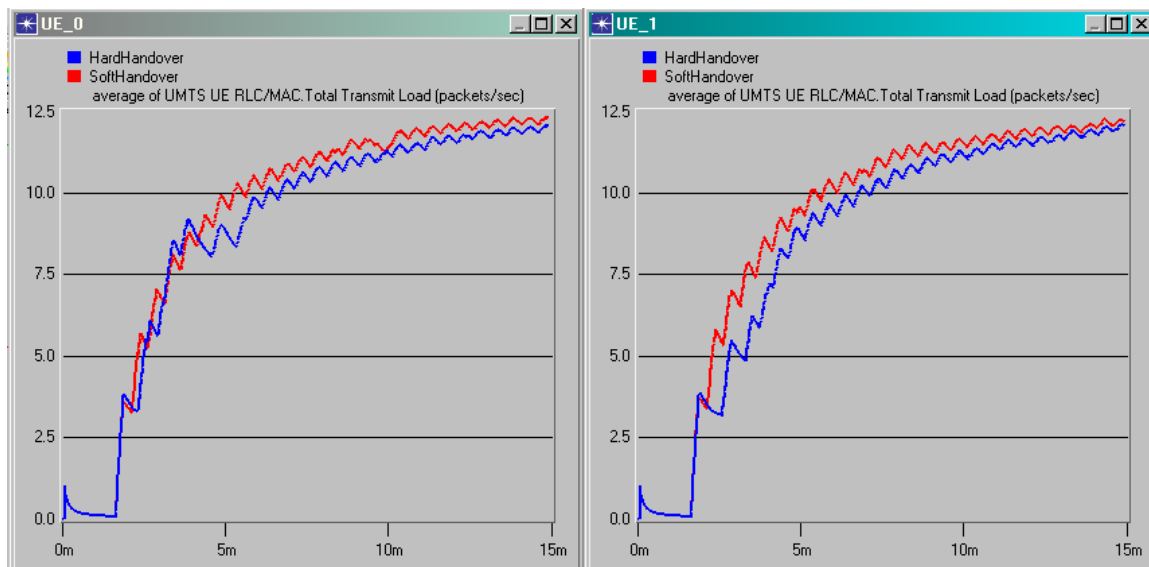


Σχήμα 6.12

Ισχύουν τα ίδια συμπεράσματα με την προηγούμενη στατιστική.

9. UE Total Transmit Load (packets / sec) που παρουσιάζει τον ολικό «φορτίο» που έχει στείλει κάθε κόμβος και στα δύο σενάρια.

Βλέπουμε στο σχήμα 6.13 το ολικό φορτίο που έχει στείλει κάθε κόμβος και για τα δυο σενάρια.



Σχήμα 6.13

Ισχύουν τα ίδια συμπεράσματα με την προηγούμενη στατιστική.

6.4 Συμπεράσματα

Βάσει αυτών των στατιστικών και των σεναρίων, φαίνεται ότι το Soft Handover είναι σε ορισμένες περιπτώσεις πιο αποδοτικό και λιγότερο δαπανηρό (σε χρόνο και ενέργεια) από το Hard Handover. Όμως, όχι μόνο δεν μπορούμε να αποφύγουμε τη χρήση του Hard Handover, αλλά υπάρχουν περιπτώσεις που μόνο Hard Handover μπορεί να χρησιμοποιηθεί.

Όπως έχει ήδη αναφερθεί, ένα handover για το οποίο χρειάζεται αλλαγή της συχνότητας του φορέα πρέπει πάντα είναι hard handover, γιατί δεν μπορούν να κρατηθούν συνδέσεις με πολλά Node-Bs (όπως γίνεται στο soft handover) όταν τα Node-Bs λειτουργούν σε διαφορετικές συχνότητες.

Ακόμη, λόγω του ότι το Soft Handover βασίζεται στο macro diversity, μπορούν να προκληθούν προβλήματα αν είναι περιορισμένος ο αριθμός των ραδιο – συνδέσμων που είναι ενεργοί μια χρονική στιγμή. Η όλη ιδέα του soft handover βασίζεται στον συνδυασμό της ποιότητας όλων των ραδιο – συνδέσμων που χρησιμοποιούνται εκείνη τη στιγμή από τον κινητό κόμβο. Ο περιορισμένος αριθμός των ραδιο – συνδέσμων λοιπόν, μπορεί να έχει επιρροή στην επικοινωνία των διάφορων στοιχείων του δικτύου.

Κεφάλαιο 7

Συμπεράσματα

Καμιά φορά μπορεί εύκολα κάποιος να χαθεί μέσα στις ορολογίες, στην θεωρία, στα bits και bytes. Το πιο σημαντικό όμως που δεν πρέπει ποτέ να ξεχνάμε είναι ότι όλα άρχισαν από τον άνθρωπο και όλα πρέπει σε τελική ανάλυση να κατευθύνονται προς εκεί και στην ικανοποίηση των αναγκών του χρήστη. Τέτοιες είναι λοιπόν οι ανάγκες του σημερινού χρήστη που ζητά να συνδυάζει κίνηση με σύνδεση στο δίκτυο και καλή ποιότητα υπηρεσίας. Έτσι και το UMTS σχεδιάστηκε με τέτοιο τρόπο για να προσφέρει στον μέσο χρήστη τις βασικές υπηρεσίες και να συνδυάζει επίσης πιο ανεπτυγμένες packet – switched και circuit – switched υπηρεσίες κάτω από μια συνενωμένη All – IP αρχιτεκτονική.

Συνεχίζοντας με την ιδέα ικανοποίησης του χρήστη, δεν μπορούσε να μη γίνει πρόνοια για εφικτή επικοινωνία με χρήστες άλλων συστημάτων. Για αυτό το σημείο θα βοηθήσει πολύ η πραγματοποίηση ενός «οράματος» αν μπορούμε να το αποκαλέσουμε έτσι, τη «συνένωση» των διάφορων ειδών δικτύων κάτω από ένα κοινό πρωτόκολλο network layer. Να μπορέσει να υπάρξει αυτή η κοινή πλατφόρμα που να λειτουργούν πάνω τα διάφορα δικτυακά συστήματα, ανεξάρτητα από το είδος του δικτύου και τα πρωτόκολλα που χρησιμοποιούνται στα άλλα layers του TCP/IP stack.

Η ανάγκη για κοινό network layer πρωτόκολλο εξηγήθηκε αναλυτικότερα στο δεύτερο κεφάλαιο με την ανάλυση των WLAN συστημάτων τα οποία έχουν γίνει πλέον αναπόσπαστο κομμάτι του δικτυακού κόσμου. Θα είναι μεγάλη απειρσκεψία οποιοδήποτε διαχειριστή δικτύου να μην προνοήσει για επικοινωνία του δικτύου με τα διάφορα WLAN συστήματα. Θεωρείται γεγονός λοιπόν, ότι οι UMTS χρήστες πρέπει να έχουν αποτελεσματική επικοινωνία με χρήστες WLAN συστημάτων όπως και με χρήστες LAN συστημάτων και άλλων συστημάτων κινητών δικτύων. Για παράδειγμα, ο UMTS χρήστης πρέπει να μπορεί να επικοινωνεί φωνητικά με ένα GSM χρήστη, να λαμβάνει

ένα αρχείο από ένα χρήστη σε ένα Ethernet LAN και να λαμβάνει μηνύματα πολυμέσων από ένα Bluetooth χρήστη.

Ένα από τους σημαντικότερους παράγοντες που πρέπει να ληφθούν υπόψη στην σχεδίαση και υλοποίηση του UMTS είναι η επικοινωνία με τερματικά διαμέσω του Διαδικτύου, το οποίο Διαδίκτυο όπως είναι πολύ γνωστό χρησιμοποιεί το IP πρωτόκολλο και «μεταναστεύει» προς το IPv6. Η επικοινωνία με το Διαδίκτυο είναι και ένας παράγοντας που επηρεάζει και τους σχεδιαστές των διαφόρων LAN, WLAN, σταθερών και κινητών δικτύων γενικότερα. Φαίνεται πολύ λογικό τότε, ότι το κοινό πρωτόκολλο που θα συνενώσει τον κόσμο των δικτύων είναι το IPv6 και Mobile IPv6 για τα κινητά δίκτυα.

Έχουν παρουσιαστεί οι λόγοι που το Mobile IPv6 είναι πολύ πιο αποδοτικό από το Mobile IPv4 και γιατί θα προσφέρει περισσότερα στα τρίτης γενεάς κινητά δίκτυα. Μερικοί από τους λόγους που αναφέρθηκαν είναι: ο μεγαλύτερος αριθμός διαθέσιμων διευθύνσεων, η χρήση του Dynamic Home Agent Discovery, οι ενσωματωμένοι μηχανισμοί ασφάλειας, χρήση Route Optimization και τα λοιπά. Παρουσιάζονται διάφοροι μηχανισμοί μετάβασης και φαίνεται ότι οι μηχανισμοί αυτοί παρέχουν τα αναγκαία εργαλεία για μετάβαση από το IPv4 στο IPv6. Ο κάθε μηχανισμός έχει και τα δικά του χαρακτηριστικά και μπορεί να επιλύσει διαφορετικά προβλήματα. Για παράδειγμα ο DSTM παρέχει μετάφραση μεταξύ IPv4 και IPv6 διευθύνσεων χωρίς να σπάζει την end – to – end ασφάλεια και παρέχεται εύκολα IPv6 κινητικότητα, αλλά χρειάζεται ένα σύνολο από IPv4 διευθύνσεις και αυτό μπορεί να είναι πρόβλημα (έλλειψη IPv4 διευθύνσεων). Ενώ ο NAT-PT δεν μπορεί να παρέχει end – to – end ασφάλεια, ούτε υποστηρίζει αποτελεσματική κινητικότητα. Τέλος, μερικοί tunneling μηχανισμοί απαιτούν μια multicast υποδομή σε όλο το Διαδίκτυο, πράγμα που μπορεί να μην είναι δυνατό, ή απαιτούν την δημιουργία στατικού τούνελ που είναι πολύ μη αποδοτική μέθοδος.

Μιλώντας τώρα αποκλειστικά για τα UMTS, έχουν παρουσιαστεί έξι διαφορετικά σενάρια που διαγράφουν κάποιες δυνατές περιπτώσεις λειτουργίας του UMTS με IPv4 ή

IPv6 και πως επιτυγχάνεται η επικοινωνία με εφαρμογές που τρέχουν σε hosts του Διαδικτύου. Είναι αβέβαιο το αν όντως θα υλοποιηθούν αυτά τα σενάρια ακριβώς όπως έχουν παρουσιαστεί, αλλά το EURESCOM πιστεύει ότι σε κάποια χρονική στιγμή είναι πολύ πιθανή η υλοποίησή τους. Επίσης, λόγω του ότι το UTRAN μέρος του UMTS δικτύου είναι εντελώς απομονωμένο από το κυρίως δίκτυο, μπορεί να λειτουργήσει και με άλλα είδη δικτύων, σαν WLANS [22].

Το EURESCOM αναμένει ότι τα δυο πρώτα σενάρια που επικεντρώνονται στην UMTS Έκδοση 99 πιθανό να είναι από τα πρώτα που θα υλοποιηθούν από τους διαχειριστές, όπου τα UMTS τερματικά θα είναι διπλής στοίβας και οι εφαρμογές τόσο IPv4 όσο και IPv6 και θα επικοινωνούν είτε με IPv4 είτε με IPv6 εφαρμογές σε hosts του Διαδικτύου. Τα υπόλοιπα σενάρια αναφέρονται στην All IP έκδοση του UMTS και αναμένεται να υλοποιηθούν σε μετέπειτα φάση. Το κάθε ένα από αυτά διαγράφει και διαφορετικό συνδυασμό του πρωτοκόλλου που χρησιμοποιείται από το UMTS δίκτυο, από τα τερματικά και τις εφαρμογές και του πρωτοκόλλου που χρησιμοποιείται από το Διαδίκτυο και τις εφαρμογές που τρέχουν στους hosts.

Για όσα σενάρια υποστήριζαν IPv6 κινητικότητα, η χρήση του κάθε πρωτοκόλλου IPv4 ή IPv6 δεν επηρέασε αρνητικά την φάση του UMYs handover. Για περισσότερη κατανόηση του handover έχουν παρουσιαστεί και κάποιες μελέτες προσομοιώσεων που έγιναν με την χρήση του εργαλείου OPNET. Βάσει κάποιων στατιστικών που έχουν μαζευτεί από τις προσομοιώσεις, μπόρεσαν να εξαχθούν κάποια συμπεράσματα για το Soft και Hard Handover. Συγκεκριμένα το Soft Handover σε μερικές περιπτώσεις παρουσιάζεται κάπως πιο αποδοτικό από το Hard Handover αλλά για αλλαγή συχνότητας φορέα είναι αναγκαία η χρήση του Hard Handover.

Με γνώμονα την συνένωση των δικτύων κάτω από το IPv6, το UMTS παρουσιάζεται να μπορεί να χρησιμοποιήσει τους διαθέσιμους μηχανισμούς μετάβασης και να υποστηρίξει την χρήση του IPv6, χωρίς να επηρεάζονται σε σημαντικό βαθμό η κινητικότητα του χρήστη, η επικοινωνία με άλλους hosts, το QoS και η ασφάλεια του δικτύου. Είναι αναγκαίες φυσικά κι άλλες μελέτες για καλύτερη κατανόηση των προκλήσεων της

χρήσης του IPv6 σε ένα UMTS περιβάλλον, αλλά σαν μια πρώτη ματιά φαίνεται το UMTS θα μπορέσει να αντισταθεί στις προκλήσεις αυτές και να παίζει σημαντικό ρόλο στο κόσμο των δικτύων, τόσο από τεχνολογικής πλευράς όσο και από πλευράς προσφερόμενων υπηρεσιών στον μέσο χρήστη.

Βιβλιογραφία

- [1] “Mobile Communications” Jochen Schiller
- [2] <http://3gsolutions.members.easyspace.com>
- [3] http://www.3g-generation.com/release_99.htm
- [4] <http://www.apnic.net/meetings/12/docs/1>
- [5] <http://www.computer.org/internet/v2n1/perkins.htm>
- [6] <http://www.computer.org/students/looking/summer97/ieee802.htm>
- [7] <http://www.eurescom.de/~pub-deliverables/P1000-series/P1009/D3/p1009d3.pdf>
- [8] http://www.hpl.hp.com/personal/Jean_Tourrilhes/MobileIP/known
- [9] <http://www.iec.org/online/tutorials/umts/topic01.html>
- [10] <http://www.ipv6forum.com/navbar/events/birmingham00/presentations/PDF/AskoRasanen.pdf>
- [11] http://www.ipv6forum.com/navbar/papers/MobileIPv6_Whitepaper.pdf
- [12] http://www.isoc.org/inet2001/CD_proceedings/T28/T28.htm
- [13] <http://www.kbs.uni-hannover.de/~boris/hiperlan/faq3.html>
- [14] http://www.mpirical.com/companion/mpirical_companion.html#http://www.mpirical.com/companion/UMTS/Node_B.htm
- [15] <http://www.palowireless.com/infotooth/tutorial/baseband.asp#Physical%20Characteristics>
- [16] http://www.sipcenter.com/files/Award_SIP_3GPP-2.pdf
- [17] <http://www.spectrum.ieee.org/pubs/spectrum/9908/cell.html>
- [18] <http://www.swedetrack.com/images/bluet10.htm>
- [19] <http://www.tbm.tudelft.nl/webstaf/rudiw/TB9612/UMTS/umts5.htm#5>
- [20] <http://www.telematik.informatik.uni-karlsruhe.de/~schiller>
- [21] <http://www.tml.hut.fi/Studies/Tik-110.300/1999/Essays/hiperlan2.html>
- [22] <http://www.umtsworld.com/technology/handover.htm>
- [23] <http://www.wirelessdevnet.com/channels/bluetooth/features/bluetooth.html>