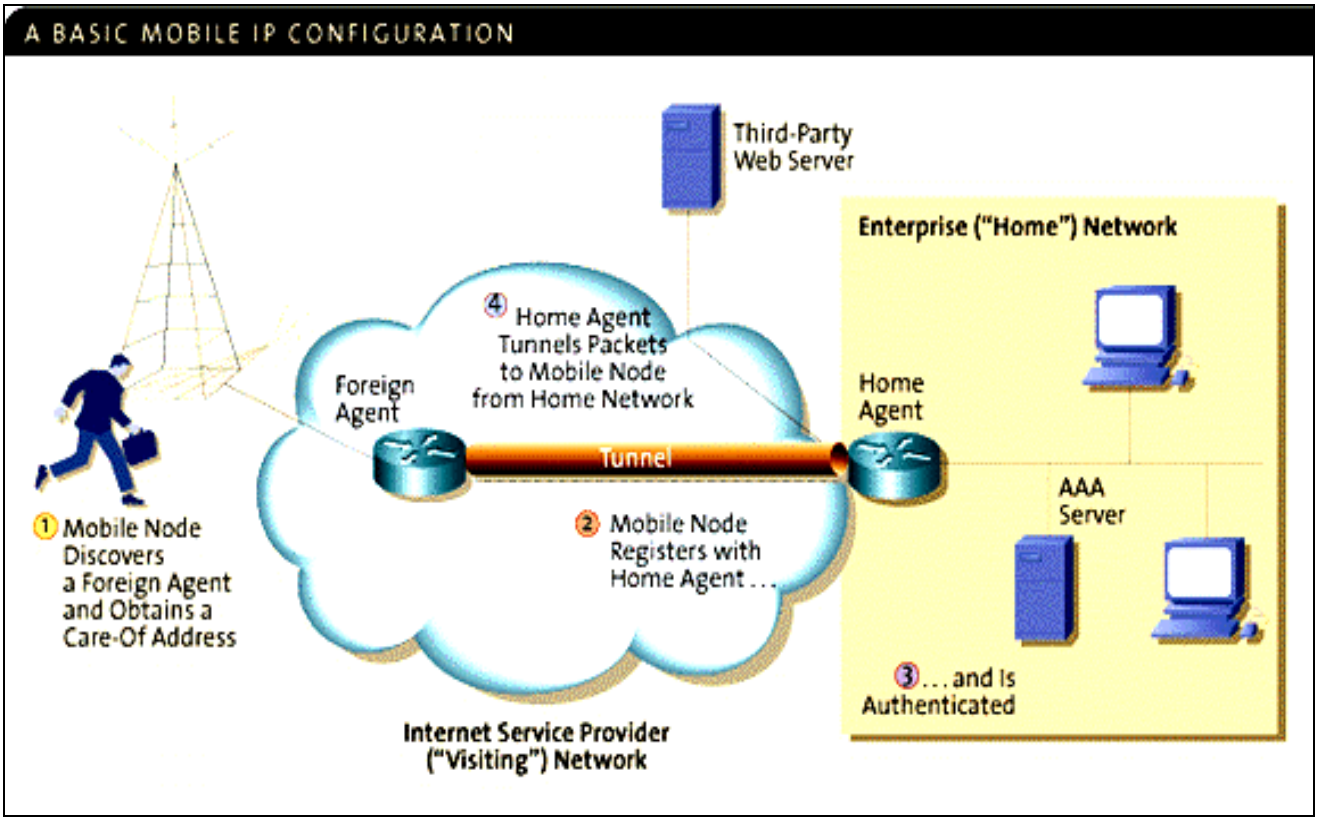
MOBILE IP

Internet Unplugged

ΤΕΙ ΚΡΗΤΗΣ
ΠΑΡΑΡΤΗΜΑ ΧΑΝΙΩΝ
ΤΜΗΜΑ ΗΛΕΚΤΡΟΝΙΚΗΣ



ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ: ΤΕΡΖΗ ΓΕΩΡΓΙΟΥ
ΕΙΣΗΓΗΤΗΣ: ΛΙΟΔΑΚΗΣ ΓΕΩΡΓΙΟΣ

ΧΑΝΙΑ 2002

ΠΡΟΛΟΓΟΣ

Οι σύγχρονες συνθήκες εργασίας έχουν δημιουργήσει ανάγκες για αυξημένη κινητικότητα ορισμένων κατηγοριών επαγγελματιών με αποτέλεσμα να καθίσταται αναγκαία η δυνατότητα διασύνδεσης τόσο με το δίκτυο της εταιρίας τους (***Virtual Private Network***), όσο και με το Διαδίκτυο ενώ θα κινούνται από περιοχή σε περιοχή.

Ειδικότερα η εφαρμογή του Mobile IP πρωτοκόλλου αναφέρεται, βασικά, στην περίπτωση όπου γίνεται χρήση κάποιας ασύρματης τεχνολογίας πρόσβασης ***Wireless LANs*** , εγκατάσταση κυψελιδωτών δικτύων τρίτης γενιάς και ***Private Mobile Radio*** συστημάτων, χωρίς βέβαια να υποβαθμίζεται η έννοια της ενσύρματης πρόσβασης .

Έτσι, το πρωτόκολλο Mobile IP έρχεται να καλύψει καταστάσεις όπου προκύπτει το λεγόμενο macro mobility management problem (υποβοήθηση χρηστών εφοδιασμένων με συσκευές όπως notebooks, PDAs , κινητά τηλεφωνά τρίτης γενιάς κλπ) κατά τη μετάβαση τους από το IP υποδίκτυο στο οποίο ανήκουν (Home network) σε ένα άλλο (Foreign Network) . Στη διαδικασία αυτή εμπλέκονται διάφορες δικτυακές συσκευές οι οποίες θα αναφέρονται ως **Home Agents** και **Foreign Agents** αντίστοιχα , ενώ δεν θα παραβλέψουμε και τα ζητήματα ασφάλειας που ανακύπτουν .

Το υπάρχον πρωτόκολλο με τη βοήθεια του οποίου γίνονται εφικτά τα παραπάνω είναι γνωστό ως **Mobile IPv4** . Οι πραγματικά κοσμογονικές αλλαγές που μελετώνται και προβλέπεται να εφαρμοστούν στο χώρο του Διαδικτύου δεν θα ήταν δυνατό να αφήσουν ανεπηρέαστο και αυτόν τον τομέα , ο οποίος μάλιστα λόγω των μεγάλων αναγκών που προβλέπεται να δημιουργηθούν αναβαθμίζεται σημαντικά , και προβλέπεται να διαδραματίσει σημαντικό ρόλο στο, όχι και τόσο μακρινό, μέλλον .

Τα παραπάνω αποτέλεσαν το ερέθισμα για την εκπόνηση της παρούσας πτυχιακής εργασίας με απώτερο στόχο να καταστήσει τα μυστικά του κτήμα των αναγνωστών της και, γιατί όχι, να δώσει ερεθίσματα για περαιτέρω «ψάξιμο» αυτού του πραγματικά πολύ ενδιαφέροντος επιστημονικού πεδίου που ασχολείται με Ασύρματες Τεχνολογίες και Δίκτυα Υπολογιστών/ Internet. Στην εργασία αυτή θα παρουσιάσουμε, ακόμα, τη διαδικασία που πρέπει να ακολουθηθεί ώστε να εφαρμόσουμε τις αρχές του πρωτοκόλλου σε ένα συμβατικό υπολογιστή. Για το σκοπό αυτό χρησιμοποιήσαμε μια δοκιμασμένη και αξιόπιστη υλοποίηση του πανεπιστημίου Stanford που εδρεύει στην California (www.Stanford.edu). Θα περιγράψουμε αναλυτικά την όλη διαδικασία ενώ στο συνοδευτικό cd υπάρχει όλο το αναγκαίο software στην περίπτωση που κάποιος επιθυμεί να πειραματιστεί στον προσωπικό του υπολογιστή.

ΚΕΦΑΛΑΙΟ 1

ΕΙΣΑΓΩΓΗ

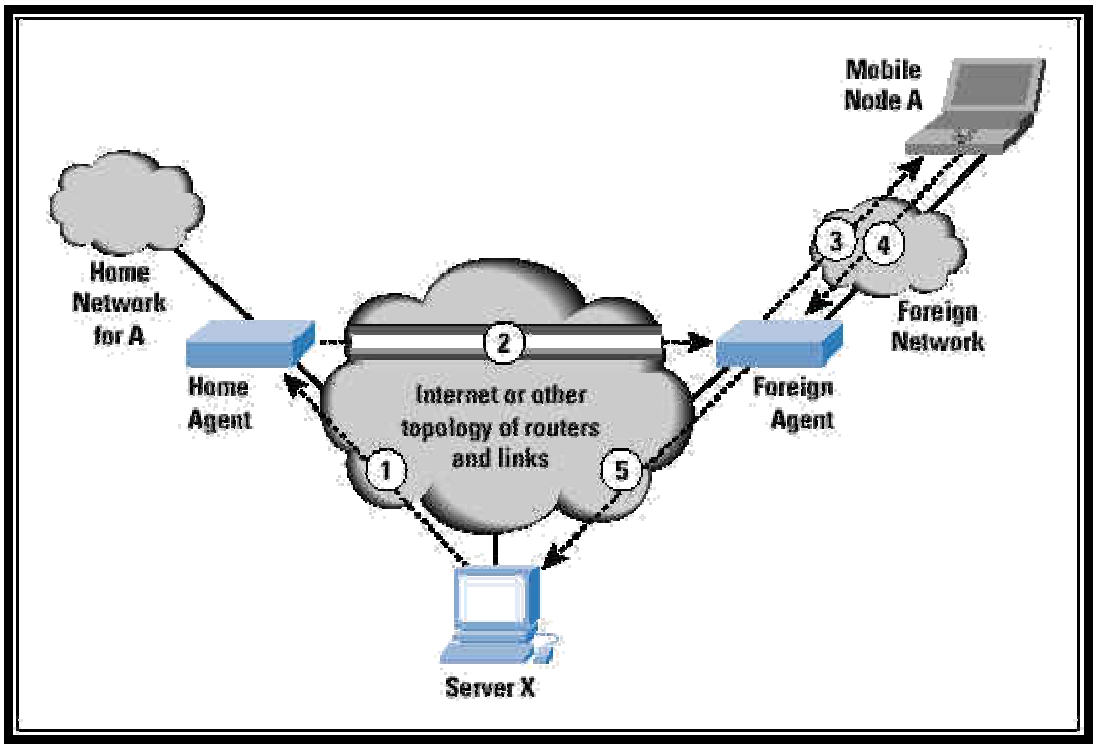
1.ΕΙΣΑΓΩΓΙΚΕΣ ΕΝΝΟΙΕΣ

1.1 Βασική Ορολογία

Αρχικά θα επιχειρήσουμε να κάνουμε απολύτως κατανοητό τον όρο «Mobile» και τι αυτός συνεπάγεται. Ο όρος αυτός υπονοεί ότι έχουμε ένα χρηστή συνδεδεμένο με μια η περισσότερες εφαρμογές στο διαδίκτυο και ότι ενώ το γεωγραφικό αρχικό σημείο σύνδεσης αλλάζει (***point of attachment***) όλες οι συνδέσεις παραμένουν ως είχαν χωρίς καμία απώλεια δεδομένων .

Γίνεται εύκολα κατανοητή η διάφορα με την περίπτωση που ένας χρηστής φορητού υπολογιστή συνδέεται με το διαδίκτυο σε μια περιοχή , διακόπτει τη σύνδεση , μετακινείται σε μια νέα περιοχή και επανασυνδέεται από αυτή.

Με τη βοήθεια του παρακάτω σχήματος θα επιχειρήσουμε να καταδείξουμε τις βασικές λειτουργίες που επιτελεί το πρωτόκολλο ώστε να ικανοποιήσει τις παραπάνω απαιτήσεις.



Σχήμα 1

Οι δρομολογητές (Routers) χρησιμοποιούν τη διεύθυνση IP η οποία βρίσκεται στο IP datagram για να επιτύχουν τη δρομολόγηση του εκάστοτε πακέτου στον προορισμό τους.

Πιο συγκεκριμένα το δικτυακό τμήμα της IP διεύθυνσης χρησιμοποιείται για να μεταφερθεί το datagram από τον αρχικό υπολογιστή στο δίκτυο στο οποίο βρίσκεται ο υπολογιστής αποδεκτής . Στη συνεχεία ο τελευταίος δρομολογητης , ο οποίος βρίσκεται στο ίδιο δίκτυο με τον υπολογιστή-αποδέκτη, χρησιμοποιεί το host portion της IP διεύθυνσης για να παραδοθεί, τελικά, το datagram στον στόχο.

Τα προβλήματα, ωστόσο, ξεκινούν όταν η IP διεύθυνση του υπολογιστή-αποδέκτη αλλάζει ενώ δεδομένα κατευθύνονται προς αυτή.

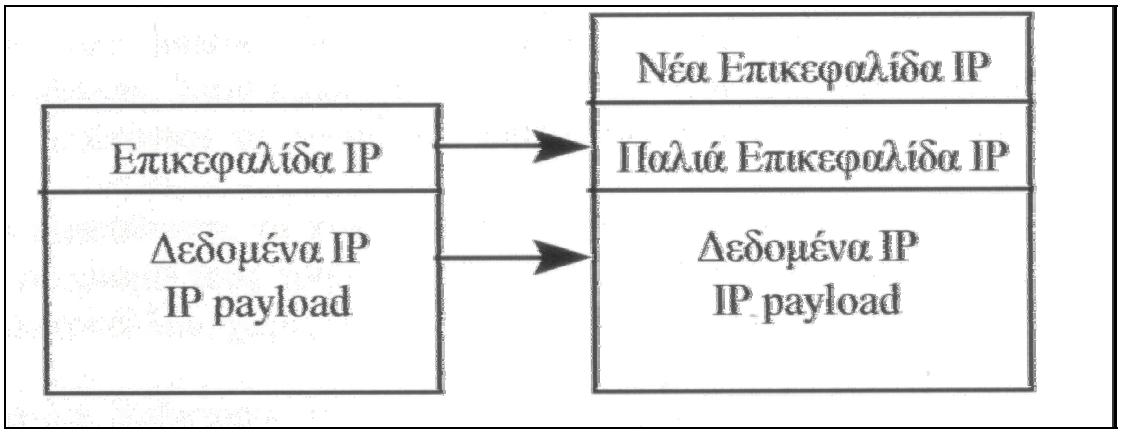
Το παραπάνω σχήμα μας δείχνει πως το πρωτόκολλο Mobile IP αντιμετωπίζει το πρόβλημα της, δυναμικά μεταβαλλόμενης, διεύθυνσης.

Έστω ένας κινητός κόμβος ο οποίος ανήκει σε ένα δίκτυο (***Home Network***), οπότε έχει μια διεύθυνση IP που παραμένει ίδια (στατική). Όταν ο κινητός κόμβος αλλάζει το σημείο σύνδεσης του από το αρχικό δίκτυο σε ένα άλλο , το επόμενο δίκτυο θεωρείται ως foreign network, (***Foreign Network***).Όταν ο κινητός κόμβος επανασυνδέεται, στο νέο δίκτυο πλέον, κάνει την παρουσία του γνωστή «εγγραφόμενος» σε ένα κόμβο του νέου δικτύου, συνήθως ένα δρομολογητή ,τον οποίο ονομάζουμε ***Foreign Agent.*** Ο κινητός κόμβος στη συνεχεία επικοινωνεί με ένα παρόμοιο υπολογιστή στο αρχικό δίκτυο, γνωστός ως ***Home Agent***, δίνοντας του την Care-Of διεύθυνση που έχει στο νέο δίκτυο. Η care-of διεύθυνση δίνει τη διεύθυνση του ***Foreign Agent*** .

Το ρόλο του ***Home agent*** όσο και του ***Foreign Agent*** αναλαμβάνουν τις συντριπτικά περισσότερες φορές δρομολογητες (Routers).

Όταν IP διαγράμματα δεδομένων ανταλλάσσονται μεταξύ του κινητού κόμβου και ενός Server X λαμβάνουν χώρα οι εξής διαδικασίες :

- Ο Server X μεταδίδει ένα διάγραμμα δεδομένων προοριζόμενο για τον κινητό κόμβο A, με τη διεύθυνση που είχε ο A Όταν ήταν συνδεδεμένος στο αρχικό δίκτυο. Το διάγραμμα δεδομένων δρομολογείται στο αρχικό δίκτυο του A. (Διαδρομή 1)
- Φτάνοντας σε αυτό αναχαιτίζεται από το δρομολογητη που έχει αναλάβει το ρόλο του ***Home Agent***. Ο δρομολογητης τοποθετεί το αρχικό διάγραμμα δεδομένων εντός νέου το οποίο έχει στην επικεφαλίδα την Care-Of διεύθυνση του κινητού κόμβου (η πιο απλά την IP διεύθυνση που έχει πλέον στο νέο δίκτυο) και επαναμεταδίδει το διάγραμμα δεδομένων. Η παραπάνω διαδικασία είναι μια από τις πιο σημαντικές που εκτελεί το πρωτόκολλο και ονομάζεται Tunneling. (Διαδρομή 2) και απεικονίζεται στο παρακάτω σχήμα.

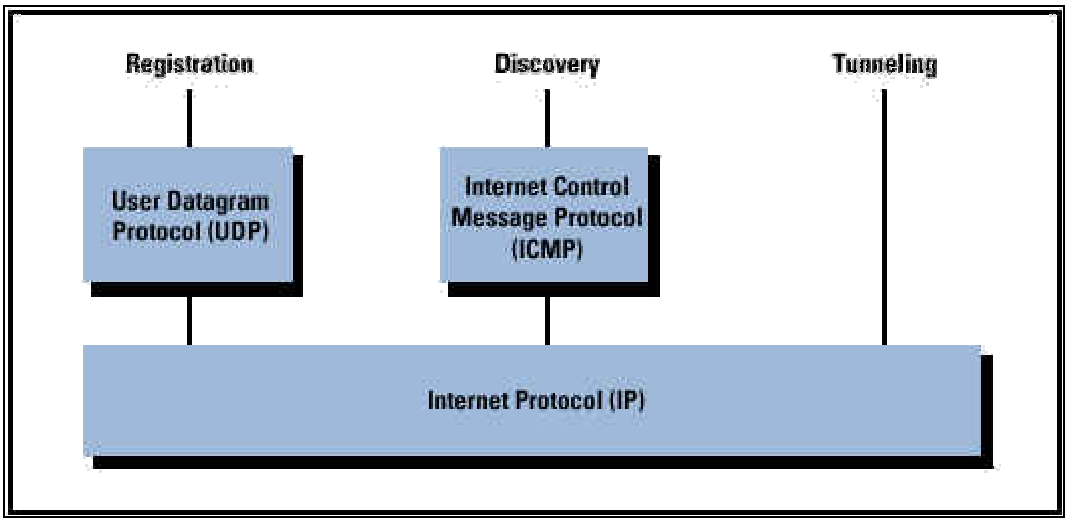


Σχήμα 2

- Ο Foreign Agent, όταν πλέον το διάγραμμα δεδομένων έχει φτάσει σε αυτόν, αφαιρεί την επικεφαλίδα IP που είχε προστεθεί σε αυτό, τοποθετεί το αρχικό διάγραμμα δεδομένων σε ένα δικτυακού επιπέδου πρωτόκολλο (Protocol Data Unit) και παραδίδει το αρχικό πακέτο στο δίκτυο (Foreign Network). (Διαδρομή 3)
- Όταν ο κινητός κόμβος Α στέλνει διαγράμματα δεδομένων IP προς τον Server X χρησιμοποιεί την IP διεύθυνση του. Στην περίπτωση που εξετάζουμε αυτή η διεύθυνση παραμένει σταθερή, συνεπώς ο Χ δεν μετακινείται. Κάθε διάγραμμα δεδομένων IP στέλνεται από τον κινητό κόμβο Α σε ένα δρομολογητη ο οποίος βρίσκεται στο foreign network με σκοπό τη δρομολόγηση του προς τον Χ.
- Το διάγραμμα δεδομένων IP που απέστειλε ο Α προς τον Χ ταξιδεύει στο δίκτυο χρησιμοποιώντας την IP διεύθυνση του Χ.

Για να υποστηρίξει τις παραπάνω λειτουργίες το πρωτόκολλο Mobile IP διαθέτει τις παρακάτω, τρεις, βασικές δυνατότητες (βλέπε σχήμα 3):

- ***Discovery***: Ο κινητός κόμβος χρησιμοποιεί μια διαδικασία ανακάλυψης πιθανών home agents και foreign agents.
- ***Registration***: Ο κινητός κόμβος χρησιμοποιεί μια διαδικασία πιστοποίησης της εγγραφής του για να ενημερώσει τον Home Agent, στον οποίο ανήκει, για την care-of διεύθυνση του.
- ***Tunneling***: Η διαδικασία αυτή χρησιμοποιείται για να προωθήσει διαγράμματα δεδομένων IP από την αρχική διεύθυνση στην care-of διεύθυνση.



Σχήμα 3

Το πρωτοκόλλου εγγραφής επικοινωνεί μεταξύ μιας εφαρμογής στον κινητό κόμβο και μιας εφαρμογής στον Home Agent, και γι'αυτο το λόγο χρησιμοποιεί πρωτόκολλο επιπέδου μεταφοράς. Λόγω του ότι η εγγραφή ***(Registration)***, είναι μια απλή συναλλαγή αιτήματος / απάντησης το υπερκείμενο πρωτόκολλο TCP ,το οποίο είναι προσανατολισμένο στην επίτευξη-διατήρηση σύνδεσης , δεν χρησιμοποιείται , καθώς η χρήση του ***User Datagram Protocol***, ως πρωτόκολλο μεταφοράς κρίνεται καταλληλότερη.

Η διαδικασία Discovery κάνει χρήση του υπάρχοντος ***Internet Control Message Protocol (ICMP)*** προσθέτοντας τις κατάλληλες επεκτάσεις στην επικεφαλίδα του πρωτοκόλλου. Το ICMP είναι πρωτόκολλο το οποίο δεν απαιτεί την ύπαρξη σύνδεσης μεταξύ κόμβων οπότε θεωρείται κατάλληλο για να φέρει σε πέρας την παραπάνω διαδικασία.

Η τελευταία διαδικασία, το ***Tunneling***, εκτελείται στο ***IP επίπεδο***.

Έχοντας αναλύσει ένα τυπικό παράδειγμα με τις βασικές λειτουργίες που εκτελεί το πρωτόκολλο, μπορούμε να συνεχίσουμε παρουσιάζοντας και αναλύοντας, με περισσότερες λεπτομέρειες , τόσο τις απαιτήσεις που υπάρχουν από το πρωτόκολλο όσο και τις προϋποθέσεις που απαιτείται να πληρούν το δίκτυο και οι συσκευές που χρησιμοποιούνται.

1.2. ΠΡΟΥΠΟΘΕΣΕΙΣ ΕΦΑΡΜΟΓΗΣ ΤΟΥ ΠΡΩΤΟΚΟΛΛΟΥ

Το Mobile IP υποθέτει ότι η διεύθυνση IP ενός κόμβου προσδιορίζει μεμονωμένα το σημείο του κόμβου της σύνδεσης στο Διαδίκτυο. Επομένως, ένας κόμβος πρέπει να βρεθεί στο δίκτυο που υποδεικνύεται από τη διεύθυνση IP του προκειμένου να παραληφθούν τα διαγράμματα δεδομένων που προορίζονται γι'αυτόν , διαφορετικά, τα διαγράμματα δεδομένων που προορίζονται για τον κόμβο θα ήταν χαμένα. Για έναν κόμβο, για να αλλάξει το σημείο σύνδεσής του χωρίς απώλεια της δυνατότητάς του να επικοινωνήσει, υπάρχουν οι εξής εναλλακτικές λύσεις:

- ο κόμβος πρέπει να αλλάξει τη διεύθυνση IP όταν αλλάζει το σημείο σύνδεσής του

- συγκεκριμένες, εικονικές, διαδρομές , για τον host , πρέπει να δημιουργηθούν σε ένα μεγάλο μέρος του φάσματος δρομολόγησης του Διαδικτύου.

Και οι δύο εναλλακτικές λύσεις είναι μη αποδεκτές. Η πρώτη καθιστά αδύνατο για έναν κόμβο να διατηρήσει τη μεταφορά και τις συνδέσεις υψηλού-στρώματος όταν αλλάζει θέση ενώ η δεύτερη έχει τα προφανή και σοβαρά προβλήματα αύξησης της κλίμακας, ιδιαίτερα εάν λάβουμε υπόψη την εκρηκτική αύξηση των πωλήσεων των κινητών υπολογιστών (notebook).

Ένας νέος, εξελικτικός, μηχανισμός απαιτείται για την προσαρμογή της κινητικότητας κόμβων μέσα στο Διαδίκτυο. Αναλυτικότερα, απαιτείται ένας μηχανισμός, ο οποίος θα επιτρέπει στους κόμβους να αλλάξουν το σημείο σύνδεσής τους στο Διαδίκτυο χωρίς αλλαγή της IP διεύθυνσης τους. Ειδικότερα:

i) Ένας κινητός κόμβος πρέπει να είναι σε θέση να επικοινωνήσει με άλλους κόμβους μετά από την αλλαγή της link-layer διασύνδεσης του χωρίς όμως αλλαγή της διεύθυνσης IP του.

ii) Ένας κινητός κόμβος πρέπει να είναι σε θέση να επικοινωνήσει με άλλους κόμβους που δεν εφαρμόζουν αυτές τις λειτουργίες κινητικότητας. Καμία βελτίωση πρωτοκόλλου δεν απαιτείται στους ξενιστές ή τους δρομολογητές που δεν ενεργούν όπως οποιεσδήποτε από τις νέες αρχιτεκτονικές οντότητες που περιγράφονται στην παράγραφο 1.2.

Όλα τα μηνύματα που χρησιμοποιούνται για να ενημερώσουν έναν άλλο κόμβο ως προς τη θέση ενός κινητού κόμβου πρέπει να επικυρωθούν προκειμένου να τον προστατεύσουν από απομακρυσμένες επιθέσεις ανακατεύθυνσης (redirect).

Η σύνδεση με την οποία ένας κινητός κόμβος εισέρχεται στο Διαδίκτυο μπορεί συχνά να είναι μια ασύρματη σύνδεση. Αυτή η σύνδεση έχει ένα ουσιαστικά χαμηλότερο εύρος ζώνης και ένα υψηλότερο ποσοστό σφαλμάτων από τα παραδοσιακά, συνδεμένα με καλώδιο δίκτυα. Επιπλέον, οι κινητοί κόμβοι είναι πιθανό να είναι φορητοί υπολογιστές, όποτε η ελαχιστοποίηση της κατανάλωσης ισχύος είναι σημαντική. Επομένως, ο αριθμός μηνυμάτων διαχείρισης που στέλνονται μέσω της σύνδεσης με την οποία ένας κινητός κόμβος είναι συνδεμένος με το Διαδίκτυο πρέπει να ελαχιστοποιηθεί, και το μέγεθος αυτών των μηνυμάτων πρέπει να κρατηθεί σε όσο το δυνατόν μικρότερη τιμή.

Το Mobile IP προορίζεται να επιτρέψει στους κόμβους να κινηθούν από ένα υποδίκτυο IP προς άλλο. Είναι εξίσου κατάλληλο για κινήσεις κόμβων μεταξύ ομοιογενών μέσων αλλά και για την κινητικότητα σε ετερογενή μέσα. Δηλαδή το Mobile IP διευκολύνει τη μετακίνηση κόμβων από ένα τμήμα δικτύου Ethernet σε ένα άλλο καθώς επίσης και προσαρμόζει τη μετακίνηση κόμβων από ένα τμήμα δικτύου Ethernet στο ασύρματο τοπικό LAN, εφ' όσον η διεύθυνση IP του κινητού κόμβου παραμένει η ίδια μετά από μια τέτοια μετακίνηση.

Κάποιος μπορεί να σκεφτεί το Mobile IP ως τη λύση του μακρο διοικητικού προβλήματος κινητικότητας, δεν είναι εξίσου καλά εφοδιασμένο, όμως, για την επίλυση του μικρό διοικητικού προβλήματος κινητικότητας, όπως παραδείγματος χάριν το handoff μεταξύ των ασύρματων πομποδεκτών, κάθε ένας από τους οποίους καλύπτει μόνο μια πολύ μικρή γεωγραφική περιοχή. Εφ' όσον δεν εμφανίζεται η μετακίνηση κόμβων μεταξύ των σημείων της σύνδεσης στα διαφορετικά υποδίκτυα IP, οι μηχανισμοί τύπου link-layer (π.χ , link-layer handoff) μπορούν να προσφέρουν τη γρηγορότερη σύγκλιση.

1.3. ΟΡΟΛΟΓΙΑ ΠΡΩΤΟΚΟΛΛΟΥ MOBILE IP

Το Mobile IP εισάγει τις ακόλουθες νέες λειτουργικές οντότητες για τις οποίες παρουσιάζουμε μια συνοπτική περιγραφή. Θα πρέπει να σημειώσουμε ότι για το υπόλοιπο της παρούσης εργασίας θα αναφερόμαστε σε αυτούς χρησιμοποιώντας την αγγλική ορολογία .

- **Κινητός κόμβος (*Mobile Node*)**

Ένας ξενιστής (Host) ή ένας δρομολογητής που αλλάζει το σημείο σύνδεσής του από το ένα δίκτυο ή υποδίκτυο σε άλλο. Ένας κινητός κόμβος μπορεί να αλλάξει τη θέση του χωρίς αλλαγή της IP διεύθυνσης του, μπορεί επίσης να συνεχίσει να επικοινωνεί με άλλους κόμβους του Διαδικτύου σε οποιαδήποτε θέση χρησιμοποιώντας (τη σταθερή) IP διεύθυνση του, υποθέτοντας ότι η συνδετικότητα σύνδεσης-στρώματος (link-layer) σε ένα τυχαίο σημείο σύνδεσης (point of attachment) είναι διαθέσιμη.

- **Οικείος πράκτορας (*Home Agent*)**

Ένας δρομολογητής στο οικείο δίκτυο ενός κινητού κόμβου ο οποίος δρομολογεί ένα διάγραμμα δεδομένων για παράδοση σε ένα κινητό κόμβο όταν είναι μακριά από το οικείο δίκτυο, και διατηρεί τις παρούσες πληροφορίες θέσης για τον κινητό κόμβο.

- **Foreign agent (*Foreign Agent*)**

Ένας δρομολογητής στο επισκεπτόμενο δίκτυο ενός κινητού κόμβου που παρέχει υπηρεσίες δρομολόγησης στον κινητό κόμβο ενώ αυτός εγγράφεται (στο νέο δίκτυο). Ο foreign agent detunnels και παραδίδει τα datagrams στον κινητό κόμβο που ανοίχτηκαν από το βασικό πράκτορα του κινητού κόμβου. Για τα datagrams που στέλνονται από έναν κινητό κόμβο, ο foreign agent μπορεί να χρησιμεύσει ως ένας προκαθορισμένος δρομολογητής για τους καταχωρημένους κινητούς κόμβους.

Σε έναν κινητό κόμβο δίνεται μια μακροπρόθεσμη διεύθυνση IP σε ένα βασικό δίκτυο. Αυτή η διεύθυνση κατοικίας αντιμετωπίζεται με τον ίδιο τρόπο όπως μια "μόνιμη" διεύθυνση IP παρέχεται σε έναν στάσιμο ξενιστή . Όταν βρίσκεται μακριά από το home network, μια "care-of address" ταυτίζεται με τον κινητό κόμβο και απεικονίζει την παρούσα

θέση του κινητού κόμβου. Ο κινητός κόμβος χρησιμοποιεί την αρχική διεύθυνση του ως διεύθυνση προέλευσης όλων των IP datagrams που στέλνει, εκτός από ορισμένες περιπτώσεις τις οποίες θα αναλύσουμε στη συνέχεια .

- **Διαφήμιση πρακτόρων (*Agent advertisement*)**

Ένα μήνυμα διαφημίσεων που υλοποιείται με την προσθήκη μιας ειδικής επέκτασης σε ένα router advertisement μήνυμα.

- **Πιστοποίηση ταυτότητας (*Authentication*)**

Η διαδικασία (που χρησιμοποιεί κρυπτογραφικές τεχνικές, για όλες τις εφαρμογές σε αυτήν την προδιαγραφή) για την εξακρίβωση της ταυτότητας του δημιουργού ενός μηνύματος.

- **Interface**

Η αλληλεπιδραστική σύνδεση ενός κόμβου

- **Κόμβος ανταπόκρισης (*Correspondent node*)**

Ένας ισότιμος κόμβος με τον οποίο επικοινωνεί ο κινητός κόμβος .Ο κόμβος αυτός μπορεί να είναι κινητός η σταθερός .

- **Care-of διεύθυνση (*Care-Of address*)**

Μια IP διεύθυνση η οποία σχετίζεται με τον κινητό κόμβο όταν αυτός βρίσκεται σε ένα foreign network. Μεταξύ των πολλαπλών care-of addresses που μπορεί να έχει ο κινητός κόμβος (μια διαφορετική για κάθε υποδίκτυο που επισκέπτεται) , αυτή που είναι συσχετισμένη με τον home agent του κινητού κόμβου ονομάζεται κύρια (primary) care-of address. Το πρωτόκολλο μπορεί να χρησιμοποιήσει δύο διαφορετικούς τύπους care-of address :

- **Foreign agent care-of address**: Ορίζεται ως η IP διεύθυνση ενός foreign agent με στην οποία ο κινητός κόμβος κάνει register.

- **Co-located care-of address:** Ορίζεται ως μια εξωτερικά αποκτηθείσα τοπική διεύθυνση που ο κινητός κόμβος έχει συνδέσει με μια από τις διασυνδέσεις (interfaces) του home network του.

- **Ανταποκρινόμενος κόμβος (*Correspondent node*)**

Μια ισοτιμία (peer) με την οποία ένας κινητός κόμβος επικοινωνεί. Ένας τέτοιος κόμβος μπορεί να είναι είτε κινητός είτε στάσιμος.

- **Foreign network (*Foreign network*)**

Οποιοδήποτε δίκτυο εκτός από το δίκτυο αρχικό δίκτυο του κινητού κόμβου.

- **Αρχική διεύθυνση (*Home address*)**

Μια διεύθυνση IP που ανατίθεται για μια εκτεταμένη χρονική περίοδο σε έναν κινητό κόμβο. Παραμένει αμετάβλητη ανεξάρτητα από το που είναι συνδεμένος ο κόμβος με το Διαδίκτυο.

- **Οικείο δίκτυο (*Home network*)**

Ένα, ουσιαστικά, εικονικό δίκτυο, το οποίο έχει ένα network prefix που ταιριάζει με αυτό της home address ενός κινητού κόμβου. Σημειώστε ότι οι τυπικοί μηχανισμοί δρομολόγησης του Mobile IP θα παραδώσουν τα διαγράμματα δεδομένων που προορίζονται στη home address ενός κινητού κόμβου στο home network του κινητού κόμβου.

- **Διεύθυνση Σύνδεσης-στρώματος (*Link-Layer Address*)**

Η διεύθυνση που χρησιμοποιείται για να προσδιορίσει ένα σημείο τέλους κάποιας επικοινωνίας σε μια φυσική σύνδεση. Χαρακτηριστικά, η διεύθυνση σύνδεσης-στρώματος είναι ένα interface διεύθυνσης ελέγχου πρόσβασης (Media Access Control) .

- **Πράκτορας κινητικότητας (*Mobility Agent*)**

Το συγκεκριμένο ρόλο μπορεί να διαδραματίσει είτε ένας βασικός πράκτορας είτε ένας foreign agent.

- **Σχέση κινητικότητας-ασφάλειας (*Mobility security association*)**

Το σύνολο του πλαισίου ασφαλείας , μεταξύ ενός ζευγαριού κόμβων, το οποίο μπορεί να εφαρμοστεί στα μηνύματα του Mobile IP

πρωτοκόλλου που ανταλλάσσονται μεταξύ τους. Κάθε πλαίσιο ασφαλείας προσδιορίζει έναν αλγόριθμο και έναν τρόπο πιστοποίησης της ταυτότητας των μηνυμάτων κάνοντας χρήση ενός key.

- **Κόμβος (Node)**

Ένας host ή ένας δρομολογητής.

- **Σχέση Ευρετηρίου παραμέτρων ασφάλειας (*Security Parameter Index*)**

Ένα ευρετήριο που προσδιορίζει το πλαίσιο ασφαλείας μεταξύ ενός ζευγαριού κόμβων εντός του διαθέσιμου πλαισίου στην ένωση ασφάλειας κινητικότητας. Οι τιμές του SPI μεταξύ 0 έως 255 είναι διατηρημένες και δεν πρέπει να χρησιμοποιηθεί σε οποιαδήποτε Mobility Security Association.

- **Σήραγγα (*Tunnel*)**

Η διαδρομή που ακολουθείται από το datagram όταν είναι μέσα σε "κάψουλα" . Το μοντέλο είναι ότι, ενώ τοποθετείται σε "κάψουλα", ένα διάγραμμα δεδομένων οδηγείται σε έναν agent, ο οποίος decapsulates το διάγραμμα δεδομένων και έπειτα το παραδίδει στον τελευταίο προορισμό του.

- **Εικονικό δίκτυο (*Virtual network*)**

Ένα δίκτυο χωρίς φυσική υπόσταση πέρα από έναν δρομολογητή. Ο δρομολογητής (π.χ., ένας home agent) γενικά διαφημίζει τη δεκτικότητα του (reachability) στο ιδεατό δίκτυο χρησιμοποιώντας τα συμβατικά πρωτόκολλα δρομολόγησης.

- **Επισκεπτόμενο δίκτυο (*Visited network*)**

Ένα δίκτυο διαφορετικό από το home network ενός κινητού κόμβου, με το οποίο ο κινητός κόμβος συνδέεται τη δεδομένη περίοδο.

- **Κατάλογος επισκεπτών (*Visited list*)**

Ο κατάλογος κινητών κόμβων που επισκέπτονται έναν ξένο πράκτορα.

- **Binding**

Ο συσχετισμός μεταξύ της home address και της care-of address του κινητού κόμβου καθώς και το χρονικό διάστημα για το οποίο ισχύει αυτός ο συσχετισμός.

Μετά την παράθεση τις βασικής ορολογίας θα επιχειρήσουμε μια πρώτη προσπάθεια να εμβαθύνουμε στα ενδότερα του πρωτοκόλλου, παρουσιάζοντας αναλυτικότερα τα βασικά χαρακτηριστικά του.

1.4. ΓΕΝΙΚΗ ΕΠΙΣΚΟΠΗΣΗ ΤΟΥ MOBILE IP

Στο συγκεκριμένο τμήμα της εργασίας θα αναλύσουμε τις βασικές υπηρεσίες που εκτελεί το πρωτόκολλο ώστε να ικανοποιήσει τις απαιτήσεις που έχουν τεθεί .

- Η υπηρεσία ***agent discovery*** , κατά την οποία τόσο οι home agents όσο και οι foreign agents δηλώνουν τη διαθεσιμότητα τους σε κάθε link για το οποίο παρέχουν υπηρεσίες . Ένας νέος, στο δίκτυο, κινητός κόμβος μπορεί να στείλει μια αίτηση για σύνδεση ούτως ώστε να ενημερωθεί για το εάν υπάρχουν κάποιοι διαθέσιμοι, για σύνδεση, agents .

- Η υπηρεσία εγγραφής ***Registration*** στην οποία όταν ένας κινητός κόμβος βρίσκεται μακριά από το home network, « καταχωρείται » στον home agent του στέλνοντας του την care-of address του. Ανάλογα με τη μέθοδο σύνδεσης του , ο κινητός κόμβος θα καταχωρηθεί είτε άμεσα είτε έμμεσα , μέσω ενός foreign agent ο οποίος διαβιβάζει την εγγραφή του στον home agent .

Ο τρόπος με τον οποίο οι υπηρεσίες αυτές συνεργάζονται μεταξύ τους παρατίθεται στη συνέχεια.

Οι ***mobility agents*** υποδηλώνουν την παρουσία τους μέσω των μηνυμάτων διαφημίσεων πρακτόρων (***Agent advertisement messages***) . Ένας κινητός κόμβος μπορεί προαιρετικά να ζητήσει ένα μήνυμα διαφημίσεων πρακτόρων από οποιουσδήποτε τοπικά συνημμένους mobility agents μέσω ενός μηνύματος παράκλησης πρακτόρων.

Στη συνέχεια ο κινητός κόμβος λαμβάνει αυτές τις διαφημίσεις πρακτόρων και καθορίζει εάν είναι στο βασικό δίκτυό του ή ένα foreign network.

Όταν ο κινητός κόμβος ανιχνεύει ότι βρίσκεται στο βασικό δίκτυό του, λειτουργεί χωρίς τη χρήση mobility services. Εάν επιστρέφει στο βασικό δίκτυό του έχοντας προηγουμένως καταχωρηθεί αλλού, ο κινητός κόμβος, μέσω ανταλλαγής μηνυμάτων Αιτήσεως εγγραφής και Απαντήσεως εγγραφής με τον home agent του, επανεγγράφεται σε αυτόν.

Όταν ένας κινητός κόμβος ανιχνεύει ότι έχει κινηθεί προς ένα foreign network, αποκτά μια care-of address στο foreign network.

Η care-of address μπορεί να καθοριστεί είτε από foreign agent advertisements είτε από κάποιο εξωτερικό μηχανισμό ανάθεσης όπως το ***Dynamic Host Configuration Protocol*** (collocated care-of address).

Ο κινητός κόμβος που λειτουργεί μακριά από το home network καταχωρεί έπειτα νέο care-of address με το βασικό πράκτορά του μέσω της ανταλλαγής ενός αιτήματος εγγραφής και του μηνύματος απάντησης εγγραφής, ενδεχομένως μέσω ενός foreign agent.

Τα διαγράμματα δεδομένων που στέλνονται στη home address του κινητού κόμβου αναχαιτίζονται από το home agent του, προωθούνται από αυτόν στην care-of address του κινητού κόμβου, παραδίδονται στο νέο υποδίκτυο που βρίσκεται ο κινητός κόμβος (είτε σε έναν foreign agent είτε από τον ίδιο τον κινητό κόμβο), και φτάνουν τελικά σε αυτόν.

Στην αντίστροφη κατεύθυνση, τα διαγράμματα δεδομένων που στέλνονται από τον κινητό κόμβο παραδίδονται γενικά στον προορισμό τους χρησιμοποιώντας τους πρότυπους μηχανισμούς δρομολόγησης IP, περνώντας, χωρίς αυτό να είναι απαραίτητο , μέσω του home agent.

Όταν ο κινητός κόμβος δεν βρίσκεται συνδεδεμένος με το home network, το Mobile IP εκτελεί tunneling μέσω πρωτοκόλλου με απώτερο σκοπό την απόκρυψη της home address του κόμβου από routers οι οποίοι βρίσκονται μεταξύ αυτό και της παρούσας τοποθεσίας του . Το tunnel τερματίζεται στην care-of address του κινητού κόμβου. Η care-of address πρέπει να είναι μια διεύθυνση στην οποία τα διαγράμματα δεδομένων πρέπει να μπορούν να παραδοθούν μέσω συμβατικών μεθόδων δρομολόγησης.

Στην CoA , το αρχικό datagram απομακρύνεται από το tunnel και παραδίδεται στον κινητό κόμβο. Το Mobile IP παρέχει δύο εναλλακτικούς τρόπους για την απόκτηση της care-of address:

1. Ένας "foreign agent care-of address " είναι μια care-of address παρεχόμενη από έναν foreign agent μέσω των μηνυμάτων διαφημίσεων πρακτόρων του. Σε αυτήν την περίπτωση, η care-of address είναι η IP διεύθυνση του foreign agent . Σε αυτόν τον τρόπο, ο foreign agent είναι το σημείο τέλους τού tunnel και όταν λαμβάνει τα ανοιγμένα διαγράμματα δεδομένων αφαιρεί την επικεφαλίδα που είχε προστεθεί σε αυτό και παραδίδει το εσωτερικό διάγραμμα δεδομένων στον κινητό κόμβο. Αυτός ο τρόπος απόκτησης της care-of address προτιμάται επειδή επιτρέπει σε πολλούς κινητούς κόμβους να μοιράζονται την ίδια care-of address και επομένως δεν τοποθετεί τις περιττές απαιτήσεις στο ήδη περιορισμένο διάστημα διευθύνσεων IPv4.

2. " Co-located care-of address " είναι η care-of address η οποία αποκτάται από τον κινητό κόμβο ως τοπική IP διεύθυνση μέσω μερικών εξωτερικών μέσων, τα οποία ο κινητός κόμβος κατόπιν συνδέει με ένα από τα network interfaces του. Η διεύθυνση μπορεί να αποκτηθεί δυναμικά ως προσωρινή διεύθυνση από τον κινητό κόμβο όπως μέσω του DHCP ή μπορεί να ανήκει στον κινητό κόμβο ως δεσμευμένη διεύθυνση για χρήση της μόνο όταν επισκέπτεται κάποιο foreign network. Οι συγκεκριμένες εξωτερικές μέθοδοι μια τοπική διεύθυνση IP για τη χρήση και δέσμευση κάποιας care-of address είναι πέρα από το πεδίο του παρόντος εγγράφου. Όταν χρησιμοποιείται co-located care-of address ο κινητός την κόμβος χρησιμεύει ως το σημείο τέλους της σήραγγας και ο ίδιος εκτελεί το decapsulation των διαγραμμάτων δεδομένων που δρομολογούνται σε αυτήν .

Η μέθοδος co-located care-of address έχει το πλεονέκτημα ότι επιτρέπει σε έναν κινητό κόμβο να λειτουργήσει χωρίς έναν foreign agent, όπως παραδείγματος χάριν, στα δίκτυα που δεν έχουν εντάξει ακόμα foreign agent στην υποδομή τους .

Αυξάνει , όμως , το φορτίο στο διάστημα διευθύνσεων IPv4 επειδή απαιτεί μια ομάδα των διευθύνσεων μέσα στο foreign network για να τεθεί στην διάθεση της επίσκεψης των κινητών κόμβων. Είναι δύσκολο να διατηρηθούν αποτελεσματικά οι ομάδες των διευθύνσεων για κάθε υποδίκτυο που μπορεί να επιτρέψει στους κινητούς κόμβους για να επισκεφτεί.

Είναι σημαντικό να γίνει κατανοητή η διάκριση μεταξύ care-of address και των foreign agents. Care-of address είναι απλά το σημείο τέλους της σήραγγας. Πράγματι, μπορεί να είναι μια διεύθυνση ενός ξένου πράκτορα (foreign agent care-of address) , αλλά άντ' αυτού να είναι μια διεύθυνση προσωρινά δεσμευμένη από τον κινητό κόμβο (collocated care-of address). Ένας foreign agent, αφ' ετέρου, είναι πράκτορας κινητικότητας που παρέχει τις υπηρεσίες στους κινητούς κόμβους.

Ένας home agent πρέπει να είναι σε θέση να προσελκύσει και να παρεμποδίσει τα διαγράμματα δεδομένων που προορίζονται στη διεύθυνση κατοικίας οποιουδήποτε από τους καταχωρημένους κινητούς κόμβους του. Χρησιμοποιώντας μηχανισμούς **Arp** αυτή η απαίτηση μπορεί να ικανοποιηθεί εάν ο home agent έχει ένα network interface στη σύνδεση που υποδεικνύεται από τη home address του κινητού κόμβου. Άλλες τοποθετήσεις του home agent σχετικά με τη βασική θέση του κινητού κόμβου είναι επίσης δυνατές χρησιμοποιώντας άλλους μηχανισμούς για τα διαγράμματα δεδομένων που προορίζονται στη διεύθυνση κατοικίας του κινητού κόμβου αν και το θέμα αποτελεί από μόνο του νέο αντικείμενο μελέτης.

Ομοίως, ένας κινητός κόμβος και ένας ενδεχόμενος ή παρών foreign agent πρέπει να είναι σε θέση να ανταλλάξει τα διαγράμματα δεδομένων χωρίς να βασίζεται αποκλειστικά σε standard μηχανισμούς δρομολόγησης IP, δηλαδή εκείνους τους μηχανισμούς που κάνουν τη διαβίβαση των αποφάσεων που βασίζονται στο δίκτυο-πρόθεμα της διεύθυνσης προορισμού στην επικεφαλίδα IP. Αυτή η απαίτηση μπορεί να ικανοποιηθεί εάν ο foreign agent και ο κινητός κόμβος επίσκεψης έχουν ένα interface στην ίδια σύνδεση. Σε αυτήν την περίπτωση, ο κινητός κόμβος και ο foreign agent απλά παρακάμπτουν τον κανονικό μηχανισμό δρομολόγησης IP τους κατά την αποστολή των διαγραμμάτων δεδομένων ο ένας στον άλλο, που απευθύνει τα πακέτα σύνδεσης-στρώματος στις αντίστοιχες διευθύνσεις σύνδεσης-στρώματός τους. Άλλες τοποθετήσεις του foreign agent σχετικά με τον κινητό κόμβο είναι επίσης δυνατές χρησιμοποιώντας άλλους μηχανισμούς για να ανταλλάξουν τα διαγράμματα δεδομένων μεταξύ αυτών των κόμβων.

Εάν ένας κινητός κόμβος χρησιμοποιεί collocated care-of address ο κινητός κόμβος πρέπει να βρεθεί στη σύνδεση που προσδιορίζεται από το πρόθεμα δικτύων αυτού care-of address. Διαφορετικά, τα διαγράμματα δεδομένων που προορίζονται για την care-of address θα ήταν μη ανακτήσιμα.

1.5. ΓΕΝΙΚΗ ΕΠΙΣΚΟΠΗΣΗ ΤΗΣ ΕΚΔΟΣΗΣ MOBILE IPv6

Το Mobile IPv6 είναι εξίσου κατάλληλο για μεταφορά δεδομένων τόσο μεταξύ ομογενών όσο και ανομοιογενών μέσων μεταφοράς . Μπορούμε να επιτύχουμε μετακίνηση ενός κόμβου από ένα τμήμα δικτύου Ethernet σε μια κυψέλη wireless LAN , με την IP του να παραμένει σταθερή .

Θα μπορούσε κάποιος να υποθέσει ότι το πρωτόκολλο κατάφερε να επιλύσει το πρόβλημα της διαχείρισης της κινητικότητας σε επίπεδο δικτύου.

Η αλήθεια είναι ότι ορισμένες μόνο περιπτώσεις, όπως η διαχείριση της κινητικότητας ορισμένων εφαρμογών (όπως το handover μεταξύ ασυρμάτων πομπών-δεκτών ο καθένας από τους οποίους καλύπτει μια πολύ μικρή γεωγραφική περιοχή) έχουν επιλυθεί εφαρμόζοντας τεχνικές link-layer.

Όταν ο κινητός κόμβος βρίσκεται εκτός του home network, κάνει register, χρησιμοποιώντας μια από τις care-of addresses του με ένα δρομολογητή , που βρίσκεται στο home network του, ζητώντας του να αναλάβει το ρόλο του home agent . Αυτός ο συσχετισμός μεταξύ της home address και της care-of address ονομάζεται binding και αυτού του είδους η εγγραφή πραγματοποιείται με την αποστολή , από τον κινητό κόμβο , ένα πακέτο το οποίο περιέχει ένα Binding update. Ο home agent απαντά με ένα πακέτο που περιέχει ένα Binding acknowledgment. Την care-of address σε αυτό το συσχετισμό εγγραφομένη με αυτή του home agent την ονομάζουμε κύρια care-of address του κινητού κόμβου .

Όταν ο κινητός κόμβος κινηθεί προς μια νέα care-of address είναι επιθυμητό τα πακέτα που έχουν ως στόχο την προηγούμενη να επαναδρομολογηθούν προς τη νέα. Αυτός είναι, άλλωστε, και ο απώτερος σκοπός του Binding update, να δρομολογεί δηλαδή πακέτα που κατευθύνονταν προς μια παλιά σε μια νέα διεύθυνση με τον ίδιο ακριβώς τρόπο που χρησιμοποιείται για τη δημιουργία tunnels για τη δρομολόγηση δεδομένων από τη home address του κινητού κόμβου στη δεδομένη κάθε χρονική στιγμή care-of address του.

Ένα άλλο ζήτημα είναι ότι, ενώ ο κινητός κόμβος βρίσκεται μακριά από το home network, κάποιοι κόμβοι σε αυτό μπορεί να αλλάξουν ρόλο η να μετακινηθούν και αυτοί όπως ο δρομολογητής που έχει αναλάβει το ρόλο του home agent, οπότε ο κινητός κόμβος μπορεί να μη γνωρίζει την IP διεύθυνση του home agent του με αποτέλεσμα τη σίγουρη απώλεια δεδομένων .

Το πρωτόκολλο παρέχει ένα μηχανισμό, γνωστό ως ***Dynamic Home Agent Address Discovery***, με τη βοήθεια του οποίου ο κινητός κόμβος κάνει register την κύρια care-of address του.

Το Binding update, το Binding acknowledgment και το Binding request χρησιμοποιούνται επίσης για να δώσουν τη δυνατότητα στους κόμβους του Mobile IPv6 να επικοινωνούν με ένα κινητό κόμβο , για να μαθαίνουν δυναμικά τα bindings του κινητού κόμβου και να τα αποθηκεύουν.

Στην περίπτωση που ο κινητός κόμβος βρίσκεται σε ένα δίκτυο εκτός του αρχικού, στην επικεφαλίδα κάθε πακέτου θέτει ως Source address την εκάστοτε care-of address του και συμπεριλαμβάνει επίσης τη Home address του, δίνοντας έτσι την αρχική διεύθυνση του. Πολλοί δρομολογητές εφαρμόζουν μια στρατηγική ασφάλειας, γνωστή και ως Ingress filtering, η οποία δεν επιτρέπει την προώθηση πακέτων τα οποία φαίνεται να έχουν τοπολογικες ανακολουθίες (η source address του πακέτου παρουσιάζει μια ανακολουθία σε σχέση με τη γεωγραφική θέση του κόμβου) οπότε, τα πακέτα αυτά δεν θα φτάσουν ποτέ στο στόχο τους . Χρησιμοποιώντας την care-of address στην επικεφαλίδα κάθε πακέτου καθίσταται δυνατή η παράκαμψη του εμποδίου αυτού καθώς και τα πακέτα θα μπορούν να κατευθυνθούν προς το στόχο τους και το ingress filtering θα μπορεί να εντοπίσει τη γεωγραφική θέση του κόμβου.

Ανακεφαλαιώνοντας , λοιπόν , έχουμε τους εξής όρους οι οποίοι εισάγονται από τη νέα έκδοση του πρωτοκόλλου :

- **Binding update**: Η επιλογή αυτή χρησιμοποιείται από τον κινητό κόμβο για να ειδοποιήσει τον ανταποκρινόμενο κόμβο η τον home agent του κινητού κόμβου για το binding τη δεδομένη χρονική στιγμή. Το Binding update , το οποίο στέλνεται στον home agent του κινητού κόμβου ώστε να γίνει εγγραφή της care-of address του ονομάζεται home registration. Κάθε πακέτο που περιλαμβάνει Binding update πρέπει να προστατεύεται με κάποιο σύστημα αυθεντικοποίησης.

- **Binding acknowledgment**: Η επιλογή αυτή χρησιμοποιείται για να βεβαιωθεί ότι έγινε η λήψη του binding update εάν αυτό ζητείται από το binding update.

- **Binding request**: Η επιλογή αυτή χρησιμοποιείται από ένα κόμβο ο οποίος ζητάει να ενημερωθεί για το binding του κινητού κόμβου τη δεδομένη χρονική στιγμή.

- **Home address**: Η επιλογή αυτή χρησιμοποιείται σε πακέτα δεδομένων που αποστέλλονται από ένα κινητό κόμβο για να ενημερώσει τον αποδέκτη για τη home address του κόμβου. Όταν ο κινητός κόμβος δεν είναι στο αρχικό δίκτυο ως home address χρησιμοποιεί την care-of address την οποία τοποθετεί στην επικεφαλίδα του πακέτου . Με αυτόν τον τρόπο ο αποδεκτής του πακέτου μπορεί να εντοπίσει τη θέση του κινητού κόμβου.

Εδώ θα πρέπει να σημειώσουμε ότι υπάρχει και αριθμός υποεπιλογών οι οποίες χρησιμοποιούνται εντός των τεσσάρων βασικών που περιγράψαμε παραπάνω. Η χρησιμότητα τους έγκειται στην ικανοποίηση εξειδικευμένων αναγκών και γι'αυτό το λόγο δεν θα αναλυθούν στην παρούσα εργασία.

1.6. ΤΥΠΟΠΟΙΗΜΕΝΑ ΜΗΝΥΜΑΤΑ ΤΟΥ MOBILE IP

Το Mobile IP χρησιμοποιεί ένα σύνολο μηνυμάτων ελέγχου, που στέλνονται με τη βοήθεια του πρωτοκόλλου ***UDP***, χρησιμοποιώντας το γνωστό ***port 434***. Οι ακόλουθοι δύο τύποι μηνυμάτων ***(Registration Request & Registration Reply messages)*** είναι πολύ σημαντικοί και θα αναλυθούν στο ***κεφάλαιο 3***, στο οποίο θα αναφερθούμε , εκτενώς ,στη διαδικασία του ***Registration*** (εγγραφής) του κινητού κόμβου με το εκάστοτε υποδίκτυο στο οποίο ανήκει.

Επιπλέον των ανωτέρω το Mobile IP, για την ανακάλυψη πρακτόρων ***(Agent discovery)***, χρησιμοποιεί τα υπάρχοντα μηνύματα ***Router advertisement*** και ***Router solicitation*** όπως αυτά καθορίστηκαν για το ICMP Router advertisement .

Το Mobile IP ορίζει ένα γενικό μηχανισμό επεκτάσεων που επιτρέπει τη μεταφορά επιπλέον πληροφοριών μεσώ μηνυμάτων έλεγχου του Mobile IP ή μεσώ ***ICMP Router Discovery*** μηνυμάτων . Οι περισσότερες από τις επεκτάσεις αυτές έχουν κωδικοποιηθεί με τη μέθοδο ***Type – Length – Value*** την οποία θα περιγράψουμε παρακάτω .

Οι επεκτάσεις επιτρέπουν τη μεταφορά μεταβλητού αριθμού πληροφοριών σε κάθε datagram κάθε φορά που τις χρησιμοποιούμε , ανάλογα με τις ανάγκες .

Το Mobile IP χρησιμοποιεί δυο διαφορετικά σετ επεκτάσεων . Το πρώτο αποτελείται από τις επεκτάσεις οι οποίες στέλνονται μέσω του πρωτοκόλλου UDP και χρησιμοποιούνται στη διαδικασία της εγγραφής (Registration). Στη συγκεκριμένη κατηγορία θα εξετάσουμε τις παρακάτω επεκτάσεις (βλέπε Κεφάλαιο 3):

Mobile – Home Authentication
Mobile – Foreign Authentication
Foreign – Home Authentication

Το δεύτερο σετ των επεκτάσεων αποτελείται από τις επεκτάσεις οι οποίες στέλνονται με το πρωτόκολλο ICMP Router Discovery και χρησιμοποιούνται για τη διαδικασία της αναγνώρισης πρακτόρων (Agent Discovery) . Στη συγκεκριμένη κατηγορία θα εξετάσουμε τις παρακάτω επεκτάσεις (βλέπε Κεφάλαιο 2):

Mobility Agent Advertisement
Prefix Lengths
One-Byte Padding

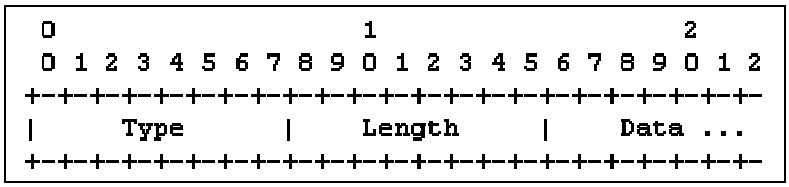
Όπως γίνεται εύκολα αντιληπτό οι επεκτάσεις και οι πληροφορίες που αυτές μεταφέρουν διαδραματίζουν πολύ σημαντικό ρόλο στη λειτουργία του πρωτοκόλλου και γι'αυτό το λόγο θα αναλυθούν λεπτομερώς στη συνέχεια .

Οι ακόλουθες υποενότητες παρέχουν τις λεπτομέρειες για τρεις ευδιάκριτες δομές των κινητών επεκτάσεων του Mobile IP:

- Τις επεκτάσεις Type - Length - Value
- Τις επεκτάσεις μεγάλου μήκους
- Τις επεκτάσεις μικρού μήκους

i. Επεκτάσεις Type - Length -Value

Το format επέκτασης Type - Length - Value που διευκρινίζεται στο παρακάτω σχήμα χρησιμοποιείται για τις επεκτάσεις που προσδιορίζονται στο παρόν έγγραφο. Δεδομένου ότι δομές αυτής της μορφής δεν ενθαρρύνουν την αποδοτικότερη χρήση των διαστημάτων τύπων επέκτασης , συνιστάται οι νέες επεκτάσεις του Mobile IP να ακολουθούν ένα από τα ακόλουθα σχήματα επέκτασης που προσδιορίζονται στο κεφάλαιο 2.



Type:

δείχνει τον συγκεκριμένο τύπο επέκτασης.

Length:

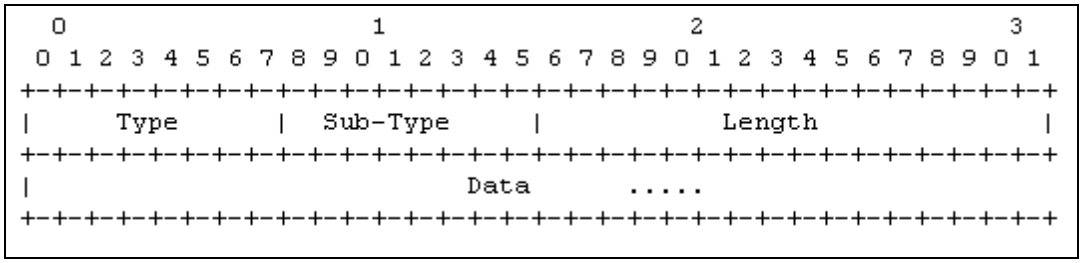
δείχνει το μήκος (σε bytes) του πεδίου στοιχείων μέσα σε αυτήν την επέκταση. Το μήκος δεν περιλαμβάνει τα bytes τύπου και μήκους .

Data:

τα συγκεκριμένα στοιχεία που συνδέονται με αυτήν την επέκταση. Αυτό το πεδίο μπορεί να είναι είτε μηδέν είτε ίσο με περισσότερα bytes στο μήκος. Το σχήμα και το μήκος του πεδίου στοιχείων καθορίζεται από τα πεδία τύπου και μήκους , που αναφέραμε παραπάνω .

ii. Επεκτάσεις μεγάλου μήκους

Οι επεκτάσεις αυτού του τύπου χρησιμοποιούνται όταν η πληροφορία που πρέπει να μεταφερθεί ξεπερνά τα 256 bytes.



Οι επεκτάσεις μεγάλου μήκους προϋποθέτουν ότι τα ακόλουθα πεδία έχουν καθοριστεί ως τα πρώτα πεδία της επέκτασης .

Type:

Στο πεδίο αυτό δηλώνεται ο τύπος ο οποίος περιγράφει το σύνολο των επεκτάσεων οι οποίες έχουν ένα κοινό τύπο πληροφοριών .

Sub-Type:

Ένας μοναδικός αριθμός ο οποίος δίνεται σε κάθε μέλος του παραπάνω συνόλου .

Length:

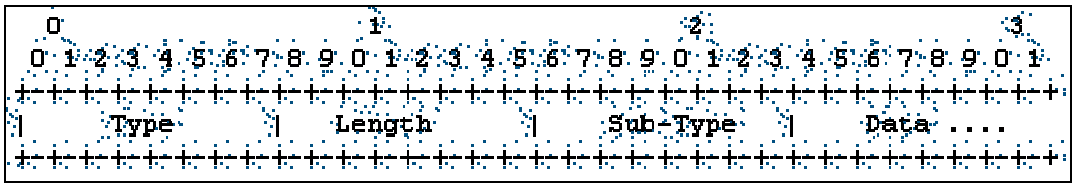
Δηλώνει το μήκος (σε bytes) του πεδίου data .

Data:

Αναφέρεται στα δεδομένα που σχετίζονται με το sub-type της επέκτασης .

iii. Επεκτάσεις μικρού μήκους

Οι επεκτάσεις αυτού του τύπου χρησιμοποιούνται όταν η πληροφορία που πρέπει να μεταφερθεί δεν ξεπερνά τα 256 bytes.



Για τα πεδία της συγκεκριμένης επέκτασης ισχύουν τα παραπάνω με τη διαφορά ότι το πεδίο Length πρέπει να είναι ίσο με το πεδίο data συν 1.

Στη συνέχεια της εργασίας , έχοντας , δώσει το στίγμα για τις λειτουργίες που εκτελεί το πρωτόκολλο καθώς και τις απαιτήσεις που υπάρχουν από αυτό θα συνεχίσουμε παρουσιάζοντας τα επιμέρους τμήματα του με περισσότερες λεπτομέρειες , όπως αυτά παρουσιάστηκαν στην εισαγωγή της εργασίας .

ΚΕΦΑΛΑΙΟ 2

ΔΙΑΔΙΚΑΣΙΑ
AGENT DISCOVERY

2.1. Εισαγωγή

Η διαδικασία agent discovery είναι η μέθοδος με την οποία ένας κινητός κόμβος καθορίζει εάν βρίσκεται συνδεδεμένος με το home network ή με ένα foreign network ενώ του δίνεται η δυνατότητα να καθορίσει το πότε έγινε η αλλαγή δικτύου καθώς επίσης , όταν είναι συνδεδεμένος με ένα foreign network , η παραπάνω μέθοδος του επιτρέπει να ανακαλύψει την care-of address του foreign agent .

Όπως προαναφέραμε το Mobile IP χρησιμοποιεί το ICMP Router Discovery ως τον πρωταρχικό μηχανισμό για το agent discovery .

Ένα agent advertisement μήνυμα δημιουργείται συμπεριλαμβάνοντας σε αυτό μια Mobility Agent advertisement extension σε κάθε ICMP Router advertisement message . ***Ένα Agent Solicitation μήνυμα είναι παρόμοιο με το ICMP Router Solicitation message με μόνη διαφορά ότι το πεδίο IP TTL (Time To Live) πρέπει να είναι ίσο με 1***, όπως θα δούμε στην παράγραφο 2.3 .

Τόσο για τα Agent Advertisement όσο και για τα Agent Solicitation μηνύματα δεν απαιτείται κάποιο είδος πιστοποίησης ως μέτρο ασφαλείας εναντίον επιθέσεων .

Στις επόμενες παραγράφους θα εξετάσουμε τα μηνύματα έλεγχου καθώς επίσης και τον τρόπο με τον οποίο οι κινητοί κομβόι , οι foreign agents και οι home agents συνεργάζονται μεταξύ τους ώστε να πραγματοποιήσουν την διαδικασία του agent discovery .

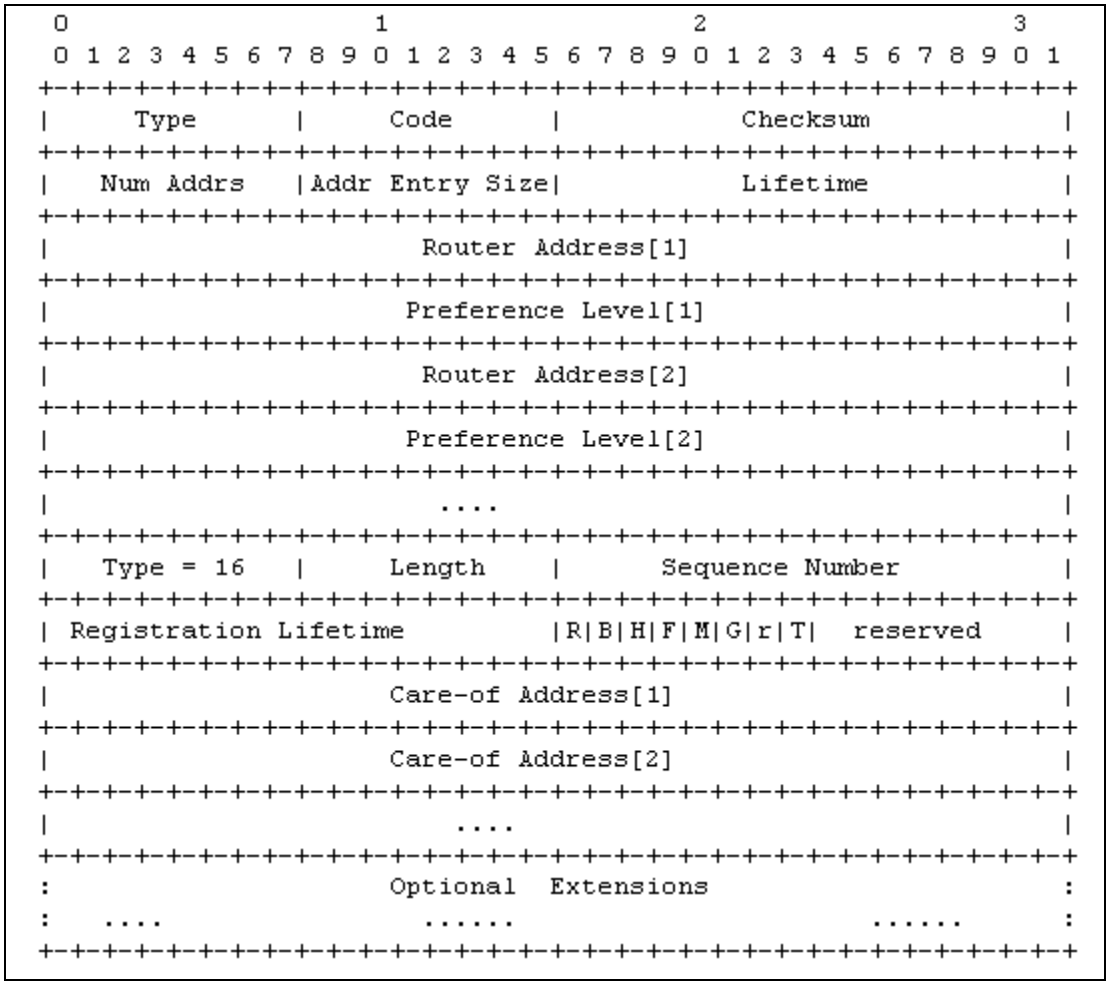
2.2. Agent Advertisement Messages

Στη συνέχεια θα αναλύσουμε τα μηνύματα που αποστέλλονται μεταξύ των εμπλεκομένων κόμβων με σκοπό την υλοποίηση του agent discovery του κινητού κόμβου στο νέο δίκτυο.

i. Mobility Agent Advertisement messages

Τα Agent Advertisements μεταδίδονται από ένα mobility agent, ο οποίος με αυτό τον τρόπο διαφημίζει τις υπηρεσίες που προσφέρει σε ένα link. Οι κινητοί κόμβοι χρησιμοποιούν αυτά τα μηνύματα για να καθορίσουν το point of attachment τους τη δεδομένη χρονική στιγμή .

Ένα Agent Advertisement message περιλαμβάνει μια Mobility Agent advertisement extension η οποία χρησιμοποιείται για να δηλώσει στον παραλήπτη ότι πρόκειται για ICMP Router advertisement message το οποίο στάλθηκε από κάποιο mobility agent . Η παραπάνω επέκταση που περιγράψαμε απεικονίζεται στο παρακάτω σχήμα :



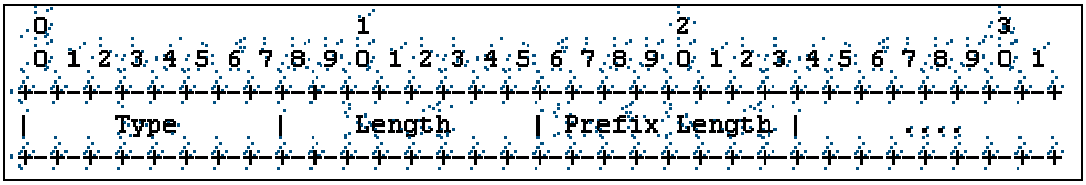
Παράδειγμα μηνύματος Agent Advertisement με χρήση ICMP πρωτοκόλλου

- Το πεδίο ***Type*** παίρνει την τιμή ***16*** η οποία υποδηλώνει ότι πρόκειται για μήνυμα τύπου agent advertisement .
- Το πεδίο ***Length*** παίρνει την τιμή ***6+4N*** όπου **N** ο αριθμός των care-of διευθύνσεων.
- Το πεδίο ***Sequence number*** μας δίνει των αριθμό των agent advertisement μηνυμάτων που έστειλε ο home agent από τη στιγμή που ενεργοποιήθηκε .
- Το πεδίο ***Lifetime*** μας δείχνει ποιο είναι το μεγαλύτερο χρονικό διάστημα , σε δευτερόλεπτα , για το οποίο ο home agent είναι διατεθειμένος να δεχθεί αίτηση εγγραφής από ένα κινητό κόμβο .
- Το πεδίο ***R*** δηλώνει ότι η έγγραφη στο συγκεκριμένο κόμβο είναι απαραίτητη ακόμα και για τους κόμβους οι οποίοι έχουν ήδη αποκτήσει care-of address από τον συγκεκριμένο foreign agent εάν παρέλθει το χρονικό διάστημα που δηλώνεται στο πεδίο lifetime .
- Το πεδίο ***B*** υποδηλώνει ότι ο foreign agent είναι απασχολημένος και δεν δέχεται αιτήσεις εγγραφής από κινητούς κόμβους.
- Το πεδίο ***H*** δηλώνει ότι ο συγκεκριμένος υπολογιστής λειτουργεί ως home agent στο συγκεκριμένο δίκτυο .
- Το πεδίο ***F*** δηλώνει ότι ο συγκεκριμένος υπολογιστής λειτουργεί ως foreign agent στο συγκεκριμένο δίκτυο .
- Το πεδίο ***M*** δηλώνει ότι ο συγκεκριμένος υπολογιστής μπορεί να χειριστεί πακέτα τα οποία χρησιμοποιούν Minimal Encapsulation .
- Το πεδίο ***G*** δηλώνει ότι ο συγκεκριμένος υπολογιστής μπορεί να χειριστεί πακέτα τα οποία χρησιμοποιούν Generic Routing Encapsulation.
- Το πεδίο ***r*** είναι ίσο με μηδέν και ουσιαστικά αγνοείται κατά τη λήψη .
- Για το πεδίο ***Reserved*** ισχύ ότι και για το πεδίο **r** .
- Το πεδίο ***Y*** δηλώνει ότι ο συγκεκριμένος υπολογιστής υποστηρίζει τη συμπίεση επικεφαλίδας κατά το πρότυπο Van Jacobson .
- Το πεδίο ***care-of address*** δηλώνει ότι οι care-of διευθύνσεις υποστηρίζονται από το συγκεκριμένο υπολογιστή εάν το bit **F** είναι ενεργοποιημένο.

ii. Prefix Length Extension

Αρκετές φορές, η συγκεκριμένη επέκταση ακολουθεί τη ***Mobility Agent Advertisement extension*** και ο σκοπός της , πιθανής , παρουσία της είναι να δηλώσει των αριθμό των bits του προθέματος του δικτύου που ανήκουν στις διευθύνσεις των δρομολογητών που είναι καταχωρημένοι στο ICMP Router Advertisement τμήμα του Agent Advertisement .

Η Prefix Length Extension έχει την παρακάτω μορφή:

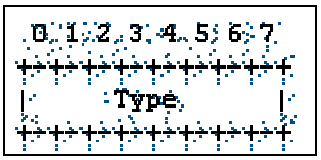


- Το πεδίο Type παίρνει την τιμή 19 , για να αναγνωριστεί από τον παραλήπτη ως Prefix Length Extension
- Το πεδίο Length έχει την τιμή N , όπου N είναι η τιμή (συνήθως μηδέν) , του πεδίου Num Address του ICMP Router Advertisement τμήματος του Agent Advertisement .
- Τα bits του πεδίου Prefix Lengths καθορίζουν σε ποιο δίκτυο ανήκει ο ανταποκρινόμενος δρομολογητής ο οποίος είναι καταχωρημένος στο ICMP Router Advertisement τμήμα του Agent Advertisement .

Οι Prefix Length Extensions χρησιμοποιούνται από τον κινητό κόμβο για να καθορίσει εάν έχει κινηθεί από ένα υποδίκτυο σε ένα άλλο.

iii. One-byte Padding Extension

Λόγω του ότι αρκετές εφαρμογές το IP πρωτοκόλλου θεωρούν ότι τα μηνύματα του ICMP θα έχουν ζυγό αριθμό Bytes . Εάν το μήκος μιας ICMP advertisement είναι μονό τότε χρησιμοποιούμε τη συγκεκριμένη επέκταση για να εξασφαλίσουμε συμβατότητα με όλες τις εφαρμογές . Η επέκταση αυτή πρέπει να είναι η τελευταία επέκταση σε κάθε Agent Advertisement . Η One-byte Padding Extension έχει την παρακάτω μορφή:



Παρατηρούμε ότι , σε αντίθεση με τις άλλες επεκτάσεις του Mobile IP , η συγκεκριμένη έχει ένα μόνο byte χωρίς να είναι παρόντα τα πεδία Data ή Field .

- Το πεδίο ***Type*** παίρνει την τιμή 0.

2.3. Νεα ICMP μηνύματα στο IPv6

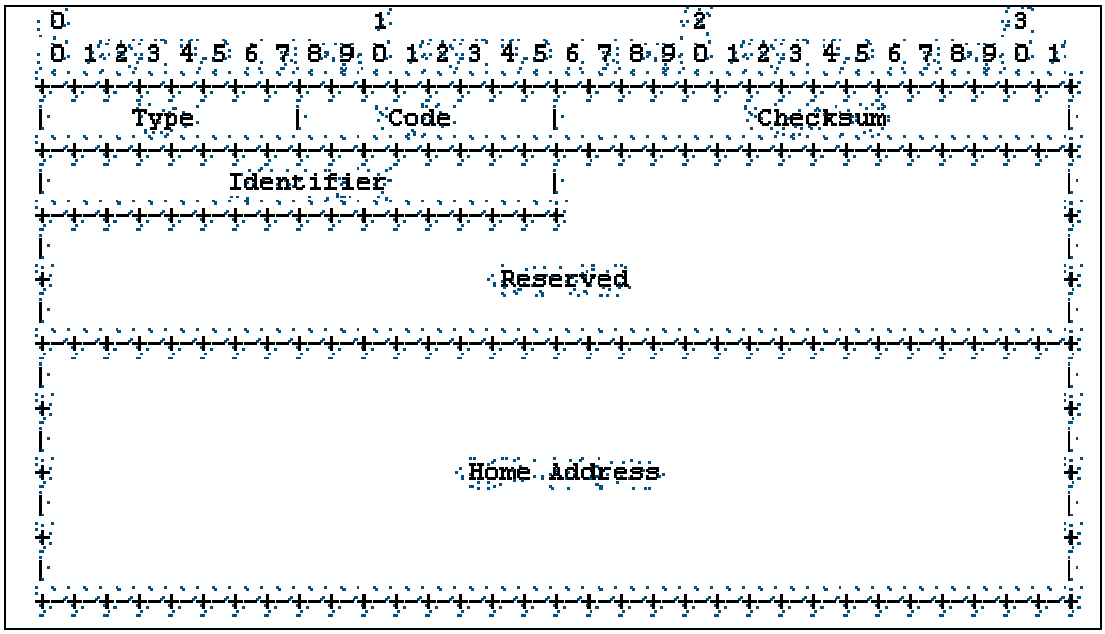
Στο σημείο αυτό θα πρέπει να σημειώσουμε και τις εξελίξεις που υπάρχουν στην εξελιγμένη έκδοση του πρωτοκόλλου Mobile IP .

Πιο συγκεκριμένα σε αυτή προστίθενται 4 νέοι τύποι ICMP μηνυμάτων , δυο για χρήση στους μηχανισμούς Dynamic Home Address Discovery και δυο για χρήση στους μηχανισμούς απαρίθμησης – διαμόρφωσης του πρωτοκόλλου.

i. Home Agent Address Discovery Request message

Το ICMP Home Agent Address Discovery Request μήνυμα χρησιμοποιείται από τον κινητό κόμβο με σκοπό να ξεκινήσει το δυναμικό μηχανισμό ανεύρεσης διεύθυνσης ενός home agent.

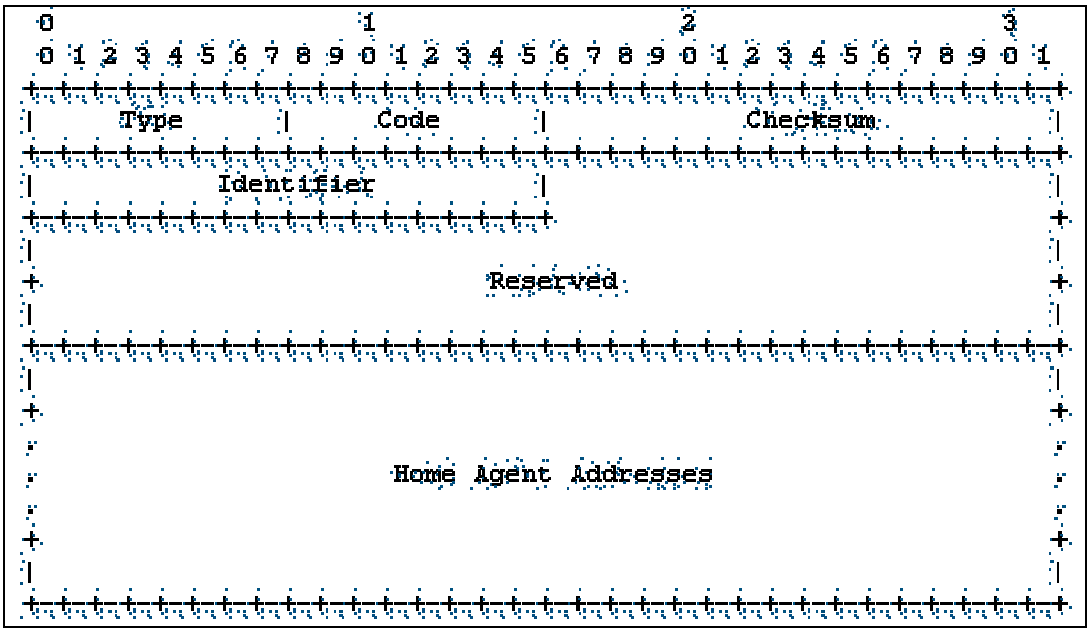
Όταν επιχειρείται μια έγγραφη κινητού κόμβου με ένα home agent , ο κινητός κόμβος μπορεί να χρησιμοποιήσει αυτό το μηχανισμό για να ανακαλύψει τη διεύθυνση ενός ή περισσοτέρων δρομολογητών οι οποίοι λειτουργούν ως home agents στο δίκτυο στο οποίο επιχειρεί να εγγραφεί.



- Η τιμή του πεδίου ***Type*** δεν έχει καθοριστεί ακόμη .
- Το πεδίο ***Code*** παίρνει την τιμή μηδέν .
- Το πεδίο ***Checksum*** αναφέρεται στο ICMP .
- Το πεδίο ***Identifier*** βοηθά στο να συγκρίνει και να ταιριάζει τα Home Agent Address Discovery Reply & Home Agent Address Discovery Request messages .
- Το πεδίο ***Reserved*** δεν χρησιμοποιείται. Πρέπει πάντως να έχει αρχικοποιηθεί στην τιμή μηδέν από τον αποστολέα και να αγνοηθεί από τον παραλήπτη .
- Το πεδίο ***Home Address*** αναφέρεται στην αρχική διεύθυνση του κινητού κόμβου από την οποία αποστέλλεται το Home Agent Address Discovery message .

ii. Home Agent Address Discovery Reply message

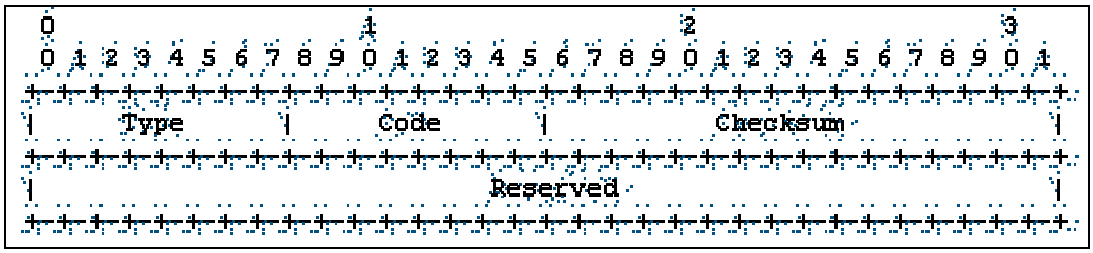
Το ICMP Home Agent Address Discovery Reply μήνυμα χρησιμοποιείται από τον home agent για να απαντήσει σε ένα κινητό κόμβο που χρησιμοποιεί τον παραπάνω μηχανισμό. Όταν ο home agent λαμβάνει ένα Home Agent Address Discovery Request μήνυμα απαντά με το παραπάνω μήνυμα , δίνοντας μια λίστα με τους δρομολογητές που λειτουργούν ως home agents στο home network του κινητού κόμβου .



- Η τιμή του πεδίου ***Type*** δεν έχει καθοριστεί ακόμη .
- Το πεδίο ***Code*** παίρνει την τιμή μηδέν .
- Το πεδίο ***Checksum*** αναφέρεται στο ICMP .
- Το πεδίο ***Identifier*** το οποίο χρησιμοποιείται από το Home Agent Address Discovery Request μήνυμα .
- Το πεδίο ***Reserved*** δεν χρησιμοποιείται. Πρέπει πάντως να έχει αρχικοποιηθεί στην τιμή μηδέν από τον αποστολέα και να αγνοηθεί από τον παραλήπτη .
- Το πεδίο ***Home Agent Addresses*** είναι μια λίστα των home agents στο αρχικό δίκτυο του κινητού κόμβου. Ο αριθμός των διευθύνσεων αυτών φαίνεται από το υπολειπόμενο μήκος το πακέτου δεδομένων , του Mobile IPv6 , το οποίο μεταφέρει το Home Agent Discovery Reply message (το οποίο θα έχει μηδενική τιμή)

iii. Mobile Prefix Solicitation message

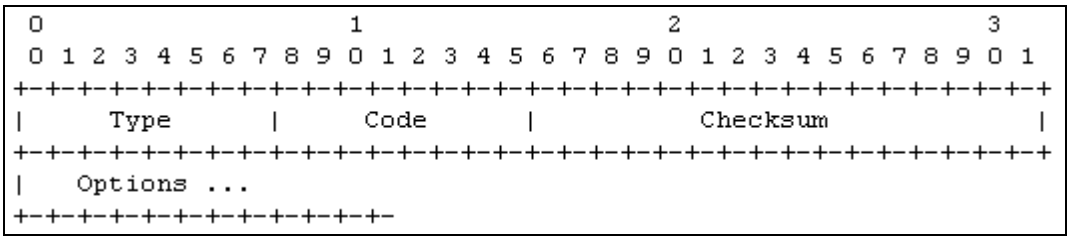
Το ICMP Mobile Prefix Solicitation μήνυμα χρησιμοποιείται από ένα κινητό κόμβο για να ζητήσει το πρόθεμα του home υποδικτύου ούτως ώστε να μπορέσει να επανακτήσει prefixes τα οποία είναι διαθέσιμα από τους home agents και μπορούν να χρησιμοποιηθούν για να διαμορφώσουν μια η περισσότερες home addresses ή να διατηρήσουν μια πριν καταστεί μη έγκυρη .



- Η τιμή του πεδίου ***Type*** δεν έχει καθοριστεί ακόμη .
- Το πεδίο ***Code*** παίρνει την τιμή μηδέν .
- Το πεδίο ***Checksum*** αναφέρεται στο ICMP .
- Το πεδίο ***Reserved*** δεν χρησιμοποιείται.

iv. Mobile Prefix Advertisement message

Το ICMP Mobile Prefix Advertisement μήνυμα χρησιμοποιείται από τον home agent για να μοιράσει πληροφορίες σε ένα κινητό κόμβο σχετικά με προθέματα στο home network τα οποία θα μπορεί να χρησιμοποιήσει Όταν θα βρεθεί σε κάποιο foreign network. Το μήνυμα αυτό στέλνεται ως απάντηση σε ένα Mobile Prefix Solicitation μήνυμα .

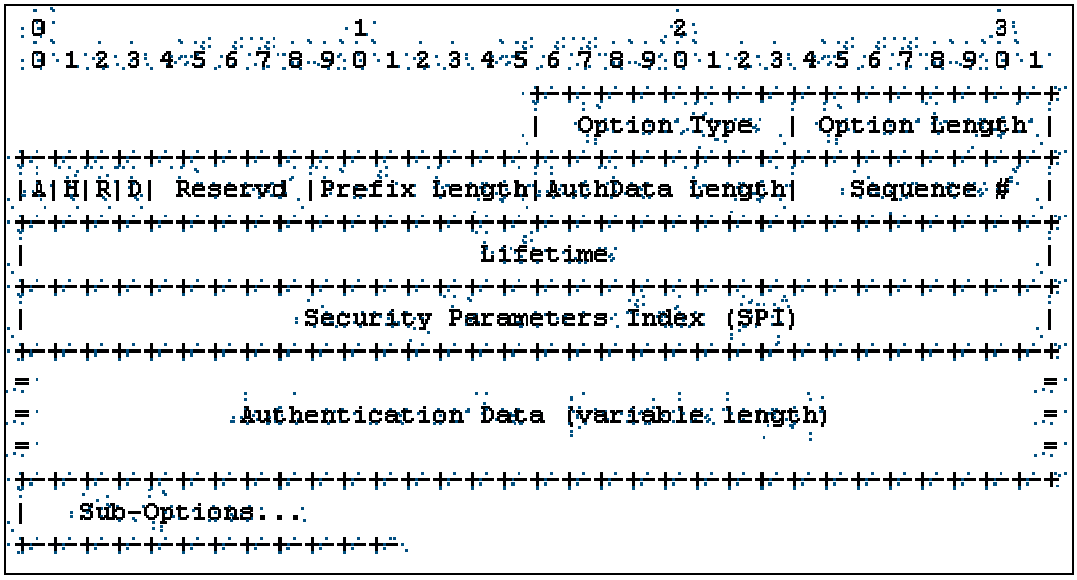


- Η τιμή του πεδίου ***Type*** δεν έχει καθοριστεί ακόμη .
- Το πεδίο ***Code*** παίρνει την τιμή μηδέν .
- Το πεδίο ***Checksum*** αναφέρεται στο ICMP .

Παρατηρώντας τα νέα μηνύματα που εισάγει η τελευταία έκδοση του πρωτοκόλλου παρατηρούμε ότι αρκετά πεδία δεν έχουν καθοριστεί ακόμη πλήρως ενώ είναι εμφανής οι ομοιότητες που υπάρχουν μεταξύ τους συμβάλλοντας , έτσι , στην βελτίωση της αξιοπιστίας που απαιτείται να παρουσιάζει στη λειτουργία του .

v. Binding update message

Το binding update message, στην υλοποίηση Mobile IPv6, είναι κωδικοποιημένο κατά το πρότυπο type-length-value .

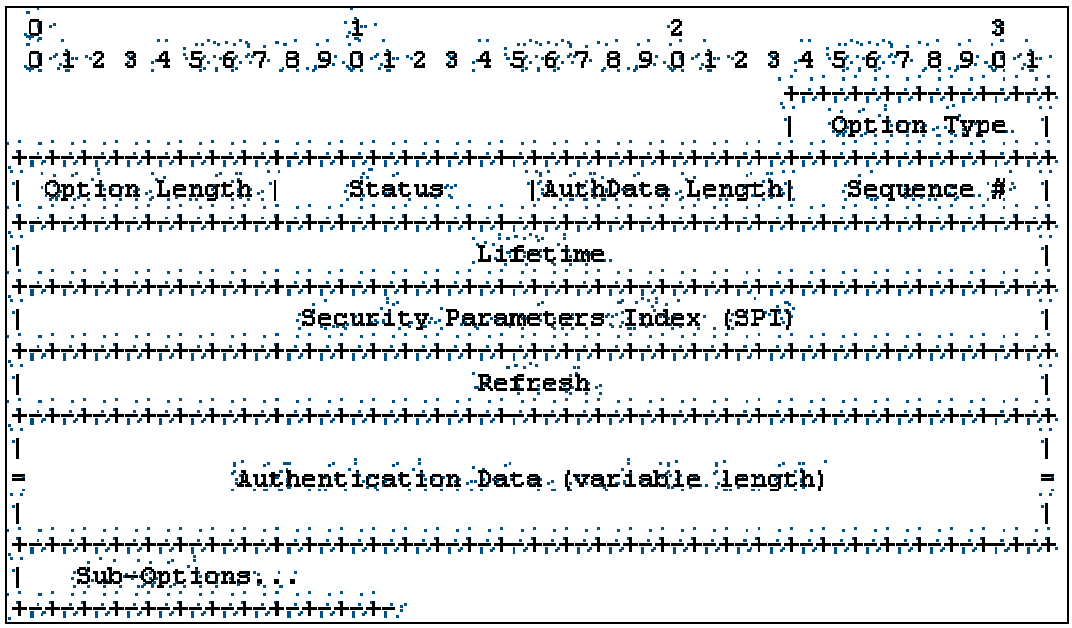


- Το πεδίο ***Option Type*** παίρνει την τιμή **198**
- Το πεδίο ***Option Length*** δίνει το μήκος της option χωρίς να συμπεριλαμβάνονται τα Option Type & Option Length .
- Το ***Acknowledge bit*** πρέπει να τεθεί ίσο με 1 , από τον κινητό κόμβο , ώστε να ζητήσει την απάντηση , δηλαδή ένα Binding acknowledgment , όταν ληφθεί το binding update που απέστειλε .
- Το ***Home Registration bit H*** παίρνει την τιμή 1 , από τον κινητό κόμβο , ζητώντας από τον κόμβο που λαμβάνει το μήνυμα να λειτουργήσει ως ο home agent του .
- Το ***Router bit (R),*** όταν έχει την τιμή 1 ,υποδηλώνει ότι ο κόμβος που το αποστέλλει είναι δρομολογητης .
- Το ***Duplicate Address Detection bit*** παίρνει την τιμή 1 ,από τον κινητό κόμβο , με σκοπό να ζητήσει από τον home agent να ελέγξει το home network του για την ύπαρξη διπλών διευθύνσεων.
- Το πεδίο ***Reservd*** δεν χρησιμοποιείται .
- Το πεδίο ***Prefix Length*** πρέπει να έχει την τιμή 0 εάν το bit H δεν είναι ενεργοποιημένο .
- Το πεδίο ***AuthDataLength*** δείχνει το μήκος του πεδίου Authentication Data.

- Το πεδίο ***Sequence #*** είναι ένας 8-bit αριθμός που στέλνεται από τον κινητό κόμβο για να αντιστοιχίσει τα binding update messages με τα binding acknowledgment massages .
- Το πεδίο ***Lifetime*** είναι ένας 32-bit αριθμός ο οποίος δείχνει τον αριθμό που απομένει, σε δευτερόλεπτα, πριν το binding message θεωρηθεί μη έγκυρο.
- Το ***Security Parameter Index (SPI) ,***είναι ένας 32-bit αριθμός ο οποίος , σε συνδυασμό με την IP διεύθυνση , χαρακτηρίζει μοναδικά το Binding Security Association για το συγκεκριμένο διάγραμμα δεδομένων .
- Το πεδίο ***Authentication Data ,*** είναι ένας μεταβλητού μήκους αριθμός ο οποίος χρησιμοποιείται για να ασφαλίσει το Binding update .

vi. Binding Acknowledgment message

Το binding acknowledgment message είναι κωδικοποιημένο σύμφωνα με το type-length-value πρότυπο .



- Το πεδίο ***Option Type*** παίρνει την τιμή 7.
- Το πεδίο ***Option Length*** δίνει το μήκος της option χωρίς να συμπεριλαμβάνονται τα Option Type & Option Length .
- Το πεδίο ***Status*** είναι ένας 8-bit αριθμός ο οποίος μας δηλώνει τη διαθεσιμότητα του Binding update .

Εάν η τιμή του πεδίου είναι μικρότερη του 128 τότε το Binding update έγινε αποδεκτό από τον κόμβο που το έλαβε όποτε και παίρνει την τιμή :

0 Binding update accepted

Εάν η τιμή είναι μεγαλύτερη του 128 τότε το Binding update δεν έγινε αποδεκτό από τον κόμβο που το έλαβε όποτε παίρνει τις παρακάτω τιμές οι οποίες υποδεικνύουν την λόγο που οδήγησε στην απόρριψη του μηνύματος :

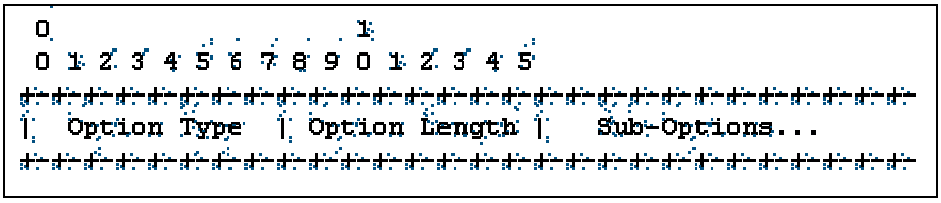
128 Reason Unspecified
130 Administratively Prohibited
131 Insufficient Recourses
132 Home registration not supported
133 Not home subnet
136 Incorrect interface identifier length
137 Not home subnet for this mobile node
138 Duplicate address detection failed
139 No security association
140 Mobile router prefix length sub-option failed
141 Sequence number too small

- Το πεδίο ***AuthDataLength*** δείχνει το μήκος του πεδίου Authentication Data.
- Το πεδίο ***Sequence*** # είναι ένας 8-bit αριθμός που στέλνεται από τον κινητό κόμβο για να αντιστοιχίσει τα binding update messages με τα binding acknowledgment massages .
- Το πεδίο ***Lifetime*** είναι ένας 32-bit αριθμός ο οποίος δείχνει τον αριθμό που απομένει, σε δευτερόλεπτα, πριν το binding message θεωρηθεί μη έγκυρο.
- Το ***Security Parameter Index (SPI) ,***είναι ένας 32-bit αριθμός ο οποίος , σε συνδυασμό με την IP διεύθυνση , χαρακτηρίζει μοναδικά το Binding Security Association για το συγκεκριμένο διάγραμμα δεδομένων .
- Το πεδίο ***Refresh*** το οποίο δείχνει το χρονικό διάστημα , σε δευτερόλεπτα , το οποίο πρέπει να μεσολαβεί μεταξύ της αποστολής δυο διαδοχικών Binding update από τον κινητό κόμβο .

- Το πεδίο ***Authentication Data ,*** είναι ένας μεταβλητού μήκους αριθμός ο οποίος χρησιμοποιείται για να ασφαλίσει το Binding update .

vii. Binding Request message

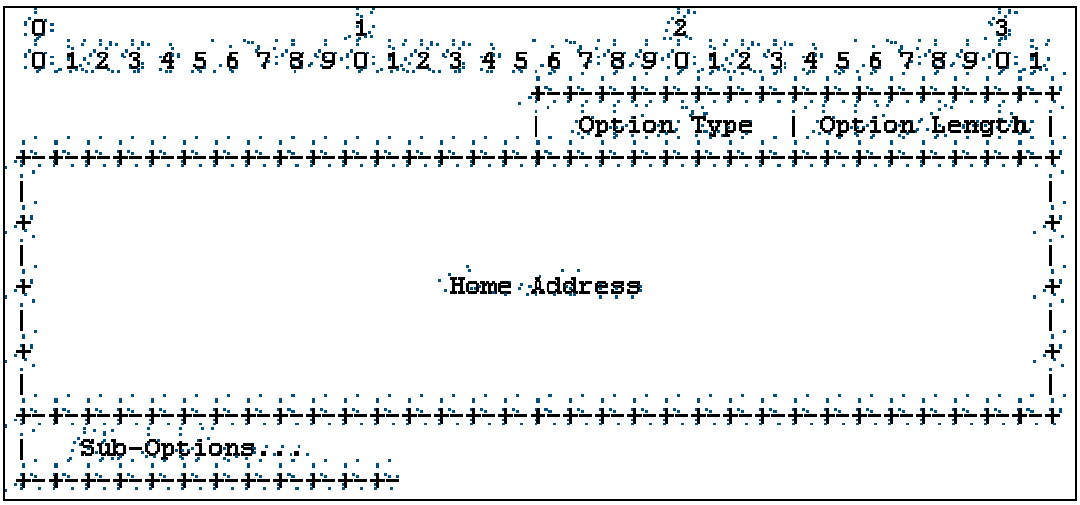
Το binding request message είναι κωδικοποιημένο σύμφωνα με το type-length-value πρότυπο .



- Το πεδίο ***Option Type*** , στο συγκεκριμένο μήνυμα , παίρνει την τιμή 8.
- Το πεδίο ***Option Length*** δίνει το μήκος της option χωρίς να συμπεριλαμβάνονται τα Option Type & Option Length .

viii. Home Address message

Το home address message είναι κωδικοποιημένο σύμφωνα με το type-length-value πρότυπο .



- Το πεδίο ***Option Type*** παίρνει την τιμή 201.
- Το πεδίο ***Option Length*** δίνει το μήκος της option χωρίς να συμπεριλαμβάνονται τα Option Type & Option Length .
- Το πεδίο ***Home Address*** δηλώνει την αρχική διεύθυνση του κινητού κόμβου που στέλνει το μήνυμα .

2.4. AGENT ADVERTISEMENT MESSAGES ΚΑΙ IPv6

Έχοντας παρουσιάσει τη μορφή του μηνύματος που αποστέλλεται από τους δρομολογητές για να υποδηλώσουν την παρουσία τους σε κάθε ενδιαφερόμενο κινητό κόμβο που βρίσκεται στο υποδίκτυο τους , θα εξετάσουμε τις αλλαγές που εισαγάγει η εξελιγμένη μορφή του πρωτοκόλλου .

Σύμφωνα με τα , έως τώρα ισχύοντα , οι δρομολογητες ήταν υποχρεωμένοι να αποστέλλουν τα παραπάνω μηνύματα με μια ,ελάχιστη, χρονική διάρκεια 3 δευτερολέπτων . Το σκεπτικό της παραπάνω κίνησης ήταν ότι τα μηνύματα θα έπρεπε να παράγονται ανά σύντομα χρονικά διαστήματα , ώστε οι κινητοί κόμβοι να ενημερώνονται για την παρουσία τους σε μικρό χρονικό διάστημα , αλλά όχι τόσο συχνά που να θεωρούν την απουσία ενός τέτοιου μηνύματος ως αστοχία του δρομολογητή , καθώς αυτό μπορεί να ελεγχθεί με τη χρήση ενός εξειδικευμένου αλγόριθμου .

Το πρόβλημα , ωστόσο , είναι ότι στην παραπάνω περίπτωση δεν παρέχεται έγκαιρη ειδοποίηση στους κινητούς κόμβους για το εάν έχουν μετακινηθεί σε άλλο δίκτυο ή όχι . Οι κινητοί κόμβοι ανιχνεύουν την πιθανή μετακίνηση τους εάν ενημερωθούν για την παρουσία νέων δρομολογητών ενώ δεν λαμβάνουν μηνύματα από τους παλιούς .Οι κινητοί κόμβοι πρέπει να είναι σε θέση να ανιχνεύουν γρήγορα εάν μετακινήθηκαν ώστε να αποκτήσουν μια νέα care-of διεύθυνση και να αποστείλουν Binding Updates ώστε να ενημερώσουν και να εγγραφούν με το Home agent τους .

Για την επίλυση του παραπάνω ζητήματος το Mobile IPv6 επιτρέπει την αποστολή μηνυμάτων από τους δρομολογητές πιο συχνά . Πιο συγκεκριμένα , σε δίκτυα όπου ο δρομολογητής περιμένει να παράσχει υπηρεσίες σε κινητούς κόμβους (π.χ σε ασύρματα δίκτυα) ή σε δίκτυα στα οποία λειτουργεί ως home agent θα πρέπει να είναι διαμορφωμένος έτσι ώστε να έχει μικρές τιμές MinRtrAdvInterval (Minimum Retrieval Advertisement Interval) και MaxRtrAdvInterval (Maximum Retrieval

Advertisement Interval) ώστε να αποστέλλει Router Advertisements πιο συχνά. Οι προτεινόμενες τιμές γι'αυτά τα όρια είναι :

- ***MinRtrAdvInterval 0.05 seconds***
- ***MaxRtrAdvInterval 1.5 seconds***

Θα πρέπει να σημειώσουμε ότι οι τιμές αυτές πρέπει να είναι επανακαθοριζόμενες και θα πρέπει να λαμβάνεται σοβαρά υπ'οψην το είδος του δικτύου πριν αποδώσουμε κάποια τιμή σε αυτές .

Όταν ο δρομολογητης στέλνει μηνύματα πιο συχνά από το καθορισμένο όριο δεν χρειάζεται να συμπεριλάβει όλες τις επεκτάσεις τις οποίες αναλύσαμε παραπάνω αλλά θα πρέπει να συμπεριλαμβάνει τουλάχιστον μια Prefix Information στην οποία το πεδίο R θα πρέπει να είναι ενεργοποιημένο .

2.5. AGENT SOLICITATION MESSAGES ΚΑΙ IPv6

Εκτός από το παραπάνω όριο υπάρχει ένα ακόμη το οποίο επέβαλλε η προγενέστερη έκδοση και ειδικότερα τον περιορισμό του αριθμού των Router Solicitation μηνυμάτων . Πιο συγκεκριμένα κάθε δρομολογητης μπορούσε να αποστείλει έως 3 τέτοια μηνύματα το καθένα από τα οποία πρέπει να έχει 4 δευτερόλεπτα διαφορά με το άλλο . Το αποτέλεσμα είναι, και εδώ , η καθυστέρηση του κινητού κόμβου στο να καταλάβει εάν άλλαξε δίκτυο ώστε να αποκτήσει νέα care-of διεύθυνση .

Η νέα έκδοση του πρωτοκόλλου επιτρέπει την αποστολή περισσοτέρων μηνυμάτων , όταν ο κινητός κόμβος βρίσκεται εκτός του αρχικού του δικτύου . Τα όρια που θέτει το πρωτόκολλο είναι τα εξής :

- Ο κινητός κόμβος ο οποίος δεν έχει care-of διεύθυνση μπορεί να στείλει περισσότερα από τα καθορισμένα , από το πρωτόκολλο , μηνύματα .
- Ο ρυθμός αποστολής μηνυμάτων πρέπει να είναι περιορισμένος αν και ο κινητός κόμβος μπορεί να αποστέλλει μηνύματα πιο συχνά . Το χρονικό διάστημα μεταξύ των μηνυμάτων εξαρτάται από τον τύπο του δικτύου .
- Ο κινητός κόμβος , ο οποίος έχει αποκτήσει μια care-of διεύθυνση , δεν θα πρέπει να στέλνει Router solicitations στο δρομολογητή στον οποίο έχει εγγραφεί εκτός εάν διαπιστώσει

ότι έχει μετακινηθεί σε άλλο δίκτυο (όποτε η care-of διεύθυνση που είχε δεν είναι πια έγκυρη και, συνεπώς βρίσκεται στην αναζήτηση νέου).

2.6. ΔΟΜΙΚΑ ΣΤΟΙΧΕΙΑ ΣΕ ΕΝΑ MOBILE IP ΔΙΚΤΥΟ

Στην παράγραφο αυτή θα εξετάσουμε ποιες είναι οι απαιτήσεις που θα πρέπει να πληρούν οι υπολογιστές που προορίζονται να εξυπηρετήσουν τις ανάγκες του πρωτοκόλλου . Πρόκειται για απαιτήσεις οι οποίες πρέπει να πληρούνται στο ακέραιο ώστε να έχουμε τα προσδοκώμενα αποτελέσματα . Αρχικά θα εξετάσουμε ποιες είναι οι προϋποθέσεις που πρέπει να πληρούνται στην παρούσα έκδοση και στη συνέχεια θα παραθέσουμε τις μελλοντικές απαιτήσεις υποστήριξης της νέας έκδοσης .

Στόχος της παρούσας παραγράφου είναι να ανακεφαλαιώσει τις παραπάνω ενότητες του κεφαλαίου ούτως ώστε ο αναγνώστης να κατανοήσει με σαφήνεια τόσο τα προβλήματα που υπήρχαν όσο και τις λύσεις που προτείνονται .

1. ΑΠΑΙΤΗΣΕΙΣ ΓΙΑ ΕΝΑ MOBILE IPv4 ΔΙΚΤΥΟ

i. Routers

Αρχικά θα εξετάσουμε τις απαιτήσεις που υπάρχουν από τους δρομολογητές , οι οποίοι εκτελούν το ρόλο του Home agent & Foreign agent . Γνωρίζουμε ότι κάθε mobility agent ο οποίος δεν μπορεί να ανακαλυφθεί από link-layer πρωτόκολλο πρέπει να χρησιμοποιεί agent advertisements . Εάν πάλι δεν υφίσταται αυτό το πρόβλημα η χρήση των μηνυμάτων αυτών εναπόκειται στον εν λόγω agent . Θα πρέπει να τονίσουμε , πάντως , ότι όλοι οι mobility agents πρέπει να απαντούν στα agent solicitation messages που λαμβάνουν .

Ανάλογες είναι και οι διαδικασίες που χρησιμοποιούνται στα agent advertisement messages & agent solicitation messages εκτός από μερικές διαφοροποιήσεις , τις οποίες αναφέρουμε παρακάτω :

- Ο mobility agent πρέπει να περιορίζει το ρυθμό αποστολής agent advertisement messages , η μέγιστη τιμή που απαιτουν καθορίζεται έτσι ώστε αυτά να μην χρησιμοποιούν μεγάλο μέρος του διαθέσιμου bandwidth .

- Ο mobility agent , συνήθως , ρυθμίζεται έτσι ώστε να στέλνει agent advertisement messages όταν λαμβάνει agent solicitation messages για τον λόγο που προαναφέραμε .

Εάν το home network δεν είναι ένα εικονικό δίκτυο τότε ο home agent κάθε κινητού κόμβου πρέπει να βρίσκεται στο link το οποίο καθορίζει η home address του κινητού κόμβου και τα agent advertisement messages , που στέλνονται από τον home agent στο συγκεκριμένο link , πρέπει να έχουν το bit ***H*** ενεργοποιημένο . Με τον τρόπο αυτό οι κινητοί κόμβοι καθορίζουν ότι όντως βρίσκονται στο home network . Κάθε agent advertisement messages που στέλνονται από τον home agent σε κάποιο άλλο link (στην περίπτωση που αυτός είναι mobility agent και εξυπηρετεί περισσότερα από ένα links) δεν πρέπει να έχουν ενεργοποιημένο το bit H εκτός εάν ο δρομολογητής έχει και σε αυτό το link το ρόλο του home agent .

Στην περίπτωση που το home network του κινητού κόμβου είναι εικονικό δίκτυο , δηλαδή το home network δεν έχει άλλη φυσική υπόσταση εκτός από αυτή του κινητού κόμβου , τότε δεν υπάρχει και κάποιο link στο οποίο θα στέλνονται agent advertisement messages . Σε αυτή την περίπτωση ο κινητός κόμβος αντιμετωπίζεται σαν να είναι πάντοτε εκτός του , υποτιθέμενου , αρχικού δικτύου του .

ii. Mobile nodes

Συνεχίζοντας, παρουσιάζουμε τις προϋποθέσεις που πρέπει να πληροί ο κινητός κόμβος ώστε να μπορεί να συνεργαστεί με το πρωτόκολλο . Κάθε κινητός κόμβος πρέπει να μπορεί να χρησιμοποιεί agent solicitation messages . Τα μηνύματα αυτά πρέπει να χρησιμοποιούνται μόνο όταν δεν υπάρχουν agent advertisement messages και όταν δεν έχει καθοριστεί η care-of address μέσω του link-layer πρωτοκόλλου . Ο κινητός κόμβος , για να φέρει σε πέρας το agent solicitation χρησιμοποιεί τις standard διαδικασίες που καθορίστηκαν για το ICMP Router Solicitation για χρήση σε ενσύρματα δίκτυα εκτός από το ότι ο κινητός κόμβος μπορεί να αναζητήσει συχνότερα από μία φορά κάθε τρία δευτερόλεπτα (που καθορίζει το ICMP Router Solicitation) τα agent solicitation messages , και ότι ένας κινητός κόμβος που τη δεδομένη χρονική περίοδο δεν συνδέεται με οποιοδήποτε foreign agent αναζητά τα agent solicitation messages περισσότερες φορές από ότι επιτρέπει η συνηθισμένη ρύθμιση των δρομολογητών .Ο ρυθμός με τον οποίο ένας κινητός κόμβος στέλνει τα agent solicitation messages πρέπει να καθοριστεί ανάλογα με τη λειτουργία που

θέλει να επιτελέσει . Ο κινητός κόμβος μπορεί να στείλει τρία αρχικά agent solicitation messages με μέγιστο ρυθμό μετάδοσης ένα ανά δευτερόλεπτο ψάχνοντας για έναν agent. Στη συνέχεια, όμως, ο ρυθμός αποστολής των μηνυμάτων πρέπει να μειωθεί ώστε να περιοριστεί η δέσμευση του διαθέσιμου bandwidth . Τα επόμενα agent solicitation messages πρέπει να σταλούν χρησιμοποιώντας έναν δυαδικό εκθετικό μηχανισμό που διπλασιάζει το διάστημα μεταξύ των διαδοχικών agent solicitation messages , μέχρι ένα μέγιστο διάστημα.

Το μέγιστο διάστημα πρέπει να επιλεγεί κατάλληλα , βασισμένο στα χαρακτηριστικά των μέσων από τα οποία ο κινητός κόμβος ζητά τα μηνύματα και , σε κάθε περίπτωση , να είναι ίσο με ένα τουλάχιστον λεπτό μεταξύ δυο διαδοχικών agent solicitation messages .

Ενώ ο κινητός κόμβος βρίσκεται στη διαδικασία ανεύρεσης ενός agent , ο κινητός κόμβος δεν πρέπει να αυξήσει το ρυθμό με τον οποίο στέλνει τις παρακλήσεις εκτός αν έχει λάβει μια θετική ένδειξη ότι έχει κινηθεί προς ένα νέο link . Αφού, πλέον, έχει κάνει register με κάποιον agent, ο κινητός κόμβος θα πρέπει να αυξήσει το ρυθμό αποστολής των μηνυμάτων μόνο όταν έχει μετακινηθεί σε άλλο δίκτυο (όποτε έχει ξεκινήσει η διαδικασία εγγραφής σε κάποιο agent από την αρχή). Σε όλες τις περιπτώσεις , τα προτεινόμενα διαστήματα μεταξύ διαδοχικών agent solicitation messages είναι τυπικές τιμές τις οποίες οι κινητοί κόμβοι μπορούν να μεταβάλλουν με μικρές όμως αποκλίσεις .

Οι κινητοί κόμβοι πρέπει να επεξεργαστούν τα λαμβανόμενα agent advertisement messages . Ένας κινητός κόμβος μπορεί να διακρίνει ένα τέτοιο από άλλες χρήσεις του ICMP Router Advertisement message με την εξέταση του αριθμού των advertised addresses και του συνολικού μήκους του πεδίου IP . Όταν το συνολικό μήκος IP δείχνει ότι το μήνυμα ICMP είναι μεγαλύτερο από αυτό που απαιτείται για το δεδομένο αριθμό των advertised addresses , τα υπόλοιπα στοιχεία ερμηνεύονται ως μια ή περισσότερες επεκτάσεις . Η παρουσία μιας mobility agent advertisement extension προσδιορίζει τη advertisement ως agent advertisement.

Εάν υπάρχουν περισσότερες από μια advertised addresses , ο κινητός κόμβος πρέπει να επιλέξει την πρώτη διεύθυνση για την αρχική προσπάθεια εγγραφής του. Εάν η προσπάθεια εγγραφής αποτύχει , ο κινητός κόμβος ξαναδοκιμάζει την προσπάθεια με τις επόμενες advertised addresses στη συνέχεια.

Όταν χρησιμοποιούνται πολλαπλές μέθοδοι agent discovery, ο κινητός κόμβος πρέπει πρώτα να προσπαθήσει την εγγραφή με agents που περιλαμβάνουν mobility agent advertisement extension από εκείνους που ανακαλύπτονται με άλλα μέσα. Αυτή η προτίμηση μεγιστοποιεί την πιθανότητα ότι η εγγραφή θα αναγνωριστεί , ελαχιστοποιώντας με αυτόν τον τρόπο τον αριθμό προσπαθειών εγγραφής .

Στη συνέχεια θα αναλύσουμε τους δυο πρωταρχικούς μηχανισμούς που χρησιμοποιεί ο κινητός κόμβος για να ανιχνεύσει εάν έχει μετακινηθεί από ένα υποδίκτυο σε ένα άλλο .

- ***Αλγόριθμος 1***

Η συγκεκριμένη μέθοδος βασίζεται στο πεδίο Lifetime του ICMP Router Advertisement option τμήματος του Agent Advertisement . Ο κινητός κόμβος σημειώνει τη χρονική διάρκεια που δείχνει το συγκεκριμένο πεδίο κάθε φορά που λαμβάνει Agent Advertisements. Εάν το χρονικό διάστημα παρέλθει χωρίς να έχει λάβει άλλο Agent Advertisement από τον ίδιο agent, τότε υποθέτει έχει χάσει επαφή μαζί του .Εάν είχε λάβει κάποιο Agent Advertisement από άλλο agent (στο οποίο το πεδίο Lifetime δεν έχει λήξει) μπορεί να επιχειρήσει να εγγραφεί με αυτόν τον agent ειδάλλως θα πρέπει να επιχειρήσει την ανακάλυψη ενός νέου .

- ***Αλγόριθμος 2***

Η δεύτερη μέθοδος χρησιμοποιεί προθέματα δικτύου . Πιο συγκεκριμένα τα Mobile Prefix Length Extensions μπορούν να χρησιμοποιηθούν από τον κινητό κόμβο για να καθορίσει εάν έχει λάβει ένα νεοεισερχόμενο μήνυμα από το ίδιο υποδίκτυο με αυτό που ανήκει η care-of διεύθυνση που έχει . Εάν τα προθέματα διαφέρουν τότε μπορεί να υποθέσει ότι έχει μετακινηθεί σε άλλο υποδίκτυο . Στην περίπτωση που ο κινητός κόμβος έχει αποκτήσει μια foreign agent care-of address δεν θα πρέπει να χρησιμοποιεί τη συγκεκριμένη μέθοδο εκτός εάν τόσο ο προηγούμενος agent όσο και ο επόμενος συμπεριλαμβάνουν στα Agent Advertisement messages Mobile Prefix Length Extensions .

Κάτι ανάλογο ισχύει και στην περίπτωση που ο κινητός κόμβος χρησιμοποιεί co-located care-of address καθώς θα πρέπει ο agent του να συμπεριλαμβάνει στα Agent Advertisement messages Mobile Prefix Length Extensions και να γνωρίζει το πρόθεμα του δικτύου της care-of address που χρησιμοποιεί . Στην περίπτωση που η μέθοδος αυτή δείξει ότι ο κινητός κόμβος μετακινήθηκε τότε έχει την επιλογή , αντί να επανεγγραφεί με την care-of address του , να επιχειρήσει να εγγραφεί με κάποιο foreign agent .

Κλείνοντας θα εξετάσουμε την περίπτωση όπου ο κινητός κόμβος αναγνωρίζει ότι επέστρεψε στο home network του καθώς λαμβάνει ένα Agent Advertisement message από τον home agent του όποτε και θα πρέπει να προσπαθήσει να επανεγγραφεί σε αυτόν . Πριν γίνει αυτό όμως θα πρέπει να κάνει ορισμένες αλλαγές όπως να διαμορφώσει τον κατάλογο των δρομολογητών που έχει αποθηκεύσει . Πρόκειται για μια διαδικασία την οποία θα εξετάσουμε λεπτομερώς στο παρακάτω κεφάλαιο .

2. ΑΠΑΙΤΗΣΕΙΣ ΓΙΑ ΕΝΑ MOBILE IPv6 ΔΙΚΤΥΟ

Θα ξεκινήσουμε τη συγκεκριμένη ενότητα αναφέροντας ορισμένες απαιτήσεις οι οποίες είναι κοινές τόσο για τους δρομολογητές όσο και για τους κινητούς κόμβους .

- Κάθε κόμβος πρέπει να μπορεί να διαχειριστεί την Home Address επιλογή η οποία συμπεριλαμβάνεται σε κάθε πακέτο δεδομένων .
- Κάθε κόμβος πρέπει να μπορεί να επεξεργαστεί τη Binding Update επιλογή και να επιστρέφει ένα Binding Acknowledgment , εάν το bit A είναι ενεργοποιημένο .

i. Routers

Οι παρακάτω πρόσθετες απαιτήσεις έχουν τεθεί για τους δρομολογητές :

- Κάθε δρομολογητής πρέπει να έχει την ικανότητα αποστολής της Advertisement Interval επιλογής για να βοηθήσει τους κινητούς κόμβους στην ανίχνευση της κίνησης τους .
- Κάθε δρομολογητής πρέπει να περιλαμβάνει τουλάχιστον ένα πρόθεμα με το bit R ενεργοποιημένο και την πλήρη IP διεύθυνση του .

Εδώ θα πρέπει να σημειώσουμε ορισμένες επιπλέον απαιτήσεις που υπάρχουν από τους δρομολογητές που αναλαμβάνουν το ρόλο του Home agent .

- Κάθε Home Agent πρέπει να μπορεί να αναχαιτίζει πακέτα τα οποία προορίζονται για τον κινητό κόμβο τον οποίο εξυπηρετεί ενώ ο κόμβος δεν βρίσκεται στο home network .
- Κάθε Home Agent πρέπει να μπορεί να εκτελέσει τη διαδικασία του encapsulate στα πακέτα που αναχαίτισε ώστε, μεσώ του tunneling , να τα προωθήσει στην αρχική care-of address του κόμβου .
- Κάθε Home Agent πρέπει να διατηρεί μια Home agent list για κάθε link το οποίο εξυπηρετεί ως home agent .
- Κάθε Home Agent πρέπει να υποστηρίζει την αποστολή ICMP Mobile Prefix Advertisements και να απαντά σε Mobile Prefix Solicitations .

ii Mobile Nodes

- Κάθε κινητός κόμβος του IPv6 πρέπει να μπορεί να εκτελεί IPv6 decapsulation .
- Κάθε κινητός κόμβος του IPv6 πρέπει να υποστηρίζει την αποστολή Binding Update μηνυμάτων καθώς επίσης τη λήψη και αποστολή Binding Acknowledgment .
- Κάθε κινητός κόμβος του IPv6 πρέπει να υποστηρίζει το μηχανισμό δυναμικής ανεύρεσης Home agents .
- Κάθε κινητός κόμβος του IPv6 πρέπει να υποστηρίζει τη λήψη Binding requests και να απαντά με την αποστολή Binding Updates .
- Κάθε κινητός κόμβος του IPv6 πρέπει να υποστηρίζει την αποστολή πακέτων δεδομένων τα οποία περιέχουν την Home address επιλογή . Αυτή η επιλογή πρέπει να συμπεριλαμβάνεται σε όλα τα πακέτα που αποστέλλει ο κινητός κόμβος ενώ βρίσκεται εκτός του Home network .
- Κάθε κινητός κόμβος του IPv6 πρέπει να υποστηρίζει τη λήψη Mobile Prefix Advertisements και να έχει τη δυνατότητα να επαναδιαμορφώσει τη home address του με βάση τις πληροφορίες που υπάρχουν σε αυτά .

ΚΕΦΑΛΑΙΟ 3

ΔΙΑΔΙΚΑΣΙΑ REGISTRATION

3.1. ΕΠΙΣΚΟΠΗΣΗ ΔΙΑΔΙΚΑΣΙΑΣ ΕΓΓΡΑΦΗΣ

Ο μηχανισμός εγγραφής του Mobile IP είναι ένας ευέλικτος τρόπος επικοινωνίας που επιτρέπει στους κινητούς κόμβους να δηλώνουν τη δεδομένη ανά πάσα χρονική στιγμή κατάσταση τους στο home agent του.

Οι κινητοί κόμβοι χρησιμοποιούν το μηχανισμό αυτό για να :

- ζητήσουν την προώθηση όταν επισκέπτονται ένα foreign network .
- ενημερώσουν τον home agent τους για την care-of διεύθυνση τους .
- ανανεώσουν την εγγραφή που πρόκειται να λήξει
- επανεγγραφούν με το αρχικό δίκτυο, αν και όταν επιστρέψουν σε αυτό .

Με τα μηνύματα εγγραφής ανταλλάσσονται πληροφορίες μεταξύ των κινητών κόμβων και των foreign agents (σε μερικές περιπτώσεις) και των home agents . Η εγγραφή δημιουργεί η μεταβάλλει ένα mobility binding στον home agent, συσχετίζοντας τη home address του κινητού κόμβου με την care-of address για το καθορισμένο, από το πεδίο lifetime, χρονικό διάστημα .

Αρκετές , ακόμη , προαιρετικές δυνατότητες είναι διαθέσιμες στη διαδικασία εγγραφής οι οποίες επιτρέπουν στον κινητό κόμβο :

- Να ανακαλύψει τη home address του
- Να διατηρήσει πολλαπλές , ταυτόχρονες συνδέσεις ώστε αντίγραφα κάθε διαγράμματος δεδομένων ,μεσώ του tunneling, να οδηγούνται σε κάθε ενεργή care-of διεύθυνση .
- Να επανεγγραφεί μια care-of διεύθυνση ενώ διατηρεί αλλά mobility bindings .
- Να ανακαλύπτει τη διεύθυνση του home agent του .

Ειδικότερα, το πρωτόκολλο Mobile IP καθορίζει δυο διαφορετικούς τρόπους registration , ένα με τη βοήθεια foreign agent ο οποίος αναμεταδίδει την έγγραφη στον home agent και ένας με τη χρήση του home agent του κινητού κόμβου . Το ποιον από τους δυο τρόπους θα χρησιμοποιηθεί καθορίζεται με βάση τα παρακάτω κριτήρια :

- Εάν ο κινητός κόμβος εγγράφεται χρησιμοποιώντας μια care-of address , τότε πρέπει να εγγραφεί χρησιμοποιώντας ένα foreign agent .
- Εάν ο κινητός κόμβος χρησιμοποιεί co-located care-of address και λάβει agent advertisement message από ένα foreign agent , ο οποίος ανήκει στο ίδιο δίκτυο με αυτό στο οποίο ανήκει η care-of address θα πρέπει να εγγραφεί με αυτόν τον foreign agent . Στην αντίθετη περίπτωση θα πρέπει να εγγραφεί με τον home agent του .
- Εάν ο κινητός κόμβος έχει επιστρέψει στο αρχικό δίκτυο τότε πρέπει να επανεγγραφεί κατευθείαν στον home agent του .

Και οι δυο προαναφερθείσες περιπτώσεις εγγραφής χρησιμοποιούν την ανταλλαγή Registration request & Registration reply messages . Όταν η έγγραφη γίνεται με τη χρήση foreign agent , για να ολοκληρωθεί επιτυχώς η διαδικασία πρέπει να ακολουθηθεί η εξής διαδικασία :

- Ο κινητός κόμβος στέλνει ένα Registration request μήνυμα στο foreign agent .
- Ο foreign agent επεξεργάζεται το μήνυμα και το προωθεί στον home agent.
- Ο home agent στέλνει ένα Registration reply μήνυμα στον foreign agent επιτρέποντας ή απορρίπτοντας την αίτηση εγγραφής.
- Ο foreign agent επεξεργάζεται το Registration reply και ενημερώνει τον κινητό κόμβο για την απάντηση της αίτησης του .

Εάν ο κινητός κόμβος εγγράφεται κατευθείαν με τον home agent , ακολουθείται η εξής διαδικασία :

- Ο κινητός κόμβος στέλνει ένα Registration request μήνυμα στον home agent .
- Ο home agent στέλνει ένα Registration reply μήνυμα στον κινητό κόμβο και ενημερώνει τον κινητό κόμβο για την απάντηση της αίτησης του.

3.2. Authentication

Όλοι οι κινητοί κομβόι , οι home agent , και foreign agent πρέπει να μπορούν να υποστηρίξουν mobility security association τα οποία υπάρχουν στις SPI & IP διευθύνσεις . Στην περίπτωση των κινητών κόμβων το ρόλο αυτό παίρνει η Home address . Τα μηνύματα εγγραφής μεταξύ του κινητού κόμβου και του home agent πρέπει να πιστοποιούνται , κάτι που γίνεται με τη βοήθεια μιας ειδικής επέκτασης την οποία θα εξετάσουμε σε παρακάτω ενότητα .

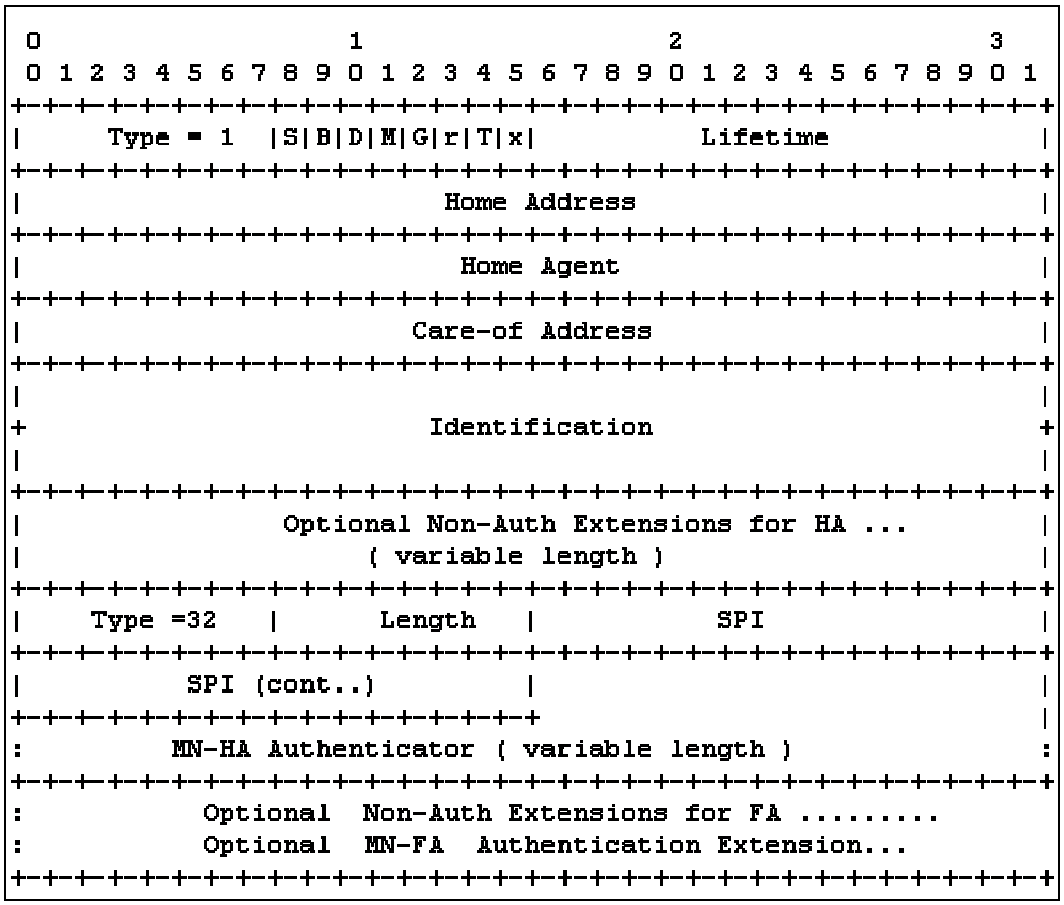
Τα παρακάτω σχήματα απεικονίζουν τη μορφή των μηνυμάτων που προαναφέραμε και παρατίθενται ούτως ώστε ο αναγνώστης να αποκτήσει μια όσο το δυνατόν μεγαλύτερη εξοικείωση με αυτό το πραγματικά πολύ λεπτό σημείο του πρωτοκόλλου , τα μηνύματα ελέγχου .

i. Registration Request

Το UDP πεδίο παίρνει τις τιμές :

Source Port ***μεταβλητή***
Destination Option ***434***

Η UDP επικεφαλίδα ακολουθείται από τα πεδία του Mobile IP τα οποία περιγράφουμε παρακάτω:



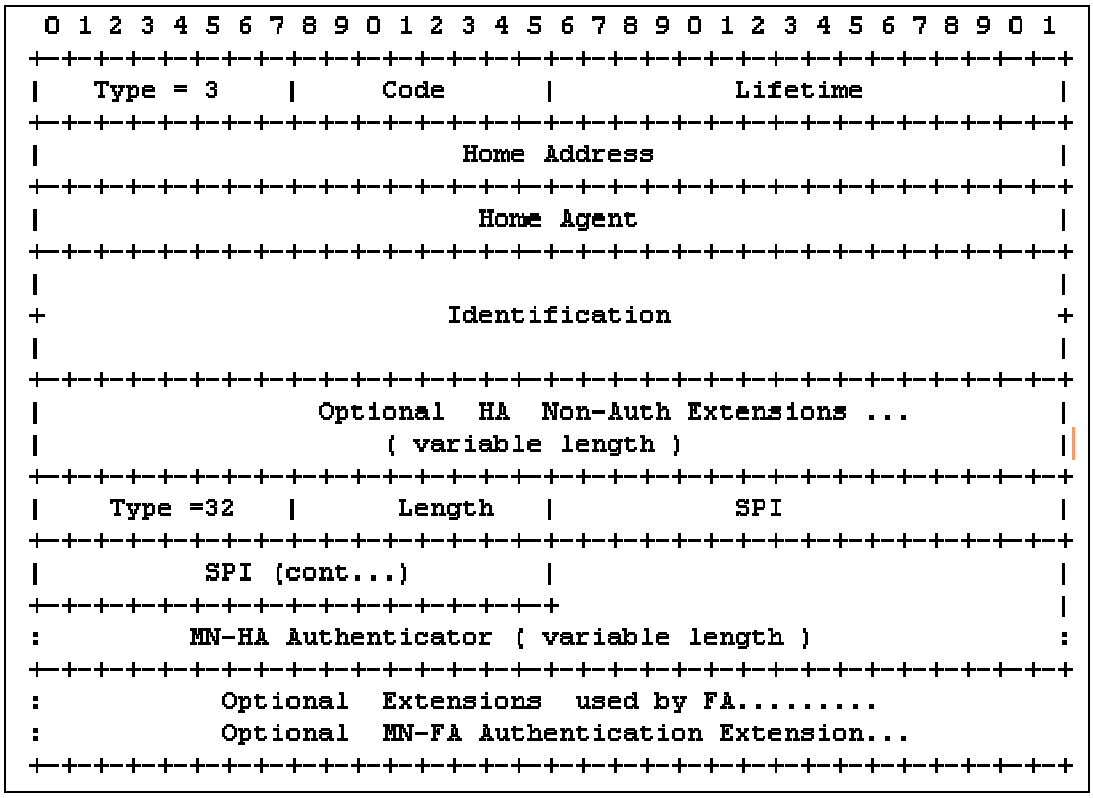
- Το πεδίο ***Type*** όταν έχει την τιμή 1 υποδηλώνει ότι πρόκειται για μήνυμα αίτησης εγγραφής .
- Το πεδίο ***S*** αναφέρεται σε πολλαπλά bindings . Ο κινητός κόμβος αιτείται στον home agent να διατηρήσει τα προηγούμενα bindings που είχε . Με αυτή την επιλογή ο home agent δρομολογεί πολλαπλά IP διαγράμματα σε όλες τις care-of addresses του κινητού κόμβου τις οποίες έχει εγγράψει κάτι που μπορεί να φανεί πολύ χρήσιμο, για τη βελτίωση της αξιοπιστίας, σε περιπτώσεις ασύρματων δικτύων .
- Το πεδίο ***B*** αναφέρεται στη μετάδοση διαγραμμάτων δεδομένων . Ο κινητός κόμβος δηλώνει ότι θέλει να λαμβάνει αυτά τα διαγράμματα τα οποία θα λάμβανε εάν βρισκόταν στο home network .
- Το πεδίο ***D*** δηλώνει ότι ο κινητός κόμβος έχει collocated care-of address οπότε θα κάνει decapsulation των πακέτων που λαμβάνει μόνος του.

- Το πεδίο ***M*** δηλώνει ότι ο home agent θα πρέπει να χρησιμοποιήσει τη μέθοδο Minimal Encapsulation .
- Το πεδίο ***V*** δείχνει ότι ο home agent θα πρέπει να χρησιμοποιήσει τη συμπίεση επικεφαλίδας κατά το πρότυπο του Van Jacobson.
- Το πεδίο ***G*** υποδηλώνει ότι ο home agent θα πρέπει να χρησιμοποιήσει GRE encapsulation.
- Το πεδίο ***Lifetime*** δείχνει το χρονικό διάστημα , σε δευτερόλεπτα , πέρα από το (εάν δεν υπάρξει επικοινωνία μεταξύ home agent και κινητού κόμβου) οποίο η έγγραφη θα θεωρηθεί ως ανενεργή .
- Στο πεδίο ***home address*** υπάρχει η αρχική IP διεύθυνση του κινητού κόμβου .
- Στο πεδίο ***home agent*** δηλώνεται η IP διεύθυνση του home agent .
- Στο πεδίο ***care-of address*** δηλώνεται η IP διεύθυνση στο τέλος της σήραγγας . Ο home agent πρέπει να προωθήσει τα πακέτα που λαμβάνει με την αρχική IP διεύθυνση του κινητού κόμβου προς αυτή τη διεύθυνση .
- Στο πεδίο ***Identification*** υπάρχει ένας 64-bit αριθμός , οποίος δημιουργείται από τον κινητό κόμβο και χρησιμοποιείται για την σύγκριση του συγκεκριμένου αριθμού μεταξύ των αιτήσεων εγγραφής και των απαντήσεων εγγραφής (πρέπει να είναι ο ίδιος) για λόγους ασφαλείας .
- Το πεδίο ***Extensions*** χρησιμοποιείται ως επέκταση του παραπάνω πεδίου , για βελτίωση της παρεχόμενης ασφάλειας .

ii. Registration Reply

Στη συνέχεια μπορούμε να παρατηρήσουμε τη μορφή που έχει το μήνυμα έλεγχου απάντησης έγγραφης οπότε και θα διαπιστώσουμε ότι οι διαφορές με το μήνυμα έλεγχου αίτησης έγγραφης δεν είναι σημαντικές .

Πράγματι τα περισσότερα πεδία είναι ίδια , αν και όπως θα περίμενε κανείς , η σημασία που αυτά παίρνουν είναι σε μερικές τουλάχιστον περιπτώσεις διαφορετική . Το πρωτόκολλο που χρησιμοποιείται για την αποστολή και αυτού του μηνύματος έλεγχου είναι το UDP .



- Το πεδίο ***Type*** παίρνει την τιμή **3** για να υποδηλώσει ότι πρόκειται για μήνυμα απάντησης εγγραφής.
- Το πεδίο ***Code*** υποδηλώνει το αποτέλεσμα της αίτησης εγγραφής .
- Το πεδίο ***Lifetime*** μας δείχνει το χρόνο μετά τον οποίο η έγγραφη θα θεωρείται λήξασα , εφόσον βέβαια είχε γίνει αποδεκτή την αρχή.
- Το πεδίο ***Home address*** μας δίνει την IP διεύθυνση του κινητού κόμβου .
- Το πεδίο ***Home agent*** μας δίνει την IP διεύθυνση του Home agent .
- Το πεδίο ***Identification*** είναι ένας 64 bit αριθμός με ίδιο σκοπό με αυτό που αναφέρθηκε παραπάνω.
- Το πεδίο ***Extensions*** ακολουθεί το σταθερό τμήμα του Registration reply message. Οι επεκτάσεις , και σε αυτό το τμήμα του πρωτοκόλλου διαδραματίζουν πολύ σημαντικό ρόλο και θα παρουσιαστούν αναλυτικά στην ενότητα 3.5 .

Οι παρακάτω τιμές έχουν οριστεί για χρήση στο πεδίο ***Code*** :

Registration successful:

0 Registration accepted
1 ***Registration accepted, but simultaneous bindings not supported***

Registration denied by foreign agent:

64 Reason unspecified
65 Administratively prohibited
66 Insufficient resources
67 Mobile node failed authentication
68 Home agent failed authentication
69 Requested lifetime too long
70 Poorly formed request
71 Poorly formed reply
72 Requested encapsulation unavailable
73 Reserved and unavailable
77 Invalid care-of address
78 Registration timeout
80 Home network unreachable (ICMP error received)
81 Home agent host unreachable (ICMP error received)
82 Home agent port unreachable (ICMP error received)
88 Home agent unreachable (ICMP error received)

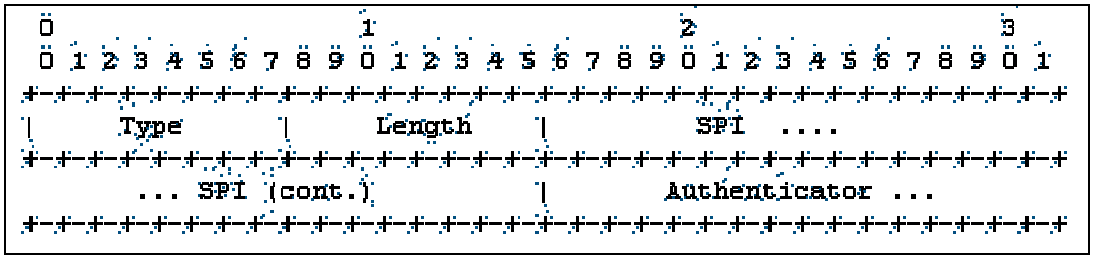
Registration denied by home agent:

128 Reason unspecified
129 Administratively prohibited
130 Insufficient resources
131 Mobile node failed authentication
132 Foreign agent failed authentication
133 Registration identification mismatch
134 Poorly formed request
135 Too many simultaneous mobility bindings
136 Unknown home agent address

3.3. ΔΟΜΗ ΤΩΝ REGISTRATION EXTENSIONS

i. Mobile-Home Authentication Extension

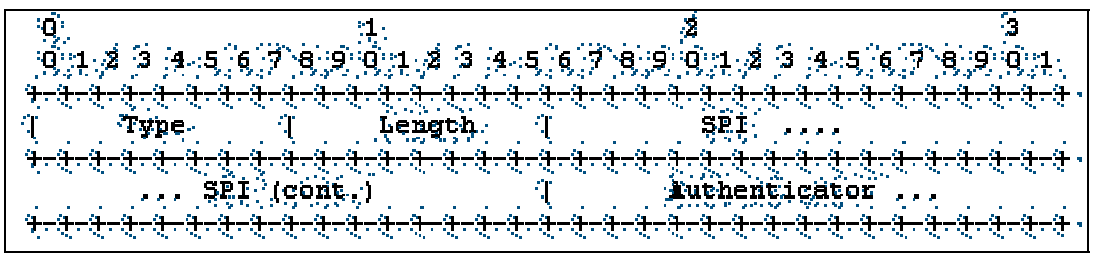
Σε κάθε Registration request πρέπει να υπάρχει μόνο μια επέκταση που να επιτρέπει την αυθεντικοποίηση ενώ το ίδιο ισχύει και στα Registration replies που παράγονται από τον Home agent . Η επέκταση έχει την παρακάτω μορφή :



- Το πεδίο ***Type*** παίρνει την τιμή **32**.
- Το πεδίο ***Length*** παίρνει την τιμή 4 συν τον αριθμό των bytes του authenticator .
- Το πεδίο ***SPI*** έχει μήκος 4 bytes.
- Το πεδίο Authenticator έχει μεταβλητό μήκος. Ο Authenticator προστατεύει το φορτίο του UDP και τα πεδία Type , Length και SPI .

ii. Mobile-Foreign Authentication Extension

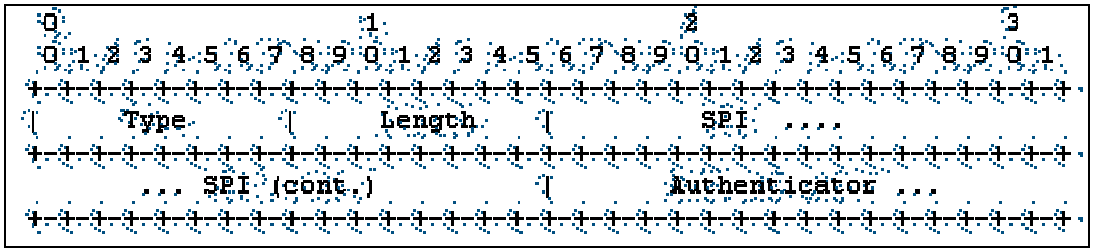
Η επέκταση αυτή μπορεί να χρησιμοποιηθεί σε Registration requests & replies όπου μεταξύ του κινητού κόμβου και του foreign agent υπάρχει μια mobility security association .



- Το πεδίο ***Type*** παίρνει την τιμή **33**.
- Το πεδίο ***Length*** παίρνει την τιμή 4 συν τον αριθμό των bytes του authenticator .
- Το πεδίο ***SPI*** έχει μήκος 4 bytes.
- Το πεδίο Authenticator έχει μεταβλητό μήκος. Ο Authenticator προστατεύει το φορτίο του UDP και τα πεδία Type , Length και SPI .

iii. Foreign-Home Authentication Extension

Η επέκταση αυτή μπορεί να χρησιμοποιηθεί σε Registration requests & replies όπου μεταξύ του κινητού κόμβου και του foreign agent υπάρχει μια mobility security association .



- Το πεδίο ***Type*** παίρνει την τιμή **34**.
- Το πεδίο ***Length*** παίρνει την τιμή 4 συν τον αριθμό των bytes του authenticator .
- Το πεδίο ***SPI*** έχει μήκος 4 bytes.
- Το πεδίο ***Authenticator*** έχει μεταβλητό μήκος. Ο Authenticator προστατεύει το φορτίο του UDP και τα πεδία Type , Length και SPI .

3.4. ΑΠΑΙΤΗΣΕΙΣ ΑΠΟ ΤΟΥΣ MOBILE NODES ΓΙΑ ΤΗ ΔΙΑΔΙΚΑΣΙΑ ΤΟΥ REGISTRATION

Ο κινητός κόμβος θα πρέπει να είναι διαμορφωμένος με μια net mask και μια mobility agent association για κάθε ένα από τους home agents του. Θα ήταν εξαιρετικά χρήσιμο εάν ο κόμβος ήταν εφοδιασμένος με την home address και τις IP διευθύνσεις ενός ή περισσοτέρων home agents καθώς δεν θα ήταν αναγκασμένος να καταφύγει στις διαδικασίες ανεύρεσης τους , τουλάχιστον όχι των συγκεκριμένων .

Στην περίπτωση που ο κινητός κόμβος δεν είναι εφοδιασμένος με την home address τότε μπορεί να χρησιμοποιήσει εξειδικευμένες επεκτάσεις για την ανεύρεση της , διαφορετικά θα θέσει στο πεδίο Home Address του μηνύματος Registration Request την τιμή 0.0.0.0 .

Για κάθε έγγραφη η οποία εκκρεμεί ο κινητός κόμβος διατηρεί αποθηκευμένες τις ακόλουθες πληροφορίες:

- Τη link-layer διεύθυνση του foreign agent στον οποίο απέστειλε τη registration request
- Την IP διεύθυνση του κόμβου που προορίζεται να δεχτεί τη registration request
- Την care-of address που χρησιμοποιείται στη registration request
- Την τιμή του πεδίου Identification που έστειλε στη registration request
- Την τιμή του πεδίου Lifetime
- Το υπολειπόμενο χρονικό διάστημα του πεδίου Lifetime της εκκρεμούσας εγγραφής.

Ο κινητός κόμβος ξεκινά τη διαδικασία εγγραφής όταν ανιχνεύσει ότι μετακινήθηκε από το δίκτυο στο οποίο βρισκόταν . Όταν διαπιστώσει κάτι τέτοιο στέλνει μια registration request η οποία επιτρέπει, στον δρομολογητή που λειτουργεί ως home agent του, να κάνει τις απαραίτητες αλλαγές στο mobility binding που είχε δημιουργήσει για αυτόν . Στην περίπτωση που επιστρέψει στο home network η αίτηση επανεγγραφής σε αυτό έχει ως αποτέλεσμα το σβήσιμο των mobility bindings που διατηρούσε ο home agent για αυτόν . Γίνεται εύκολα κατανοητό ότι, εάν ο κινητός κόμβος , βρίσκεται στο home network, τα mobility bindings είναι περιττά .

Υπάρχουν , ωστόσο , και άλλες περιπτώσεις για τις οποίες ο κινητός κόμβος θα πρέπει να επανεγγραφεί με το foreign agent του,

όπως π.χ η περίπτωση που αυτός έχει εκτελέσει επανεκκίνηση ή όταν η διάρκεια που καθορίζεται από το πεδίο Lifetime πλησιάζει προς τη λήξη της .

Στην περίπτωση που ο κινητός κόμβος δεν έχει ενδείξεις ότι έχει μετακινηθεί σε άλλο δίκτυο και λαμβάνει agent advertisements από άλλους agents δεν θα πρέπει να τις λαμβάνει υπόψη του εφόσον, βέβαια , συνεχίζει να λαμβάνει παρόμοια μηνύματα από τον foreign agent που έχει εγγραφεί και το χρονικό διάστημα για το οποίο η έγγραφη με αυτόν δεν θεωρείται λήξασα δεν έχει παρέλθει .

Για να γίνουν ευκολότερα κατανοητά τα παραπάνω θα παραθέσουμε τις ενδεικτικές τιμές που δίνονται στα πεδία του Registration request μηνύματος στην περίπτωση της εγγραφής με την care-of διεύθυνση του foreign agent:

```
      UDP fields:
        Source Port = <any>
        Destination Port = 434
      Registration Request fields:
        Type = 1
        S=0,B=0,D=0,M=0,G=0
        Lifetime = the Registration Lifetime copied from the
          Mobility Agent Advertisement Extension of the
          Router Advertisement message
        Home Address = the mobile node's home address
        Home Agent = IP address of mobile node's home agent
        Care-of Address = the Care-of Address copied from the
          Mobility Agent Advertisement Extension of the
          Router Advertisement message
        Identification = Network Time Protocol timestamp or Nonce
      Extensions:
        An authorization-enabling extension (e.g., the
Mobile-Home Authentication Extension)
```

Όπως βλέπουμε τα πεδίο του UDP πρωτοκόλλου δείχνουν ως πόρτα προορισμού την 434 , η οποία είναι και η default πόρτα για μηνύματα του συγκεκριμένου πρωτοκόλλου , ενώ ως προς την πόρτα εισόδου δεν υπάρχει περιορισμός . Στο πεδίο Type δίνεται η τιμή 1, η οποία υποδηλώνει ότι πρόκειται για μήνυμα Registration request . Στα bits S,B,D,M,G δίνεται η τιμή 0 ,στο πεδίο Lifetime δίνεται η τιμή που βρίσκεται στο αντίστοιχο πεδίο του Router advertisement message ενώ και η care-of address συμπληρώνεται με τον ίδιο τρόπο . Στο πεδίο Home address βρίσκεται η home address του κινητού κόμβου και στο Home agent η IP διεύθυνση του home agent .

Ανάλογα με τις ιδιαίτερες απαιτήσεις που έχουμε σε κάθε περίπτωση στα bits S,B,D,M,G δίνονται τιμές μεταξύ 0 και 1 . Στην υποθετική περίπτωση που ο κινητός κόμβος θέλει να στέλνονται σε αυτόν διαγράμματα δεδομένων από το αρχικό του δίκτυο , υποστηρίζει όλες τις μορφές encapsulation και δεν υποστηρίζει την ύπαρξη simultaneous bindings τα bits θα πρέπει να είχαν τις τιμές:

S=0, B=D=M=G=1

Με τη βοήθεια του παραπάνω παραδείγματος πήραμε μια ιδέα για το συνδυασμό των τιμών που μπορούν να δοθούν στα bit ελέγχου και στη συνέχεια θα εξετάσουμε με περισσότερες λεπτομέρειες την , ιδιαίτερη , σημασία τους .

Ο κινητός κόμβος μπορεί να θέσει το bit **S** σε κατάσταση 1 για να ζητήσει , από τον home agent , να διατηρήσει τα προηγούμενα mobility bindings διαφορετικά ο τελευταίος θα τα διαγράφει και στη θέση τους θα αποθηκεύει τα νέα . Η διατήρηση simultaneous bindings χρησιμοποιείται στην περίπτωση που ο κινητός κόμβος μετακινείται σε ασύρματο δίκτυο και βρίσκεται εντός της ακτίνας μετάδοσης περισσοτέρων του ενός foreign agents . Ο home agent προωθεί αντίγραφα κάθε διαγράμματος δεδομένων σε όλες τις care-of διευθύνσεις όποτε ο κινητός κόμβος λαμβάνει πολλαπλά αντίγραφα .

Ο κινητός κόμβος μπορεί να θέσει το bit **D** σε κατάσταση 1 εάν , για να εγγραφεί σε ένα agent , χρησιμοποιεί co-located care-of address (διαφορετικά θα πρέπει να πάρει την τιμή 0).

Ο κινητός κόμβος μπορεί να θέσει το bit **B** σε κατάσταση 1 για να ζητήσει από τον home agent τη λήψη διαγραμμάτων δεδομένων από το αρχικό δίκτυο . Ο τρόπος με τον οποίο τα διαγράμματα αυτά προωθούνται στον κινητό κόμβο εξαρτάται από τον τύπο της care-of addresses με την οποία έχει εγγραφεί αυτός και η οποία δηλώνεται με το bit D.

- Εάν έχει τη τιμή 1 , τότε ο κινητός κόμβος θα εκτελέσει decapsulate των διαγραμμάτων δεδομένων που φτάνουν σε αυτόν μόνος του (χρήση co-located care-of address) . Για να προωθηθεί ένα τέτοιο διάγραμμα , ο home agent θα πρέπει να εκτελέσει tunneling στο διάγραμμα αυτό ενώ η αντίστροφη διαδικασία θα εκτελεστεί από τον κινητό κόμβο (όπως και για κάθε άλλο αντίστοιχο πακέτο) .

- Εάν έχει την τιμή 0 , αυτό δηλώνει ότι ο κινητός κόμβος έχει εγγραφεί χρησιμοποιώντας την care-of address ενός foreign agent οπότε τα διαγράμματα δεδομένων που θα φτάσουν σε αυτόν θα έχουν γίνει decapsulate από το foreign agent . Στην περίπτωση αυτή η προώθηση δεδομένων γίνεται αφού πρώτα ο home agent τα encapsulate σε ένα unicast διάγραμμα δεδομένων με προορισμό τη home address του κινητού κόμβου και στη συνέχεια εκτελέσει tunneling στο τελικό διάγραμμα στέλνοντας το στην care-of address του κινητού κόμβου . Στη συνέχεια ο foreign agent , του κινητού κόμβου , εκτελεί την αντίστροφη διαδικασία , δηλαδή decapsulates το διάγραμμα , όποτε το περιεχόμενο που φτάνει στον κόμβο είναι το αρχικό unicast διάγραμμα . Ο αποδέκτης εκτελεί και αυτός με τη σειρά του decapsulate στο διάγραμμα, κάτι που συνεπάγεται ότι έχει αυτή τη δυνατότητα . Στην αντίθετη περίπτωση το bit B πρέπει να τεθεί ίσο με 0 .

Ο κινητός κόμβος μπορεί να θέσει σε κατάσταση 1 το bit **M** και , προαιρετικά , το bit **G** μόνο εάν ο κινητός κόμβος έχει τη δυνατότητα να εκτελέσει αυτόνομα decapsulate στα διαγράμματα δεδομένων που λαμβάνει ή ο foreign agent του έχει δηλώσει ότι υποστηρίζει encapsulation αυτού του είδους , μέσω των σχετικών bits στο agent advertisement μήνυμα .

Το πεδίο **Lifetime** καθορίζεται λαμβάνοντας υπόψη τις παρακάτω περιπτώσεις:

- Εάν ο κινητός κόμβος εγγράφεται με ένα foreign agent τότε η τιμή του συγκεκριμένου πεδίου δεν θα πρέπει να υπερβαίνει την τιμή που δήλωνε το agent advertisement μήνυμα . Όταν η μέθοδος με την οποία γίνεται γνωστή η care-of address δεν χρησιμοποιεί το πεδίο Lifetime , τότε μπορούμε να δώσουμε τη default τιμή του ICMP Router Advertisement Lifetime (1800 seconds) .
- Στην περίπτωση που ο κινητός κόμβος ζητά από τον home agent τη διαγραφή ενός συγκεκριμένου mobility binding , στέλνοντας ένα Registration request μήνυμα τότε στο πεδίο Lifetime δίνεται η τιμή 0.

- Στο πεδίο Lifetime δίνεται η τιμή 0 στην περίπτωση που ο κινητός κόμβος επιστρέφει στο αρχικό δίκτυο όποτε και επιχειρεί να επανεγγραφεί με τον home agent του , διαγράφοντας όλα τα mobility bindings .

Στο πεδίο **Home address** δηλώνεται η Home address του κινητού κόμβου , στην περίπτωση που είναι γνωστή , ειδάλλως παίρνει την τιμή 0.

Το πεδίο **Home agent** περιέχει την τη διεύθυνση του home agent που εξυπηρετεί τον κινητό κόμβο , εφόσον είναι γνωστή . Στην αντίθετη περίπτωση χρησιμοποιείται η μέθοδος δυναμικής ανακάλυψης της διεύθυνσης .

Τέλος , στο πεδίο **Care-of address** δηλώνεται η Care-of address με την οποία επιθυμεί , ο κινητός κόμβος , να εγγραφεί . Στην ειδική περίπτωση που ο κινητός κόμβος επιθυμεί να επανεγγράψει όλες τις Care-of addresses του τότε πρέπει να τοποθετήσει τη home address του .

Το πεδίο **Identification** εξαρτάται από τον τύπο προστασίας που χρησιμοποιεί για την αντιμετώπιση επιθέσεων επανάληψης , σε συνδυασμό με τον home agent του , και θα το εξετάσουμε στο Κεφάλαιο 6 .

1. Επέκταση με σκοπό την επίτευξη αυθεντικοποίησης
2. Στην περίπτωση που υπάρχει , κάθε επέκταση που δεν έχει ως σκοπό την αυθεντικοποίηση και αναμένεται να χρησιμοποιηθεί από τον foreign agent .
3. Η επέκταση τύπου Mobile-Foreign Authentication .

3.5. Λήψη Registration replies μηνυμάτων

Στην ενότητα αυτή θα εξετάσουμε τις πιθανές απαντήσεις που μπορεί να λάβει ένας κινητός κόμβος ως απάντηση των registration request μηνυμάτων που απέστειλε και εξετάσαμε παραπάνω . Τα μηνύματα αυτά μπορούν να κατηγοριοποιηθούν στις εξής περιπτώσεις:

- Η αίτηση έγινε αποδεκτή
- Η αίτηση απορρίφθηκε από τον foreign agent
- Η αίτηση απορρίφθηκε από τον home agent

Ο τρόπος αντίδρασης του κινητού κόμβου σε κάθε περίπτωση θα εξεταστεί στη συνέχεια .

i. Η Registration request έγινε αποδεκτή

Ο κινητός κόμβος , στην περίπτωση αυτή , προχωρά στον επανακαθορισμό της λίστας των δρομολογητών του ώστε να πληρεί τις απαιτήσεις του νέου point of attachment .

Όταν εγγράφεται σε ένα foreign network θα πρέπει να ανανεώσει την έγγραφη του πριν παρέλθει το χρονικό διάστημα που ορίζει το Lifetime . Όπως αναφέραμε και παραπάνω , για κάθε αίτηση εγγραφής η οποία εκκρεμεί ο κινητός κόμβος πρέπει να αποθηκεύσει το υπολειπόμενο χρονικό διάστημα όπως επίσης και το υπολειπόμενο χρονικό διάστημα από την αρχική αίτηση εγγραφής . Όταν λάβει μια έγκυρη απάντηση πρέπει να ελαττώσει την τιμή του χρονικού διαστήματος που έχει αποθηκεύσει κατά χρονικό διάστημα ίσο με αυτό που ελάττωσε ο home agent το αντίστοιχο πεδίο . Η διαδικασία αυτή είναι ισοδύναμη με την υπόθεση κατά την οποία ο κινητός κόμβος ξεκινά ένα εικονικό χρονόμετρο , ορίζοντας ως τιμή για το Lifetime αυτή που έχει αποθηκεύσει , από τη στιγμή που έστειλε την αίτηση εγγραφής έως ότου λάβει μια απάντηση .

Εφόσον η χρονομέτρηση ξεκινά αφού ο κόμβος στείλει την αίτηση έχουμε εξασφαλίσει ότι θα επανεγγραφεί πριν παρέλθει το δεδομένο χρονικό διάστημα .

ii. Μη αποδεκτή Registration request

Εάν η αίτηση εγγραφής του κινητού κόμβου δεν γίνει αποδεκτή τότε θα πρέπει να αποθηκεύσει τα αιτία που οδήγησαν στην απόρριψη της αίτησης ώστε να μπορέσει να τα διορθώσει. Η αιτιολογία βρίσκεται στο πεδίο Code του registration reply και τα πιθανά μηνύματα είναι τα εξής:

Code 69: **Denied by Foreign Agent, Lifetime Too Long**

Στην περίπτωση αυτή στο πεδίο Lifetime του registration reply message θα αναγράφεται η μέγιστη τιμή την οποία ο foreign agent είναι διατεθειμένος να δεχτεί σε κάθε registration request message . Ο κινητός κόμβος μπορεί να ξαναεπιχειρήσει να εγγραφεί με τον συγκεκριμένο agent θέτοντας το Lifetime στο registration request message μικρότερο η ίσο με αυτή την τιμή.

Code 133: **Denied by Home Agent, Identification Mismatch**

Στην περίπτωση αυτή το πεδίο Identification του registration reply message θα περιέχει μια τιμή που θα επιτρέπει στον κινητό κόμβο να συγχρονιστεί με τον home agent , βασισμένη στον τύπο προστασίας που χρησιμοποιούν για να αντιμετωπίσουν replay attacks . Ο κινητός κόμβος πρέπει να προσαρμόσει τις παραμέτρους που χρησιμοποιεί για τον υπολογισμό του πεδίου αυτού πριν στείλει νέο registration request message.

Code 136: **Denied by Home Agent, Unknown home agent address**

Ο κωδικός αυτός επιστρέφεται από τον home agent όταν ο κινητός κόμβος εκτελεί dynamic home agent address resolution. Στην περίπτωση αυτή το πεδίο home agent του registration reply message θα περιέχει τη unicast IP διεύθυνση του home agent που απαντά . Ο κινητός κόμβος πρέπει να προσαρμόσει τις παραμέτρους που χρησιμοποιεί για τον υπολογισμό του Identification πεδίου πριν στείλει νέο registration request message.

3.6. ΑΠΑΙΤΗΣΕΙΣ ΑΠΟ ΤΟΥΣ FOREIGN AGENTS ΓΙΑ ΤΗ ΔΙΑΔΙΚΑΣΙΑ ΤΟΥ REGISTRATION

Οι foreign agents , κατά τη διαδικασία της εγγραφής διαδραματίζουν ένα μάλλον παθητικό ρόλο . Αναμεταδίδουν τα registration request messages από τους κινητούς κόμβους προς τους home agents και , στην περίπτωση που παρέχουν την care-of address εκτελούν το decapsulate των διαγραμμάτων δεδομένων . Πρέπει, ακόμη, να αποστέλλουν ανά τακτά χρονικά διαστήματα agent advertisement messages για να υποδηλώσουν την παρουσία τους στο δίκτυο .

Ένας foreign agent δεν πρέπει να μεταδίδει registration request messages εκτός από την περίπτωση που αναμεταδίδει ένα μήνυμα που έλαβε από ένα κινητό κόμβο προς τον home agent του, ενώ κάτι ανάλογο ισχύει και για τα registration reply messages (με την αντίθετη από την προαναφερθείσα κατεύθυνση βέβαια) .

i. Ρυθμίσεις και πεδία εγγραφών

Κάθε foreign agent πρέπει να έχει μια care-of διεύθυνση ενώ για κάθε εκκρεμούσα εγγραφή πρέπει να διατηρεί μια λίστα με τους επισκεπτόμενους κόμβους η οποία θα περιέχει τις παρακάτω πληροφορίες:

- Τη Link-layer Source address του κινητού κόμβου
- Την Home address του κινητού κόμβου ή την co-located care-of address
- Την IP διεύθυνση προορισμού
- Τη UDP source port
- Τη Home agent address
- Το πεδίο Identification
- Την τιμή του Lifetime πεδίου
- Το υπολειπόμενο χρονικό διάστημα της εκκρεμούσας ή της παρούσας εγγραφής .

Ο foreign agent, συνήθως, ρυθμίζεται έτσι ώστε να περιορίζει τον αριθμό των εγγραφών που εκκρεμούν και παρακολουθεί τις πρώτες 5 .Οι επόμενες , πιθανές , αιτήσεις απορρίπτονται επιστρέφοντας στον κινητό κόμβο των κωδικό 66 .

Για την αποφυγή συμφόρησης , ο foreign agent έχει την δυνατότητα να διαγράψει οποιαδήποτε αίτηση εγγραφής η οποία παραμένει σε αυτή την κατάσταση για περισσότερο από 7 δευτερόλεπτα , επιστρέφοντας στον απορριπτόμενο κινητό κόμβο τον κωδικό 78 (Registration timeout).

Όπως και με κάθε κόμβο στο διαδίκτυο , ο foreign agent μπορεί να μοιράζεται κάποια mobility security association . Όταν αναμεταδίδει ένα registration request message από ένα κινητό κόμβο σε ένα home agent , και έχει κοινά mobility security associations με τον home agent πρέπει να προσθέσει μια Foreign-Home Authentication Extension στην αίτηση και πρέπει να ελέγξει το registration reply message για την ύπαρξη της συγκεκριμένης επέκτασης . Ανάλογα , στην περίπτωση του κοινού mobility security association με τον κινητό κόμβο. όταν λαμβάνει κάποιο registration request message πρέπει να ελέγξει για την ύπαρξη της Mobile-Foreign Authentication Extension την οποία έχει προσθέσει στο registration reply message .

3.7. Λήψη Registration Request messages

Στην περίπτωση που ο foreign agent δεχτεί ένα registration request message από ένα κινητό κόμβο , ελέγχει ότι η διεύθυνση του home agent δεν ανήκει σε κάποιο από τα υποδίκτυα που εξυπηρετεί . Όταν ο έλεγχος δείξει ότι αυτό δεν ισχύει , ο foreign agent αναμεταδίδει το μήνυμα στον υποδεικνυόμενο home agent . Αντίθετα , εάν ο έλεγχος δώσει θετικά αποτελέσματα , υπάρχουν δυο δυνατότητες , δηλαδή να δεχτεί ή να απορρίψει την αίτηση . Η πρώτη περίπτωση έχει ως αποτέλεσμα την εγγραφή και την προώθηση των μηνυμάτων του κινητού κόμβου . Η δεύτερη περίπτωση , όμως , παρουσιάζει αρκετές ιδιομορφίες και θα την εξετάσουμε περισσότερο .

Η πρώτη ενέργεια του foreign agent είναι να στείλει ένα registration request message στον κινητό κόμβο με τον κατάλληλο κωδικό εξηγώντας το λόγο απόρριψης της αίτησης . Εφόσον ο κινητός κόμβος συνεχίζει να στέλνει μηνύματα, ο foreign agent τα καταγράφει και συμπληρώνει τη λίστα που διατηρεί (για αυτόν) με τα νέα στοιχεία . Τα αρχικά στοιχεία που αφορούν το συγκεκριμένο κινητό κόμβο δεν διαγράφονται ούτε μεταβάλλονται έως ότου ο foreign agent λάβει ένα registration reply message που να υποδηλώνει ότι πραγματοποιήθηκε η έγγραφη .

Ειδικότερα, προκύπτουν οι παρακάτω περιπτώσεις:

i. Προώθηση Έγκυρων Registration requests

Εφόσον η αίτηση γίνει αποδεκτή από τον foreign agent την αναμεταδίδει στον home agent . Δεν πρέπει , όμως , να μεταβάλλει κανένα από τα πεδία που βρίσκονται στο μήνυμα καθώς στην αντίθετη περίπτωση είναι πολύ πιθανό ότι θα υπάρξει πρόβλημα στην πιστοποίηση του μηνύματος από τον home agent .

Στις αρμοδιότητες του foreign agent είναι ακόμη η επεξεργασία και η αφαίρεση των επεκτάσεων που ακολουθούν τη Mobile-Home authentication extension .

Στο μήνυμα το οποίο αναμεταδίδει ο foreign agent πρέπει να διαμορφώσει τα παρακάτω πεδία ως εξής:

IP πεδία:

IP Source address: Πρέπει να περιέχει τη διεύθυνση του foreign agent στο υποδίκτυο στο οποίο ανήκει.

IP Destination address: Πρέπει να περιέχει τη διεύθυνση του home agent όπως αυτή εμφανίζεται στο home agent πεδίο του registration request message.

UDP πεδία:

UDP Source port: Μεταβλητή
UDP Destination port: 434

Μετά την προώθηση του registration request message ο foreign agent αρχίζει να χρονομετρά το υπολειπόμενο της εκκρεμούσας αίτησης . Εάν το διάστημα αυτό παρέλθει χωρίς να λάβει έγκυρη απάντηση διαγράφει τον κινητό κόμβο από τη λίστα που διατηρεί .

ii. Απόρριψη Μη-Έγκυρων Registration Requests

Στην περίπτωση που ο foreign agent αρνηθεί το registration request message που έλαβε από ένα κινητό κόμβο , για οποιοδήποτε λόγο θα πρέπει να τον ενημερώσει με την αποστολή registration reply message

το οποίο θα περιέχει και τον κατάλληλο κωδικό . Στο ενδεχόμενο αυτό , τα πεδία Home address , Home agent και Identification του registration reply message αντιγράφονται από το registration request message .

Στο μήνυμα το οποίο αναμεταδίδει ο foreign agent πρέπει να διαμορφώσει τα παρακάτω πεδία ως εξής:

IP πεδία:

IP Source address: Στο πεδίο αυτό αντιγράφεται ότι υπάρχει στο IP Destination address του registration request message.

IP Destination address: Στο πεδίο αυτό αντιγράφεται ότι υπάρχει στο IP Source address του registration request message.

UDP πεδία:

UDP Source port: 434

UDP Destination port: Στο πεδίο αυτό αντιγράφεται ότι υπάρχει στο UDP Source port του registration request message.

3.8. Λήψη Registration Replies messages

Όταν ο foreign agent λάβει ένα έγκυρο registration reply message από τον home agent του κινητού κόμβου , ανανεώνει τη διατηρούμενη λίστα με τους επισκεπτόμενους κινητούς κόμβους και στη συνέχεια μεταφέρει το registration reply message σε αυτόν .

Στη συνέχεια, θα παρουσιάσουμε με λεπτομέρειες τις παραπάνω διαδικασίες .

Εφόσον ο foreign agent λάβει ένα registration reply message ψάχνει στη λίστα των επισκεπτόμενων κόμβων για να ελέγξει εάν υπάρχει κάποια εκκρεμούσα αίτηση εγγραφής με την ίδια home address με αυτή που δηλώνεται στο registration reply message . Εάν δεν βρει κάτι τέτοιο τότε η αίτηση αγνοείται με το σκεπτικό ότι ο κινητός κόμβος θα έχει προχωρήσει τη διαδικασία εγγραφής και με κάποιο άλλο foreign agent .

Ένας άλλος τομέας που ελέγχει είναι αυτός της πιστοποίησης . Πιο συγκεκριμένα , στην περίπτωση που μεταξύ home agent και foreign agent υπάρχει ένα mobility security association τότε στο Registration

Reply message πρέπει να υπάρχει μόνο μια Foreign-Home authentication extension. Το πεδίο Authenticator της επέκτασης αυτής είναι και ο βασικός τομέας έλεγχου .

Η ύπαρξη περισσοτέρων ή η ανυπαρξία των συγκεκριμένων επεκτάσεων θα έχει ως αποτέλεσμα το μήνυμα απάντησης θα αγνοηθεί και το γεγονός αυτό θα καταχωρηθεί στο αρχείο του foreign agent ως αστοχία σχετικά με το θέμα της ασφάλειας . Στη συνέχεια θα απορρίψει την αίτηση εγγραφής και θα αποστείλει ένα registration reply message στο πεδίο Code του οποίου θα αναγράφεται το νούμερο 68 .

Στην περίπτωση που το registration reply message πληροί τις παραπάνω προϋποθέσεις , προωθείται προς τον κινητό κόμβο . Ο foreign agent πρέπει επίσης να ενημερώσει τη λίστα των επισκεπτόμενων κόμβων για να απεικονίσει τα αποτελέσματα του αιτήματος εγγραφής του κινητού κόμβου , όπως αυτά υποδεικνύονται από το πεδίο Code του registration reply message . Εάν το πεδίο Code δείχνει ότι ο home agent έχει αποδεχθεί την εγγραφή και το πεδίο Lifetime είναι διαφορετικό από το μηδέν, ο foreign agent θα θέσει το πεδίο Lifetime στη λίστα των επισκεπτόμενων κόμβων στο minimum των ακόλουθων δύο τιμών:

- Της τιμής που προσδιορίζεται στο πεδίο Lifetime του registration reply message και
- Της τιμής που καθορίζει ο foreign agent για το μέγιστο επιτρεπόμενο όριο του πεδίου Lifetime για το οποίο μπορεί να δεχτεί μια αίτηση εγγραφής.

Όπως προαναφέραμε , ο foreign agent δεν πρέπει να τροποποιήσει κανένα από τα πεδία του registration reply message που βρίσκονται στο σταθερό τμήμα του μηνύματος καθώς επίσης και της Mobile-Home Authentication Extension . Σε αντίθετη περίπτωση , είναι πολύ πιθανό να παρατηρηθεί αποτυχία πιστοποίησης της ταυτότητας του κινητού κόμβου. Επιπλέον, ο foreign agent πρέπει να εκτελέσει τις ακόλουθες , επιπρόσθετες , διαδικασίες:

- Να επεξεργαστεί και να αφαιρέσει οποιεσδήποτε επεκτάσεις μετά από την Mobile-Home Authentication Extension

- Εάν θεωρηθεί απαραίτητο , μπορεί να επισυνάψει τις δικές του non-authentication Extensions
- Να επισυνάψει την Mobile-Foreign Authentication Extension, εάν ο foreign agent μοιράζεται μια mobility security association με τον κινητό κόμβο.

Μετά την προώθηση ενός έγκυρου registration reply message στον κινητό κόμβο, ο foreign agent οφείλει να ενημερώσει τη λίστα των επισκεπτόμενων κόμβων για αυτήν την εγγραφή λαμβάνοντας υπόψη τις εξής παραμέτρους . Εάν το registration reply message δείχνει ότι η εγγραφή έγινε αποδεκτή από το home agent , ο foreign agent συγχρονίζει το εικονικό χρονόμετρό , με το οποίο μετρούσε το πεδίο Lifetime της εγγραφής , με αυτό που δηλώνεται στο αντίστοιχο πεδίο του registration reply message .

Σε αντίθεση με το συγχρονισμό του κινητού κόμβου με το registration Lifetime ο foreign agent θεωρεί ότι αυτό το Lifetime αρχίζει όταν διαβιβάζει το registration reply message , εξασφαλίζοντας έτσι ότι ο foreign agent δεν θα ακυρώσει την εγγραφή πριν πράξει κάτι τέτοιο ο κινητός κόμβος .

Στην περίπτωση ,όμως , που το registration reply message δείχνει ότι η εγγραφή απορρίφθηκε από το home agent , ο foreign agent διαγράφει όσα στοιχεία έχει αποθηκεύσει για αυτήν την αποπειραθείσα εγγραφή από τη λίστα των επισκεπτόμενων κόμβων του .

3.9. ΑΠΑΙΤΗΣΕΙΣ ΑΠΟ ΤΟΥΣ HOME AGENTS ΓΙΑ ΤΗ ΔΙΑΔΙΚΑΣΙΑ ΤΟΥ REGISTRATION

Οι home agents διαδραματίζουν ένα καθοριστικό ρόλο στη διαδικασία εγγραφής . Ο home agent λαμβάνει το registration request message από τον κινητό κόμβο (μέσω ενός foreign agent), ενημερώνει το αρχείο με τα mobility bindings που διατηρεί για αυτόν τον κινητό κόμβο, και εκδίδει ένα registration reply message σε απάντηση για κάθε registration request message που λαμβάνει.

Ένας home agent δεν στέλνει registration reply messages πάρα μόνο για να απαντήσει σε ένα registration request message που λαμβάνει ενώ , σε καμία περίπτωση , δεν πρέπει να παραγάγει ένα registration request message για να δείξει ότι το χρονικό διάστημα που υποδηλώνεται στο πεδίο Lifetime έχει παρέλθει .

3.10. ΕΙΔΙΚΕΣ ΡΥΘΜΙΣΕΙΣ ΣΤΑ ΠΕΔΙΑ ΕΓΓΡΑΦΩΝ

Γνωρίζουμε ότι κάθε home agent έχει μια IP διεύθυνση και το prefix size για το home network. Πρέπει , ακόμη , να διαμορφωθεί με την mobility security association κάθε εξουσιοδοτημένου κινητού κόμβου τον οποίο εξυπηρετεί ως home agent.

Όταν ο home agent αποδέχεται ένα έγκυρο Registration Request από έναν κινητό κόμβο τον οποίο και εξυπηρετεί τότε πρέπει να δημιουργήσει ή να τροποποιήσει την είσοδο για αυτόν τον κινητό κόμβο στη mobility binding list που διατηρεί και η οποία θα περιέχει:

- Την ***Home Address*** του κινητού κόμβου
- Την ***care-of address*** του κινητού κόμβου
- Το πεδίο ***Identification*** από το Registration Reply message
- Την τιμή του πεδίου ***Lifetime*** που δίνει το υπολειπόμενο χρονικό διάστημα της διάρκειας ζωής της εγγραφής

Ο home agent προσφέρει , προαιρετικά , την ικανότητα να συνδέσει δυναμικά μια Home Address με έναν κινητό κόμβο μετά τη λήψη ενός Registration Request από εκείνο τον κινητό κόμβο.

Ο home agent διατηρεί επίσης τα mobility binding list με τους διάφορους foreign agents . Κατά τη λήψη ενός Registration Request message από ένα foreign agent και εφόσον ο home agent μοιράζεται ένα mobility security association με αυτόν , ο home agent πρέπει να ενσωματώσει το πεδίο Authenticator στην απαραίτητη Foreign-Home Authentication Extension που περιέχεται στο μήνυμα , το οποίο θα βασίζεται σε αυτό το mobility security association.

Ομοίως, κατά την αποστολή ενός Registration Reply message σε έναν foreign agent (εάν ο home agent μοιράζεται ένα mobility binding με αυτόν) ο home agent πρέπει να συμπεριλάβει μια Foreign-Home Authentication Extension στο μήνυμα (η οποία θα βασίζεται σε αυτό το mobility security association).

3.11. ΛΗΨΗ REGISTRATION REQUEST MESSAGES

Εάν ο home agent αποδέχεται ένα εισερχόμενο Registration Request message , οφείλει να ενημερώσει το mobility binding αρχείο που διατηρεί με τα στοιχεία των κινητών κόμβων και να αποστείλει ένα Registration Reply message με έναν κατάλληλο κώδικα . Στην αντίθετη περίπτωση (όπου ο home agent αρνείται το Registration Request message) , οφείλει να στείλει ένα Registration Reply message με έναν κατάλληλο κώδικα , στο πεδίο Code , που θα προσδιορίζει το λόγο για τον οποίο το αίτημα απορρίφθηκε .

i. Έλεγχοι εγκυρότητας των Registration Request messages

Το πρώτο σημείο ελέγχου του Registration Request message εστιάζεται στον έλεγχο του UDP checksum καθώς στην περίπτωση που βρεθεί ότι η τιμή του είναι μη μηδενική πρέπει να απορριφθεί από τον home agent .

Το επόμενο σημείο ελέγχου του Registration Request message εστιάζεται στον έλεγχο πιστοποίησης της ταυτότητας του. Η διαδικασία αυτή περιλαμβάνει τα ακόλουθα στάδια:

α) Ο home agent ελέγχει για την παρουσία μιας authorization-enabling extension ,ώστε να εκτελέσει την υποδεδειγμένη πιστοποίηση ταυτότητας.

Μόνο μια authorization-enabling extension πρέπει να είναι παρούσα στο Registration Request message και ο home agent ελέγχει την τιμή του πεδίου Authenticator στην επέκταση ή το ότι η τιμή του authenticator έχει ελεγχθεί από έναν άλλο agent με τον οποίο έχει μια σχεση ασφάλειας. Ο home agent απορρίπτει την εγγραφή του κινητού κόμβου και στέλνει ένα Registration Reply message στον κινητό κόμβο με τον κωδικό 131

- Εάν δεν βρίσκεται η παραπάνω επέκταση στο Registration Request message
- Εάν υπάρχει περισσότερες από μια φορές,
- Εάν το πεδίο Authenticator είναι άκυρο.

Στις παραπάνω περιπτώσεις το αίτημα απορρίπτεται και το σφάλμα καταγράφεται ως εξαίρεση ασφάλειας.

β) Ο home agent ελέγχει ότι το πεδίο Identification του Registration Request message είναι σωστό χρησιμοποιώντας το πλαίσιο που επιλέγεται από το SPI μέσα στην authorization-enabling extension. Η συγκεκριμένη διαδικασία θα περιγραφεί αναλυτικά στο Κεφάλαιο 6 όπου θα παρουσιάσουμε τα ζητήματα ασφαλείας που ανακύπτουν . Εάν η παραπάνω προϋπόθεση δεν ισχύει , ο home agent απορρίπτει το αίτημα και στέλνει ένα Registration Reply message στον κινητό κόμβο με τον κωδικό 133,το οποίο συμπεριλαμβάνει το Identification πεδίο. Ο home agent δεν εκτελεί καμία περαιτέρω επεξεργασία με ένα τέτοιο αίτημα, ενώ , και σε αυτή την περίπτωση , το αίτημα απορρίπτεται και το σφάλμα καταγράφεται ως εξαίρεση ασφάλειας.

γ) Εάν ο home agent μοιράζεται μια mobility security association με τον foreign agent, πρέπει να ελέγξει για την παρουσία μιας έγκυρης επέκτασης Foreign-Home Authentication Extension. Και σε αυτήν την περίπτωση , ακριβώς μια τέτοια επέκταση πρέπει να είναι παρούσα στο Registration Request message και ο home agent ελέγχει την τιμή του πεδίου Authenticator στην επέκταση. Ο home agent απορρίπτει την εγγραφή του κινητού κόμβου και στέλνει ένα Registration Reply message στον κινητό κόμβο με τον κωδικό 132

- Εάν δεν βρίσκεται καμία Foreign-Home Authentication Extension,
- Εάν υπάρχει περισσότερες από μια φορές,
- Εάν το πεδίο Authenticator είναι άκυρο.

Όπως και στην προηγούμενη διαδικασία ,το αίτημα απορρίπτεται από τον home agent και το σφάλμα καταγράφεται ως εξαίρεση ασφάλειας.

Εκτός από τον έλεγχο της πιστοποίησης ταυτότητας του Registration Request message, οι home agents πρέπει να ελέγχουν εάν τα εν λόγω μηνύματα στέλνονται προς την subnet-directed broadcast address του home network (ενώ θα έπρεπε να προωθούνται ως unicast προς το home agent).

Στη συγκεκριμένη περίπτωση ο home agent απορρίπτει το αίτημα και επιστρέφει ένα Registration Reply message με τον κωδικό 136. Το μήνυμα περιέχει τη διεύθυνση του unicast home agent, έτσι ώστε ο κινητός κόμβος να μπορεί να επανεκδώσει το Registration Request message με τη σωστή διεύθυνση των home agents.

Θα πρέπει να αναφέρουμε ότι μερικοί δρομολογητές αλλάζουν τη διεύθυνση προορισμού IP ενός διαγράμματος δεδομένων από μια subnet-directed broadcast address σε 255.255.255.255 πριν την προωθήσουν στο υποδίκτυο προορισμού. Σε αυτήν την περίπτωση, οι home agents που προσπαθούν να ανακτήσουν dynamic home agent discovery requests

δεν θα μπορούν να δουν τέτοια πακέτα .Κατά την ρύθμιση των υπολογιστών που προορίζονται να δράσουν ως home agents πρέπει να προετοιμαστούν τόσο για τη subnet-directed broadcast address όσο και για τη 255.255.255.255 address εάν επιθυμούν να υποστηρίζουν τη dynamic home agent discovery (δυναμική ανακάλυψη βασικών πρακτόρων).

ii. Αποδοχή Έγκυρων Registration Request messages

Εάν το Registration Request message ικανοποιεί τους ελέγχους που περιγράψαμε στην παραπάνω παράγραφο και ο home agent είναι σε θέση να χειριστεί το αίτημα κάνοντας τις απαραίτητες αλλαγές τότε πρέπει να ενημερώσει τον mobility binding κατάλογο του (σε ότι αφορά τα στοιχεία για τον αιτούμενο κινητό κόμβο) και να επιστρέψει ένα Registration Reply message σε αυτόν . Σε αυτήν την περίπτωση, ο κώδικας απάντησης θα είναι είτε **0** (εάν ο home agent υποστηρίζει ταυτόχρονα mobility bindings) είτε **1** σε διαφορετική περίπτωση.

Ο home agent ενημερώνει το αρχείο όπου καταγράφει τα mobility bindings του κινητού κόμβου που εξυπηρετεί βασιζόμενος στα πεδία του Registration Request message ως εξής:

-- Εάν η τιμή του πεδίου Lifetime έχει την τιμή 0 και η care-of address που αναγράφεται στο αντίστοιχο πεδίο είναι ίδια με τη home address του κινητού κόμβου τότε ο home agent διαγράφει όλα τα στοιχεία που είχε αποθηκεύσει στο mobility binding κατάλογο και αφορούσαν τον αιτούμενο κινητό κόμβο. Τα παραπάνω ερμηνεύονται , από τον home agent , ως αίτηση του κινητού κόμβου για το σταμάτημα παροχής υπηρεσιών σε αυτόν .

-- Εάν η τιμή του πεδίου Lifetime έχει την τιμή 0 και η care-of address που αναγράφεται στο αντίστοιχο πεδίο δεν είναι ίδια με τη home address του κινητού κόμβου τότε ο home agent διαγράφει μόνο τη συγκεκριμένη διεύθυνση , από το mobility binding κατάλογο που είχε αποθηκεύσει για τον αιτούμενο κινητό κόμβο. Οποιεσδήποτε άλλες ενεργές καταχωρήσεις που περιέχουν άλλη care-of address θα παραμείνουν ενεργές.

-- Εάν η τιμή του πεδίου Lifetime δεν έχει την τιμή 0 ο home agent προσθέτει την care-of address που δηλώνεται από το Registration Request message στο mobility binding κατάλογο που είχε αποθηκεύσει για τον αιτούμενο κινητό κόμβο.

Εφόσον το bit **S** έχει την τιμή 1 και ο home agent υποστηρίζει ταυτόχρονους συσχετισμούς κινητικότητας οι προηγούμενες δεσμευτικές καταχωρήσεις κινητικότητας διατηρούνται, διαφορετικά ο home agent αφαιρεί όλες τις προηγούμενες καταχωρήσεις στο δεσμευτικό κατάλογο κινητικότητας για τον κινητό κόμβο.

Σε όλες τις περιπτώσεις, ο home agent είναι υποχρεωμένος να στείλει ένα Registration Reply message στη διεύθυνση από την οποία προήλθε το Registration Request message (η οποία μπορεί να ανήκει σε ένα διαφορετικό foreign agent από αυτόν του οποίου η care-of address εγγράφεται) .

Εάν ο home agent μοιράζεται μια mobility security association με τον foreign agent του οποίου η care-of address επανεγγράφεται και , ο συγκεκριμένος foreign agent είναι διαφορετικός από αυτόν που αναμετέδωσε το Registration Request message, τότε ο home agent στέλνει επιπροσθέτως ένα Registration Reply message σε αυτόν . Ο home agent δεν πρέπει να στείλει μια τέτοια απάντηση εάν δεν μοιράζεται κάποια mobility security association με το συγκεκριμένο foreign agent. Στην περίπτωση που δεν σταλθεί καμία απάντηση, ο κατάλογος επισκεπτών του foreign agent θα λήξει όταν παρέλθει το χρονικό διάστημα που δηλώνεται στο πεδίο Lifetime.

Ο home agent δεν πρέπει να αυξήσει την τιμή του χρονικού διαστήματος που δηλώνεται στο πεδίο Lifetime από αυτήν που προσδιορίζεται από τον κινητό κόμβο στο Registration Reply message. Εντούτοις, δεν είναι σφάλμα για τον κινητό κόμβο να ζητήσει ένα Lifetime πιο μακροχρόνιο από αυτό που ο βασικός πράκτορας είναι διατεθειμένος να αποδεχθεί. Σε αυτήν την περίπτωση, ο home agent απλά μειώνει το πεδίο Lifetime σε μια αποδεκτή τιμή και την επιστρέφει μέσω του Registration Reply message. Η παραπάνω τιμή ενημερώνει τον κινητό κόμβο για το χρονικό διάστημα για το οποίο ισχύει η εγγραφή του με αυτόν και πριν το τέλος του οποίου θα πρέπει να την έχει ανανεώσει. Μετά από το τέλος αυτού του χρονικού διαστήματος, ο home agent διαγράφει τα στοιχεία της εγγραφής από τον mobility binding κατάλογο του.

Εάν ληφθεί ένα αίτημα εγγραφής το οποίο είναι όμοιο με ένα αντίστοιχο μήνυμα , το οποίο έχει γίνει αποδεκτό , η νέα τιμή του πεδίου Lifetime δεν θα πρέπει να είναι μεγαλύτερη από την τιμή που είχε οριστεί αρχικά . Σημειώνουμε ότι το μήνυμα θεωρείται όμοιο όταν οι τιμές των πεδίων home address,care-of address και lifetime είναι ίδιες .

iii. Απόρριψη Μη Έγκυρων Registration Request messages

Εάν το Registration Request message δεν ικανοποιεί τους ελέγχους που περιγράψαμε στην παράγραφο 3.9.3 ή ο home agent δεν είναι σε θέση να χειριστεί το αίτημα κάνοντας τις απαραίτητες αλλαγές τότε ο πρέπει να σταλεί ένα Registration Reply message στον κινητό κόμβο με έναν κώδικα που δείχνει το λόγο για το σφάλμα.

Εάν στην αναμετάδοση του αιτήματος συμμετείχε ένας foreign agent, αυτό του επιτρέπει να διαγράψει την εκκρεμούσα είσοδο στη λίστα των επισκεπτόμενων κόμβων που διατηρεί. Επίσης, αυτό ενημερώνει τον κινητό κόμβο να καθορίσει το λόγο που οδήγησε στο σφάλμα έτσι ώστε να προσπαθήσει να το διορθώσει και να εκδώσει ένα άλλο αίτημα.

Σε αυτή την ενότητα θα αναφέρουμε τους βασικότερους λόγους που μπορεί να οδηγήσουν στην απόρριψη του Registration Request message αναφέροντας και την τιμή που παίρνει το πεδίο Code για κάθε έναν από αυτούς. Περισσότερες πληροφορίες για τον τρόπο σύνταξης των Registration Reply messages θα παραθέσουμε στην παρακάτω ενότητα .

Οι περισσότεροι λόγοι για την απόρριψη μιας αίτησης εγγραφής είναι διαχειριστικής φύσης. Παραδείγματος χάριν, ένας home agent μπορεί να περιορίσει τον αριθμό ταυτόχρονων εγγραφών για έναν κινητό κόμβο, με την απόρριψη οποιωνδήποτε εγγραφών που θα τον ανάγκαζαν να υπερβεί το όριό του.

- Στην περίπτωση αυτή το Registration Reply message στο πεδίο Code θα έχει την τιμή **135**.

Ομοίως, ένας home agent μπορεί να αρνηθεί την παροχή υπηρεσιών στους κινητούς κόμβους που έχουν εισέλθει σε περιοχές τις οποίες , θεωρητικά , δεν καλύπτει .

- Στην περίπτωση αυτή το Registration Reply message στο πεδίο Code θα έχει την τιμή **129**.

Τα αιτήματα με μη μηδενικές τιμές σε δεσμευμένα πεδία απορρίπτονται με την αιτιολογία poorly formed request.

- Στην περίπτωση αυτή το Registration Reply message στο πεδίο Code θα έχει την τιμή **134.**

3.12. ΑΠΟΣΤΟΛΗ REGISTRATION REPLY MESSAGES

Εφόσον ο home agent αποδέχεται ένα Registration Request message πρέπει , στη συνέχεια , να ενημερώσει το αρχείο στο οποίο αποθηκεύει τα mobility bindings του κινητού κόμβου και να στείλει ένα Registration Reply message με έναν κατάλληλο κώδικα.

Στην αντίθετη περίπτωση (όπου ο home agent έχει αρνηθεί το αίτημα) πρέπει να στείλει ένα Registration Reply message με έναν κατάλληλο κώδικα με έναν κατάλληλο κώδικα που προσδιορίζει το λόγο για τον οποίο το αίτημα απορρίφθηκε.

Στις ακόλουθες ενότητες θα παραθέσουμε με λεπτομέρειες τις τιμές που πρέπει να παρέχει ο home agent στα πεδία των Registration Reply messages.

i. IP/UDP πεδία

Στην ενότητα αυτή θα αναλύσουμε τους συγκεκριμένους κανόνες σύμφωνα με τους οποίους οι κινητοί κόμβοι επιλέγουν τιμές για τα IP και UDP πεδία στα Registration Reply messages.

- **IP Source Address:**

  Αντιγράφεται από το πεδίο IP Destination Address του Registration Request message εκτός εάν χρησιμοποιήθηκε multicast ή broadcast διεύθυνση όποτε τίθεται η τιμή που αναγράφεται στο πεδίο IP Source Address του Registration Reply message.

- **IP Destination Address:**

  Αντιγράφεται από την IP Source Address του Registration Request message.

- **UDP Source Port:**

  Αντιγράφεται από το πεδίο UDP Destination Port του Registration Request message.

- **UDP Destination Port:**

  Αντιγράφεται από το πεδίο UDP Source Port του Registration Request message.

Κατά την αποστολή του Registration Reply message σε απάντηση ενός Registration Request message που ζήτησε τη διαγραφή του κινητού κόμβου (το πεδίο Lifetime είναι μηδέν και η care-of address είναι ίση με τη home address του κινητού κόμβου) και στο οποίο η IP Source Address έχει τη home address του κινητού κόμβου (αυτό είναι η κανονική μέθοδος που χρησιμοποιείται από έναν κινητό κόμβο για να επανεγγραγραφεί στο βασικό δίκτυό του ,όταν επιστρέφει σε αυτό), η IP Destination Address του Registration Reply message θα πάρει την home address του κινητού κόμβου, όπως αυτή αντιγράφεται από την IP Source Address του Registration Request message.

Σε αυτήν την περίπτωση ο home agent πρέπει να διαβιβάσει την απάντηση του Registration Reply message στο home network όπως στην περίπτωση που ο κινητός κόμβος ήταν σε αυτό, παρακάμπτοντας οποιοδήποτε είσοδο που υπάρχει στο mobility binding κατάλογο που μπορεί ακόμα να υπάρξει στον home agent για τον κινητό κόμβο προορισμού.
Ειδικότερα, για ένα κινητό κόμβο που επιστρέφει στο home network, αφού έχει καταχωρηθεί με μια care-of address, εάν το νέο Registration Request message του δεν γίνει αποδεκτό από τον home agent, ο mobility binding κατάλογος για τον κινητό κόμβο θα δείχνει ότι τα διαγράμματα δεδομένων που απευθύνονται στον κινητό κόμβο πρέπει να προωθηθούν στην, εγγεγραμμένη, care-of address του κινητού κόμβου. Ωστόσο κατά την αποστολή του Registration Reply message, και εφόσον αυτό έχει απορριφθεί , ο συγκεκριμένος κατάλογος πρέπει να αγνοηθεί και ο home agent πρέπει να το προωθήσει ωσάν αυτός να βρισκόταν στο home network .

ii. Πεδία του Registration Reply message

Σε αυτό το τμήμα θα αναλύσουμε τους συγκεκριμένους κανόνες μέσα από τους οποίους οι home agent επιλέγουν τις τιμές για τα πεδία μέσα στη σταθερό τμήμα του Registration Reply message.

Το πεδίο **Code** του Registration Reply message επιλέγεται σύμφωνα με τους κανόνες που προσδιορίσαμε στις προηγούμενες ενότητες. Κατά την απάντηση σε ένα ,αποδεκτό, αίτημα εγγραφής, ο home agent πρέπει να θέσει την τιμή 1 εάν δεν υποστηρίζει τις ταυτόχρονες εγγραφές.

Το πεδίο **Lifetime** πρέπει να αντιγραφεί από το αντίστοιχο πεδίο του Registration Request message, εκτός αν η ζητούμενη τιμή είναι μεγαλύτερη από το μέγιστο χρονικό διάστημα για το οποίο ο home agent είναι πρόθυμος να παρέχει την απαιτούμενη υπηρεσία. Σε αυτή την περίπτωση, η διάρκεια ζωής τίθεται στο χρονικό διάστημα για το οποίο η υπηρεσία θα παρασχεθεί πραγματικά από το home agent. Αυτό το μειωμένο Lifetime είναι η μέγιστη διάρκεια ζωής που επιτρέπεται από το home agent (για αυτόν τον κινητό κόμβο και τη δεδομένη care-of address του).

Εάν το πεδίο **Home Address** του Registration Request message είναι διαφορετικό από το μηδέν, πρέπει να αντιγραφεί στο πεδίο Home Address του παραπάνω μηνύματος. Διαφορετικά, εάν το συγκεκριμένο πεδίο του αιτήματος εγγραφής είναι μηδέν, ο home agent πρέπει να μεριμνήσει για την επιλογή μιας Home Address για τον κινητό κόμβο, και να τοποθετήσει την επιλεγμένη διεύθυνση στο Home Address πεδίο του μηνύματος Registration Reply message.

Εάν το πεδίο **Home Agent** στο Registration Request message περιέχει μια διεύθυνση unicast αυτού του home agent, αυτό το πεδίο πρέπει να αντιγραφεί στο home agent πεδίο του Registration Reply message. Διαφορετικά, ο home agent πρέπει να θέσει το συγκεκριμένο πεδίο της απάντησης εγγραφής στη unicast διεύθυνση του. Σε αυτήν την τελευταία περίπτωση, ο home agent πρέπει να απορρίψει την εγγραφή με έναν κατάλληλο κώδικα (π.χ., **136**) για να αποτρέψει τον κινητό κόμβο από μια ενδεχόμενη ταυτόχρονη καταχώρηση με δύο ή περισσότερους home agents.

iii. Επεκτάσεις

Αυτό το τμήμα περιγράφει τη δομή των απαραίτητων και των προαιρετικών επεκτάσεων του Mobile IP τις οποίες ένας home agent επισυνάπτει στο Registration Reply message.

Η δομή που πρέπει να ακολουθηθεί είναι η ακόλουθη:

α) Η IP header, ακολουθούμενη από την UDP header, ακολουθούμενη από το fixed-length τμήμα του Registration Reply message,

β) Εάν είναι παρούσες, κάθε non-authentication Extensions που χρησιμοποιούνται από τον κινητό κόμβο (που μπορούν προαιρετικά να χρησιμοποιηθούν από τον foreign agent),

γ) Η Mobile-Home Authentication Extension επέκταση,

δ) Εάν είναι παρούσες, οποιεσδήποτε non-authentication Extensions επεκτάσεις που χρησιμοποιούνται μόνο από τον foreign agent, και

ε) Εάν είναι παρούσα ,κάθε Foreign-Home Authentication Extension.

Σημειώστε ότι οι επεκτάσεις (α) και (γ) πρέπει να εμφανιστούν σε κάθε Registration Reply message που στέλνεται από τον home agent, ενώ οι επεκτάσεις (β), (δ), και (ε) είναι προαιρετικές. Εντούτοις, η επέκταση (ε) πρέπει να περιληφθεί όταν ο home agent και ο foreign agent μοιράζονται μια mobility security association.

ΚΕΦΑΛΑΙΟ 4

ΔΙΑΔΙΚΑΣΙΑ
Tunneling

4.1. ΕΙΣΑΓΩΓΗ

Σε αυτό το κεφάλαιο θα περιγράψουμε πώς οι κινητοί κόμβοι, οι home agents, και (ενδεχομένως) οι foreign agents συνεργάζονται για να προωθήσουν τα datagrams προς και από τους κινητούς κόμβους που συνδέονται με ένα foreign network. Ο κινητός κόμβος αρχικά ενημερώνει το home agent του για την παρούσα θέση του και στη συνέχεια, χρησιμοποιώντας τη διαδικασία εγγραφής, που περιγράφεται στο Κεφάλαιο 3 και (εφόσον αυτή πραγματοποιηθεί) ξεκινούν και το τελικό στάδιο του πρωτοκόλλου, το οποίο και θα εξετάσουμε .

Η προώθηση των πακέτων πραγματοποιείται με την εφαρμογή των εξής μεθόδων:

- ***IP within IP encapsulation***
- ***Minimal encapsulation***
- ***GRE encapsulation (Generic Routing Encapsulation)***

Τόσο οι home agents όσο και οι foreign agents πρέπει να υποστηρίζουν την προώθηση των πακέτων δεδομένων χρησιμοποιώντας τη μέθοδο IP in IP encapsulation, ενώ η παραπάνω απαίτηση ισχύει και για την περίπτωση όπου οποιοσδήποτε κινητός κόμβος χρησιμοποιεί co-located care-of address.

Η Minimal encapsulation και η GRE encapsulation είναι εναλλακτικές μέθοδοι encapsulation που μπορούν να χρησιμοποιηθούν προαιρετικά από τους home agents \ foreign agents και τους κινητούς κόμβους. Η χρήση κάποιας εκ αυτών των εναλλακτικών μορφών καθίσταται επιτακτική όταν ζητείται από τον κινητό κόμβο, ενώ ειδάλλως βρίσκεται στην κρίση των home agents.

Τόσο οι προαναφερόμενες μέθοδοι όσο και οι απαιτήσεις που πρέπει να πληρούνται από τους κινητούς κόμβους αλλά και από τους home agents \ foreign agents, παρουσιάζονται στις παρακάτω ενότητες .

4.2. ΑΠΑΙΤΗΣΕΙΣ ΔΟΜΙΚΩΝ ΣΤΟΙΧΕΙΩΝ ΤΟΥ MOBILE IP ΓΙΑ ΤΗ ΔΙΑΔΙΚΑΣΙΑ ΤΟΥ TUNNELLING

Στις ενότητες που ακολουθούν θα εξετάσουμε τις , ιδιαίτερες , προϋποθέσεις που πρέπει να πληρούνται από τους υπολογιστές που προορίζονται να καλύψουν τις ανάγκες του πρωτοκόλλου για την προώθηση των πακέτων δεδομένων στο χρήστη.

i. Απαιτήσεις από τους κινητούς κόμβους για το Tunneling

Όταν συνδέεται με το home network του ο κινητός κόμβος λειτουργεί χωρίς την υποστήριξη των υπηρεσιών κινητικότητας με τον ίδιο τρόπο δηλαδή όπως οποιοσδήποτε σταθερός υπολογιστής ή δρομολογητής. Η ανάλυση της μεθόδου με την οποία ένας κινητός κόμβος επιλέγει έναν προκαθορισμένο δρομολογητή όταν συνδέεται με το home network του, ή όταν βρίσκεται εκτός αυτού και χρησιμοποιεί co-located care-of address, έχει ήδη αναλυθεί και δεν παρουσιάζεται στην παρούσα εργασία, απλά υπενθυμίζουμε ότι τα ICMP Router advertisement messages βρίσκουν εφαρμογή και σε αυτό το πεδίο .

Όταν εγγράφεται σε ένα foreign network, ο κινητός κόμβος επιλέγει τον default δρομολογητή που θα τον εξυπηρετεί με βάση τους ακόλουθους κανόνες:

- Εάν ο κινητός κόμβος εγγράφεται χρησιμοποιώντας μια foreign agent care-of address, χρησιμοποιεί τον foreign agent του ως τον default δρομολογητή του. Η MAC διεύθυνση του συγκεκριμένου agent μπορεί να βρεθεί από τα Agent Advertisement messages διαφορετικά ο κινητός κόμβος πρέπει να επιλέξει τον default δρομολογητή του μεταξύ αυτών που δηλώνουν τη διαθεσιμότητα τους μεσώ των ICMP Agent Advertisement messages που λαμβάνει (και έχουν την prefix διεύθυνση του υποδικτύου στο οποίο βρίσκεται) .

- Εάν ο κινητός κόμβος εγγράφεται άμεσα με το home agent του χρησιμοποιώντας co-located care-of address πρέπει να επιλέξει τον default δρομολογητή του μεταξύ αυτών που δηλώνουν τη διαθεσιμότητα τους σε οποιοδήποτε από τα ICMP Agent

Advertisement messages που λαμβάνει και για τα οποία η care-of address και Router Address , που υπάρχει στο αντίστοιχο πεδίο , ταιριάζουν (με την έννοια ότι βρίσκονται στο ίδιο υποδίκτυο). Στην περίπτωση που η care-of address του κινητού κόμβου ταιριάζει με την IP διεύθυνση προέλευσης του Agent Advertisement message τότε ο κινητός κόμβος θεωρεί εκείνη την διεύθυνση προέλευσης IP ως μια άλλη πιθανή επιλογή για το ρόλο του default δρομολογητή του . Το network prefix μπορεί να ληφθεί από την Prefix-Length Extension του ICMP Agent Advertisement μηνύματος.

ii. Απαιτήσεις από τους Foreign agents για το Tunneling

Κατά την παραλαβή ενός encapsulated διαγράμματος δεδομένων που στέλνεται προς μια care-of address, ένας foreign agent πρέπει να συγκρίνει την διεύθυνση προορισμού που αναγράφεται εσωτερικά με τις καταχωρήσεις που έχει αποθηκεύσει στον κατάλογο επισκεπτών του. Όταν ο προορισμός δεν ταιριάζει με τη διεύθυνση οποιουδήποτε κινητού κόμβου στον κατάλογο επισκεπτών του τότε ο foreign agent δεν πρέπει να διαβιβάσει το datagram χωρίς τροποποιήσεις στην αρχική επικεφαλίδα IP (διαφορετικά είναι πιθανό να δημιουργηθεί ένας βρόχος δρομολόγησης (routing loop) όποτε το διάγραμμα δεδομένων πρέπει να απορριφθεί). Το ICMP Destination Unreachable message δεν πρέπει να σταλεί όταν ένας foreign agent αδυνατεί να διαβιβάσει ένα εισερχόμενο διάγραμμα δεδομένων καθώς , σε αντίθετη περίπτωση , ο foreign agent διαβιβάζει το διάγραμμα δεδομένων στον κινητό κόμβο.

Ο foreign agent δεν πρέπει ακόμη να στέλνει ICMP Agent Advertisement messages που να δηλώνουν την ύπαρξη κάποιου κινητού δρομολογητή σε άλλους δρομολογητές που βρίσκονται στο ίδιο domain με αυτόν ή σε οποιοδήποτε κινητό κόμβο που βρίσκεται στον κατάλογο επισκεπτών του.

Πρέπει , επίσης , να καθοδηγήσει τα διαγράμματα δεδομένων που λαμβάνει από τους καταχωρημένους κινητούς κόμβους. Αυτό σημαίνει ότι ο foreign agent θα πρέπει ,τουλάχιστον, να ελέγξει το IP Header Checksum, τη μείωση του IP Time To Live πεδίου , να κάνει τις απαραίτητες αλλαγές στο IP Header Checksum, και να διαβιβάσει τα διαγράμματα δεδομένων στο default δρομολογητή.

Κάθε foreign agent πρέπει να υποστηρίζει τις βασικές λειτουργίες του Reverse Tunneling το οποίο θα παρουσιάσουμε στη συνέχεια .

iii. Απαιτήσεις από τους Home agents για το Tunneling

Ο home agent πρέπει να είναι σε θέση να αναχαιτίσει οποιαδήποτε διαγράμματα δεδομένων στο home network που απευθύνονται στον κινητό κόμβο ενώ αυτός έχει εγγραφεί σε κάποιο foreign network.

Ο home agent πρέπει , ακόμα , να εξετάσει το πεδίο IP Destination Address όλων των διαγραμμάτων δεδομένων που αναχαιτίζει για να δει εάν είναι ίσο με τη home address οποιουδήποτε από τους κινητούς κόμβους του που έχουν εγγραφεί σε κάποιο foreign network. Σε αυτή την περίπτωση προωθεί το διάγραμμα δεδομένων στην care-of address του κινητού κόμβου. Εάν ο βασικός πράκτορας υποστηρίζει την προαιρετική ικανότητα των πολλαπλών simultaneous mobility bindings προωθεί ένα αντίγραφο σε κάθε care-of address που έχει καταχωρήσει για αυτόν στο δεσμευτικό κατάλογο κινητικότητας του. Στην περίπτωση που ο κινητός κόμβος δεν έχει κανέναν παρόντα mobility binding , ο home agent δεν πρέπει να προσπαθήσει να αναχαιτίσει τα διαγράμματα δεδομένων που προορίζονται για τον κινητό κόμβο και έτσι δεν θα λάβει τέτοια διαγράμματα δεδομένων. Εντούτοις, εάν ο home agent είναι ένας δρομολογητής που έχει επιφορτιστεί και με τη δρομολόγηση της κυκλοφορίας «κοινών» IP πακέτων, είναι πολύ πιθανή η λήψη τέτοιων διαγραμμάτων δεδομένων για τη διαβίβαση στο home network. Σε αυτήν την περίπτωση πρέπει να υποθέσει ότι ο κινητός κόμβος είναι στο home network και απλά να προωθήσει το διάγραμμα σε αυτό .

Οι home agents πρέπει να εκτελούν decapsulate στα πακέτα που απευθύνονται σε αυτούς και τα έστειλε ένας κινητός κόμβος με σκοπό τη διατήρηση της θέσης του μυστική .

Εάν η τιμή του πεδίου Lifetime για ένα δεδομένο mobility binding λήξει πριν ο home agent λάβει ένα άλλο έγκυρο αίτημα εγγραφής για εκείνο τον κινητό κόμβο τότε ο συσχετισμός διαγράφεται από το mobility binding list ενώ δεν πρέπει να στείλει οποιοδήποτε μήνυμα απάντησης εγγραφής απλά και μόνο επειδή το binding του κινητού κόμβου έχει λήξει. Τα στοιχεία που διατηρούσε ο foreign agent στον κατάλογο επισκεπτών του για τον κινητό κόμβο θα διαγραφούν, πιθανώς την ίδια στιγμή που το binding θα θεωρηθεί λήξαν και στον home agent. Όταν παρέλθει το χρονικό διάστημα που ορίζει το πεδίο Lifetime και το mobility binding λήξει, ο home agent πρέπει να το διαγράψει αλλά να διατηρήσει οποιαδήποτε άλλα (μη-ληγμένα) ταυτόχρονα mobility bindings που κρατά για τον κινητό κόμβο.

Όταν ο home agent λαμβάνει ένα διάγραμμα δεδομένων, το οποίο προορίζονταν για έναν από τους κινητούς κόμβους του που έχει εγγραφεί σε κάποιο foreign network εξετάζει το συγκεκριμένο διάγραμμα δεδομένων που ελέγχει για το εάν είναι ήδη τοποθετημένο σε κάψα (encapsulated).

Σε αυτή την περίπτωση, ισχύουν ειδικοί κανόνες στην προώθηση εκείνου του διαγράμματος δεδομένων προς τον κινητό κόμβο:

-- Εάν η εσωτερική (τοποθετημένη σε κάψα) Destination Address είναι η ίδια με την εξωτερική Destination Address (του κινητού κόμβου), ο home agent εξετάζει την εξωτερική Source Address του τοποθετημένου σε κάψα διαγράμματος δεδομένων (η διεύθυνση προέλευσης της σήραγγας). Εάν αυτή η εξωτερική Source Address είναι η ίδια με την care-of address του κινητού κόμβου, ο home agent απορρίπτει το διάγραμμα δεδομένων προκειμένου να αποτραπεί ένας πιθανός βρόχος δρομολόγησης. Εάν δεν ισχύουν τα παραπάνω ο home agent διαβιβάζει το διάγραμμα δεδομένων στον κινητό κόμβο. Προκειμένου να διαβιβαστεί το διάγραμμα δεδομένων σε αυτήν την περίπτωση, ο home agent αλλάζει απλά την εξωτερική Destination Address βάζοντας την care-of address.

Στην αντίθετη περίπτωση (η εσωτερική διεύθυνση προορισμού δεν είναι η ίδια ως εξωτερική διεύθυνση προορισμού), ο home agent encapsulates το διάγραμμα δεδομένων πάλι (nested encapsulation), με τη νέα Destination Address στην οποία δίνεται η τιμή της care-of address του κινητού κόμβου. Δηλαδή ο βασικός πράκτορας διαβιβάζει ολόκληρο το διάγραμμα δεδομένων στον κινητό κόμβο με τον ίδιο τρόπο όπως οποιοδήποτε διάγραμμα δεδομένων (που τοποθετείται σε κάψα ή όχι).

4.3. TUNNELING ΚΑΙ ΔΡΟΜΟΛΟΓΗΤΕΣ ΕΝ ΚΙΝΗΣΕΙ

Ένας κινητός κόμβος μπορεί να είναι ένας δρομολογητής, ο οποίος είναι αρμόδιος για την εξασφάλιση της κινητικότητας ενός ή περισσότερων δικτύων που κινούνται μαζί, ίσως σε ένα αεροπλάνο, ένα σκάφος, ένα τραίνο ή ένα αυτοκίνητο. Οι κόμβοι που συνδέονται με ένα δίκτυο που εξυπηρετείται από τον κινητό δρομολογητή μπορούν οι ίδιοι να είναι σταθεροί κόμβοι ή κινητοί κόμβοι ή δρομολογητές. Στη συνέχεια της εργασίας αυτά τα δίκτυα θα καλούνται "κινητά δίκτυα".

Ο κινητός δρομολογητης , συνήθως ,λειτουργεί ως foreign agent και παρέχει την care-of address στους κινητούς κόμβους που συνδέονται με το κινητό δίκτυο το οποίο εξυπηρετεί .

Η τυπική δρομολόγηση διαγραμμάτων δεδομένων σε έναν κινητό κόμβο μέσω ενός κινητού δρομολογητή εμφανίζεται στο ακόλουθο παράδειγμα:

1) Έστω ένας υπολογιστής lap-top ο οποίος αποσυνδέεται από το home network του και αργότερα επανασυνδέεται σε ένα δίκτυο από το κάθισμα ενός αεροσκάφους. Ο υπολογιστής lap-top χρησιμοποιεί το πρωτόκολλο Mobile IP για να εγγραφεί σε αυτό το foreign network, χρησιμοποιώντας μια foreign agent care-of address που ανακαλύπτεται μέσω ενός Agent Advertisement message που απέστειλε ο foreign agent ο οποίος βρίσκεται εντός του αεροσκάφους.

2) Το δίκτυο του αεροσκάφους είναι από μόνο του ένα κινητό δίκτυο . Υποθέστε ότι ο κόμβος που λειτουργεί ως foreign agent στα αεροσκάφη χρησιμεύει επίσης ως ο προκαθορισμένος δρομολογητής που συνδέει το δίκτυο αεροσκαφών με το υπόλοιπο Διαδίκτυο. Όταν το αεροσκάφος είναι στο home network του αυτός ο δρομολογητής είναι συνδεμένος με κάποιο σταθερό δίκτυο στην έδρα της αεροπορικής εταιρίας. Ενώ το αεροσκάφος βρίσκεται στον αέρα , αυτός ο δρομολογητής εγγράφεται κατά διαστήματα , μεσώ ασύρματης ζεύξης , με μια σειρά foreign agents στο έδαφος. Ο home agent αυτού του δρομολογητή είναι ένας κόμβος στο σταθερό δίκτυο στην έδρα της αεροπορικής εταιρίας.

3) Κάποιος ανταποκρινόμενος κόμβος στέλνει ένα διάγραμμα δεδομένων στον υπολογιστή notebook, απευθύνοντας το στη home address του lap-top. Αυτό το διάγραμμα δεδομένων καθοδηγείται αρχικά στο βασικό δίκτυο του notebook.

4) Ο home agent του notebook αναχαιτίζει το διάγραμμα δεδομένων στο home network και το προωθεί στην care-of address του lap-top, η οποία σε αυτό το παράδειγμα είναι η διεύθυνση του κόμβου που λειτουργεί ως δρομολογητής και foreign agent στο αεροσκάφος. Η προώθηση των δεδομένων στην έδρα της αεροπορικής εταιρίας γίνεται με συμβατικές μεθόδους .

5) Εκεί το διάγραμμα δεδομένων αναχαιτίζεται και οδηγείται προς την care-of address που στην περίπτωση μας ανήκει στον foreign agent που βρίσκεται στο έδαφος .Το αρχικό datagram έχει υποστεί encapsulation δυο φορές (nested encapsulation).Μια φορά από τον home agent του notebook και μια από τον home agent του αεροσκάφους .

6) Ο foreign agent στο έδαφος decapsulates το διάγραμμα δεδομένων, αποδίδοντας το αρχικό διάγραμμα με το πεδίο destination address να υποδεικνύει την care-of address του notebook. Ο επίγειος foreign agent στέλνει το προκύπτον διάγραμμα δεδομένων μέσω ασύρματης ζεύξης στο αεροσκάφος.

7) Ο foreign agent στα αεροσκάφη decapsulates το διάγραμμα δεδομένων, αποδίδοντας το αρχικό διάγραμμα δεδομένων από τον αντίστοιχο κόμβο, με το πεδίο destination address να υποδεικνύει την care-of address του notebook. Ο foreign agent του αεροσκάφους παραδίδει το διάγραμμα δεδομένων στο δίκτυο του αεροσκάφους στη link-layer διεύθυνση του notebook.

Αυτό το παράδειγμα αφορά την περίπτωση στην οποία ένας κινητός κόμβος είναι συνδεμένος με ένα κινητό δίκτυο (δηλαδή ο κινητός κόμβος είναι κινητός όσον αφορά το δίκτυο, το οποίο είναι επίσης κινητό όσον αφορά το έδαφος).

Εάν, άντ' αυτού, ο κόμβος είναι σταθερός , όσον αφορά το κινητό δίκτυο (το κινητό δίκτυο είναι το σταθερό βασικό δίκτυο του κόμβου), μία εκ των δύο παρακάτω μεθόδων μπορεί να χρησιμοποιηθεί για να μεταφέρει τα διαγράμματα δεδομένων από τους αντίστοιχους κόμβους στο σταθερό κόμβο.

- Ένας home agent διαμορφώνεται έτσι ώστε να έχει μια μόνιμη εγγραφή για το σταθερό κόμβο, η οποία θα δείχνει τη διεύθυνση του κινητού δρομολογητή ως μια care-of address η οποία ανήκει σε ένα σταθερό υπολογιστή. Ο home agent είναι αρμόδιος για να δηλώσει τη διαθεσιμότητα του για τη δημιουργία και διατήρηση των συνδέσεων κάνοντας χρήση συμβατικών μεθόδων δρομολόγησης προς το σταθερό κόμβο. Και σε αυτήν τη περίπτωση το αρχικό datagram υποστεί encapsulation) δυο φορές (nested encapsulation).

- Εναλλακτικά, ο κινητός δρομολογητής δηλώνει τη διαθεσιμότητα του για τη δημιουργία και διατήρηση των συνδέσεων το σε ολόκληρο κινητό δίκτυο χρησιμοποιώντας τα κανονικά πρωτόκολλα δρομολόγησης IP μέσω μιας αμφίδρομης σήραγγας με τον home agent του .Με αυτή τη μέθοδο αποφεύγουμε την ανάγκη για χρησιμοποίηση της nested encapsulation μεθόδου.

4.4. ΜΕΘΟΔΟΙ ΠΡΟΩΘΗΣΗΣ ΤΩΝ DATAGRAMS

Στις παραγράφους που ακολουθούν θα αναλύσουμε τους δυνατούς τρόπους με τη βοήθεια των οποίων το διάγραμμα δεδομένων υφίσταται τις απαραίτητες αλλαγές και προωθείται προς τον κινητό κόμβο . Η διαδικασία αυτή ονομάζεται Encapsulation ενώ η αντίστροφη διαδικασία Decapsulation . Η χρησιμοποίηση Encapsulation και Decapsulation συχνά θα αναφέρεται και ως Tunneling ενώ τα σημεία που εκτελούνται οι παραπάνω διαδικασίες θεωρούνται ως η αρχή και το τέλος του τούνελ, αντίστοιχα .

Πιο συγκεκριμένα αναφέρουμε ότι το Encapsulation χρησιμοποιείται ως ένας τρόπος για να παρακάμψουμε τη συμβατική δρομολόγηση των πακέτων χρησιμοποιώντας έναν ενδιάμεσο προορισμό , ο οποίος υπό άλλες συνθήκες δεν θα χρησιμοποιούνταν λαμβάνοντας υπόψη την IP Destination Address.

i. IP Within IP Encapsulation

Στη συγκεκριμένη ενότητα θα περιγράψουμε τον τρόπο με τον οποίο ένα IP datagram τοποθετείται εντός ενός άλλου IP datagram, μεταφερόμενο πλέον σαν ωφέλιμο φορτίο .

Η μέθοδος αυτή χρησιμοποιείται για να επιτύχουμε την παράκαμψη της συμβατικής δρομολόγησης ώστε το πακέτο να προωθηθεί στη διεύθυνση του home agent του κινητού κόμβου και στη συνέχεια να οδηγηθεί σε αυτόν . Όταν τα διαγράμματα φτάσουν σε αυτόν υφίστανται την αντίστροφη διαδικασία ώστε να επαναδημιουργηθεί το αρχικό διάγραμμα το οποίο , στη συνέχεια , οδηγείται στον προορισμό του όπως αυτός αναγράφεται στο πεδίο IP Destination Address.

Για να γίνουν ευκολότερα κατανοητά τα παραπάνω παραθέτουμε το εξής γράφημα σημειώνοντας ότι τα σημεία source ,encapsulator , decapsulator και destination είναι ξεχωριστοί υπολογιστές , επιφορτισμένοι με τις συγκεκριμένες διαδικασίες:

Source ---> Encapsulator ---> Decapsulator ---> Destination

Ο υπολογιστής στον οποίο εκτελείται το Encapsulation θεωρείται το ***entry point*** του τούνελ ενώ ο αντίστοιχος στον οποίο εκτελείται το Decapsulation το ***exit point*** του .

Το Encapsulation χρησιμοποιείται από το πρωτόκολλο Mobile IP ως ένας τρόπος για την προώθηση των πακέτων από το home network του κινητού κόμβου σε ένα agent ο οποίος θα χρησιμοποιήσει συμβατικές μεθόδους δρομολόγησης προς τον κινητό κόμβο . Μπορεί , ακόμη , να χρησιμοποιηθεί όταν ο αποστολέας θέλει να καθορίσει ένα συγκεκριμένο δικτυακό δρομολόγιο που θα ακολουθήσει το διάγραμμα , με πιο συνηθισμένο λόγο για αυτό να είναι η επιλογή δρομολογητών με αυξημένα χαρακτηριστικά ασφαλείας .

Οι λόγοι που έχουν οδηγήσει στην καθιέρωση του Encapsulation παραγκωνίζοντας ανάλογες μεθόδους είναι οι εξής:

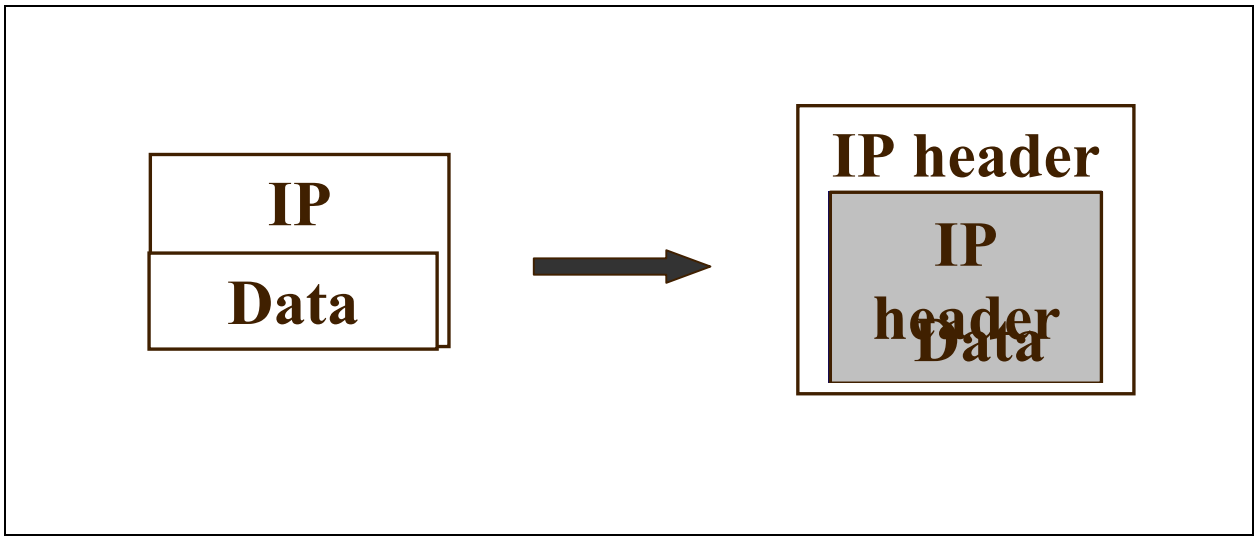
1. Η αυξημένη ασφάλεια που προσφέρει ,συγκριτικά με αυτές .
2. Η συμβατότητα που παρουσιάζει με τη χρήση συμβατικών δρομολογητών , ή αλλιώς η μη ύπαρξη ιδιαιτέρων απαιτήσεων από αυτούς.
3. Το γεγονός ότι τα πακέτα αυτά δεν αντιμετωπίζουν προβλήματα στο να φτάσουν στον παραλήπτη τους όταν αυτός χρησιμοποιεί εφαρμογές firewall .
4. Το γεγονός ότι δεν απαιτείται καμιά αλλαγή στα πακέτα αυτά από τους ενδιάμεσους δρομολογητές.

Βέβαια , πέρα από τα πλεονεκτήματα που αναφέραμε υπάρχουν και κάποια μειονεκτήματα τα οποία , όμως , αντιμετωπίζονται σαν αναγκαίο κακό καθώς θεωρούνται ως δευτερεύοντα μπροστά στα παραπάνω . Ενδεικτικά αναφέρουμε τα εξής:

1. Τα διαγράμματα που έχουν υποστεί Encapsulation είναι , σε γενικές γραμμές , μεγαλυτέρου μεγέθους σε σχέση με τα αρχικά .
2. Το Encapsulation δεν μπορεί να χρησιμοποιηθεί παρά μόνο εάν είναι , εκ των προτέρων , γνωστό ότι ο κόμβος που βρίσκεται στο exit point του τούνελ μπορεί να εκτελέσει decapsulate στο datagram που λαμβάνει .

Για να επιτύχουμε το encapsulation ενός διαγράμματος δεδομένων με τη συγκεκριμένη μέθοδο θα πρέπει να τοποθετηθεί σε αυτό μια εξωτερική IP επικεφαλίδα πριν από αυτή που ήδη υπάρχει .

Το παρακάτω σχήμα απεικονίζει, γραφικά, τον τρόπο με τον οποίο επιτυγχάνεται κάτι τέτοιο:



Η εξωτερική IP Header Source Address και η Destination Address είναι αυτές που καθορίζουν τα entry και exit points του τούνελ καθώς υποδεικνύουν τον αποστολέα και τον παραλήπτη αντίστοιχα . Η εσωτερική IP επικεφαλίδα παραμένει αναλλοίωτη από τη διαδικασία (εκτός από το πεδίο TTL η τιμή του οποίου ελαττώνεται όπως θα αναλύσουμε στη συνέχεια) και παραμένει έτσι έως ότου παραδοθεί στο exit point του τούνελ . Εάν υπάρξει λόγος μπορούν να προστεθούν και άλλες επικεφαλίδες όπως η IP Authentication Header (η οποία τοποθετείται μεταξύ της εξωτερικής και της εσωτερικής IP επικεφαλίδας).

Στα πεδία που αφορούν την εξωτερική IP επικεφαλίδα δίνονται οι ακόλουθες τιμές μετά τη διαδικασία του encapsulation:

Version:

Στο πεδίο αυτό δίνεται η τιμή **4** ή **6** ανάλογα με την έκδοση του πρωτοκόλλου.

IHL:

Το πεδίο Internet Header Length μας δείχνει το μήκος της εξωτερικής IP επικεφαλίδας σε λέξεις των 32 bits.

TOS:

Το πεδίο Type of Service αντιγράφεται από την εσωτερική IP επικεφαλίδα.

Total Length:

Το πεδίο αυτό μας δίνει το μήκος ολόκληρου του encapsulated IP datagram, συμπεριλαμβάνοντας την εξωτερική, την εσωτερική αλλά και τα δεδομένα.

Identification, Flags, Fragment Offset:

Το Fragment Offset bit πρέπει να πάρει την τιμή που έχει το αντίστοιχο πεδίο στην εσωτερική IP επικεφαλίδα. Για τα υπόλοιπα δυο πεδία έχουμε αναφερθεί σε προηγούμενες ενότητες.

Time To Live:

Το πεδίο TTL της εξωτερικής IP επικεφαλίδας παίρνει μια τιμή η οποία είναι επαρκής για τη μεταφορά του encapsulated διαγράμματος στο exit point του τούνελ.

Protocol:

Στο πεδίο αυτό δίνεται η τιμή **4** ή **6** ανάλογα με την έκδοση του πρωτοκόλλου.

Header Checksum:

Στο πεδίο αυτό δίνεται η Internet Header Checksum της εξωτερικής IP επικεφαλίδας.

Source Address:

Στο Source Address πεδίο υπάρχει η IP διεύθυνση του υπολογιστή που βρίσκεται στο entry point του τούνελ.

Destination Address:

Στο Destination Address πεδίο υπάρχει η IP διεύθυνση του υπολογιστή που βρίσκεται στο exit point του τούνελ.

Options:

Στο πεδίο Options υπάρχουν όλες οι επιλογές που αναφέρονται στην εσωτερική IP επικεφαλίδα αν και υπάρχει η δυνατότητα προσθήκης νέων εάν αυτό κρίνεται απαραίτητο .

Κατά τη διαδικασία του encapsulate ενός διαγράμματος δεδομένων το πεδίο TTL , της εσωτερικής IP επικεφαλίδας ελαττώνεται κατά 1 εάν το tunneling είναι μέρος της προώθησης του διαγράμματος διαφορετικά παραμένει αναλλοίωτο . Στην περίπτωση που η τιμή που προκύπτει μετά την ελάττωση είναι μηδενική το διάγραμμα απορρίπτεται και στον αποστολέα επιστρέφεται ένα ICMP Time Exceeded μήνυμα .

Κάτι ανάλογο συμβαίνει και στη διαδικασία του decapsulation καθώς εάν ο υπεύθυνος υπολογιστής διαπιστώσει ότι η τιμή του εσωτερικού διαγράμματος είναι μηδενική τότε απορρίπτει το μήνυμα . Εάν δεν υπάρχει τέτοιο πρόβλημα τότε η τιμή του πεδίου ελαττώνεται κατά 1 και το διάγραμμα προωθείται προς τον παραλήπτη .

Μια από τις πιο επικίνδυνες καταστάσεις που μπορεί να συμβεί στο συγκεκριμένο τμήμα του δικτύου (αναφερόμαστε στο εικονικό τούνελ) είναι η δημιουργία Routing loops (βρόγχοι δρομολόγησης). Ας υποθέσουμε ότι ένα διάγραμμα δεδομένων φτάνει σε ένα δρομολογητή με σκοπό την προώθηση του και αυτός αποφασίζει ότι το συγκεκριμένο διάγραμμα πρέπει να υποστεί τη διαδικασία του encapsulation πριν εκτελέσει τη συγκεκριμένη δράση .

Στην περίπτωση αυτή μπορεί να συμβούν τα εξής:

- Εάν η IP Source Address του διαγράμματος ταιριάζει με την IP διεύθυνση του δρομολογητή για οποιοδήποτε από τα υποδίκτυα που αυτός εξυπηρετεί τότε πρέπει να απορριφθεί.
- Στην περίπτωση που η IP Source Address του διαγράμματος ταιριάζει με την IP διεύθυνση του exit point του τούνελ (το οποίο συνήθως επιλέγεται από το δρομολογητή βασιζόμενος στην IP Destination Address που βρίσκεται στην επικεφαλίδα του IP διαγράμματος) τότε το διάγραμμα πρέπει να απορριφθεί.

Μετά την αποστολή ενός encapsulated διαγράμματος είναι πιθανή η λήψη από τον υπεύθυνο υπολογιστή ενός ICMP μηνύματος από κάποιο ενδιάμεσο δρομολογητή . Ανάλογα με το περιεχόμενο του μηνύματος ο συγκεκριμένος υπολογιστής θα κάνει τις απαραίτητες ενέργειες . Στην περίπτωση που το παραληφθέν μήνυμα περιέχει αρκετές πληροφορίες ο κόμβος μπορεί να απαντήσει με ένα μήνυμα ιδίου τύπου το οποίο θα αποσταλεί με προορισμό τον αποστολέα του αρχικού διαγράμματος δεδομένων .Η διαδικασία αυτή είναι γνωστή ως ***αναμετάδοση του ICMP μηνύματος εντός του τούνελ*** .

Τα ICMP μηνύματα τα οποία υποδηλώνουν την ύπαρξη λάθους στην επεξεργασία ενός datagram συμπεριλαμβάνουν ένα αντίγραφο τμήματος του datagram που προκάλεσε το σφάλμα .Η αναμετάδοση του μηνύματος προϋποθέτει ότι ο υπολογιστής που διενεργεί τη διαδικασία του encapsulation έχει την ικανότητα να αφαιρέσει την εξωτερική IP επικεφαλίδα από το αντίγραφο του τμήματος του διαγράμματος που παραλαμβάνει .

Στη συνέχεια θα εξετάσουμε τα μηνύματα αυτά (με ποιους κωδικούς στέλνονται και ποιες είναι οι πληροφορίες που μπορούμε να αντλήσουμε από αυτά):

- **Destination Unreachable (Type 3)**

Τα μηνύματα αυτού του είδους αντιμετωπίζονται από τον υπεύθυνο υπολογιστή ανάλογα με την τιμή του πεδίου Code .

Όπως γνωρίζουμε το μοντέλο που αναλύουμε έχει σχεδιαστεί, πρωτίστως, για την εξυπηρέτηση κινητών κόμβων. Εάν σε ένα υποδίκτυο ο δρομολογητης έχει κάποιο πακέτο δεδομένων που προορίζεται για κάποιο κόμβο ο οποίος βρέθηκε σε αυτό (περίπτωση μετακινούμενου κινητού κόμβου) που εξυπηρετεί τότε για να επιτευχθεί η προώθηση θα πρέπει να γίνουν αλλαγές στην τιμή του Destination Unreachable Code .

- **Network Unreachable (Code 0)**

Τα μηνύματα αυτού του είδους αποστέλλονται στον αρχικό αποστολέα .Εάν ο προορισμός του αρχικού μηνύματος (πριν το encapsulation) βρίσκεται στο ίδιο δίκτυο με τον υπολογιστή που εκτελεί την παραπάνω διαδικασία το Destination Unreachable μήνυμα θα έχει τον κωδικό 1 (Host Unreachable) καθώς , υποθετικά ,το διάγραμμα δεδομένων έφτασε στο σωστό δίκτυο και ο encapsulator προσπαθεί να δημιουργήσει την εντύπωση ότι ο αρχικός προορισμός βρίσκεται στο τοπικό δίκτυο ακόμη και αν δεν ισχύει αυτό. Διαφορετικά θα επιστρέψει ένα Destination Unreachable μήνυμα με το πεδίο Code να έχει την τιμή 0.

- **Host Unreachable (Code 1)**

Ο encapsulator μεταδίδει Host Unreachable μηνύματα στον αποστολέα του αρχικού μηνύματος (πριν το encapsulation).

- **Protocol Unreachable (Code 2)**

Όταν ο encapsulator λάβει αυτό το μήνυμα πρέπει να απαντήσει με το Destination Unreachable μήνυμα με τον κωδικό 0 ή 1 στον αποστολέα αρχικού μηνύματος (πριν το encapsulation).

- **Port Unreachable (Code 3)**

Ο συγκεκριμένος κωδικός δεν πρέπει να ληφθεί πότε από τον encapsulator καθώς η εξωτερική IP διεύθυνση δεν αντιστοιχεί σε κάποιο port number .

- **Datagram Too Big (Code 4)**

Ο encapsulator πρέπει να αναμεταδώσει το μήνυμα αυτό στον αποστολέα του αρχικού μηνύματος (πριν το encapsulation).

- **Source Route Failed (Code 5)**

Ο συγκεκριμένος κωδικός πρέπει να αντιμετωπιστεί από τον encapsulator και δεν πρέπει να μεταδοθεί προς τον αποστολέα του αρχικού μηνύματος (πριν το encapsulation).

- **Source Quench (Type 4)**

Ο encapsulator δεν πρέπει να αναμεταδώσει ICMP Source Quench μηνύματα προς τον αποστολέα του αρχικού μηνύματος (πριν το encapsulation).

- **Redirect (Type 5)**

Ο encapsulator μπορεί να χειριστεί τα μηνύματα αυτά μόνος του και δεν πρέπει να τα αναμεταδώσει προς τον αποστολέα του αρχικού μηνύματος (πριν το encapsulation).

- **Time Exceeded (Type 11)**

Τα συγκεκριμένα μηνύματα αναφέρουν πιθανές περιπτώσεις βρόγχων δρομολόγησης εντός του τούνελ .Η λήψη τέτοιων μηνυμάτων από τον encapsulator πρέπει να αναφέρεται στον αποστολέα του αρχικού μηνύματος (πριν το encapsulation) ως Host Unreachable (Type 3 Code 1).

- **Parameter Problem (Type 12)**

Εάν το μήνυμα Parameter Problem αναφέρεται σε ένα πεδίο το οποίο αντιγράφηκε από το αρχικό μήνυμα (πριν το encapsulation) τότε ο encapsulator μπορεί να το αναμεταδώσει προς τον αποστολέα του αρχικού μηνύματος. Διαφορετικά, και εφόσον το πρόβλημα οφείλεται σε ενέργεια του encapsulator, η αναμετάδοση του μηνύματος δεν πρέπει να γίνει προς τον αποστολέα .

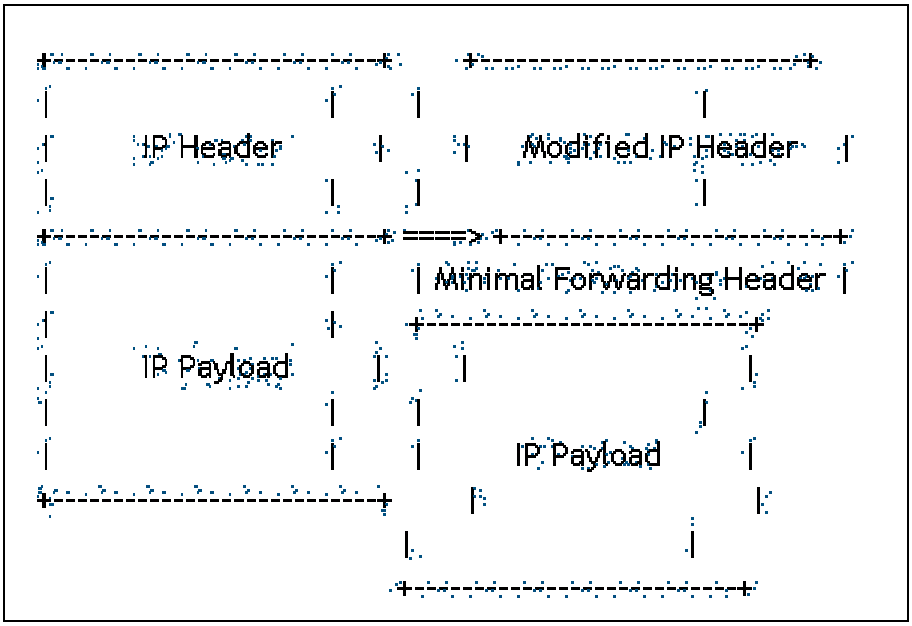
ii. Minimal Encapsulation Within IP

Στη συγκεκριμένη ενότητα θα αναλύσουμε μια μέθοδο encapsulation με την οποία το αρχικό IP διάγραμμα τοποθετείται μέσα σε ένα άλλο με τη διαφορά ότι η επικεφαλίδα είναι μικρότερη από αυτή που προκύπτει από την προηγούμενη μέθοδο .

Αυτό συμβαίνει επειδή η μέθοδος που εξετάζουμε μεταβάλλει το περιεχόμενο της IP επικεφαλίδας προσθέτοντας (όσο το δυνατό) λιγότερες πληροφορίες σε αντίθεση με την προηγούμενη που χρησιμοποιεί την πρώτη ανέπαφη και προσθέτει πληροφορίες στο εξωτερικό αντίτυπο της .

Θα πρέπει να σημειώσουμε ότι προκειμένου να εφαρμόσουμε τη συγκεκριμένη μέθοδο θα πρέπει τα πακέτα δεδομένων να μην έχουν κατακερματιστεί πριν την εφαρμογή της καθώς δεν υπάρχει αρκετός χώρος στη Minimal Forwarding Header ώστε να συμπεριλάβει τις επιπλέον πληροφορίες .

Το παρακάτω σχήμα απεικονίζει γραφικά τη διαδικασία που περιγράψαμε:



Όπως φαίνεται και από το παραπάνω σχήμα το encapsulation πραγματοποιείται τοποθετώντας την Minimal Forwarding Header εντός του διαγράμματος .

Η χρησιμοποίηση της συγκεκριμένης μεθόδου είναι προαιρετική .

Η IP επικεφαλίδα του αρχικού datagram μεταβάλλεται και ακολουθείται από την Minimal Forwarding Header επικεφαλίδα και στη συνέχεια έχουμε το περιεχόμενο του datagram του οποίο παραμένει ως είχε .

Η αλλαγή της IP επικεφαλίδας εστιάζεται στα παρακάτω πεδία:

- Το πεδίο ***Protocol*** αντικαθίσταται από τον κωδικό **55** που υποδηλώνει τη συγκεκριμένη μέθοδο.

- Το πεδίο ***Destination Address*** αντικαθίσταται από την IP διεύθυνση του κόμβου που λειτουργεί ως το exit point του τούνελ .

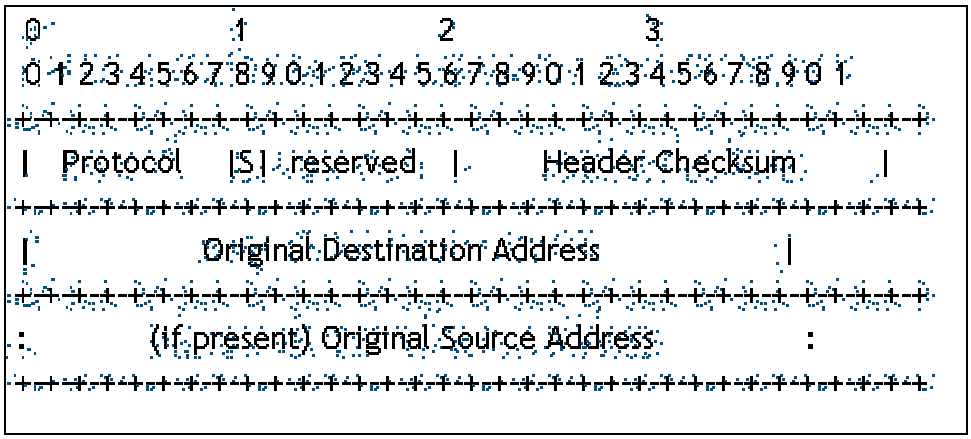
- Εάν ο encapsulator υπολογιστής δεν είναι ο αποστολέας του διαγράμματος τότε το πεδίο ***Source Address*** αντικαθίσταται από την IP διεύθυνση του.

- Το πεδίο ***Total Length*** αυξάνεται κατά αριθμό ίσο με το μέγεθος της Minimal Forwarding Header που προστίθεται στο διάγραμμα .Ο αριθμός αυτός είναι ίσος με **12** ή **8** bytes ανάλογα με το εάν το Original Source Address Present bit **(S)** έχει την τιμή 1 ή όχι αντίστοιχα .

- Το πεδίο ***Header Checksum*** επαναϋπολογίζεται ή ανανεώνεται ώστε να συμβαδίζει με τις προαναφερθείσες αλλαγές.

Αξιοσημείωτο είναι το γεγονός ότι , σε αντίθεση με την IP Within IP μέθοδο , το πεδίο TTL παραμένει αναλλοίωτο κατά τη διάρκεια του encapsulation. Κατά την προώθηση του διαγράμματος η τιμή του συγκεκριμένου πεδίου ελαττώνεται κατά τα πρότυπα της συμβατικής δρομολόγησης. Εφόσον το πεδίο TTL παραμένει στην IP επικεφαλίδα μετά το encapsulation , οι μεταπηδήσεις των πακέτων από κόμβο σε κόμβο εντός του τούνελ, είναι ανιχνεύσιμες μεσώ της εντολής trace route.

Το format της Minimal Forwarding επικεφαλίδας παρουσιάζεται στο παρακάτω σχήμα:



- Το πεδίο ***Protocol*** αντιγράφεται από την IP επικεφαλίδα του αρχικού μηνύματος .
- Το πεδίο ***Original Source Address*** αναφέρεται στο bit **S**

Η τιμή του είναι ίση με **0** εάν το παραπάνω πεδίο δεν είναι παρόν όποτε το μήκος της Minimal Forwarding Header στην περίπτωση αυτή είναι **8** bytes.

Η τιμή του είναι ίση με **1** εάν το παραπάνω πεδίο είναι παρόν όποτε το μήκος της Minimal Forwarding Header στην περίπτωση αυτή είναι **12** bytes.

- Το πεδίο ***Reserved*** στέλνεται έχοντας την τιμή **0.**
- Στο πεδίο ***Header Checksum*** δίνεται η τιμή 0 για ευκολία στον υπολογισμό του. Στην τιμή που θα προκύψει δεν συμπεριλαμβάνεται η IP επικεφαλίδα και το μήκος δεδομένων που αντιστοιχεί στο IP φορτίο.
- Το πεδίο ***Original Destination Address*** αντιγράφεται από την IP επικεφαλίδα του αρχικού μηνύματος .

Κατά την εκτέλεση της διαδικασίας του decapsulate στο διάγραμμα δεδομένων τα πεδία που βρίσκονται στη Minimal Forwarding Header επανατοποθετούνται στην IP επικεφαλίδα και η προσθήκη σε αυτή απομακρύνεται . Επιπροσθέτως ,το πεδίο Total Length ελαττώνεται κατά μια τιμή ίση με το μήκος της Minimal Forwarding Header που αφαιρείται ενώ το πεδίο Header Checksum επαναϋπολογίζεται ή ανανεώνεται.

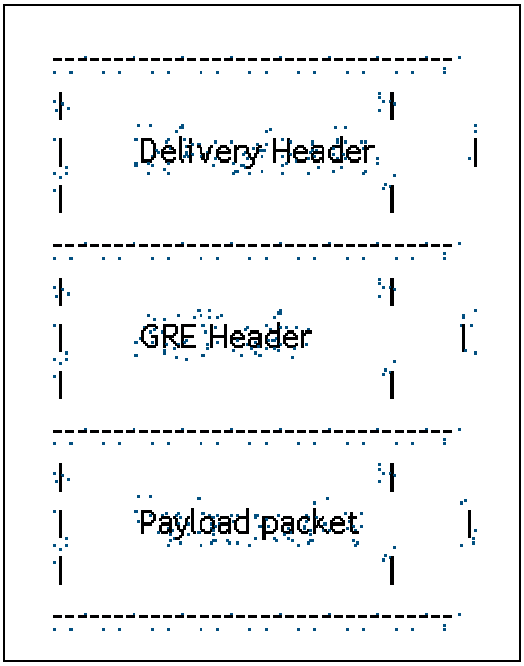
Ο encapsulator μπορεί να χρησιμοποιήσει υπάρχοντες μηχανισμούς δρομολόγησης όπως η κατακερμάτιση του διαγράμματος (εκτός εάν το Don’t Fragment bit έχει την τιμή 1 στην επικεφαλίδα IP).

iii. Generic Routing Encapsulation (GRE)

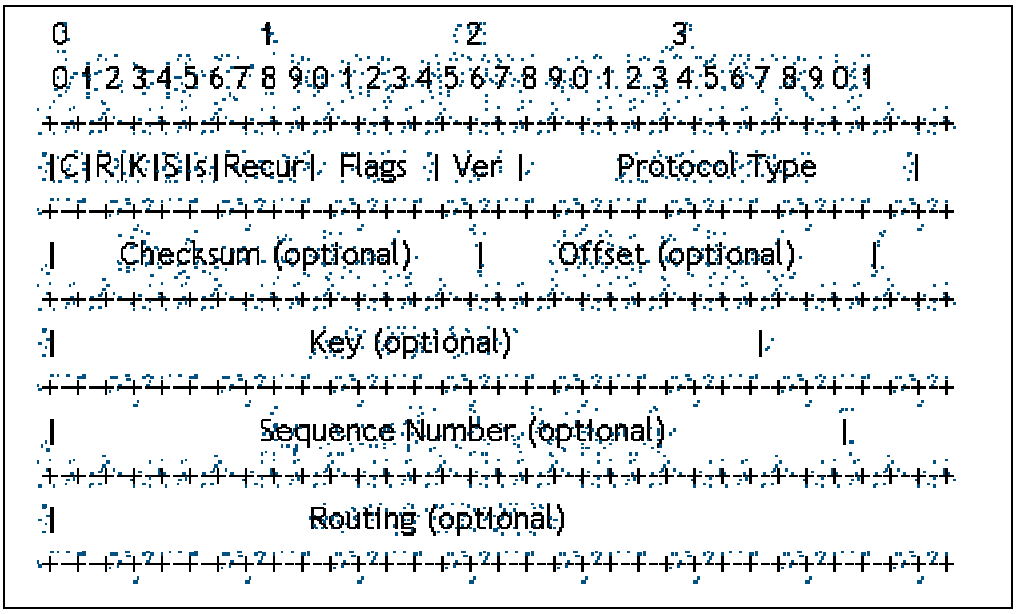
Με τη μέθοδο αυτή το πακέτο δεδομένων το οποίο πρέπει να προωθηθεί υφίσταται αρχικά encapsulation σε ένα GRE πακέτο και στη συνέχεια , το προκύπτον πακέτο , ακολουθεί την ίδια διαδικασία σύμφωνα με κάποια εκ των δυο μεθόδων που προαναφέραμε .

Συμπεραίνουμε , λοιπόν , ότι η συγκεκριμένη μέθοδος είναι ένα είδος "ελαφρού" encapsulation και δεν θεωρείται απαραίτητη παρά μόνο σε περιπτώσεις που απαιτείται δρομολόγηση με το συγκεκριμένο τρόπο (γεγονός αρκετά σπάνιο).

Η μορφή του πακέτου που προκύπτει από το encapsulation κατά τη Generic Routing Encapsulation μέθοδο θα έχει την μορφή του σχήματος:



ενώ η μορφή του GRE Header θα έχει τη μορφή που απεικονίζεται στο επόμενο σχήμα :



- Το πεδίο ***Flags and version*** έχει μήκος 2 bytes με το bit 0 να θεωρείται ως το Most Significant bit ενώ το bit 15 Least Significant bit. Τα bits **13-15** χρησιμοποιούνται για το πεδίο **Version** ενώ τα bits **8-12** είναι ελεύθερα για πιθανή μελλοντική χρήση και μεταδίδονται έχοντας την τιμή **0**.

    1. Εάν το bit ***Checksum Present (bit 0)*** έχει την τιμή **1** τότε το πεδίο Checksum είναι παρόν και περιέχει χρήσιμες πληροφορίες .

    2. Εάν το bit ***Routing Present (bit 1)*** έχει την τιμή **1** αυτό συνεπάγεται ότι τα Checksum **και** Offset πεδία είναι παρόντα στο GRE πακέτο .

    3. Εάν το bit ***Key Present (bit 2)*** έχει την τιμή **1** αυτό συνεπάγεται ότι το πεδίο Key είναι παρόν .

    4. Εάν το bit ***Sequence Number Present (bit 3)*** έχει την τιμή **1** αυτό συνεπάγεται ότι το πεδίο Sequence Number Present είναι παρόν .

    5. Το bit ***Strict Source Route (bit 4)*** πρέπει να έχει την τιμή **1** εάν όλες οι διαδρομές δρομολόγησης περιέχουν Strict Source Routes.

6. Τα bits ***Recursion Control (bits 5-7)*** περιέχουν μη προσημασμένους ακέραιους οι οποίοι δηλώνουν τον αριθμό των επιπρόσθετων encapsulations που μπορούν να γίνουν. Η default τιμή είναι **0**.

7. Τα bits ***Version Number (bits 13-15)*** πρέπει να περιέχουν την τιμή **0**.

- Το πεδίο ***Protocol Type*** έχει μήκος 2 bytes και περιέχει τον τύπο του πρωτοκόλλου που χρησιμοποιεί το πακέτο δεδομένων (συνήθως το Ethernet).

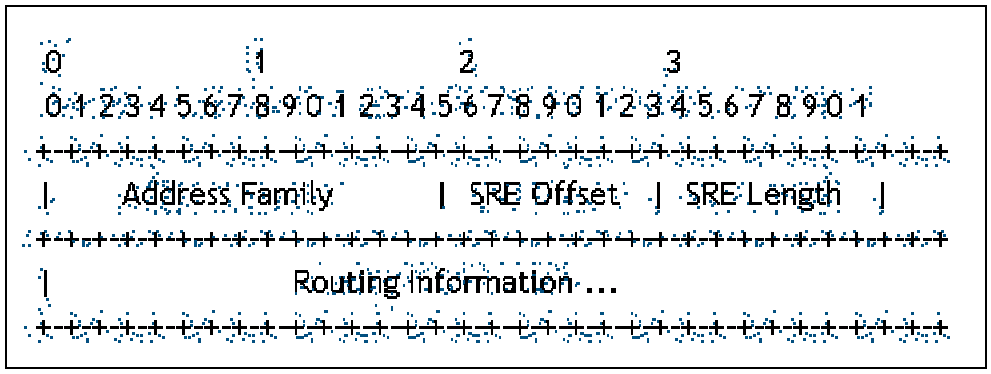
- Το πεδίο ***Offset*** έχει μήκος 2 bytes και δηλώνει το offset byte από την αρχή του πεδίου Routing έως το byte που ξεκινάει το Source Route Entry.

- Το πεδίο ***Checksum*** έχει μήκος 2 bytes και περιέχει το IP Checksum της GRE επικεφαλίδας και του πακέτου δεδομένων .

- Το πεδίο ***Key*** έχει μήκος 4 bytes και περιέχει τιμές που συμπεριλήφθηκαν από τον encapsulator. Χρησιμοποιείται από τον παραλήπτη για να εξακριβώσει την ταυτότητα του αποστολέα του πακέτου.

- Το πεδίο ***Sequence Number*** έχει μήκος 4 bytes και περιέχει έναν 32 bit ακέραιο που συμπεριλήφθηκε από τον encapsulator. Χρησιμοποιείται από τον παραλήπτη για να βάλει στην κατάλληλη σειρά τα πακέτα που έλαβε.

- Το πεδίο ***Routing*** έχει μεταβλητό μήκος και είναι παρόν μόνο όταν το Routing Present bit έχει την τιμή **1**. Το συγκεκριμένο πεδίο είναι ουσιαστικά μια λίστα από **Source Route Entries (SREs)** η μορφή των οποίων παρατίθεται στο παρακάτω σχήμα:



Το πεδίο Routing τερματίζεται με μια 'NULL' SRE, η οποία θα περιέχει μια διεύθυνση της μορφής **0x0000** και μηδενικό μήκος.

Η επεξήγηση των πεδίων που απεικονίζονται στο παραπάνω σχήμα έχει ως εξής:

Address Family (2 Bytes)

Το συγκεκριμένο πεδίο περιέχει μια τιμή μήκους δυο bytes η οποία υποδηλώνει τη σύνταξη και τη σημασία του πεδίου Routing.

SRE Offset (1 Byte)

Το συγκεκριμένο πεδίο μας υποδεικνύει το offset byte από την αρχή του πεδίου routing information έως το πρώτο byte του πεδίου source route entry.

SRE Length (1 Byte)

Το συγκεκριμένο πεδίο περιέχει τον αριθμό (σε byte) του πεδίου source route entry. Εάν η τιμή του είναι ίση με μηδέν αυτό σημαίνει ότι είναι το τελευταίο source route entry στο πεδίο routing.

Routing Information (μεταβλητου μηκους)

Το συγκεκριμένο πεδίο περιέχει πληροφορίες που μπορούν να χρησιμοποιηθούν στην προώθηση του πακέτου δεδομένων.

Η προώθηση των πακέτων που έχουν υποβληθεί στη διαδικασία του encapsulation σύμφωνα με τη GRE μέθοδο γίνεται , σε γενικές γραμμές, με τον ίδιο τρόπο που ακολουθείται και για την προώθηση πακέτων που υποβλήθηκαν σε κάποια από τις δυο προηγούμενες μεθόδους.

Στην περίπτωση που ένα τέτοιο πακέτο φτάσει σε έναν υπολογιστή οι τιμές των πεδίων Key, Sequence Number και Checksum ελέγχονται για να διαπιστωθεί εάν περιέχουν έγκυρες πληροφορίες .Εάν το πεδίο Routing Field έχει την τιμή 1 τότε το Address Family πεδίο πρέπει να ελεγχθεί ώστε να καθοριστεί ο τρόπος χρησιμοποίησης των πληροφοριών που περιέχονται στα πεδία SRE Length,SRE Offset και Routing Information.Όταν όλες οι SRE έχουν ελεγχθεί αφαιρείται η GRE επικεφαλίδα ,το πεδίο TTL του διαγράμματος δεδομένων ελαττώνεται και το διάγραμμα προωθείται ακολουθώντας συμβατικές μεθόδους δρομολόγησης.

ΚΕΦΑΛΑΙΟ 5

Διαφορές μεταξύ Mobile IPv4 και Mobile IPv6

5.1. ΕΙΣΑΓΩΓΗ

Έχοντας παρουσιάσει αναλυτικά τις βασικές διαδικασίες του πρωτοκόλλου και τις απαιτήσεις που υπάρχουν από τους υπολογιστές που προορίζονται να καλύψουν τις ανάγκες του συνεχίζουμε παραθέτοντας τις διαφοροποιήσεις που υπάρχουν μεταξύ τις παρούσης έκδοσης (IPv4) και της, υπό ανάπτυξη, μελλοντικής (IPv6).

Αρκετές αναφορές , κυρίως σε ότι αφορά τα μηνύματα ελέγχου της νέας έκδοσης παρουσιάστηκαν παράλληλα με τα αντίστοιχα της έως τώρα χρησιμοποιούμενης ώστε να γίνουν ευκολότερα κατανοητές οι οποίες διάφορες τους.

Όπως προαναφέραμε, η συγκεκριμένη έκδοση βρίσκεται ακόμη σε πρώιμο στάδιο και αναμένεται να αποτελέσει τμήμα της νέας έκδοσης του Internet, ένα project γνωστό και ως IPng (IP next generation).Στην παρούσα εργασία θα παρουσιάσουμε και θα αναλύσουμε τις αλλαγές εκείνες οι οποίες θεωρούνται ως παγιωμένες και δεν πρόκειται να μεταβληθούν καθώς επίσης και εκείνες για τις οποίες οι μελέτες έχουν παγιωθεί και απλώς αναμένεται η οριστική αποδοχή τους .

Η παρουσίαση των παραπάνω θα γίνει αναφερόμενοι στις αλλαγές που υπάρχουν σε ότι αφορά τον τρόπο λειτουργίας των:

- **Correspondent nodes**
- **Home agents**
- **Mobile nodes**

(Σημειώνουμε ότι για να γίνουν κατανοητές οι διάφορες θα πρέπει να έχουν γίνει κτήμα του αναγνώστη τα κεφάλαια που προηγήθηκαν.)

Η νέα έκδοση περιλαμβάνει χαρακτηριστικά τα οποία έχουν σχεδιαστεί για να υποστηρίξουν τη μετάδοση δεδομένων που απαιτούν μεγάλη ταχύτητα (όπως για παράδειγμα η μετάδοση εικόνας) τα οποία δεν ήταν διαθέσιμα στην προηγούμενη έκδοση του πρωτοκόλλου . Για την υποστήριξη των παραπάνω εισάγονται οι έννοιες ***Stateless Address Auto configuration*** και ***Neighbour Discovery***.

Στη σχεδίαση της νέας έκδοσης διατηρούνται οι έννοιες του home network, home agent και η χρήση του encapsulation για την προώθηση των πακέτων από το home network του κινητού κόμβου στην παρούσα θέση του. Αν και η διαδικασία του Discovery της care-of address του κινητού κόμβου παραμένει απαραίτητη, ο κινητός κόμβος έχει πλέον τη δυνατότητα να καθορίσει ο ίδιος την care-of address του, κάνοντας χρήση των παραπάνω εννοιών (γεγονός που συνεπάγεται ότι οι foreign agents δεν απαιτείται να πληρούν κάποιες ιδιαίτερες προϋποθέσεις για την υποστήριξη τους).

Ειδικότερα, στη νέα έκδοση οι δρομολογητες λειτουργούν ακολουθώντας τις ίδιες βασικές αρχές με την προηγούμενη έκδοση .Έτσι, όταν η care-of address του κινητού κόμβου είναι γνωστή ,η προώθηση πακέτων δεδομένων σε αυτόν γίνεται χωρίς τη βοήθεια του home agent. Η διατήρηση της συγκεκριμένης ιδιότητας κρίθηκε απαραίτητη λόγω του ότι βρισκόμαστε ακόμη σε πρώιμο στάδιο ανάπτυξης του πρωτοκόλλου και η ανάθεση νέων αρμοδιοτήτων στους home agents δεν θα πρέπει να αποκλειστεί.

Τα ζητήματα που άπτονται της ασφάλειας είναι πολύ σημαντικά και θα αναλυθούν με περισσότερες λεπτομέρειες στο επόμενο κεφάλαιο . Στη συγκεκριμένη ενότητα απλά θα αναφέρουμε ότι η μεγαλύτερη διάφορα στο συγκεκριμένο τομέα είναι ότι όλοι οι κομβόι θα ενσωματώνουν χαρακτηριστικά πιστοποίησης και κρυπτογράφησης σε όλα τα σταδία της επικοινωνίας τους. Αν και η ο βαθμός ασφάλειας που προσφέρει το πρωτόκολλο αυξάνεται κατακόρυφα δημιουργείται ένα σοβαρό πεδίο προβληματισμού καθώς η ασφάλεια επιτυγχάνεται σε βάρος της ταχύτητας με την οποία μεταδίδονται τα πακέτα.

Οι παραπάνω σκεψεις αποτελουν ένα ελαχιστο δειγμα των , αντικρουωμενων απαιτήσεων που καλούνται αν αντιμετωπίσουν οι ερευνητές ώστε να καθορισουν τα standards της νέας έκδοσης.

Παρουσιαζουμε τα αποτελεσματα των εως τωρα ερευνων τους στις παρακάτω ενότητες αφού υπενθυμίσουμε ότι τα παρακάτω έχουν εγκριθεί από την επιστημονική κοινότητα.

5.2. Λειτουργίες Correspondent Nodes

Υπενθυμίζουμε ότι ως ***Correspondent Node*** ορίζουμε κάθε κόμβο ο οποίος επικοινωνεί με τον κινητό κόμβο και ο οποιος μπορεί και ο ίδιος να είναι κινητός.

i. Λήψη πακέτων από κινητο κομβο

Τα πακετα τα οποία στελνονται από ένα κινητο κομβο και ενώ αυτος βρίσκεται συνδεδεμενος σε ένα foreign network συμπεριλαμβανουν και τη Home address option. Κάθε κομβος που λαμβανει ένα τετοιο πακετο εξεταζει τη συγκεκριμενη option και αντιγραφει την τιμη της Home address που υπαρχει σε αυτή στο ομώνυμο πεδιο. Πιθανες αλλαγες στο πεδιο Source address μπορουν να γινουν μονο όταν όλες οι διαθεσιμες options που βρισκονται στην επεκταση ***Destination Option*** έχουν υποστεί επεξεργασία .

ii. Λήψη Binding Updates

Εφοσον ο κομβος λαβει μια Binding update option θα πρεπει να ελεγχξει εαν αυτή πληροί τα παρακάτω κριτηρια:

- Το μήκος του πεδιου Option Length είναι μεγαλυτερο ή ισο με την τιμη που περιγραψαμε σε προηγούμενη παράγραφο.
- Το πακέτο πρέπει να περιέχει τη Home address option
- Η τιμη του πεδιου Sequence number της binding update option πρεπει να είναι μεγαλυτερη από την αντιστοιχη τιμη του προηγουμενου binding update option που ελαβε.

Κάθε binding update option πρεπει να ικανοποιει όλες τις παραπανω προυποθεσεις διαφορετικα απορριπτεται και το πακετο στο οποίο ανηκει δεν υφίσταται καμια περαιτερω επεξεργασια και αγνοειται.

Στην περίπτωση που το binding update option θεωρηθει ως εγκυρο τοτε ακολουθειται η παρακατω διαδικασια:

- Εάν η τιμη του πεδιου Lifetime είναι μη μηδενικη και η Care-of address δεν είναι ίδια με αυτή που καθοριζεται στο binding update option αυτό μεταφραζεται σαν αιτηση αποθηκευσης (cache) του .
- Εάν η τιμη του πεδιου Lifetime είναι μηδενικη ή η Care-of address είναι ίδια με αυτή που καθοριζεται στο binding update option αυτό μεταφραζεται σαν αιτηση διαγραφης ενός αποθηκευμενου (cache) binding update option .

iii. Αποστολή Binding Acknowledgments

Όταν ένας κόμβος λάβει ένα binding update option στο οποίο το bit A έχει την τιμή 1 τότε θα πρέπει να απαντήσει με ένα Binding Acknowledgment με σκοπό να δηλώσει ότι έλαβε το μήνυμα .Εφόσον δέχεται το binding update option και δημιουργεί μια νέα ή ανανεώνει μια παλαιότερη εγγραφή στη Binding Cache που διατηρεί και το bit A έχει την τιμή 1 στο πεδίο Status του Binding Acknowledgment τότε θα πρέπει να δοθεί μια τιμή μικρότερη του 128, διαφορετικά η τιμή του συγκεκριμένου πεδίου θα πρέπει να έχει τιμή μεγαλύτερη ή ίση του 128.

Στην περίπτωση που ο κόμβος απορρίψει τη binding update option πρέπει να αποστείλει ένα Binding Acknowledgment ακόμη και αν το bit

A είχε μηδενική τιμή ενώ το πεδίο Status πρέπει να έχει τιμή μεγαλύτερη ή ίση του 128 .

iv. Αποστολή Binding Requests

Οι έγγραφες που διατηρεί ο κόμβος στη Binding Cache πρέπει να διαγράφουν εάν παρέλθει το χρονικό διάστημα που δηλώνεται στο πεδίο Lifetime. Εάν ο κόμβος , στον οποίο αναφέρεται η έγγραφη ,είναι ενεργός (δηλαδή ανταλλάσσει πακέτα με κάποιο κινητό κόμβο) το επόμενο πακέτο δεδομένων θα προωθηθεί κανονικά προς αυτόν . Ο κινητός κόμβος θα απαντήσει με ένα Binding update προς τον αποστολέα, επιτρέποντας του έτσι την ανανέωση της εγγραφής που διατηρούσε για αυτόν έχοντας μια νέα τιμή στο πεδίο Lifetime. Η επικοινωνία συνεχίζεται κανονικά αλλά το αποτέλεσμα της όλης διαδικασίας θα είναι η καθυστέρηση στην παράδοση των πακέτων.

Εάν ο αποστολέας γνωρίζει ότι η έγγραφη είναι ενεργή στέλνει μια Binding Request option στον κινητό κόμβο με σκοπό την αποφυγή της καθυστέρησης που προκαλείται από την παραπάνω διαδικασία λόγω της διαγραφής και επαναδημιουργίας της εγγραφής που απαιτεί. Η Binding Request option μπορεί να συμπεριληφθεί σε κάθε πακέτο που κατευθύνεται προς τον κινητό κόμβο ενώ η απάντηση του τελευταίου θα είναι μια Binding update option δίνοντας του μια νέα τιμή για το πεδίο Lifetime.

v. Αποστολή πακέτων δεδομένων στον κινητό κόμβο

Πριν την αποστολή κάποιου πακέτου δεδομένων ο αποστολέας θα πρέπει να εξετάσει τη Binding Cache που διατηρεί για να δει εάν υπάρχει κάποια εγγραφή για τη διεύθυνση προορισμού του πακέτου. Εφόσον υπάρχει τότε ο αποστολέας προωθεί το πακέτο, χρησιμοποιώντας μια επικεφαλίδα Router , προς τον κινητό κόμβο .

Στην αντίθετη περίπτωση ,η προώθηση του πακέτου γίνεται χωρίς τη χρήση της προαναφερθείσας επικεφαλίδας. Εάν ο παραλήπτης είναι ένας κινητός κόμβος που βρίσκεται συνδεδεμένος στο home network του, το πακέτο θα φτάσει κατευθείαν σε αυτόν ειδάλλως ,θα αναχαιτιστεί από τον

home agent του και θα προωθηθεί μέσω αυτού στην δεδομένη care-of address του. Κατά την παραλαβή του ο κινητός κόμβος θα αποστείλει μια Binding Update option στον αποστολέα ώστε να δημιουργήσει μια εγγραφή για αυτόν την οποία θα χρησιμοποιήσει κατά την Αποστόλη των επόμενων πακέτων δεδομένων.

5.3. Λειτουργία των Home agents

i. Εγγραφή βασικής Care-Of Address

Όταν ο κόμβος λάβει ένα Binding update πρέπει να το ελέγξει και να αναγνωρίσει τον τύπο της option (δηλαδή τι ζητάει ο αποστολέας από τον παραλήπτη) όπως περιγράψαμε σε παραπάνω ενότητα. Στη συνεχεία θα εξετάσουμε τη διαδικασία με την οποία επεξεργάζεται η option που πληροί τις απαραίτητες προϋποθέσεις και η οποία ζητά από τον παραλήπτη να αναλάβει το ρόλο του home agent για τον υπολογιστή-αποστολέα, εγγράφοντας την care-of address του.

Πριν την επεξεργασία του Binding update ο home agent πρέπει να εκτελέσει μια σειρά από ελέγχους τους οποίους παρουσιάζουμε ευθύς αμέσως:

- Εάν ο αποστολέας δεν είναι δρομολογητης που μπορεί να εξυπηρετήσει ένα home agent τότε το Binding update απορρίπτεται στέλνοντας ένα Binding acknowledgment το οποίο στο πεδίο Status θα έχει τον κωδικό 132 (***home registration not supported***)
- Εάν το Duplicate Address Detection bit έχει την τιμή 1 στο Binding update, ο home agent πρέπει να ελέγξει το home network του κινητού κόμβου ώστε να βρει τη home address του. Στην περίπτωση που δεν ανευρεθεί τότε το Binding update απορρίπτεται στέλνοντας ένα Binding acknowledgment το οποίο στο πεδίο Status θα έχει τον κωδικό 138 (***Duplicate Address Detection Failed***).
- Στην περίπτωση που το Binding update απορριφθεί για κάποιο άλλο λόγο (π.χ ανεπαρκείς πόροι για την υποστήριξη και άλλου κινητού κόμβου) τότε ο home agent θα πρέπει να στείλει ένα Binding acknowledgment στον κινητό κόμβο στο οποίο το πεδίο Status θα έχει τον κατάλληλο κωδικό που θα υποδηλώνει το λόγο της άρνησης .

Εφόσον και μετά τους παραπάνω έλεγχους το Binding update θεωρηθεί έγκυρο τότε ο παραλήπτης αποδέχεται πλέον το ρόλο του home agent για τον κινητό κόμβο . Δημιουργεί μια νέα εγγραφή στη Binding Cache που διατηρεί ,για το συγκεκριμένο κόμβο , και στην οποία διατηρεί τα απαραίτητα στοιχεία. Ως home address του κινητού κόμβου θεωρεί την διεύθυνση αυτή που βρισκόταν στο πεδίο Home Address του πακέτου που έλαβε πρώτο ενώ ως care-of address θεωρεί την διεύθυνση αυτή που βρισκόταν στο πεδίο Source Address του αντίστοιχου πακέτου.

Ο home agent σημειώνει τη συγκεκριμένη εγγραφή ως Home registration. Οι εγγραφές με τον παραπάνω χαρακτηρισμό διαγράφονται από τη Binding Cache μόνο όταν παρέλθει το χρονικό διάστημα που δηλώνεται στο πεδίο Lifetime. Η τιμή του πεδίου αυτού δεν πρέπει να είναι μεγαλύτερη από την αντίστοιχη τιμή που ισχύει στο υποδίκτυο στο οποίο βρίσκεται συνδεδεμένος ο κινητός κόμβος.

Ανεξάρτητα με την τιμή που έχει το bit '**A**' ,ο home agent πρέπει να στείλει ένα Binding Acknowledgment στον κινητό κόμβο και στο οποίο θα δηλώνονται τα εξής:

- Το πεδίο Status πρέπει να έχει μια τιμή η οποία να υποδηλώνει την επιτυχία της διαδικασίας (της εγγραφής του κινητού κόμβου) . Η τιμή αυτή θα πρέπει να είναι μικρότερη του 128 ενώ μέχρι τώρα η μοναδική τιμή στην οποία έχει αποδοθεί κάποια σημασία είναι η τιμή 0 (Binding Update Accepted).
- Η τιμή του πεδίου Sequence Number αντιγράφεται από την αντίστοιχη τιμή που βρίσκεται στο Binding Update.
- Η τιμή του πεδίου Lifetime πρέπει να είναι ίση με το υπολειπόμενο χρονικό διάστημα (όπως αυτό δηλώνεται στη Binding Cache του home agent).
- Η τιμή του πεδίου Refresh πρέπει να έχει τιμή μικρότερη ή ίση από την τιμή του πεδίου Lifetime. Εάν η Binding Cache αποθηκεύεται σε κάποιο μέσο που δεν θα επηρεαστεί από πιθανή αστοχία (crash) του home agent τότε η τιμή του πεδίου Refresh είναι ίση με τιμή του Lifetime, διαφορετικά τίθεται σε μικρότερη τιμή ώστε να δηλώσει στον κινητό κόμβο ότι θα πρέπει να ανανεώσει την εγγραφή του πριν παρέλθει το χρονικό διάστημα πέρα από το οποίο θα θεωρηθεί μη έγκυρη . Ακόμα και δεν γίνει κάτι τέτοιο, ο home agent θα διαγράψει τη συγκεκριμένη εγγραφή από τη Binding Cache που διατηρεί μόνο όταν παρέλθει το χρονικό διάστημα που δηλώνεται στο πεδίο Lifetime.

ii. Διαγραφή βασικής Care-Of Address

Όταν ο κόμβος λάβει ένα Binding update πρέπει να το ελέγξει και να αναγνωρίσει τον τύπο της option (δηλαδή τι ζητάει ο αποστολέας από τον παραλήπτη) όπως περιγράψαμε σε παραπάνω ενότητα. Στη συνεχεία θα εξετάσουμε τη διαδικασία με την οποία επεξεργάζεται η option που πληροί τις απαραίτητες προϋποθέσεις και η οποία ζητά από τον παραλήπτη να μην λειτουργεί πλέον ως ο home agent για τον υπολογιστή-αποστολέα, διαγράφοντας την care-of address του.

Πριν την επεξεργασία του Binding update ο home agent πρέπει να εκτελέσει μια σειρά από ελέγχους τους οποίους παρουσιάζουμε ευθύς αμέσως:

- Εάν ο κόμβος που έλαβε το μήνυμα δεν έχει κάποια στοιχεία στη Binding Cache που διατηρεί για τον αποστολέα τότε απορρίπτει το Binding update και στέλνει ένα Binding Acknowledgment το οποίο στο πεδίο Status έχει την τιμή **137** (***Not Home Agent For This Mobile Node***).

Στην περίπτωση που δεν απορριφθεί το Binding update τότε πρέπει να διαγράψει οποιοδήποτε στοιχείο διατηρούσε στη Binding Cache σχετικά με αυτόν τον κόμβο και να συνεχίσει ως εξής:

- Το πεδίο Status πρέπει να έχει μια τιμή η οποία θα υποδηλώνει ότι η διαδικασία εκτελέστηκε επιτυχώς (μικρότερη του 128). Η μόνη τιμή στην οποία έχει αποδοθεί κάποια σημασία είναι η τιμή 0 με την οποία υποδηλώνεται ότι το Binding update έγινε αποδεκτό.
- Το πεδίο Sequence number αντιγράφεται από το αντίστοιχο πεδίο του Binding update.
- Το πεδίο Lifetime πρέπει να έχει την τιμή μηδέν.
- Το πεδίο Refresh πρέπει να έχει την τιμή μηδέν.

Επιπροσθέτως , ο home agent πρέπει να σταματήσει να αναχαιτίζει πακέτα δεδομένων στο home network του κινητού κόμβου με σκοπό την προώθηση τους σε αυτόν.

iii. Προώθηση πακέτων στον κινητό κόμβο

Για κάθε πακέτο δεδομένων που στέλνεται σε ένα κινητό κόμβο από τον home agent του, ο τελευταίος λειτουργεί ως Correspondent Node όποτε ισχύουν οι διαδικασίες που περιγράψαμε στην παράγραφο 5.2 . Ο home agent χρησιμοποιεί μια επικεφαλίδα Routing για να προωθήσει το πακέτο μέσω της care-of address που δηλώνεται στη Binding Cache .

Για να επιτευχθεί η προώθηση κάθε πακέτου στον κινητό κόμβο ο home agent το τοποθετεί σε ένα εικονικό τούνελ . Ως σημείο εισόδου του τούνελ θεωρείται ο home agent ενώ ως σημείο εξόδου του η care-of address του κινητού κόμβου. Όταν ο home agent ενθυλακώνει ένα πακέτο δεδομένων, τότε θέτει στο πεδίο Source address τη διεύθυνση του και στο Destination address την care-of address του κινητού κόμβου. Όταν το πακέτο φτάσει σε αυτόν εκτελεί decapsulation και το επεξεργάζεται ανάλογα με τις συνθήκες που υπάρχουν.

iv. Λήψη Router Advertisement Messages

Για κάθε link το οποίο ένας δρομολογητής εξυπηρετεί ως home agent διατηρεί μια Home Agents List στην οποία καταγράφονται όλοι οι home agents στο συγκεκριμένο υποδίκτυο. Η λίστα αυτή χρησιμοποιείται στη δυναμική ανεύρεση home agents, διαδικασία που θα περιγράψουμε σε παρακάτω ενότητα. Οι πληροφορίες για τη λίστα αυτή συγκεντρώνονται από τα router advertisement μηνύματα που στέλνουν και στα οποία στο bit **H** έχει δοθεί η τιμή **1**.

Όταν λάβει ένα έγκυρο router advertisement μήνυμα , ο home agent εκτελεί τις ακόλουθες διαδικασίες:

- Εάν το Bit **H** του router advertisement μηνύματος έχει την τιμή μηδέν τότε όλα τα στάδια τα οποία περιγράφουμε στη συνεχεία παραλείπονται. Δεν ορίζεται κάποια ειδική μεταχείριση για μηνύματα αυτού του είδους από το Mobile IP καθώς δεν αποστέλλονται από κάποιο δρομολογητη που λειτουργεί ως home agent.

- Εφόσον δεν ισχύει η παραπάνω περίπτωση, τότε αντιγράφεται η Source address από την IP επικεφαλίδα του router advertisement μηνύματος
- Καθορίζεται από το router advertisement μήνυμα η τιμή του πεδίου Lifetime για τον συγκεκριμένο home agent. (Η τιμή αυτή αντιγράφεται από το πεδίο Router Lifetime του router advertisement μηνύματος) .
- Εάν η διεύθυνση του home agent που έστειλε το router advertisement μήνυμα βρίσκεται ήδη στη Home agents list και το lifetime που δηλώνεται στο νέο μήνυμα έχει μηδενική τιμή διαγράφεται η εγγραφή που διατηρούνταν για αυτόν.
- Διαφορετικά , ανανεώνονται τα στοιχεία που υπήρχαν για αυτόν με τη νέα τιμή του lifetime
- Στην περίπτωση που η διεύθυνση δεν βρίσκεται στη λίστα και η τιμή του πεδίου lifetime δεν είναι μηδέν τότε δημιουργείται μια νέα εγγραφή για το συγκεκριμένο κόμβο.

v. Δυναμική Ανεύρεση Διευθύνσεων Home agents

Ο κινητός κόμβος, ενώ βρίσκεται συνδεδεμένος σε κάποιο foreign network, μπορεί να χρησιμοποιήσει τη μέθοδο δυναμικής ανεύρεσης διευθύνσεων home agents με σκοπό να ανακαλύψει τη διεύθυνση ενός ή περισσοτέρων δρομολογητών που λειτουργούν ως home agents στο υποδίκτυο στο οποίο βρίσκεται. Η συγκεκριμένη διαδικασία μπορεί να φανεί χρήσιμη στην περίπτωση που κάποιοι κόμβοι στο home network του κινητού κόμβου άλλαξαν ρόλο και ενώ αυτός ήταν συνδεδεμένος σε κάποιο foreign network. Για παράδειγμα ο δρομολογητής που λειτουργούσε ως ο home agent του μπορεί να αντικαταστάθηκε από κάποιον άλλο.

Όπως θα περιγράψουμε και στη συνεχεία αναλυτικότερα, ο κινητός κόμβος επιχειρεί την ανακάλυψη των διευθύνσεων των home agents, που βρίσκονται στο ίδιο υποδίκτυο με αυτόν , στέλνοντας ICMP Home Agent Address Discovery Request μηνύματα χρησιμοποιώντας την care-of διεύθυνσηςs και τη source address που βρισκόταν στο πακέτο δεδομένων που έλαβε. Εφόσον ένα μήνυμα τέτοιου είδους , ληφθεί από ένα home agent ,ο κινητός κόμβος θα λάβει ένα ICMP Home Agent Address Discovery Reply το οποίο, στο πεδίο source address θα έχει τη διεύθυνση του home agent .

Στο πεδίο Home agent addresses, του ICMP Home Agent Address Discovery Reply μηνύματος , δίνονται τιμές λαμβάνοντας υπόψην τις εξής παραμέτρους:

- Οι IP διευθύνσεις ,στο πεδίο Home Agent Addresses ,πρέπει να είναι καταχωρημένες έτσι ώστε ως πρώτη να αναγράφεται η διεύθυνση με τη μεγαλύτερη προτίμηση (που αναφέρεται στον home agent που θεωρείται ως ο καταλληλότερος για να εξυπηρετήσει τον κινητό κόμβο).
- Εφόσον υπάρχουν δυο home agents με την ίδια σειρά προτίμησης θα πρέπει να ταξινομηθούν με τυχαίο τρόπο.
- Για να αποφύγουμε την περίπτωση του κατακερματισμού ή της απόρριψης (από κάποιο ενδιάμεσο δρομολογητή) του ICMP Home Agent Address Discovery Reply μηνύματος, στην περίπτωση που το μέγεθος του (συμπεριλαμβάνοντας τη λίστα με τους home agents στο πεδίο Home Agent Addresses) υπερβεί το ελάχιστο MTU που ορίζει το πρωτόκολλο ο home agent περιορίζει τον αριθμό των IP διευθύνσεων. Για να το επιτύχει αυτό απομακρύνει τις IP διευθύνσεις οι οποίες βρίσκονται χαμηλά στη λίστα προτίμησης.

5.4. Λειτουργίες των κινητών κόμβων

i. Αποστολή πακέτων από ένα foreign network

Όταν ο κινητός κόμβος βρεθεί σε ένα foreign network συνεχίζει να χρησιμοποιεί τη home address του σε συνδυασμό με τη χρήση μιας ή περισσοτέρων care-of address . Κατά την αποστολή ενός πακέτου δεδομένων μπορεί να επιλέξει μια από αυτές με βάση τα παρακάτω κριτήρια:

- Σε ότι αφορά τις υπερκείμενες εφαρμογές του Mobile IP πρωτοκόλλου ο κινητός κόμβος χρησιμοποιεί τη home address του, ακόμη και όταν βρίσκεται σε ένα foreign network. Αυτό συμβαίνει επειδή το πρωτόκολλο έχει σχεδιαστεί έτσι ώστε να είναι αντιληπτή, από τέτοιες εφαρμογές , η κίνηση του κόμβου.

Το γεγονός αυτό κάνει ,επίσης , ορατή την κίνηση του κόμβου και στους Correspondent Nodes, με τους οποίους επικοινωνεί . Για τα αποστελλόμενα πακέτα , τα οποία αποτελούν τμήμα συνδέσεων που δημιουργήθηκαν ενώ ο κινητός κόμβος βρισκόταν στο home network, πρέπει να χρησιμοποιηθεί η home address .
Ομοίως και για την περίπτωση που έχουμε αποστελλόμενα πακέτα, τα οποία αποτελούν τμήμα συνδέσεων που δημιουργήθηκαν και συνεχίζουν να χρησιμοποιούνται παρά τη μετακίνηση του κινητού κόμβου. Στις παραπάνω περιπτώσεις το πρωτόκολλο μετατρέπει το πακέτο δεδομένων τοποθετώντας τη home address στην home address option και στο πεδίο Source address την care-of address που χρησιμοποιεί ο κινητός κόμβος. Οι παραπάνω μετατροπές αντιστρέφονται στον κόμβο που παραλαμβάνει το πακέτο, αποκαθιστώντας τη home address ως τη Source address του πακέτου πριν την οποιαδήποτε επεξεργασία του από κάποια εφαρμογή .

- Για επικοινωνία μικρού χρονικού διαστήματος ο κινητός κόμβος μπορεί να επιλέξει την χρησιμοποίηση της care-of address του ως τη source address του πακέτου (οπότε δεν απαιτείται η ύπαρξη της home address option). Εάν ο κινητός κόμβος δεν γνωρίζει , εκ των πρότερων , ότι η επικοινωνία ανήκει στη συγκεκριμένη κατηγόρια δεν θα πρέπει να χρησιμοποιήσει την care-of address του .

Στην περίπτωση που ο κινητός κόμβος βρίσκεται στο αρχικό δίκτυο δεν απαιτείται κάποιου είδους επεξεργασία από τους μηχανισμούς του πρωτοκόλλου. Το ίδιο ισχύει και στην περίπτωση που χρησιμοποιεί κάποια διεύθυνση (διαφορετική από τη home address του) ως πηγή προέλευσης του πακέτου ενώ βρίσκεται σε κάποιο foreign network (σε ότι αφορά τις εφαρμογές που προαναφέραμε).

Για κάθε άλλη περίπτωση (π.χ πακέτα δεδομένων που αποστέλλονται ενώ βρίσκεται σε κάποιο foreign network, χρησιμοποιώντας τη home address του κινητού κόμβου ως πηγή προέλευσης) απαιτείται επεξεργασία του πακέτου με σκοπό την εισαγωγή της Home Address option. Πιο συγκεκριμένα πρέπει να εκτελεστούν τα εξής βήματα:

- Κατασκευάζουμε το πακέτο θέτοντας τη home address του κινητού κόμβου ως τη Source address του πακέτου δεδομένων, θεωρώντας ότι βρίσκεται συνδεδεμένος στο home network του. Αυτό εξασφαλίζει τη διαφάνεια του πρωτοκόλλου σε άλλα υπερκείμενα πρωτόκολλα (π.χ TCP).

- Προσθέτουμε τη Home Address option στο πακέτο με την τιμή του Home Address πεδίου να έχει αντιγράφει από την τιμή του Source Address πεδίου.
- Τοποθετούμε στο πεδίο Source Address την care-of address που χρησιμοποιεί ο κινητός κόμβος.

Με την εκτέλεση της παραπάνω διαδικασίας εξασφαλίζουμε ότι το πακέτο δεδομένων δεν θα αντιμετωπίσει κάποιο πρόβλημα κατά τη δρομολόγηση του.

ii. Λήψη πακέτων δεδομένων στο foreign network

Όταν ο κινητός κόμβος βρίσκεται συνδεδεμένος σε ένα foreign network λαμβάνει πακέτα δεδομένων σύμφωνα με μια από τις παρακάτω μεθόδους:

- Πακέτα που αποστέλλονται από κόμβους, οι οποίοι δεν έχουν στοιχεία στη Binding List για τον κινητό κόμβο-παραλήπτη, μεταχειρίζονται σαν κανονικά IP πακέτα. Στη συνεχεία αναχαιτίζονται από τον home agent και προωθούνται προς την care-of address του κινητού κόμβου.
- Πακέτα που αποστέλλονται από κόμβους, οι οποίοι έχουν στοιχεία στη Binding List για τον κινητό κόμβο-παραλήπτη (μεταξύ αυτών και την care-of address του), προωθούνται με τη χρήση μιας Routing επικεφαλίδας. Το πακέτο δεδομένων κατευθύνεται προς την care-of address του, ενώ στην επικεφαλίδα αναγράφεται η home address του κινητού κόμβου. Η επεξεργασία της επικεφαλίδας γίνεται αποκλειστικά από τον κινητό κόμβο.
- Πακέτα που αποστέλλονται από κόμβους, οι οποίοι έχουν στοιχεία στη Binding List για τον κινητό κόμβο-παραλήπτη (μεταξύ αυτών και την care-of address του η οποία όμως δεν ισχύει πλέον), προωθούνται με τη χρήση μιας Routing επικεφαλίδας. Εάν ο κινητός κόμβος έστειλε ένα Binding Update μήνυμα στον home agent του (ο οποίος βρισκόταν στο προηγούμενο υποδίκτυο στο οποίο ήταν συνδεδεμένος άρα και η care-of address του και εφόσον συνεχίζει να εξυπηρετείται από αυτόν) το πακέτο δεδομένων θα αναχαιτιστεί και θα προωθηθεί από αυτόν τον home agent προς τη νέα care-of address του.

Για τα πακέτα που φτάνουν στον κινητό κόμβο με κάποια από την πρώτη ή την τρίτη μέθοδο θα πρέπει να αποστείλει ένα Binding Update μήνυμα προς τον αποστολέα του πακέτου.

Εάν το πακέτο φτάσει στον κινητό κόμβο ακολουθώντας τη διαδικασία που ορίζουμε στη δεύτερη μέθοδο, το πακέτο θα πρέπει να επεξεργαστεί από αυτόν (και πιο συγκεκριμένα η Routing επικεφαλίδα) ώστε να καταστεί διαθέσιμο και για υπερκείμενα πρωτοκόλλα (π.χ TCP).

iii. Ανίχνευση κίνησης κινητού κόμβου

Ο κινητός κόμβος μπορεί να χρησιμοποιήσει συνδυαστικά, όλους τους διαθέσιμους μηχανισμούς που ορίζονται από το πρωτόκολλο ώστε να καθορίσει εάν έχει μετακινηθεί από ένα υποδίκτυο σε ένα άλλο. Ο βασικός μηχανισμός ανίχνευσης είναι το ***IPv6 Neighbor Discovery***, ο οποίος συμπεριλαμβάνει τους μηχανισμούς Router Discovery και Neighbor Unreachability Detection.

Το Router Discovery χρησιμοποιείται, από τον κινητό κόμβο, για να ανακαλύψει νέους δρομολογητες και προθέματα δικτύων . Για να το επιτύχει αυτό μπορεί να στείλει Router Solicitation messages ή να περιμένει να λάβει Router Advertisement messages.

Βασιζόμενος στα λαμβανόμενα Router Advertisement messages δημιουργεί μια νέα έγγραφη στη Router List που διατηρεί για κάθε νέο δρομολογητη που ανακαλύπτει. Κάθε εγγραφή χαρακτηρίζεται από ένα χρονομετρητή μετά τη λήξη του οποίου (και εφόσον δεν ληφθεί νέο μήνυμα από τον συγκεκριμένο κόμβο) θεωρείται ως μη έγκυρη και διαγράφεται.

Όταν ο κινητός κόμβος βρεθεί σε ένα foreign network επιλέγει ένα δρομολογητη από αυτούς που υπάρχουν στη Router List που διατηρεί και βρίσκεται στο ίδιο υποδίκτυο με αυτόν. Στην περίπτωση αυτή είναι πολύ σημαντικό να μπορεί να αντιληφθεί αν και πότε ο συγκεκριμένος δρομολογητης είναι μη διαθέσιμος ώστε να επιχειρήσει να εγγραφεί με έναν άλλο (μέσω μιας νέας care-of address). Το παραπάνω σενάριο αποκτά ιδιαίτερη σημασία σε περιπτώσεις ασυρμάτων ζεύξεων όπου ο κινητός κόμβος θα πρέπει να δράσει γρήγορα εάν αντιληφθεί ότι πακέτα, προοριζόμενα για αυτόν από τον default δρομολογητη του, έχουν χαθεί.

Για να ανιχνεύσει εάν υπάρχει πρόβλημα επικοινωνίας μεταξύ αυτού και του δρομολογητη του ο κινητός κόμβος χρησιμοποιεί το μηχανισμό Neighbor Unreachability Detection. Ενώ ο κινητός κόμβος στέλνει μηνύματα προς ή μέσω του δρομολογητή του μπορεί να ανιχνεύσει ότι η επικοινωνία μεταξύ τους διεξάγεται κανονικά είτε μεσώ ενδείξεων από υπερκείμενα πρωτόκολλα επικοινωνίας (π.χ αίτηση αποστολής νέων δεδομένων από το TCP) είτε μέσω της λήψης Neighbor Discovery messages που στάλθηκαν ως απάντηση σε κάποιο Neighbor Solicitation message. Παρατηρούμε ότι με τη μέθοδο αυτή μπορούμε να διαπιστώσουμε την ύπαρξη πιθανού προβλήματος μόνο όταν επιχειρείται αποστολή ή λήψη πακέτων δεδομένων.

Η παραπάνω μέθοδος δεν μπορεί να χρησιμοποιηθεί ως αποκλειστική μέθοδος ύπαρξης πιθανού προβλήματος καθώς δεσμεύει σημαντικό μέρος του εύρους του δικτύου. Ως η πλέον ενδεδειγμένη μέθοδος θα πρέπει να θεωρηθεί η αξιολόγηση των Router Advertisement messages τα οποία λαμβάνει ακόμα και όταν δεν ανταλλάσσει πακέτα με το δρομολογητη του. Ιδιαίτερα, εφόσον τα μηνύματα αυτά περιλαμβάνουν και την Advertisement Interval επιλογή, ο κινητός κόμβος μπορεί να τα χρησιμοποιήσει για να διαπιστώσει τη συχνότητα με την οποία τα λαμβάνει καθώς εάν παρέλθει το χρονικό διάστημα το οποίο καθορίζουν χωρίς να ληφθεί κάποιο νέο σημαίνει ότι υπάρχουν προβλήματα στην επικοινωνία τους. Ο αριθμός των μηνυμάτων αυτών τα οποία είναι διατεθειμένος να χάσει ο κινητός κόμβος πριν ξεκινήσει διαδικασίες ανεύρεσης νέου δρομολογητη μπορεί να καθοριστεί ανάλογα με την κίνηση των πακέτων που αναμένεται να χειριστεί. Σε κάθε περίπτωση όμως, γίνεται εύκολα αντιληπτό, ότι θα πρέπει να είναι αρκετά μικρός.

iv. Δημιουργία νέας care-of address

Εφόσον ο κινητός κόμβος διαπιστώσει ότι μετακινήθηκε σε ένα νέο υποδίκτυο (δεν μπορεί να επικοινωνήσει με τον προηγούμενο δρομολογητή ή βρήκε κάποιον νέο) θα πρέπει να δημιουργήσει μια νέα care-of address, η οποία θα ανήκει στο νέο του δίκτυο. Θα πρέπει να σημειώσουμε ότι ο κινητός κόμβος μπορεί να δημιουργήσει μια νέα care-of address ανά πάσα στιγμή με μόνο περιορισμό αυτόν που υπάρχει για την αποστολή Binding Update μηνυμάτων.

Πιο συγκεκριμένα ο κινητός κόμβος δεν πρέπει να αποστέλλει Binding Updates προς τον home agent του, σχετικά με μια νέα care-of address πιο συχνά από μια φορά κάθε MAX UPDATE RATE δευτερόλεπτο. Το MAX UPDATE RATE είναι μια παράμετρος στην οποία δίνεται μια τιμή λαμβάνοντας υπόψη το εύρος ζώνης του δικτύου το οποίο θα δεσμεύσουν αυτά τα μηνύματα.

Η δημιουργία μιας νέας care-of address μπορεί να επιτευχθεί ακόμη και αν ο κινητός κόμβος δεν χρησιμοποιεί έναν νέο δρομολογητη.

Μετά τη δημιουργία μιας νέας care-of address ο κινητός κόμβος μπορεί να εκτελέσει έναν έλεγχο Duplicate Address Detection ώστε να εξακριβώσει τη μοναδικότητα της διεύθυνσης αυτής. Ο εν λόγω έλεγχος, όμως, αποτελεί ένα είδος συμβιβασμού καθώς από τη μια η εξασφαλίζεται η ασφάλεια (καθώς εάν βρεθεί ότι η διεύθυνση αυτή χρησιμοποιείται, απορρίπτεται) ενώ από την άλλη επιβραδύνεται η λειτουργία του δικτύου (καθώς προστίθενται επιπλέον πακέτα δεδομένων σε ένα, πιθανώς, ήδη αργό δίκτυο). Εκτός των παραπάνω ο έλεγχος αυτός συνεπάγεται μια επιπλέον καθυστέρηση πριν ο κινητός κόμβος μπορέσει να χρησιμοποιήσει τη νέα διεύθυνση με αποτέλεσμα την, προσωρινή, απώλεια επικοινωνίας μεταξύ αυτού και των ανταποκρινόμενων κόμβων.

Για την αποφυγή του παραπάνω προβλήματος υπάρχει η δυνατότητα εκτέλεσης του ελέγχου ασύγχρονα, ενώ δηλαδή έχει ήδη ξεκινήσει να τη χρησιμοποιεί.

v. Ανάλυση της δυναμικής ανεύρεσης διευθύνσεων Home Agents

Σε ορισμένες περιπτώσεις, όταν π.χ ο κινητός κόμβος πρέπει να αποστείλει Binding Updates στον home agent του για να εγγράψει την care-of address του, μπορεί να μην γνωρίζει τη διεύθυνση του. Στην περίπτωση αυτή ο κινητός κόμβος μπορεί να επιχειρήσει την ανακάλυψη της διεύθυνσης ενός κατάλληλου home agent στέλνοντας ένα ICMP Home Agent Address Discovery Request message στο αρχικό του υποδίκτυο. Το μήνυμα αυτό δεν πρέπει να περιλαμβάνει την Home Address option, ενώ στο πεδίο Source Address θα πρέπει να δηλώνεται η care-of address του. Όπως προαναφέραμε ο home agent που βρίσκεται στο αρχικό δίκτυο και ο οποίος λαμβάνει το μήνυμα απαντά με ένα ICMP Home Agent Address Discovery Reply message στο οποίο θα δηλώνει τη διεύθυνση του καθώς επίσης και τις διευθύνσεις άλλων home agents στο συγκεκριμένο υποδίκτυο.

Ο κινητος κομβος, αφου λαβει το ICMP Home Agent Address Discovery Reply message, μπορεί να στειλει ένα Binding Update στην IP Source Address διευθυνση (η οποία είναι η διευθυνση του home agent) ή σε καποια από τις υπολοιπες διευθυνσεις που αντιστοιχουν σε αλλους home agents. Είναι δυνατή, για παράδειγμα, η αποστολή σε όλους ενός Binding Update μηνύματος και η αναμονή του Binding Acknowledgment μηνύματος που θα δηλώνει ότι η αίτηση έγγραφης έγινε αποδεκτή, όποτε σταματά και η διαδικασία.

Εάν ο κινητός κόμβος έχει κάποια ενεργή έγγραφη με κάποιον home agent στο home network του (δεν έχει δηλαδή παρέλθει το χρονικό διάστημα που δηλώνεται στο πεδίο Lifetime) τότε θα πρέπει να ξεκινήσει την διαδικασία εγγραφής με το συγκεκριμένο κόμβο πριν δοκιμάσει κάποιον άλλο.

vi. Χρησιμοποίηση πολλαπλών Care-Of Address

Ο κινητός κόμβος έχει τη δυνατότητα να χρησιμοποιεί περισσότερες από μια care-of address ταυτοχρόνως. Πιο συγκεκριμένα, στην περίπτωση που κινείται σε ασύρματα δίκτυα (αναφερόμαστε σε ξεχωριστά επικαλυπτόμενα δίκτυα) μπορεί να δέχεται πακέτα δεδομένων από πολλαπλά links κάνοντας χρήση δυο ή περισσοτέρων care-of addresses.

Θα πρέπει να επιλέξει την βασική care-of address, εφόσον ανιχνεύσει το δίκτυο στο οποίο βρίσκεται κάνοντας χρήση του μηχανισμού ανίχνευσης κίνησης που περιγράψαμε παραπάνω. Στη συνεχεία να εγγραφεί με αυτή στον home agent του στέλνοντας ένα Binding Update μήνυμα, στο οποίο τα bit **A** (Acknowledge) και **H** (Home Registration) θα είναι ενεργοποιημένα. Για να επιτευχθούν ομαλές και γρήγορες εναλλαγές ο κινητός κόμβος διατηρεί και μετά την εγγραφή της νέας care-of address την προηγούμενη καθώς μπορεί να χρειαστεί να την ξαναχρησιμοποιήσει εάν η επόμενη, πιθανή, μετακίνηση του γίνει προς το προηγούμενο δίκτυο (με αποτέλεσμα την εξοικονόμηση χρόνου και την ελάττωση του φόρτου του δικτύου).

vi. Επιστροφή στο Home Network

Ο κινητός κόμβος αντιλαμβάνεται ότι έχει επιστρέψει στο home network του κάνοντας χρήση του μηχανισμού ανίχνευσης κίνησης και πιο συγκεκριμένα όταν οι έλεγχοι δείξουν ότι το πρόθεμα του αρχικού του δικτύου είναι ίδιο με αυτό του δικτύου στο οποίο συνδέθηκε.

Η επόμενη κίνηση του είναι η αποστολή ενός Binding Update μηνύματος προς τον home agent του στο οποίο του ζητά να σταματήσει την αναχαίτιση πακέτων δεδομένων που κατευθύνονται προς αυτόν. Στο συγκεκριμένο μήνυμα πρέπει να θέσει στην care-of address του τη home address. Όπως και στις υπόλοιπες περιπτώσεις αποστολής παρομοίων μηνυμάτων τα bits **A** (Acknowledge) και **H** (Home Registration) πρέπει να είναι ενεργοποιημένα ενώ η αποστολή του θα πρέπει να επαναλαμβάνεται έως ότου λάβει το κατάλληλο Binding Acknowledgment μήνυμα.

Αφού ο κινητός κόμβος στείλει το Binding Update μήνυμα, ο home agent του διαγράφει τα στοιχεία που διατηρούσε για αυτόν στη Binding Cache και βρίσκει τη διεύθυνση του κινητού κόμβου από το πακέτο δεδομένων. Εάν δεν είναι διαθέσιμη σε αυτό, τότε αποστέλλει Neighbor Solicitation μηνύματα με παραλήπτη τη Source IP διεύθυνση του Binding Update. Ο κινητός κόμβος απαντά με την αποστολή ενός Neighbor Advertisement μηνύματος και όσο περιμένει τη λήψη του Binding Acknowledgment δεν απαντά σε κάποιο άλλο Neighbor Solicitation μήνυμα που, πιθανώς, λάβει.

Μετά τη λήψη του Binding Acknowledgment μηνύματος ο κινητός κόμβος στέλνει ένα Neighbor Advertisement μήνυμα προς όλους τους κόμβους που βρίσκονται στο υποδίκτυο στο οποίο ανήκει ώστε να δηλώσει τη link-layer διεύθυνση που αντιστοιχεί στη home address του.

5.5. Συμβατότητα Μεταξύ των Εκδόσεων IPv4 και IPv6

Το Mobile IP σχεδιάστηκε για να λύσει προβλήματα διευθυνσιοδοτησης και προώθησης πακέτων δεδομένων στην περίπτωση που ο κόμβος μετακινηθεί σε διαφορετικά υποδίκτυα και χρειάζεται να επικοινωνεί με άλλους κόμβους κάνοντας χρήση της αρχικής του διεύθυνσης. Με τα συμβατικά πρωτόκολλα κάτι τέτοιο δεν ήταν δυνατόν καθώς το πρόθεμα του αρχικού δικτύου δεν ήταν το ίδιο με αυτό του νέου.

Η παρούσα έκδοση του Mobile IP (v4) σχεδιάστηκε με στόχο να καλύψει τις ανάγκες κινητικότητας ενός κόμβου σε ένα δίκτυο σχεδιασμένο για τη συγκεκριμένη έκδοση του πρωτοκόλλου. Η νέα έκδοση, αν και βρίσκεται σε επίπεδο σχεδιασμού ακόμη, δεν θα είναι απολύτως συμβατή με την προγενέστερη της οπότε ένας IPv4 κόμβος δεν θα μπορεί να λειτουργήσει σωστά όταν μετακινηθεί σε ένα IPv6 υποδικτυο. Στη συνεχεία της ενότητας θα παρουσιάσουμε ένα μηχανισμό επίλυσης προβλημάτων ασυμβατότητας μεταξύ δυο αλληλοσυνδεόμενων δικτύων των παραπάνω εκδόσεων.

Ο μηχανισμός αυτός βασίζεται στη χρησιμοποίηση **Dual Stack** μεταξύ δυο κόμβων IPv4 & IPv6 έκδοσης και εισάγει τον όρο **Address Mapper.** Το address mapper συσχετίζει τη home address του ενός πρωτοκόλλου (π.χ IPv4) με την care-of address του άλλου (π.χ IPv6). Λαμβάνει πακέτα δεδομένων διαφορετικών εκδόσεων και τα προωθεί, με κατάλληλες μετατροπές, προς υπερκείμενα πρωτόκολλα και αντίθετα.

Αναλυτικότερα, ας υποθέσουμε ένα σενάριο κατά το οποίο ένας IPv4 κινητός κόμβος, με IPv4/ IPv6 dual stack επικοινωνεί με έναν IPv4 correspondent node και μετακινείται σε ένα IPv6 υποδικτυο. Εάν το εν λόγω υποδικτυο δεν υποστηρίζει IPv4/ IPv6 δρομολογητες ή IPv4 μηχανισμούς γενικότερα, τότε όλοι οι παραπάνω μηχανισμοί είναι καταδικασμένοι να αποτύχουν. Αυτό γιατί ένας IPv4 κινητός κόμβος μετακινούμενος σε ένα νέο υποδικτυο περιμένει τη λήψη agent advertisement messages σε αυτό. Η IPv6 έκδοση δεν υποστηρίζει τέτοια μηνύματα, και ο κινητός κόμβος δεν μπορεί να ανιχνεύσει τη μετακίνηση του οπότε η διαδικασία της εγγραφής με ένα νέο home agent δεν θα καταστεί δυνατή.

Η κατάσταση είναι ίδια και στην περίπτωση που ο κινητός κόμβος, ευρισκόμενος σε ένα IPv4 υποδικτυο επικοινωνεί με έναν IPv6 κόμβο και μετακινείται σε ένα IPv6 υποδικτυο.

Ένα διαφορετικό σενάριο είναι αυτό κατά το οποίο ένας IPv6 κινητός κόμβος με IPv4/ IPv6 dual stack επικοινωνεί με έναν IPv6 κόμβο και μετακινείται σε ένα IPv4 υποδικτυο, οπότε αναμένει τη λήψη router advertisement messages. Τα συγκεκριμένα μηνύματα, όμως, δεν υποστηρίζονται από IPv4 υποδικτυα οπότε, και σε αυτή την περίπτωση, η διαδικασία της εγγραφής θα αποτύχει.

Η βασική διαπίστωση που συνάγεται από τα παραπάνω είναι ότι οι κινητοί κόμβοι, και στις δυο περιπτώσεις, κάνουν χρήση του dual stack και ότι χρησιμοποιούν IPv4 ή IPv6 για να επικοινωνήσουν με άλλους κόμβους. Σε αυτό το σημείο εισέρχεται το address mapper, το οποίο ξεκινά τις διαδικασίες εγγραφής, binding κτλ ενώ ανιχνεύει εάν ο κινητός κόμβος έχει μετακινηθεί σε υποδικτυα διαφορετικών εκδόσεων ή όχι. Δεσμεύει μια care-of address στο επισκεπτόμενο υποδικτυο και συσχετίζει τη home address της μιας IP έκδοσης με την care-of address της άλλης και στη συνεχεία προωθεί τα πακέτα δεδομένων στον προορισμό τους.

Στη συνέχεια θα κάνουμε συχνή αναφορά στις παρακάτω ορολογίες:

- ***IPv4 only network***

Το υποδικτυο που εφαρμόζει αποκλειστικά διαδικασίες και μηχανισμούς της IPv4 έκδοσης .

- **IPv6 only network**

Το υποδικτυο που εφαρμόζει αποκλειστικά διαδικασίες και μηχανισμούς της IPv6 έκδοσης .

- ***IPv4 mobile node***

κόμβος που υποστηρίζει IPv4/ IPv6 Dual Stack και χρησιμοποιεί μια μοναδική IPv4 διεύθυνση ως διεύθυνση του.

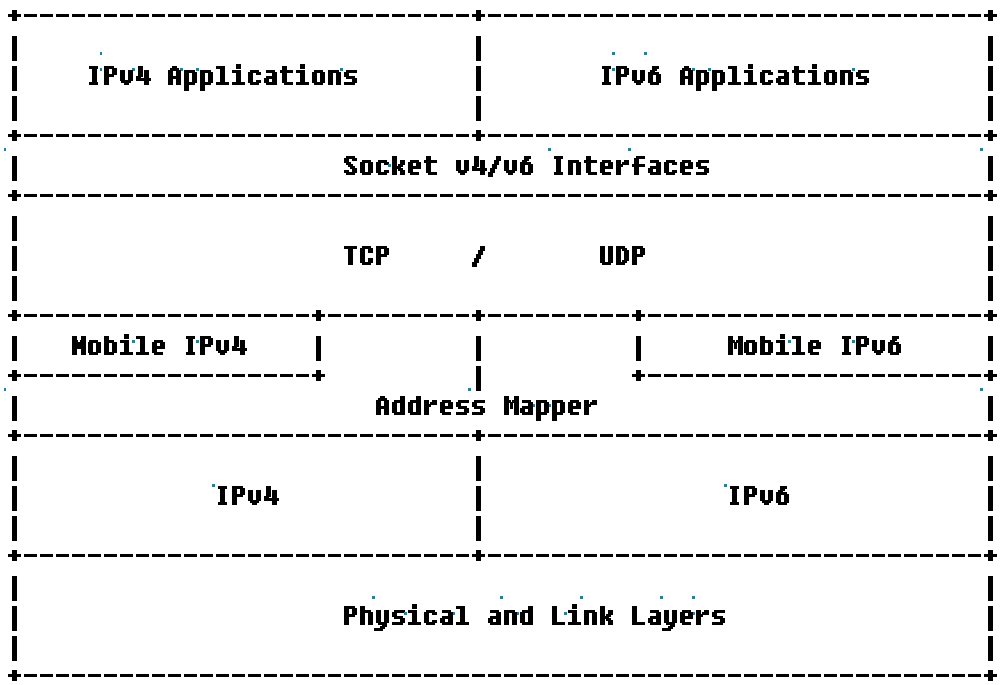
- ***IPv6 mobile node***

Κόμβος που υποστηρίζει IPv4/ IPv6 Dual Stack και χρησιμοποιεί μια μοναδική IPv6 διεύθυνση ως διεύθυνση του.

- ***IPv4/ IPv6 DNS Server***

Ένας Domain Name Server ο οποίος υποστηρίζει IPv4 σε IPv6 και αντίστροφα address mapping και μπορεί να υπηρεσίες αναζήτησης διευθύνσεων σε κόμβους.

Το dual stack μοντέλο, πέρα από τα πρωτόκολλα IPv4 και IPv6 και τις επεκτάσεις τους, χρησιμοποιεί και το address mapper (βλέπε σχήμα).



Οι δυο εκδόσεις του πρωτοκόλλου IPv4 και IPv6 επεξεργάζονται πακέτα δεδομένων IPv4 και IPv6 από και προς τους correspondent nodes αντίστοιχα.

Ο address mapper βρίσκεται μεταξυ του Mobile IP layer και του IP layer. Μπορεί να ανιχνεύσει την ύπαρξη μηνυμάτων του πρωτοκόλλου (ανεξαρτήτως έκδοσης) και να τα προωθήσει σε διαφορετικά IP πρωτόκολλα. Οπότε μπορεί να ανιχνεύσει πιθανή κίνηση μεταξύ IPv4 και IPv6 υποδικτυων και να παραδώσει IPv4 μηνύματα κάνοντας χρήση της IPv6 επικεφαλίδας .

5.6. Εφαρμογή του Address Mapper

Η εφαρμογή του address mapper παρουσιάζεται αναλυτικότερα στα παρακάτω πιθανά σενάρια:

i. Μετακίνηση από IPv4-only network σε IPv6-only network

Αρχικά, θα εξετάσουμε την περίπτωση που ένας κινητός κόμβος με IPv4 διεύθυνση, ως home address, μετακινείται σε ένα IPv6-only network .Εάν το υποδικτυο αυτό υποστηρίζει τη χρήση του Dual Stack ο κινητός κόμβος δεσμεύει μια co-located care-of address και επιχειρεί IPv4 εγγραφή. Στην αντίθετη περίπτωση ο IPv4 κινητός κόμβος δεν μπορεί να λάβει agent advertisement messages όποτε δεν μπορεί να εγγράφει στο home network του. Επειδή όμως, ο κινητός κόμβος είναι IPv4/ IPv6 Dual Stack μπορεί να λάβει τα Router Advertisement messages του IPv6 υποδικτύου. Το Address Mapper ανιχνεύει ότι το υποδικτυο δεν υποστηρίζει Dual Stack αλλά, εφόσον λαμβάνει IPv6 πακέτα δεδομένων συμπεραίνει ότι έχει μετακινηθεί σε ένα IPv6 υποδικτυο. Η IPv6 στοίβα δημιουργεί μια IPv6 care-of address χρησιμοποιώντας το πρόθεμα του επισκεπτόμενου υποδικτύου.

Στη συνεχεία, ο κινητός κόμβος δημιουργεί μια IPv4 διεύθυνση με βάση την αντίστοιχη IPv6 και ανακαλύπτει την IPv6 διεύθυνση του IPv4 home agent του, με την προϋπόθεση ότι και αυτός είναι IPv4/ IPv6 Dual Stack. Η ανακάλυψη των IPv4/ IPv6 διευθύνσεων που προαναφέραμε μπορεί να γίνει με τη βοήθεια DNS αναζητήσεων.

Εφόσον ο home agent είναι IPv4/ IPv6 Dual Stack ο κινητός κόμβος γνωρίζει την IPv6 διεύθυνση του όποτε το address mapper μπορεί να προωθήσει την IPv4 έγγραφη του σε αυτόν. Ο home agent εκτελεί decapsulate στα IPv6 πακέτα δεδομένων, λαμβάνει το μήνυμα αίτησης έγγραφης και μπορεί να ανανεώσει την care-of address του κινητού κόμβου (αν χρειαστεί). Το address mapper δημιουργεί, τέλος, ένα συσχετισμό μεταξύ της αρχικής IPv4 διεύθυνσης και της νέας IPv6 care-of address οπότε (μετά την εγγραφή με τον home agent) τα πακέτα δεδομένων προωθούνται μέσω της care-of address στον home agent.

Όπως διαπιστώνει κανείς από τα παραπάνω, πρόκειται για μια λεπτή διαδικασία για την καλύτερη κατανόηση της οποίας θα παραθέσουμε τα βήματα που απαιτούνται επιγραμματικά:

- Σε ένα IPv4 υποδικτυο, τα IPv4 πακέτα δεδομένων λαμβάνονται και υφίστανται επεξεργασία από τη στοίβα του IPv4 πρωτοκόλλου.
- Εφόσον ο κινητός κόμβος μετακινηθεί σε ένα IPv6 υποδικτυο λαμβάνει τα router advertisement μηνύματα μέσω IPv6 δρομολογητη από την IPv6 στοίβα του πρωτοκόλλου.
- Ο κινητός κόμβος αποκτά μια IPv6 care-of address στο επισκεπτόμενο υποδικτυο, μέσω της IPv6 διεύθυνσης δημιουργεί μια IPv4 διεύθυνση και στη συνεχεία ανακαλύπτει την IPv6 διεύθυνση του home agent του. Σημειώνουμε ότι οι μηχανισμοί με τους οποίους δεσμεύεται μια IPv6 care-of address και χαρτογραφούνται οι IPv4 και IPv6 διευθύνσεις δεν θα αναλυθούν στην παρούσα εργασία.
- Το address mapper προωθεί τα IPv4 μηνύματα εγγραφής στον home agent και δημιουργεί ένα συσχετισμό μεταξύ της home address και της care-of address.
- Τα πακέτα δεδομένων που προορίζονται για τον κινητό κόμβο αρχικά προωθούνται στο home network του απ'οπου ο home agent εκτελεί tunneling προς την IPv4 care-of address. Τα εν λόγω πακέτα υφίστανται decapsulation στον κινητό κόμβο.
- Ο κινητός κόμβος λαμβάνει πακέτα δεδομένων μεσώ του IPv6 πρωτοκόλλου.

ii Μετακίνηση από IPv6-only network σε IPv4-only network

Στην περίπτωση αυτή εγγράφεται με μια IPv6 διεύθυνση και μετακινείται σε ένα IPv4 υποδικτυο, όποτε δεν μπορεί να λάβει IPv6 πακέτα δεδομένων. Εφόσον ο κινητός κόμβος είναι IPv4/ IPv6 Dual Stack λαμβάνει agent advertisement massages από το IPv4 υποδικτυο. Το address mapper ανιχνεύει την μετακίνηση στο IPv4 υποδικτυο και δεσμεύει μια co-located care-of address. Στη συνέχεια δημιουργεί μια IPv6 διεύθυνση (η οποία είναι συμβατή με το IPv4) και ανακαλύπτει την IPv4 διεύθυνση του home agent.

Έχοντας, πλέον, τη διεύθυνση του home agent προωθεί τα μηνύματα εγγραφής του IPv6 σε αυτόν μέσω της IPv4 στοίβας. Ο IPv6 home agent decapsulates τα binding update μηνύματα και ανανεώνει την care-of address του κινητού κόμβου (εάν αυτό χρειαστεί). Τα πακέτα δεδομένων που προορίζονται για τον κινητό κόμβο αρχικά φτάνουν στον home agent και στη συνεχεία οδηγούνται προς τον κινητό κόμβο.

Η παραπάνω διαδικασία μπορεί να συνοψιστεί στα παρακάτω βήματα:

- Σε ένα IPv6 υποδικτυο τα πακέτα δεδομένων λαμβάνονται και υφίστανται επεξεργασία από τον κινητό κόμβο.
- Ο κινητός κόμβος που μετακινείται σε ένα IPv4 υποδικτυο λαμβάνει agent advertisement massages από τον IPv4 foreign agent.
- Δεσμεύει μια IPv4 care-of address και στη συνεχεία, με βάση αυτή, δημιουργεί μια IPv6 διεύθυνση και ανακαλύπτει τη διεύθυνση του home agent.
- Το address mapper προωθεί τα IPv6 μηνύματα στον home agent ο οποίος εκτελεί decapsulate σε αυτά και ανανεώνει την care-of address, αν αυτό είναι απαραίτητο.
- Τα πακέτα δεδομένων που προορίζονται για τον κινητό κόμβο φτάνουν στο home network του και στη συνεχεία προωθούνται προς την IPv4 care-of address όπου και υφίστανται επεξεργασία από τον κινητό κόμβο.

ΚΕΦΑΛΑΙΟ 6

Protocol Security

6.1. Εισαγωγή

Στο συγκεκριμένο κεφαλαίο θα παρουσιάσουμε τις απειλές που καλείται να αντιμετωπίσει το Mobile IP στη νέα του έκδοση (v6). Εξυπακούεται ότι οι ίδιες απειλές υφίστανται και για την παρούσα έκδοση του πρωτοκόλλου ωστόσο θεωρήσαμε σκόπιμο να επικεντρωθούμε στη νέα έκδοση ώστε να έχουμε τη δυνατότητα να παρουσιάσουμε όλες τις τελευταίες εξελίξεις στο συγκεκριμένο θέμα.

Η προσπάθεια μας θα επικεντρωθεί στην παρουσίαση όσο το δυνατόν περισσότερων πιθανών τρόπων παρεμπόδισης της λειτουργίας του πρωτοκόλλου από τη σκοπιά του επιτεθεμένου καθώς και τις πιθανές συνέπειες που θα κληθεί να αντιμετωπίσει ο απλός χρήστης.

Όπως είδαμε, το Mobile IPv6 καθορίζει ότι κάθε κόμβος του μπορεί να λειτουργήσει ως ανταποκρινόμενος κόμβος ο οποίος θα λαμβάνει Binding Update messages και θα αποθηκεύει τα στοιχεία που χρειάζονται, σε κάθε περίπτωση, στη Binding Cache List που διατηρεί. Κάθε κόμβος, όμως, έχει τη δυνατότητα να αγνοήσει τα Binding Update messages που λαμβάνει και να συνεχίσει την αποστολή πακέτων δεδομένων προς την Home address. Επιπροσθέτως, ο correspondent node μπορεί να είναι και ο ίδιος ένας κινητός κόμβος.

Θα πρέπει να σημειώσουμε ότι οι, συντριπτικά, περισσότερες απειλές βασίζονται στη διαδικασία αποστολής-λήψης των Binding Update

messages ιδιαίτερα στην περίπτωση που ο correspondent node επεξεργάζεται το εν λόγω μήνυμα μόνος του, με στόχο τη δημιουργία μιας, μη εξουσιοδοτημένης, εγγραφής στη Binding Cache List ή την επεξεργασία του Home Address πεδίου στην επικεφαλίδα του πακέτου δεδομένων.

Με βάση τις παραπάνω, αρχικές, σκέψεις μπορούμε να καταλήξουμε στο συμπέρασμα ότι ο κινητός κόμβος και ο home agent του θα πρέπει να έχουν δημιουργήσει έναν αμφίδρομο συσχετισμό ασφάλειας μεταξύ τους, πριν ο κινητός κόμβος αρχίσει να μετακινείται σε κάποια αλλά υποδικτυα. Με την παραπάνω υπόθεση δεν εννοούμε ότι ο κινητός κόμβος θα πρέπει να ξεκινά πάντα τη σύνδεση του από το home network, απλά ότι θα πρέπει να έχει υπάρξει κάποιο είδος πιστοποίησης τόσο για το Binding Update Binding μήνυμα όσο και για το Acknowledgment μήνυμα.

Στην πραγματικότητα, όμως, δεν υπάρχει κάποιος συσχετισμός ασφάλειας μεταξύ κινητού και ανταποκρινόμενου κόμβου. Ρόλο σε αυτό διαδραματίζει και η ανυπαρξία κάποιου αλγόριθμου που να μπορεί να χρησιμοποιηθεί για την παραπάνω διαδικασία, δηλαδή να υποστηρίζει ένα δυναμικά μεταβαλλόμενο συσχετισμό ασφαλείας.

Οι επιθέσεις που είναι πιθανό να κληθεί να αντιμετωπίσει ένα Mobile IP δίκτυο κατατάσσονται στις εξής κατηγορίες:

- ***Passive Attacks (Παθητικές επιθέσεις)***

Σε αυτού του είδους τις επιθέσεις ο επιτιθέμενος διαβάζει πακέτα δεδομένων που μετακινούνται στο δίκτυο, αλλά δεν έχει τη δυνατότητα να τα αποθηκεύσει σε κάποιο μέσο για περαιτέρω επεξεργασία. Στην κατηγορία αυτή εντάσσονται οι επιθέσεις ανίχνευσης κωδίκων ασφαλείας (password sniffing attacks).

- ***Active Attacks (Ενεργές επιθέσεις)***

Σε αυτού του είδους τις επιθέσεις ο επιτιθέμενος διαβάζει πακέτα δεδομένων που μετακινούνται στο δίκτυο και έχει τη δυνατότητα να τα αποθηκεύσει σε κάποιο μέσο για περαιτέρω επεξεργασία.

6.2. Γενική επισκόπηση των απειλών

Ως πιο επικίνδυνη απειλή, για το πρωτόκολλο, μπορούμε να θεωρήσουμε την πιθανότητα αλλαγής του προορισμού των πακέτων δεδομένων (redirect). Η επίθεση αυτή έχει ως στόχο τη διαδρομή που ακολουθούν τα πακέτα από τον ένα κόμβο στον άλλο και πραγματοποιείται αλλάζοντας τα μηνύματα έλεγχου ώστε αυτά να καταλήξουν σε υπολογιστή που έχει ορίσει ο επιτιθέμενος . Η παραπάνω διαδικασία επιτρέπει στον επιτιθέμενο να εισέλθει στον, εικονικό, διάδρομο επικοινωνίας που δημιούργησαν οι δυο κόμβοι. Τέτοιου είδους επιθέσεις μπορούν να πραγματοποιηθούν από απομακρυσμένες, γεωγραφικά, θέσεις καθώς οι επιτεθέμενοι δεν χρειάζεται να βρίσκονται στο υποδικτυο με τους κόμβους.

Εξίσου επικίνδυνη απειλή είναι η DoS (***Denial of Service***) επίθεση, με την οποία ο επιτιθέμενος μπορεί να μπλοκάρει κάθε είδους επικοινωνία του κόμβου ή η ύπαρξη ενός επιτιθεμένου σε ένα ασύρματο δίκτυο ο οποίος μπορεί να προκαλέσει το ίδιο αποτέλεσμα.

Με δεδομένη την ανυπαρξία κάποιου συσχετισμού ασφαλείας μεταξύ κινητού και correspondent node συμπεραίνουμε ότι οι δυο κομβόι εκτίθενται σε μεγάλο αριθμό απειλών τις οποίες θα επιχειρήσουμε να ταξινομήσουμε ευθύς αμέσως:

- **Παραποίηση των εγγραφών της Binding Cache List**

-- Δημιουργία μη εξουσιοδοτημένης εγγραφής στον Home agent.
-- Δημιουργία μη εξουσιοδοτημένης εγγραφής στον ανταποκρινόμενο κόμβο.

- **Denial of Service**

-- Παρεμπόδιση της επικοινωνίας του κινητού κόμβου με άλλους κόμβους.
-- Παρεμπόδιση της επικοινωνίας του correspondent node με άλλους κόμβους.
-- Παρεμπόδιση του home agent για την εξυπηρέτηση κινητών κόμβων.

- **Αποκάλυψη κρίσιμων πληροφοριών**

-- Αποκάλυψη κόμβων που λειτουργούν ως home agents

Μετά την ταξινόμηση των απειλών θα επιχειρήσουμε την ίδια διαδικασία και για τους επιτιθέμενους κόμβους ανάλογα με τη θέση που βρίσκονται:

- Κόμβος, οπουδήποτε στο διαδίκτυο που επιτίθεται εναντίον κόμβου που εξυπηρετεί το Mobile IP πρωτόκολλο.
- Κόμβος που βρίσκεται στο ίδιο υποδικτυο με τον κινητό κόμβο
- Κόμβος που βρίσκεται στο ίδιο υποδικτυο με τον ανταποκρινόμενο κόμβο
- Κόμβος που βρίσκεται στο ίδιο υποδικτυο με τον home agent
- Κόμβος που βρίσκεται στο εικονικό τμήμα μεταξύ του ανταποκρινόμενου κόμβου και του home agent
- Κόμβος που βρίσκεται στο εικονικό τμήμα μεταξύ του κινητού κόμβου και του ανταποκρινόμενου κόμβου

6.3. Αναλυτική παρουσίαση των απειλών

Στη συνεχεία θα εξετάσουμε, λεπτομερώς, τις προαναφερθείσες (παράγραφος 6,2) απειλές ανάλογα με τις δυνατότητες του επιτιθεμένου και διατηρώντας την ταξινόμηση που προηγήθηκε. Για κάθε απειλή θα παρουσιάζουμε το σενάριο που εξετάζουμε, την απειλή, το αποτέλεσμα που θα έχει αν εκτελεστεί επιτυχώς καθώς επίσης και τον τρόπο αντίδρασης σε αυτή.

Το σχήμα που ακολουθεί έχει το ρόλο ενός, κατατοπιστικού, ευρετηρίου για τις απειλές που ακολουθούν:

	Attack	Attacker location	Effect	Remarks
A.	1	Anywhere	MITM/DoS	Needs to know Home Address
	2	Anywhere	MITM/DoS	Needs to know Home Address
	3	Anywhere	DoS	No prior knowledge needed
B.	1	MN's link	MITM/DoS	Using only BUs
	2	MN's link	MITM/DoS	Using non-MIPv6 mechanisms
	3	Close to MN	MITM/DoS	Tamper with radio interface
	4	MN's link	MITM/DoS	Tampering Binding Acks
C.	1	CN's link	MITM/DoS	Using non-MIPv6 mechanisms
D.	1	HA's link	MITM/DoS	
	2	HA's link	Multiple	Acting as a Home Agent
E.	1	CN->HA link	Masq/DoS	Attack without BUs
	2	CN->HA link	MITM/DoS	Defeat Home Address check
F.	1	MN->CN link	DoS	Attack without BUs
	2	MN->CN link	MITM/DoS	Immune to ingress filtering
G.	1	MN's (past) link	MITM/DoS	Fool temporary HA
H.	1	Anywhere	Disclosure	Topology information exposed
	2	Anywhere	DDoS	Use HA as a reflector
	3	Anywhere	DDoS	Use CN as a reflector

i. Παραποίηση των πληροφοριών της Binding Cache List

Σενάριο A.1:

Ο κινητός κόμβος ανταλλάσσει πακέτα δεδομένων με ένα correspondent node. Ο επιτιθέμενος κόμβος γνωρίζει την home address του κινητού κόμβου.

Απειλή A.1:

Ο επιτιθέμενος κόμβος μπορεί να στείλει ένα Binding Update μήνυμα στον correspondent node κάνοντας τον να νομίζει ότι ο κινητός κόμβος μετακινήθηκε (όποτε απέκτησε μια νέα care-of address) και ανανεώνει τα στοιχεία που διατηρούσε στην Binding Cache List για αυτόν.

Αποτέλεσμα Α.1:

Τα πακέτα δεδομένων που προορίζονταν για τον κινητό κόμβο κατευθύνονται, τώρα, προς τον επιτιθέμενο κόμβο (redirect). Ο επιτιθέμενος κόμβος χρειάζεται να γνωρίζει τη home address του κινητού κόμβου και, προαιρετικά, τη διεύθυνση κάποιου από τους correspondent nodes.

Ο επιτιθέμενος κόμβος μπορεί να στείλει ένα Binding Update μήνυμα και στον κινητό κόμβο όποτε ουσιαστικά βρίσκεται στο μέσο της διαδρομής που ακολουθούν τα πακέτα από και προς τον κινητό και τον correspondent node (γεγονός που τον καθιστά ικανό να ελέγχει πλήρως την επικοινωνία τους).

Υπενθυμίζουμε ότι η συγκεκριμένη απειλή υφίσταται μόνο όταν δεν υπάρχει κάποιος συσχετισμός ασφάλειας μεταξύ κινητού και correspondent node και αναφέρεται επειδή δεν έχει προταθεί κάποια λύση για αυτό το ζήτημα (αν και θεωρείται βέβαιο ότι θα υπάρξουν λύσεις στο μέλλον).

Αντίδραση Α.1:

Ο κινητός κόμβος αντιλαμβάνεται ότι δεν λαμβάνει πακέτα δεδομένων όποτε στέλνει ένα Binding Update μήνυμα στον correspondent node.

Για την αποφυγή της απειλής αυτής ο correspondent node δεν πρέπει να ανανεώνει τη Binding Cache List που διατηρεί όταν λάβει ένα Binding Update μήνυμα αν δεν ελέγξει, πρώτα, ότι αυτό εστάλη από εξουσιοδοτημένο κόμβο.

Η συγκεκριμένη επίθεση μπορεί να κατηγοριοποιηθεί ως DoS attack.

<u>Σενάριο Α.2:</u>

Ένα ICMP Destination Unreachable μήνυμα μπορεί να σταλεί εάν τα πακέτα δεδομένων από τον correspondent node δεν φτάνουν στην care-of address του κινητού κόμβου.

Απειλή Α.2:

Το παραπάνω μήνυμα μπορεί να σταλεί από επιτιθέμενο κόμβο, εκ μέρους του κινητού κόμβου, σε ένα correspondent node.

Αποτέλεσμα Α.2:

Ο correspondent node διαγράφει τον κινητό κόμβο από τη Binding Cache List που διατηρεί, όποτε τα πακέτα δεδομένων που προορίζονται για αυτόν προωθούνται από τον home agent (με αποτέλεσμα την σημαντική καθυστέρηση στην παράδοση τους) και, εφόσον η συγκεκριμένη επίθεση εκτελεστεί επιτυχώς σε πολλούς κινητός κόμβους, την κατάρρευση του δικτύου.

Και η συγκεκριμένη επίθεση μπορεί να κατηγοριοποιηθεί ως DoS attack.

Αντίδραση Α.2:

Η συγκεκριμένη επίθεση μπορεί να πραγματοποιηθεί, τηρουμένων κάποιων αναλογιών, σε όλα τα πρωτόκολλα επικοινωνίας οπότε δεν μπορούμε να εξάγουμε κάποια σενάρια αντίδρασης ειδικά για το Mobile IP .

Στα παραπάνω σενάρια απειλών εξετάσαμε τους τρόπους με τους οποίους μπορεί να παραποιηθούν τα στοιχεία που υπάρχουν στη Binding Cache List ενός correspondent node. Όπως είδαμε όμως ως τέτοιος μπορεί να θεωρηθεί και ένας κινητός κόμβος (λόγω του ότι είναι η μια άκρη του εικονικού διαδρόμου που δημιουργείται για την παράδοση των πακέτων δεδομένων με την προϋπόθεση ότι στην άλλη άκρη βρίσκεται ένας, επίσης κινητός, κόμβος). Στην περίπτωση αυτή ο κινητός κόμβος διατηρεί και αυτός μια Binding Cache List με στοιχεία για τον κόμβο που βρίσκεται στην άλλη άκρη. Συνεπώς ισχύουν οι απειλές που περιγράψαμε παραπάνω συν μια ακόμα που ισχύει για τη συγκεκριμένη περίπτωση.

<u>Σενάριο Α.3:</u>

Ο κινητός κόμβος κάνει μια VoIP (Voice over IP) κλήση στον, επίσης κινητό, correspondent node και στέλνει ένα Binding Update μήνυμα όποτε και αυτός απαντά με ένα ανάλογο μήνυμα και ανανεώνει της πληροφορίες που διατηρεί στη Binding Cache List του. Ο επιτιθέμενος μπορεί να προσδιορίσει τις διευθύνσεις τους εάν παρακολουθούσε το υποδικτυο με τη χρήση κατάλληλων μέσων.

Απειλή Α.3:

Ο επιτιθέμενος κόμβος μπορεί να στείλει ένα Binding Update μήνυμα είτε στον κινητό είτε στον correspondent node και να διακόψει την επικοινωνία τους. Εφόσον εκτελούσε μια passive attack θα μπορούσε απλά να παρακολουθεί την κλήση και να συλλέγει όποιες πληροφορίες θεωρεί σκόπιμο.

Αποτέλεσμα Α.3:

Το αποτέλεσμα θα είναι η προώθηση των πακέτων δεδομένων σε λάθος προορισμό έχοντας ως αποτέλεσμα το DoS ή παραβίαση προσωπικών δεδομένων λόγω της παρακολούθησης της συνομιλίας .

Αντίδραση Α.3:

Ο τρόπος αντίδρασης στην περίπτωση αυτή είναι όμοιος με αυτόν που περιγράφηκε στην αντίστοιχη παράγραφο του σεναρίου Α.1.

<u>Σενάριο Α.4:</u>

Ο κινητός κόμβος ανταλλάσσει πακέτα δεδομένων με ένα ανταποκρινόμενο κόμβο και ο επιτιθέμενος κόμβος γνωρίζει την home address του κινητού κόμβου.

Απειλή Α.4:

Ο επιτιθέμενος κόμβος ή ένας ιός στέλνουν μεγάλο αριθμό πλαστών Binding Update μηνυμάτων με στόχο την υπερφόρτωση του γεμίζοντας τη Binding Cache List που διατηρεί με στοιχεία που αναφέρονται σε εικονικούς κόμβους παρεμποδίζοντας, έτσι, την εγγραφή άλλων κόμβων.

Αποτέλεσμα Α.4:

Το αποτέλεσμα της επίθεσης είναι η παρεμπόδιση έγγραφης άλλων κόμβων. Και η συγκεκριμένη επίθεση μπορεί να κατηγοριοποιηθεί ως DoS attack.

Αντίδραση Α.4:

Κάθε κόμβος που λαμβάνει Binding Update μηνύματα θα πρέπει να τα εξετάζει μόνο όταν ελέγξει και βεβαιωθεί για την εγκυρότητα τους και την εγκυρότητα του αποστολέα ενώ θα πρέπει να έχει τη δυνατότητα απόρριψης τους.

ii. Απειλές από κόμβους στο ίδιο υποδίκτυο με τον κινητό κόμβο

Υπάρχουν αρκετοί τρόποι οι οποίοι, ανάλογα με το μέσο πρόσβασης που χρησιμοποιούμε (ασύρματα δίκτυα ή Ethernet LAN's), μπορούν να χρησιμοποιηθούν για να εκτελεστεί μια επίθεση σε ένα κινητό κόμβο του πρωτοκόλλου. Η συγκεκριμένη απειλή, την οποία θα παρουσιάσουμε στη συνεχεία, αποτελεί κοινό τόπο για όλα τα πρωτόκολλα επικοινωνίας.

Σενάριο Β.1:

Ειδικότερα, στην περίπτωση των ασύρματων δικτύων, ο επιτιθέμενος θα μπορέσει να αποκτήσει τη δυνατότητα έλεγχου της κατεύθυνσης των πακέτων δεδομένων μόνο στην περίπτωση που καταφέρει να αναλάβει το ρόλο του βασικού δρομολογητη που εξυπηρετεί τον κινητό κόμβο.

Απειλή Β.1:

Έχοντας τη δυνατότητα, παθητικής, παρακολούθησης του δικτύου ο επιτιθέμενος κόμβος μπορεί να ανακαλύψει τη διεύθυνση του correspondent node καθώς επίσης και με ποιο κινητό κόμβο επικοινωνεί είτε ανταλλάσσοντας πακέτα δεδομένων (είτε στέλνοντας Binding Updates). Αυτό θα του επιτρέψει την αποστολή ενός Binding Update μηνύματος στον correspondent node ή στον κινητό κόμβο.

Αποτέλεσμα Β.1:

Το αποτέλεσμα θα είναι η δρομολόγηση των πακέτων δεδομένων σε διαφορετικό, από τον επιθυμητό, προορισμό.

Αντίδραση Β.1:

Το παραπάνω σενάριο μπορεί να αποφευχθεί με τη χρήση ενός είδους πιστοποίησης της νομιμότητας του κόμβου που στέλνει το ληφθέν Binding Update μήνυμα.

<u>Σενάριο Β.1:</u>

Ο επιτιθέμενος δεν αρκείται στην παθητική παρακολούθηση της κυκλοφορίας των πακέτων δεδομένων σε αυτό και επιχειρεί να αναλάβει ένα πιο δραστήριο ρόλο.

Απειλή Β.2:

Επιχειρεί να βρεθεί μεταξύ του κινητού και του correspondent node με σκοπό να "πείσει" τον κινητό κόμβο ότι correspondent node, με τον οποίο συνομιλεί, βρίσκεται στο ίδιο υποδικτυο με αυτόν.

Αποτέλεσμα Β.2:

Ο επιτιθέμενος θα έχει τη δυνατότητα να μεταβάλλει το περιεχόμενο των πακέτων δεδομένων . Σε ένα ασύρματο ή ενσύρματο δίκτυο ο επιτιθέμενος δεν έχει τη δυνατότητα να εμποδίσει τα router advertisement μηνύματα από το να φτάσουν στον κινητό κόμβο. Μπορεί, ωστόσο, να στείλει ο ίδιος ένα τέτοιο μήνυμα (προσποιούμενος το δρομολογητή) αμέσως μετά την αποστολή του αντίστοιχου μηνύματος από τον κανονικό δρομολογητή παρακάμπτοντας, έτσι, τις εντολές που υπάρχουν σε αυτό.

Αντίδραση Β.2:

Εφόσον η παραπάνω απειλή δεν αποτελεί ιδιαίτερο χαρακτηριστικό του πρωτοκόλλου δεν προκύπτει κάποιο συμπέρασμα αποκλειστικά για αυτό.

Σενάριο Β.3:

Κάνοντας χρήση των παραπάνω σεναρίων και έχοντας ασύρματη πρόσβαση σε ένα τοπικό δίκτυο ο επιτιθέμενος μπορεί να οδηγήσει τον κινητό κόμβο σε ένα άλλο δίκτυο στο οποίο θα λειτουργεί ως δρομολογητης. Στην περίπτωση αυτή χρησιμοποιεί το αρχικό δίκτυο, ως ο μοναδικός υπολογιστής σε αυτό.

Απειλή Β.3:

Ο επιτιθέμενος κόμβος θα έχει τη δυνατότητα να ελέγχει τα πακέτα δεδομένων που στέλνει και λαμβάνει.

Αποτέλεσμα Β.3:

Στη συγκεκριμένη περίπτωση ενεργής επίθεσης ο κινητός κόμβος συνεχίζει την επικοινωνία του με τον correspondent node αλλά τα στοιχεία που έχει ο τελευταίος στην Binding Cache List περιέχουν τη διεύθυνση του επιτιθέμενου. Τα παραποιημένα πακέτα δεδομένων οδηγούνται προς τον κινητό κόμβο μεσώ του επιτιθέμενου αφού αλλάξει την care-of address από τη δικιά του σε αυτή του κινητού κόμβου (οπότε ο τελευταίος παραμένει εντελώς ανυποψίαστος για την ύπαρξη του εισβολέα).

Στην περίπτωση ενός ***wide area wireless network (ασύρματο δίκτυο μεγάλης περιοχής)*** η παρεμβολή είναι δυνατή υποκλέπτοντας τα πακέτα δεδομένων μέσω ανίχνευσης της χρησιμοποιούμενης συχνότητα. Πρόκειται για μια εξαιρετικά πολυδάπανη, λόγω του απαιτούμενου εξοπλισμού, διαδικασία η οποία προσφέρει τη δυνατότητα επίθεσης από οποιαδήποτε απόσταση.

Αντίδραση Β.3:

Ο κινητός κόμβος θα πρέπει να έχει τη δυνατότητα πιστοποίησης της ταυτότητας του σημείου πρόσβασης του κάθε χρονική στιγμή.

iii. Απειλές από κόμβους στο ίδιο υποδίκτυο με τον home agent

Σενάριο Γ.1:

Ο κινητός κόμβος βρίσκεται στο home network του όπως και ο επιτιθέμενος κόμβος ο οποίος γνωρίζει τη διεύθυνση του correspondent node.

Απειλή Γ.1:

Η απειλή έγκειται στην δυνατότητα αποστολής Binding update μηνυμάτων στον correspondent node, με τον οποίο επικοινωνεί ο κινητός κόμβος, και να παρεμποδίσει την επικοινωνία τους.

Ο επιτιθέμενος μπορεί να μπει μεταξύ κινητού και ανταποκρινόμενου κόμβου στέλνοντας ένα Binding update μήνυμα, εκ μέρους του ανταποκρινόμενου κόμβου, στον κινητό κόμβο λέγοντας ότι, ο πρώτος, είναι κινητός κόμβος και τη δεδομένη χρονική στιγμή μετακινήθηκε σε άλλο υποδίκτυο. Ταυτόχρονα στέλνει ένα Binding update μήνυμα στον correspondent node λέγοντας ότι η διεύθυνση του κινητού κόμβου είναι η διεύθυνση του. Εφόσον ο ανταποκρινόμενος κόμβος δεν ελέγχει εάν η Home address και η care-of address βρίσκονται στο ίδιο υποδίκτυο ο επιτιθέμενος κόμβος έχει καταφέρει το στόχο του.

Αποτέλεσμα Γ.1:

Το αποτέλεσμα θα είναι η προώθηση των πακέτων δεδομένων σε μια ανεπιθύμητη care-of address, γεγονός που ταξινομεί την επίθεση αυτή σαν DoS attack.

Αντίδραση Γ.1:

Οι κόμβοι θα πρέπει να ελέγχουν εάν ο αποστολέας είναι εξουσιοδοτημένος να στέλνει Binding update μηνύματα, με βάση αξιολόγησης τη home address που δηλώνεται σε αυτά.

<u>Σενάριο Γ.2:</u>

Με τον επιτιθέμενο κόμβο στο ίδιο υποδίκτυο με τον κινητό κόμβο και τον home agent του μπορεί αυτός να υποκλέψει ένα Binding update μήνυμα που στέλνει ο κινητός κόμβος (ενώ βρίσκεται σε κάποιο άλλο υποδίκτυο).

Απειλή Γ.2:

Στη συνέχεια εξαπατά τον home agent, αναγκάζοντας τον να στείλει ένα Binding request μήνυμα στον κινητό κόμβο χωρίς αυτό να χρειάζεται. Τέτοια μηνύματα μπορούν να σταλούν και από άλλους κόμβους καθυστερώντας το δίκτυο.

Αποτέλεσμα Γ.2:

Τα αποτελέσματα της συγκεκριμένης επίθεσης είναι:

1. DoS attack για τον κινητό κόμβο καθώς μπορεί να οδηγήσει σε απόρριψη το Binding update μήνυμα.

2. Ο επιτιθέμενος υποδύεται τον home agent και αναχαιτίζει τα πακέτα δεδομένων που προορίζονται για τον κινητό κόμβο.

3. Ο κινητός κόμβος μπορεί να σταματήσει την αποστολή Binding update μηνυμάτων για να διατηρήσει την τοποθεσία του απόρρητη αν και αποδεικνύεται μάταιο καθώς ο επιτιθέμενος γνωρίζει την care-of address που έχει κάθε στιγμή.

4. Αποστολή μεγάλου αριθμού Binding update μηνυμάτων στον κινητό κόμβο (Binding update flooding).

Αντίδραση Γ.2:

Ο κινητός κόμβος θα πρέπει να πιστοποιεί τα Binding request μηνύματα και να επεξεργάζεται μόνο όσα προέρχονται από κόμβους που βρίσκονται στη binding list του.

Σενάριο Γ.3:

Ο επιτιθέμενος κόμβος βρίσκεται στο ίδιο υποδίκτυο με τον κινητό κόμβο και τον home agent του και παρακολουθεί την επικοινωνία τους.

Απειλή Γ.3:

Όταν το θεωρήσει σκόπιμο μπορεί να στείλει ένα Binding update μήνυμα με το πεδίο Lifetime ίσο με μηδέν.

Αποτέλεσμα Γ.3:

Το αποτέλεσμα θα είναι να διαγράφουν τα στοιχεία που διατηρούνταν για αυτόν στην binding list κάνοντας τον home agent να πιστεύει ότι ο κινητός κόμβος επανήλθε στο home network του (όποτε δεν τον χρειάζεται).

Αντίδραση Γ.3:

Ο home agent θα πρέπει να αυθεντικοποιεί κάθε Binding update μήνυμα που λαμβάνει πριν προχωρήσει σε αλλαγή των στοιχείων της binding list που διατηρεί.

6.4. Συμπεράσματα για την ασφάλεια του πρωτοκόλλου

Με βάση τα πιθανά σενάρια απειλών που αναμένεται να αντιμετωπίσει το πρωτόκολλο και με την εμπειρία που υπάρχει από την προηγούμενη έκδοση καταλήγουμε, στα ακόλουθα συμπεράσματα:

- Απαίτηση για ύπαρξη ασφάλειας για τα Binding Update μηνύματα: Αν και το συμπέρασμα αυτό ήταν από τα προαπαιτούμενα στη σχεδίαση της νέας έκδοσης ο μηχανισμός με τον οποίο θα επιτυγχάνεται κάτι τέτοιο θα πρέπει να καλύπτει τις ιδιαιτερότητες του και για αυτό το λόγο δεν χρησιμοποιείται κάποιος από τους υπάρχοντες .

- Θα πρέπει να είναι εξαιρετικά δύσκολο για ένα επιτιθέμενο που βρίσκεται εκτός του εικονικού τούνελ μεταξύ του κινητού και του correspondent node να υποκλέψει πακέτα δεδομένων και να επιχειρήσει, στη συνέχεια, να τα οδηγήσει κάπου άλλου. Η δυσκολία αυτή θα έγκειται στο γεγονός ότι θα πρέπει να μαντέψει έναν αριθμό (ανάλογα με τον αλγόριθμο κρυπτογράφησης που θα χρησιμοποιεί ο μηχανισμός κλειδώματος) που θα αποτελείται από μεγάλο αριθμό ψηφίων.
- Ο κινητός κόμβος πρέπει να έχει τη δυνατότητα διατήρησης της ανωνυμίας του.
- Πρέπει να έχει τη δυνατότητα να χρησιμοποιήσει εναλλακτικούς αλγόριθμους κρυπτογράφησης (παραλλαγές του ίδιου) και μηχανισμούς .Όλες οι εφαρμογές του πρωτοκόλλου πρέπει να ορίζουν ένα μηχανισμό και αλγόριθμο ο οποίος θα μπορεί να χρησιμοποιηθεί για την επίτευξη συμβατότητας με αλλά πρωτόκολλα.
- Τα Router Advertisement messages που στέλνονται από τον home agent στον κινητό κόμβο πρέπει να χρησιμοποιούν αλγόριθμους κρυπτογράφησης.
- Όλοι οι χρησιμοποιούμενοι μηχανισμοί, συμμετρικοί ή ασύμμετροι, πρέπει να είναι ικανοί να διαμορφωθούν ώστε να διαχειριστούν πιθανές επεκτάσεις του δικτύου.
- Οι αριθμοί των μηνυμάτων έλεγχου που ανταλλάσσονται μεταξύ κινητού κόμβου, ανταποκρινόμενου κόμβου και home agent θα πρέπει να είναι όσο το δυνατόν μικρότεροι ώστε να μην δεσμεύουν μεγάλο μέρος του διαθέσιμου bandwidth. Η παραπάνω απαίτηση πηγάζει από το γεγονός ότι ορισμένοι κινητοί κόμβοι μπορεί να λειτουργούν σε ασύρματα δίκτυα με περιορισμένο εύρος μετάδοσης δεδομένων.
- Ο ανταποκρινόμενος κόμβος πρέπει να έχει τη δυνατότητα απόρριψης Binding Update μηνυμάτων που εστάλησαν από ένα κινητό κόμβο. Εάν συμβεί κάτι τέτοιο ο κινητός κόμβος θα πρέπει να σταματήσει να στέλνει τέτοια μηνύματα για ένα μικρό χρονικό διάστημα.

ΚΕΦΑΛΑΙΟ 7

Εφαρμογή του Mobile IP

7.1. Εισαγωγή

Έχοντας, πλέον, παρουσιάσει αναλυτικά τις εξελίξεις αλλά και τον τρόπο σκέψης του working group που έχει αναλάβει την εξέλιξη του πρωτοκόλλου θα προχωρήσουμε σε πιο πρακτικά ζητήματα. Έτσι στο συγκεκριμένο κεφάλαιο θα επιχειρήσουμε να παρουσιάσουμε τις διαδικασίες και τους τρόπους που ακολουθούνται για την υλοποίηση της εφαρμογής του πρωτοκόλλου στα δυο από τα πιο δημοφιλή λειτουργικά συστήματα (Windows, Linux). Στο σημείο αυτό θα πρέπει να σημειώσουμε ότι θα αναφερθούμε περισσότερο στο λειτουργικό σύστημα Linux, παρά το γεγονός ότι αυτό υπολείπεται σημαντικά σε δημοτικότητα από τα Windows. Ο λόγος είναι λίγο πολύ γνωστός καθώς πρόκειται για ένα λειτουργικό σύστημα το οποίο βασίζεται σε μια εντελώς διαφορετική φιλοσοφία. Έτσι, ενώ το λειτουργικό της Microsoft είναι μια καθαρά εμπορική εφαρμογή, τις οποίας ο κώδικας παρέχεται στους χρηστές ως έχει (δίνοντας τους τη δυνατότητα για μικρές επεμβάσεις σε σημεία που δεν επιδρούν καθοριστικά στη λειτουργία του και απαιτεί την απόκτηση έγγραφης άδειας για πειραματισμούς σε θέματα που άπτονται τον τρόπο λειτουργίας του kernel) ενώ στον αντίποδα τα πράγματα είναι εντελώς διαφορετικά. Το Linux βασίζει την ανάπτυξη του στους απανταχού χρηστές δίνοντας τους τη δυνατότητα να το διαμορφώσουν ανάλογα με τις ανάγκες τους και να εφαρμόσουν τις τελευταίες εξελίξεις που υπάρχουν στον τομέα αυτό δίνοντας τους την ευκαιρία να πειραματιστούν.

7.2. Εφαρμογή του IPv6 στα Windows XP

Οι εξελίξεις που υπάρχουν στο δημοφιλές λειτουργικό (στις διάφορες εκδόσεις του) εστιάζονται σε πειραματισμούς που γίνονται εντός της Microsoft και κάποιων στενά συνεργαζόμενων πανεπιστημίων (Lancaster University) οι οποίες αφορούν το λειτουργικό ***Windows 2000 Server*** και έχουν ως στόχο την ενσωμάτωση της έκδοσης IPv6 (στο πλαίσιο της μετεξέλιξης του Internet γενικότερα, project γνωστό και ως **IP Next Generation (IPng**). Τα αποτελέσματα από τις προσπάθειες αυτές έχουν ενσωματωθεί στην τελευταία και πολυδιαφημισμένη έκδοση, τα ***Windows XP***. Αρχικά, για να διαπιστώσουμε εάν το λειτουργικό είναι συμβατό με την έκδοση IPv6 αρκεί να πληκτρολογήσουμε στην γραμμή εντολών (***Command Prompt***) την εντολή ***ipv6 if***. Εάν είναι εγκατεστημένο θα δούμε τα ***ipv6 interfaces*** και τις ρυθμίσεις τους ενώ διαφορετικά θα λάβουμε αρνητική απάντηση. Στην περίπτωση αυτή πληκτρολογούμε την εντολή ***ipv6 install***. Πρέπει να σημειώσουμε ότι η εντολή αυτή είναι ουσιαστικά μονόδρομος καθώς δεν μπορούμε να το εγκαταστήσουμε ακολουθώντας την κλασσική μέθοδο, δηλαδή στο ***Network Connections folder*** να πατήσουμε το ***Add***.

Οι αλλαγές που έχουν ενσωματωθεί στα υπάρχοντα Winsock (Windows Sockets) βασίζονται στη σύσταση RFC 2553 με τις ακόλουθες εξαιρέσεις:

- Τα header files που ορίζονται σε αυτή δεν εφαρμόζονται στα Windows XP.
- Η δομή των Windows XP socket δεν περιλαμβάνει το sa_len.
- Η χαρτογράφηση των IPv4 διευθύνσεων δεν ακολουθεί το πρότυπο της σύστασης RFC 2525.
- Δεν υποστηρίζουν τις λειτουργίες interface identification όπως αυτές περιγράφονται στο Κεφάλαιο 4.

Η πλατφόρμα Windows SDK (Software Development Kit) ενσωματώνει ένα εκτελέσιμο αρχείο το οποίο ονομάζεται ***Checkv4.exe*** και το οποίο ελέγχει γραμμές κώδικα για να διαπιστώσει αν και τι αλλαγές χρειάζεται να γίνουν σε αυτόν ώστε το λειτουργικό να υποστηρίζει τη νέα έκδοση του πρωτοκόλλου.

Για να δούμε την IPv6 διεύθυνση μας πληκτρολογούμε την εντολή ***ipv6 if*** και στη συνέχεια κοιτάζουμε για το interface με την link-level διεύθυνση μας η οποία θα έχει τη μορφή ***aa-bb-cc-dd-ee-ff***. Ως default επιλογή το λειτουργικό δημιουργεί link-level διευθύνσεις για κάθε interface που αντιστοιχεί σε ένα εγκατεστημένο Ethernet προσαρμογέα δικτύου. Οι διευθύνσεις αυτές θα έχουν το πρόθεμα ***FE::/64***.

Στη συνέχεια παραθέτουμε ένα παράδειγμα που δείχνει το αποτέλεσμα της εντολής ***ipv6 if:***

```
Interface 4: Ethernet: Local Area Connection
uses Neighbor Discovery
link–layer address: 00-b0-d0-23-47-33
preferred link–local fe80::2b0:d0ff:fe23:4733, life infinite
multicast interface–local ff01::1, 1 refs, not reportable
multicast link–local ff02::1, 1 refs, not reportable
multicast link–local ff02::1:ff23:4733, 1 refs, last reporter,
6 seconds until report
link MTU 1500 (true link MTU 1500)
current hop limit 128
reachable time 36500ms (base 30000ms)
retransmission interval 1000ms
DAD transmits 1
Interface 3: 6to4 Tunneling Pseudo–Interface
does not use Neighbor Discovery
preferred global 2002:9d3c:89d9::9d3c:89d9, life infinite
link MTU 1280 (true link MTU 65515)
current hop limit 128
reachable time 0ms (base 0ms)
retransmission interval 0ms
DAD transmits 0
Interface 2: Automatic Tunneling Pseudo–Interface
does not use Neighbor Discovery
preferred link–local fe80::200:5efe:157.60.137.217, life infinite
preferred global ::157.60.137.217, life infinite
```

Link MTU 1280 (true link MTU 65515)
current hop limit 128
reachable time 0ms (base 0ms)
retransmission interval 0ms
DAD transmits 0
Interface 1: Loopback Pseudo–Interface
does not use Neighbor Discovery
link–layer address:
preferred link–local :: 1, life infinite
preferred link–local fe80::1, life infinite
link MTU 1500 (true link MTU 1500)
current hop limit 128
reachable time 40500ms (base 30000ms)
retransmission interval 1000ms
DAD transmits 1

Στο παράδειγμα αυτό το Interface 4 ανταποκρίνεται σε έναν εγκατεστημένο Ethernet προσαρμογέα ο οποίος είναι αυτός που δηλώνεται στον Network Connection folder. Η link-local διεύθυνση για το interface είναι η fe80::d0ff:fe23:4733. Παρατηρώντας την παραπάνω αναφορά μπορεί να διαπιστώσει κανείς αρκετά από αυτά που αναφέραμε στην πράξη με πιο ενδιαφέρον το εξής :

Interface 3: 6to4 Tunneling Pseudo–Interface

Βλέπουμε, δηλαδή την ύπαρξη ενός interface με σκοπό την επίτευξη συμβατότητας μεταξύ των δυο εκδόσεων του πρωτοκόλλου.

Το interface 2 χρησιμοποιείται για το tunneling των πακέτων δεδομένων ενώ το interface 3 για το loopback.

Η link-local διεύθυνση είναι ένας συνδυασμός του προθέματος του δικτύου ***FE80::/64*** και του IPv6 identifier, ο οποίος είναι ένας 64 bit αριθμός που αποκτάται από έναν εξειδικευμένο μηχανισμό. Η διεύθυνση αυτή αντιστοιχίζεται στον προσαρμογέα ενώ αντί του παραπάνω μηχανισμού μπορεί να χρησιμοποιηθεί η μήκους 48 bit διεύθυνση του προσαρμογέα όπως αυτή δηλώνεται στη μνήμη ROM του (Media Access Control address).

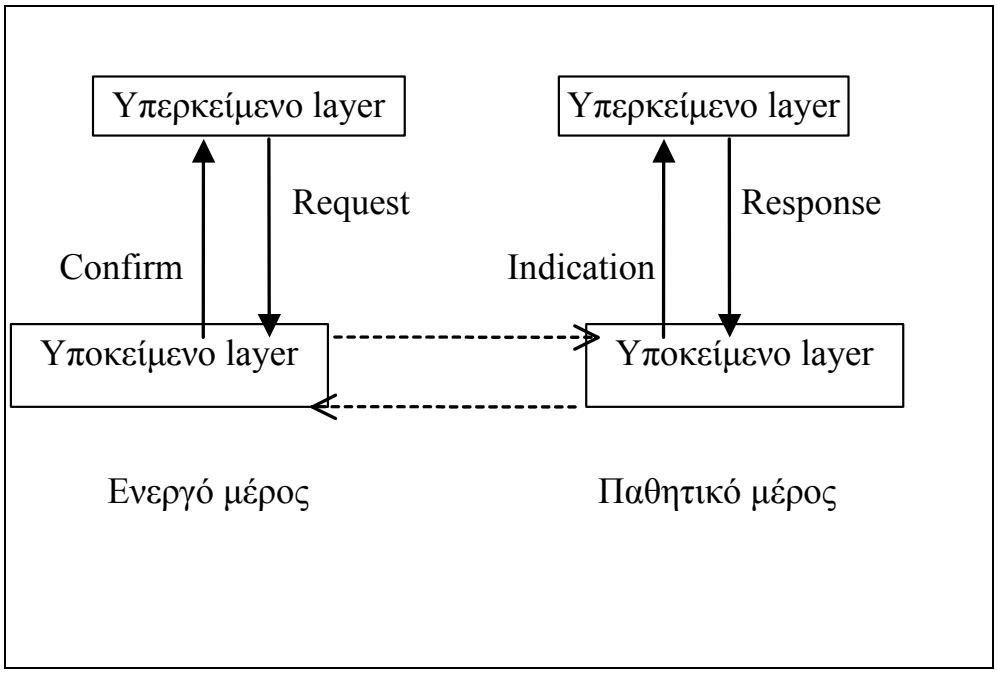
Η απεγκατάσταση του IPv6 μπορεί να γίνει πληκτρολογώντας την εντολή ***ipv6 uninstall*** στη γραμμή εντολών.

7.3. Εφαρμογή του Mobile IPv4 στο Linux

Έχοντας ως βάση τα προηγούμενα κεφάλαια θα επιχειρήσουμε να συνδέσουμε τις λειτουργίες που εκτελεί το πρωτόκολλο με το λειτουργικό σύστημα περιγράφοντας τον τρόπο με τον οποίο πρέπει να προσαρμοστεί ώστε να επιτύχουμε την ομαλή λειτουργία του. Θα ξεκινήσουμε αναλύοντας την αρχιτεκτονική του λειτουργικού, στο βαθμό που μας αφορά, θεωρώντας ορισμένους βασικούς όρους που αυτό εισάγει ως γνωστούς (π.χ daemon).

Στην υλοποίηση που θα αναλύσουμε σε κάθε βασικό στοιχείο του πρωτοκόλλου αντιστοιχεί μια kernel stack και ένας daemon (τον οποίο θα αποκαλούμε και user program) ο οποίος τρέχει στο user space. Η Mobile IP kernel stack εκτελεί όλες τις εργασίες που καθορίζει το πρωτόκολλο και είναι ανεξάρτητη από την αντίστοιχη του TCP/IP ενώ ο daemon παρέχει επιπλέον λειτουργίες κάνοντας πιο ευέλικτη τη χρήση του Mobile IP.

Το user program επικοινωνεί με την kernel stack δημιουργώντας μια ***primitive***. Πρόκειται για ένα μήνυμα μεταξύ δυο επικοινωνούντων layers (π.χ το user space και η kernel stack) με σκοπό την εξυπηρέτηση μιας αίτησης. Η αίτηση αυτή προέρχεται από ένα ενεργό μέρος, όπως ο κινητός κόμβος προς ένα παθητικό όπως ο home agent ή ο foreign agent. Στο ενεργό μέρος ένα υπερκείμενο layer στέλνει μια ***Request primitive,***για να ζητήσει την εξυπηρέτηση μιας λειτουργίας από ένα υποκείμενο layer το οποίο απαντά με μια ***Confirmation primitive*** για να δηλώσει ότι η συγκεκριμένη υπηρεσία είναι διαθέσιμη. Πριν την αποστολή της επιβεβαίωσης τα υποκείμενα layers στα δυο μέρη θα πρέπει να ανταλλάξουν ένα ζεύγος μηνυμάτων για να συγχρονίσουν την παροχή της υπηρεσίας. Χαρακτηριστικό παράδειγμα είναι η αποστολή και η λήψη των Registration request και Registration reply μηνυμάτων. Μετά από αυτό, στο παθητικό μέρος το υποκείμενο layer στέλνει μια ***Indication primitive*** στο υπερκείμενο layer ώστε να ενημερωθεί με τη σειρά του για τη διαθεσιμότητα της υπηρεσίας για να λάβει μια ***Response primitive*** με την οποία θα υποδηλώνεται, από το υπερκείμενο layer, ότι η υπηρεσία θα πρέπει να τεθεί σε ισχύ. Οι παραπάνω διαδικασίες απεικονίζονται στο σχήμα 1, που ακολουθεί:



7.4. Υπηρεσίες Υποστήριξης

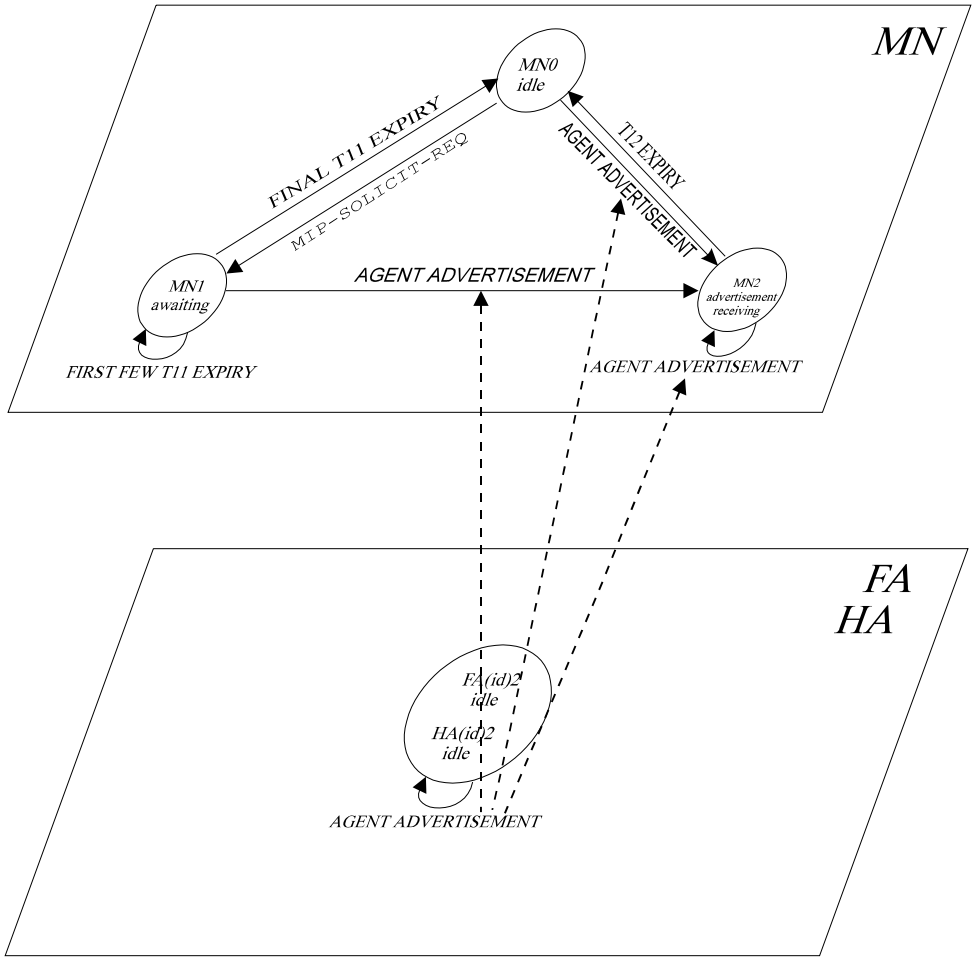
Οι υπηρεσίες υποστήριξης δεν είναι άλλες από την ***agent discovery*** και τη ***registration*** και εφαρμόζονται με τη χρήση ***soft states*** (ενδιαμέσων καταστάσεων). Τα soft states ελέγχονται με κατάλληλους ***timers*** (χρονομετρητές), εκτός από την περίπτωση που είναι αδρανοποιημένες. Η χρήση των timers βελτιώνει τη σταθερότητα του συστήματος ακόμα και σε περιπτώσεις που μηνύματα έλεγχου που αφορούν τις εν λόγω υπηρεσίες δεν έφτασαν στον προορισμό τους.

Στη διαδικασία του agent discovery τόσο ο home agent όσο και ο foreign agent εκτελούν μια διαδικασία μόνο, αποστέλλουν agent advertisement messages ενώ ο κινητός κόμβος μπορεί να βρίσκεται σε μια εκ των τριών καταστάσεων: είτε είναι αδρανής είτε αναμένει είτε λαμβάνει τα συγκεκριμένα μηνύματα .

Στο σημείο αυτό, με στόχο την ευκολότερη κατανόηση, θα ορίσουμε αυθαίρετα χρονομετρητές τους οποίους θα χρησιμοποιήσουμε στα διαγράμματα που θα ακολουθήσουν. Σημειώνουμε ότι, για ευκολία του αναγνώστη, οι timers που θα ξεκινούν με **1** θα αναφέρονται στον κινητό κόμβο (mobile node ή **MN**), με **2** στον foreign agent (**FA**) και με **3** στον home agent (**HA).**

TIMER	ΤΙΘΕΤΑΙ ΑΠΟ	ΧΡΗΣΙΜΟΠΟΙΕΙΤΑΙ ΓΙΑ	ΕΑΝ ΛΗΞΕΙ ΤΟΤΕ ΕΧΟΥΜΕ
T11	**MN**	**Αναμονή κάποιου Solicitation μηνύματος**	**Επανάληψη αποστολής Agent Solicitation**
T12	**MN**	**Διαθεσιμότητα του Agent**	**Διαγραφή των στοιχείων του Agent**
T13	**MN**	**Αναμονή κάποιου Registration μηνύματος**	**Επανάληψη αποστολής Registration Request**
T14	**MN**	**Registration lifetime**	**Ανάλογα με την κατάσταση του**
T22	**FA**	**Χρονικό διάστημα μεταξύ δυο διαδοχικών Advertisement**	**Επανάληψη αποστολής Advertisement μηνύματος**
T23	**FA**	**Αναμονή κάποιου Registration μηνύματος**	**Ανάλογα με την κατάσταση του**
T24	**FA**	**Registration lifetime**	**Ανάλογα με την κατάσταση του**
T32	**HA**	**Χρονικό διάστημα μεταξύ δυο διαδοχικών Advertisement**	**Επανάληψη αποστολής Advertisement μηνύματος**
T33	**HA**	**Αναμονή κάποιου Registration μηνύματος**	**Ανάλογα με την κατάσταση του**
T34	**HA**	**Registration lifetime**	**Ανάλογα με την κατάσταση του**

Μετά την παρουσίαση των timers μπορούμε να παρουσιάσουμε σχηματικά τον τρόπο λειτουργίας της Agent Discovery διαδικασίας αναπαριστώντας ταυτόχρονα τόσο τη λειτουργία του mobile node όσο και αυτή των foreign και home agents.



Διάγραμμα 1.1

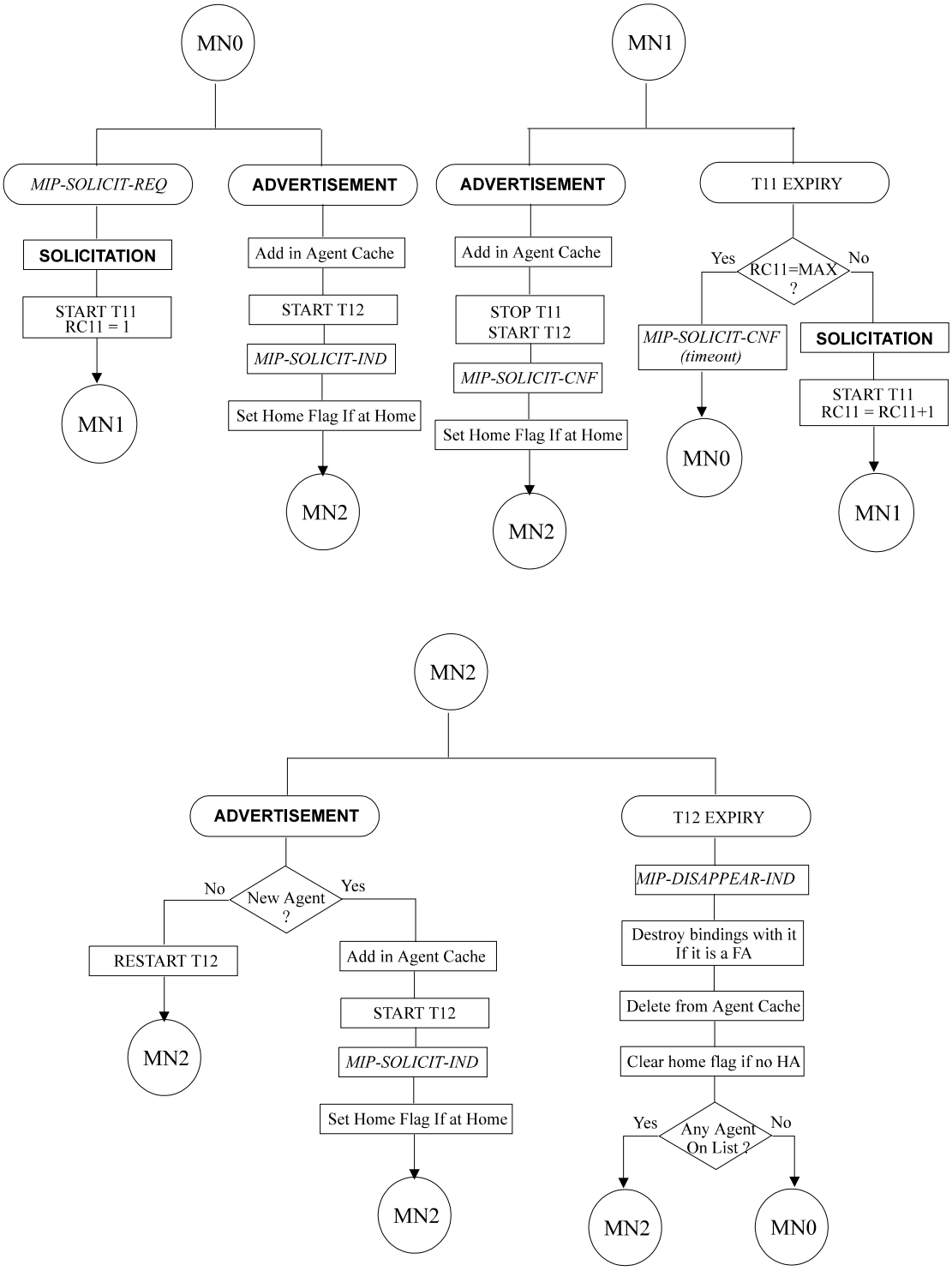
Το διάγραμμα 1.1 μας δείχνει τις μεταβάσεις που εκτελούνται κατά τη διαδικασία του agent discovery.

Ο timer **T11** αφορά την επανάληψη της αποστολής των Agent Solicitation μηνυμάτων ενώ ο **T12** μας δείχνει κατά πόσο ένας agent είναι διαθέσιμος για να εξυπηρετήσει τον κινητό κόμβο ή όχι. Εάν το χρονικό διάστημα που ορίζει παρέλθει ο κινητός κόμβος πλέον δεν έχει καμία σχέση με αυτόν.

Στη συνέχεια θα παραθέσουμε ένα δεύτερο πίνακα με όλα τα είδη των πιθανών primitives ταξινομημένα ανάλογα με τον κόμβο που τα αποστέλλει.

PRIMITIVE	ΚΟΜΒΟΣ	ΛΟΓΟΣ ΑΠΟΣΤΟΛΗΣ
MIP-SOLICIT-REQ	**MN**	**Αίτηση αποστολής Agent Solicitation**
MIP-SOLICIT-CNF	**MN**	**Επιβεβαίωση λήψης Agent Advertisement μετά από MIP-SOLICIT-REQ**
MIP-SOLICIT-IND	**MN**	**Ένδειξη λήψης Agent Advertisement χωρίς κάποια αίτηση**
MIP-DISAPPEAR-IND	**MN**	**Ένδειξη ότι ο agent δεν είναι διαθέσιμος**
MIP-REGISTER-REQ	**MN/FA**	**Αίτηση αποστολής Registration Request**
MIP-REGISTER-RESP	**FA/HA**	**Αίτηση αποστολής Registration Reply**
MIP-REGISTER-IND	**FA/HA**	**Ένδειξη λήψης Registration Request**
MIP-REGISTER-CNF	**MN/FA**	**Επιβεβαίωση λήψης Registration Request**

Η MIP-SOLICIT- REQ primitive στέλνεται από ένα user program ώστε να οδηγήσει τον kernel stack στην αποστολή ενός agent solicitation μηνύματος. Στο διάγραμμα που ακολουθεί, και απεικονίζει τη διαδικασία του agent discovery αποκλειστικά για τον κινητό κόμβο, η MIP-SOLICIT-IND primitive δηλώνει ότι ο kernel stack έλαβε ένα Agent Advertisement μήνυμα ενώ η MIP-SOLICIT-CNF primitive επιβεβαιώνει την αποστολή και λήψη της MIP-SOLICIT- REQ.


MN0
MIP-SOLICIT-REQ
ADVERTISEMENT
SOLICITATION
START T11
RC11 = 1
MN1
Add in Agent Cache
START T12
MIP-SOLICIT-IND
Set Home Flag If at Home
MN2
MN1
ADVERTISEMENT
T11 EXPIRY
Add in Agent Cache
STOP T11
START T12
MIP-SOLICIT-CNF
Set Home Flag If at Home
MN2
Yes
RC11=MAX
?
No
MIP-SOLICIT-CNF
(timeout)
MN0
SOLICITATION
START T11
RC11 = RC11+1
MN1
MN2
ADVERTISEMENT
T12 EXPIRY
No
New Agent
?
Yes
RESTART T12
MN2
Add in Agent Cache
START T12
MIP-SOLICIT-IND
Set Home Flag If at Home
MN2
MIP-DISAPPEAR-IND
Destroy bindings with it
If it is a FA
Delete from Agent Cache
Clear home flag if no HA
Yes
Any Agent
On List ?
No
MN2
MN0

Όταν είμαστε στην κατάσταση **MN0**, στην οποία θεωρούμε ότι ο κινητός κόμβος βρίσκεται σε θέση αναμονής, και ο kernel stack λάβει μια MIP-SOLICIT- REQ primitive τότε στέλνει ένα agent solicitation μήνυμα, θέτει τον timer επανάληψης αποστολής RC11 σε κατάσταση 1 και ο κινητός κόμβος αλλάζει την κατάσταση του στην **MN1** (αναμονή solicitation μηνυμάτων). Εάν λάβει ένα agent advertisement μήνυμα ο kernel stack προσθέτει τα στοιχεία του συγκεκριμένου agent στη λίστα που διατηρεί, ξεκινά τον timer T12 για να διαπιστώσει τη διαθεσιμότητα του παραπάνω agent, ενημερώνει το user program στέλνοντας μια MIP-SOLICIT- IND primitive στο κατάλληλο socket, θέτει σε κατάσταση 1 τον home flag (εάν πρόκειται για μήνυμα που προέρχεται από home agent) και τίθεται σε κατάσταση **MN2** (αναμονή λήψης agent advertisement μηνύματος).

Στην περίπτωση που ο κινητός κόμβος βρίσκεται, αρχικά, στην κατάσταση **MN1** αναμένει τη λήψη agent advertisement μηνύματος σε απάντηση ενός agent solicitation μηνύματος. Όταν λάβει ένα τέτοιο μήνυμα η αντίδραση του kernel stack είναι ίδια με αυτή της περίπτωσης που βρισκόταν στην κατάσταση **MN0** με μόνη διαφορά τον timer T11 που πρέπει να σταματήσει. Εάν παρέλθει το χρονικό διάστημα που αυτός ορίζει και ο κινητός κόμβος δεν έχει φτάσει των μέγιστο αριθμό επανάληψης αποστολής μηνυμάτων (maximum retransmission number), ο kernel stack θα ξαναστείλει το agent solicitation μήνυμα, θα επανεκκινήσει τον timer T11 και θα αυξήσει την τιμή του RC11 timer κατά 1. Εάν συμπληρωθεί ο μέγιστος αριθμός επανάληψης αποστολής μηνυμάτων και δεν έχει ληφθεί ένα agent advertisement μήνυμα ο kernel stack θα στείλει μια MIP-SOLICIT- CNF primitive, η οποία θα περιέχει ένα ειδικό timeout κωδικό για να ενημερώσει το user program για το γεγονός αυτό.

Στην κατάσταση **MN2**, τέλος, ο κινητός κόμβος έχει διαθέσιμους έναν ή περισσότερους home agents. Όταν λάβει ένα agent advertisement μήνυμα ο kernel stack θα το χειριστεί με τον ίδιο τρόπο σαν να βρισκόταν στην κατάσταση **MN0** εάν αυτό προέρχεται από ένα home agent για τον οποίο δεν έχει κάποια στοιχεία. Διαφορετικά, επανεκκινά τον timer T12 για να επαναβεβαιώσει τη διαθεσιμότητα του home agent. Εάν παρέλθει το χρονικό διάστημα που αυτός ορίζει ο kernel stack θα ενημερώσει το user program, μεσώ μιας MIP-DISAPPEAR-IND primitive, ότι ο συγκεκριμένος agent δεν είναι πλέον διαθέσιμος όποτε διαγράφονται όλα τα αποθηκευμένα στοιχεία που υπήρχαν για αυτόν στον agent table και ο home agent flag τίθεται στην κατάσταση 0, εάν δεν υπάρχουν άλλοι home agents. Ο κόμβος παραμένει στην κατάσταση **MN2** έως ότου δεν υπάρχουν άλλοι home agents στον agent table.

Στη διαδικασία του ***Registration*** υπάρχουν ***4 πιθανές καταστάσεις*** για τους ***mobile nodes*** και για τους ***home-foreign agents***. Οι καταστάσεις αυτές είναι:

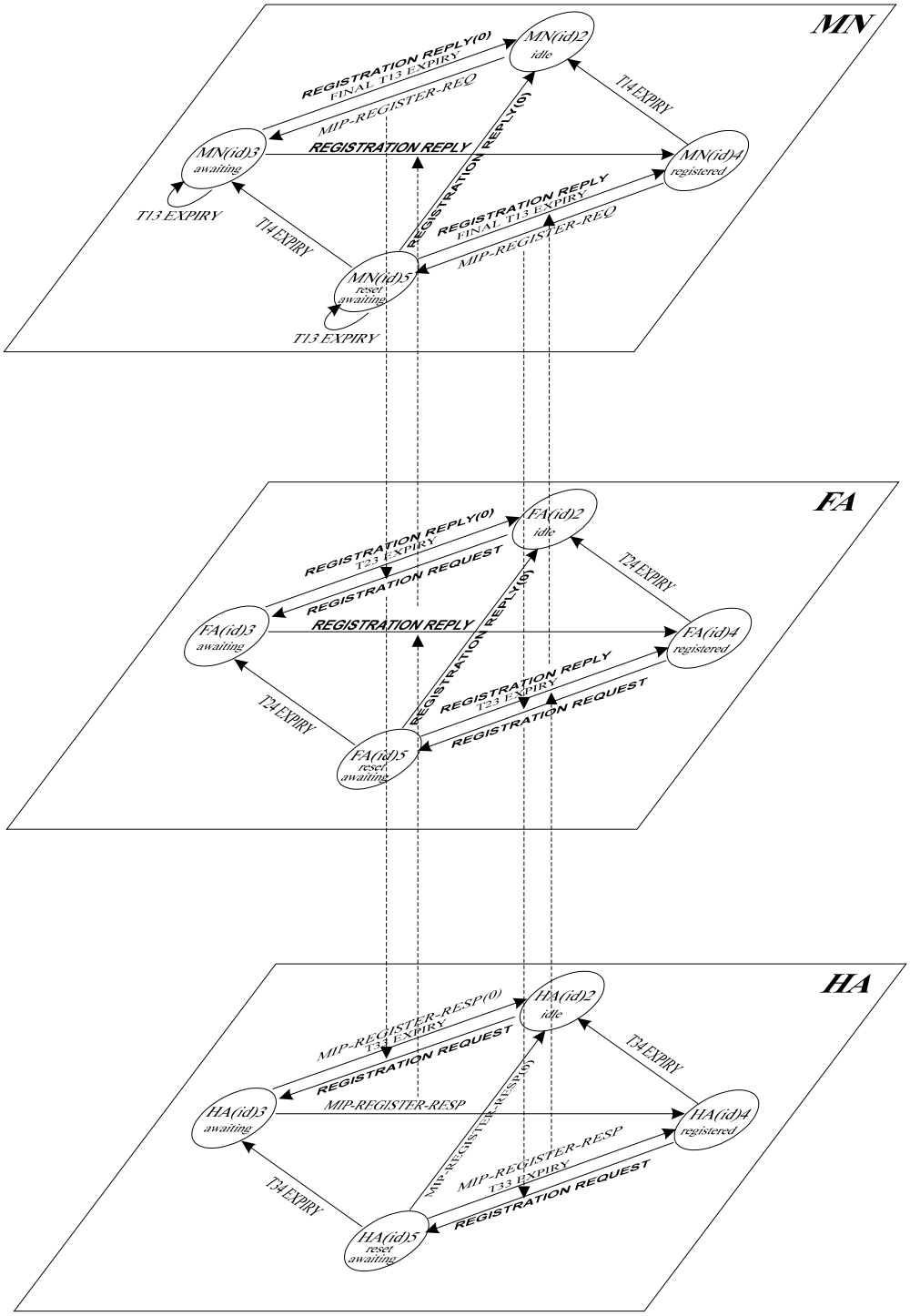
- ***Κατάσταση αναμονής***
- ***Αναμονή επίτευξης εγγραφής***
- ***Επίτευξη εγγραφής***
- ***Αναμονή διαγραφής εγγραφής***

Το παρακάτω διάγραμμα απεικονίζει τις μεταβάσεις που πραγματοποιούνται κατά τη συγκεκριμένη διαδικασία, στον κινητό κόμβο. Λόγω του ότι μπορεί να υπάρχουν πολλαπλές έγγραφες ενός κινητού κόμβου, χρησιμοποιούμε τους κωδικούς MN(id)2, για να αναπαραστήσουμε τη συγκεκριμένη κατάσταση ενώ το id δηλώνει την εγγραφή του κόμβου τη δεδομένη χρονική στιγμή.

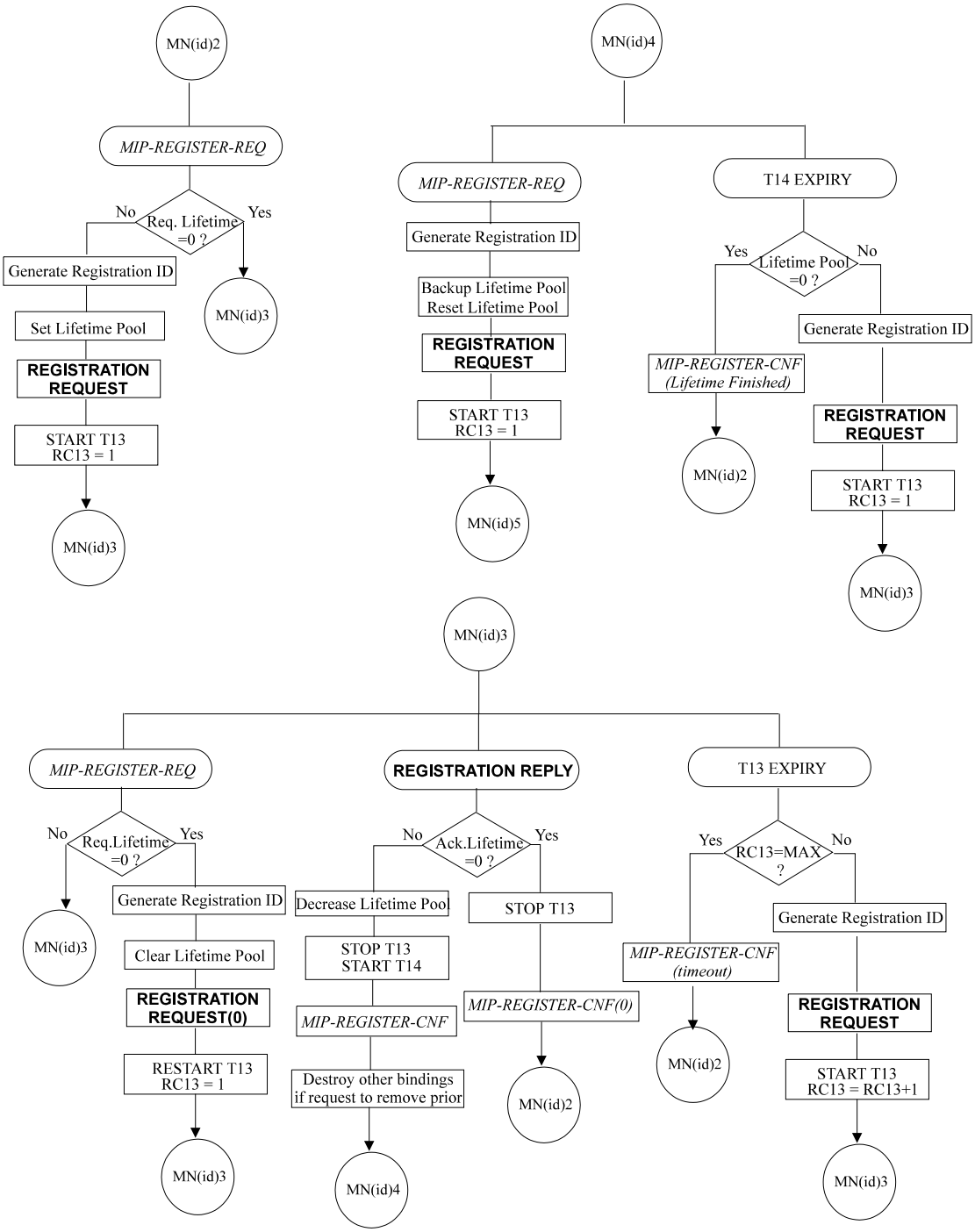
Οι timers T13, T23, T33 χρησιμοποιούνται για να χρονομετρήσουν την αντίδραση σε ένα registration request μήνυμα του κινητού κόμβου, του foreign agent και home agent αντίστοιχα. Η λήξη κάποιου από τους χρονομετρητές θα έχει ως αποτέλεσμα τη μετάθεση της εγγραφής στην προηγούμενη κατάσταση. Πιο συγκεκριμένα, εάν βρίσκεται στην κατάσταση αναμονής επίτευξης εγγραφής θα μετακινηθεί στην κατάσταση αναμονής ενώ αν βρίσκεται σε κατάσταση αναμονής διαγραφής της εγγραφής θα μετακινηθεί στην προηγούμενη κατάσταση, δηλαδή θα παραμείνει εγγεγραμμένος στον agent του. Συμπεραίνουμε, λοιπόν, ότι η προηγούμενη κατάσταση είναι έγκυρη έως ότου σταλεί και επιβεβαιωθεί ένα νέο registration/deregistration μήνυμα.

Οι timers T14, T24, T34 χρησιμοποιούνται για το registration lifetime στον κινητό κόμβο, στον foreign agent και στον home agent αντίστοιχα. Η λήξη κάποιου από αυτούς τους timers σημαίνει ότι το συγκεκριμένο binding θεωρείται ως μη έγκυρο.

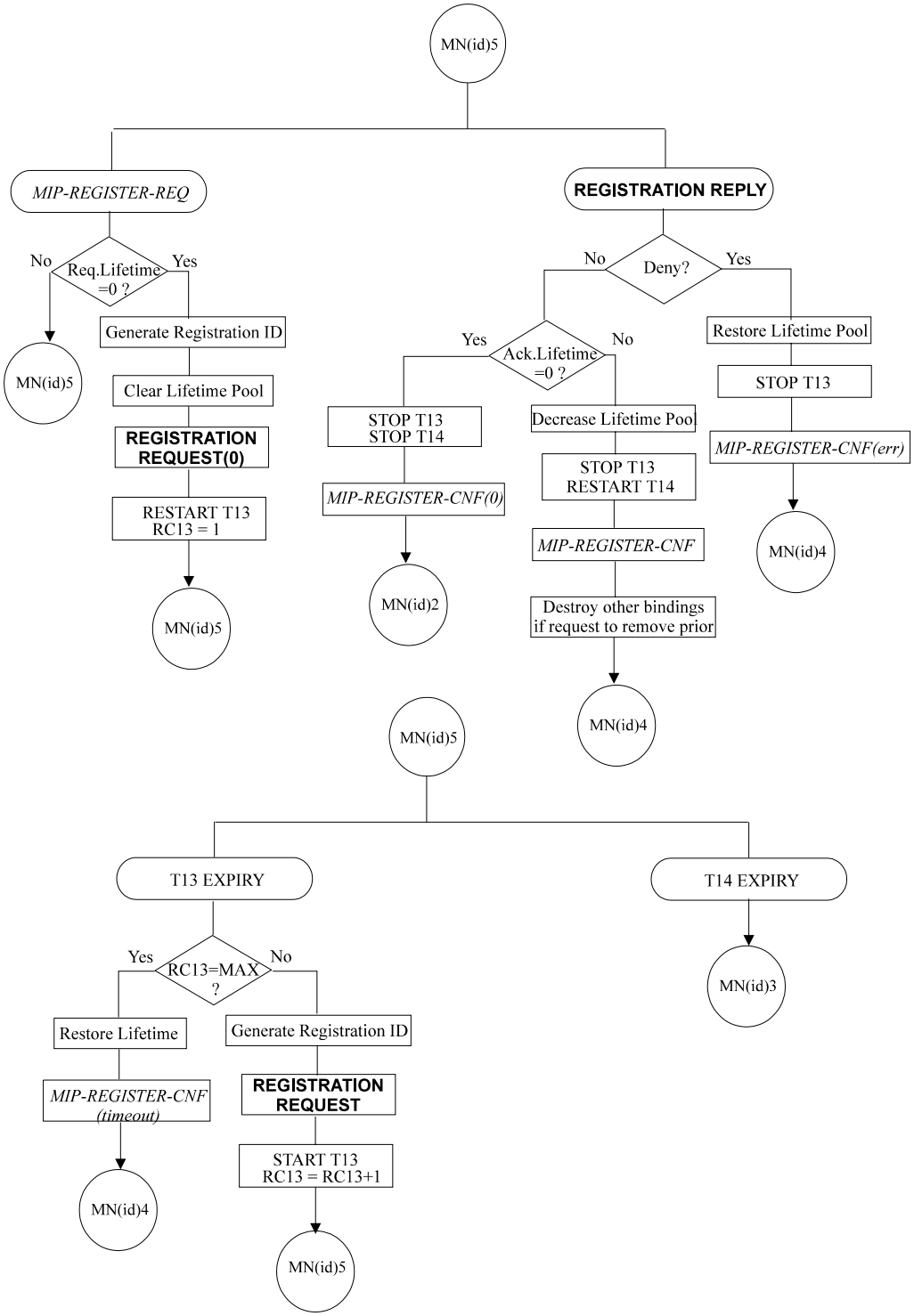
Τα παρακάτω διαγράμματα απεικονίζουν τις πιθανές μεταβατικές καταστάσεις, κατά τη διαδικασία της εγγραφής, για τον κινητό κόμβο.



Οι διακεκομμένες γραμμές υποδηλώνουν την αποστολή μηνυμάτων μεταξύ των κόμβων. Έτσι, όταν ένας κόμβος στέλνει μια MIP-REGISTER-RESP primitive στον kernel stack του home agent αυτός αλλάζει κατάσταση από την HA3 στην HA4 ενώ μεταδίδει registration reply μηνύματα στον foreign agent. Όταν ο foreign agent λάβει τα μηνύματα αλλάζει κατάσταση από την FA3 στην FA4 ενώ προωθεί το μήνυμα στον κινητό κόμβο ο οποίος όταν το λάβει αλλάζει κατάσταση από την MN3 στην MN4 ενώ αποστέλλει μια MIP-REGISTER-CNF primitive στο user program του κινητού κόμβου.



(Συνεχίζεται)


MN(id)5
MIP-REGISTER-REQ
REGISTRATION REPLY
No
Req.Lifetime =0 ?
Yes
Generate Registration ID
MN(id)5
Clear Lifetime Pool
REGISTRATION REQUEST(0)
RESTART T13 RC13 = 1
MN(id)5
No
Deny?
Yes
Yes
Ack.Lifetime =0 ?
No
STOP T13 STOP T14
MIP-REGISTER-CNF(0)
MN(id)2
Decrease Lifetime Poo
STOP T13 RESTART T14
MIP-REGISTER-CNF
Destroy other bindings if request to remove prior
MN(id)4
Restore Lifetime Pool
STOP T13
MIP-REGISTER-CNF(err)
MN(id)4
MN(id)5
T13 EXPIRY
T14 EXPIRY
Yes
RC13=MAX ?
No
Restore Lifetime
MIP-REGISTER-CNF (timeout)
MN(id)4
Generate Registration ID
REGISTRATION REQUEST
START T13 RC13 = RC13+1
MN(id)5
MN(id)3

Στα συγκεκριμένα διαγράμματα η MIP-SOLICIT-CNF primitive χρησιμοποιείται για να επιβεβαιώσει την αποστολή μιας MIP-REGISTER-REQ primitive και σημαίνει ότι ο kernel stack έχει λάβει ένα Registration Reply message.

Στην κατάσταση **MN(id)2**, όταν ο kernel stack λάβει μια MIP-REGISTER-REQ primitive, δεν πραγματοποιείται καμία δράση ενώ τα στοιχεία που υπήρχαν για τη συγκεκριμένη έγγραφη διαγράφονται. Διαφορετικά, ο kernel stack αυθεντικοποιεί την έγγραφη, θέτει το lifetime στην τιμή που ορίζεται από το Registration message, ξεκινά τον T13 timer, θέτει τον RC13 timer στην τιμή 1 και αλλάζει την κατάσταση του σε **MN(id)3**.

Στην κατάσταση **MN(id)3** ο κινητός κόμβος περιμένει να λάβει ένα Registration request message. Όταν γίνει αυτό ο kernel stack σταματά τον timer T13. Εάν το lifetime του μηνύματος είναι ίσο με 0 τότε θα στείλει μια MIP-REGISTER-CNF(0) primitive για να ενημερώσει το user program ότι η αίτηση εγγραφής απορρίφθηκε. Στην αντίθετη περίπτωση ο kernel stack θα προσαρμόσει το lifetime σε αυτό του μηνύματος, θα ξεκινήσει τον timer T14, θα στείλει μια MIP-REGISTER-CNF primitive για να ενημερώσει το user program ότι η αίτηση εγγραφής έγινε αποδεκτή και αλλάζει την κατάσταση του σε **MN(id)4**.

Στην κατάσταση **MN(id)4** ο κινητός κόμβος έχει ήδη κάποιο mobility binding. Όταν λάβει μια MIP-REGISTER-REQ primitive από το user program ο kernel stack επαναυθεντικοποιεί την έγγραφη, αποθηκεύει την τιμή του lifetime για την περίπτωση που η νέα αίτηση εγγραφής αποτύχει, θέτει το lifetime στη νέα τιμή που ορίζει το μήνυμα, ξεκινά τον timer T13, επαναθέτει τον timer RC13 στην τιμή 1 και αλλάζει την κατάσταση του σε **MN(id)3**.

Στην κατάσταση **MN(id)5** ο κινητός κόμβος διατηρεί ένα έγκυρο mobility binding ενώ αναμένει την έγκριση της αίτησης του για μια νέα εγγραφή. Όταν λάβει το Registration Reply message ο kernel stack σταματά τον timer T13. Εάν η αίτηση εγγραφής δεν έγινε αποδεκτή ανακτά την τιμή του lifetime που είχε αποθηκεύσει, ενημερώνει το user program και αλλάζει την κατάσταση του σε **MN(id)4**. Διαφορετικά εάν το lifetime του μηνύματος είναι 0 στέλνει μια MIP-REGISTER-CNF(0) primitive για να ενημερώσει το user program για την απόρριψη της αίτησης και σταματά την προσπάθεια εγγραφής με το συγκεκριμένο agent. Στην αντίθετη περίπτωση ο kernel stack προσαρμόζει το lifetime σε αυτό του μηνύματος, ξεκινά τον timer T14, στέλνει μια MIP-REGISTER-CNF primitive για να ενημερώσει το user program ότι η νέα αίτηση εγγραφής έγινε αποδεκτή και αλλάζει την κατάσταση του σε **MN(id)4**.

Εάν ο timer T13 λήξει ενώ ο κινητός κόμβος βρίσκεται στην κατάσταση **MN(id)5** και δεν έχει φτάσει τον μέγιστο αριθμό των επιτρεπομένων επαναλήψεων εκπομπής ο kernel stack επαναυθεντικοποιεί την έγγραφη, ξαναστέλνει ένα Registration request message, ξαναξεκινά τον timer T13 και αυξάνει την τιμή του timer RC13 κατά 1. Μετά τη συμπλήρωση του μέγιστου αριθμού των επιτρεπομένων επαναλήψεων εκπομπής ο kernel stack στέλνει μια MIP-REGISTER-CNF primitive για να ενημερώσει το user program ότι η νέα αίτηση εγγραφής δεν έγινε αποδεκτή, επαναφέρει την αποθηκευμένη τιμή του lifetime και αλλάζει την κατάσταση του σε **MN(id)4**.

Στην περίπτωση που ο timer T14 λήξει ενώ ο κινητός κόμβος βρίσκεται στην κατάσταση **MN(id)5** τότε το mobility binding που διατηρούσε δεν είναι πλέον έγκυρο όποτε επιστρέφει στην κατάσταση **MN(id)3.**

7.4. ΥΛΟΠΟΙΗΣΗ ΤΟΥ MOBILE IPv4

Με βάση τα παραπάνω εισαγωγικά ως προς τον τρόπο με τον οποίο διαχειρίζεται αλλά και επεμβαίνει το πρωτόκολλο στο λειτουργικό σύστημα ***Linux*** θα παρουσιάσουμε μια πρακτική εφαρμογή του.

Η επιλογή της συγκεκριμένης υλοποίησης έγινε έχοντας ως βασικά κριτήρια την εύκολη εφαρμογή του, για πειραματικούς σκοπούς, την ελευθερία που παρέχει το λειτουργικό σύστημα σε τυχόν αλλαγές και πειραματισμούς καθώς επίσης και για τις μικρές απαιτήσεις που έχει από το δίκτυο στο οποίο εφαρμόζεται.

Για την εξασφάλιση τόσο της σταθερότητας όσο και της συμβατότητας με το υπάρχον δίκτυο επιλέξαμε την έκδοση **MIPv4** και όχι την πολλά υποσχόμενη, αλλά σε πειραματικό στάδιο ακόμη, **MIPv6.**

Η υλοποίηση υποστηρίζει όλες τις δυνατότητες αλλά και τις απαιτήσεις που έχουν τόσο οι κινητοί κόμβοι όσο και οι home agents. Το μεγαλύτερο πλεονέκτημα της, όμως, έγκειται στο γεγονός ότι δεν προϋποθέτει την ύπαρξη κάποιου ειδικά διαμορφωμένου υπολογιστή στο επισκεπτόμενο δίκτυο, ο οποίος θα κληθεί να αναλάβει το ρόλο του foreign agent κερδίζοντας, έτσι, πολλούς πόντους στο θέμα της ευελιξίας. Το γεγονός αυτό έχει επιτευχθεί με την υποστήριξη της μετακίνησης του κινητού κόμβου κάνοντας χρήση **μόνο** co-located care-of address.

Θα πρέπει στο σημείο αυτό να αναφέρουμε ότι εάν στο επισκεπτόμενο δίκτυο βρίσκεται κάποιος υπολογιστής κατάλληλα διαμορφωμένος τότε υπάρχει η δυνατότητα χρησιμοποίησης του και, συνεπώς απόκτησης από τον κινητό κόμβο μιας care-of address.

✓ ΠΑΡΕΧΟΜΕΝΟ SOFTWARE ΓΙΑ ΤΗΝ ΥΛΟΠΟΙΗΣΗ

i) ΜΕΤΑΤΡΟΠΕΣ ΣΤΟΝ KERNEL

Ο kernel της υλοποίησης βρίσκεται στο directory ./kernel και περιλαμβάνει το patch για τον kernel της έκδοσης που θα χρησιμοποιήσουμε.

ii) ΑΛΛΑΓΕΣ ΣΤΟΥΣ DAEMONS

Ο κώδικας που χρειάζεται για τις απαιτούμενες αλλαγές στους daemons βρίσκεται στο directory ./daemons.

iii) SCRIPTS

Κάποια scripts υποστήριξης βρίσκονται στο directory ./scripts. Το ./etc directory περιέχει κάποια απαραίτητα configuration αρχεία ενώ το directory ./sbin περιέχει ένα script που χρησιμοποιείται για τον έλεγχο του daemon του κινητού κόμβου.

iv) ΣΥΝΟΔΕΥΤΙΚΑ ΕΓΓΡΑΦΑ

Οδηγίες χρήσεως βρίσκονται στο directory ./doc .

ΟΔΗΓΙΕΣ ΕΓΚΑΤΑΣΤΑΣΗΣ ΤΗΣ ΥΛΟΠΟΙΗΣΗΣ

Στη συνέχεια, θα περιγράψουμε τις αλλαγές που απαιτείται να γίνουν στον kernel και τους user-level daemons που χειρίζονται τα μηνύματα έλεγχου του πρωτοκόλλου.

i) Εφαρμογή του patch στον kernel

Το patch που χρησιμοποιήσαμε αντιστοιχεί στον kernel έκδοσης 2.2.12, η καρδιά του Redhat 6.1, το οποίο είναι και το λειτουργικό στο έγιναν οι απαραίτητες αλλαγές. Προϋποτίθεται ότι πρέπει να έχουμε σωστά εγκατεστημένο όλο το source tree του kernel.

Πληκτρολογούμε:

```
cd /usr/src

gzip-cd linux-2.2.12.tar.gz |tar xvf -
```

Με τις παραπάνω εντολές τοποθετούμε το source tree του kernel στη σωστή θέση.

Το επόμενο βήμα θα είναι η εφαρμογή του patch στο source tree του kernel. Αρχικά το αντιγράφουμε στη θέση που βρίσκεται το προηγούμενο και αφού πρώτα με την εντολή **cd** έχουμε μετακινηθεί στο αρχικό directory.

Πληκτρολογούμε:

patch -p1< mip-kernel-2.2.5.patch

ii) Διαμόρφωση του kernel

Πληκτρολογούμε:

Make xconfig

και επιβεβαιώνουμε ότι οι παρακάτω επιλογές είναι ενεργοποιημένες, ελέγχοντας τις επιλογές δικτύου (***networking options***).

- ***Mobile IP support***
- ***IP advanced router***
- ***IP tunneling***
- ***Kernel/User netlink socket***
- ***Routing messages***

Πληκτρολογούμε:

cd /usr/include
rm -rf asm linux
ln -s/usr/src/linux/include/asm asm
ln -s/usr/src/linux/include/ linux linux
make bzimage

ώστε να βεβαιωθούμε ότι τα συγκεκριμένα paths οδηγούν στο διαμορφωμένο source tree του kernel

iii) Διαμόρφωση των daemons

Πριν προχωρήσουμε στη διαμόρφωση των daemons πρέπει να ελέγξουμε αν τα paths:

/usr/include/asm
/usr/include/ linux

οδηγούν στον διαμορφωμένο source tree του kernel. Στη συνέχεια πηγαίνουμε στο directory που περιέχει τους daemons και πληκτρολογούμε:

make all

τόσο ο daemon του κινητού κόμβου (***mhd***) όσο και αυτός του home agent ***(had)*** θα έχουν τοποθετηθεί στα directories ./mhd και ./had.

Θα πρέπει να εγκαταστήσουμε το διαμορφωμένο kernel image τόσο στον κινητό κόμβο όσο και στον home agent. Στη συνέχεια αντιγράφουμε τα αρχεία που βρίσκονται στο directory ./scripts στα αντίστοιχα directories.

iv) Home agent

Τοποθετούμε τον daemon had στο /sbin.

v) Κινητός κόμβος

Τοποθετούμε τον daemon mhd στο /sbin.

ΠΑΡΑΜΕΤΡΟΠΟΙΗΣΗ ΚΑΙ ΕΦΑΡΜΟΓΗ ΤΗΣ ΥΛΟΠΟΙΗΣΗΣ

Στην παρούσα ενότητα θα παρουσιάσουμε τις ρυθμίσεις που χρειάζεται να πραγματοποιήσουμε τόσο στον daemon του κινητού κόμβου όσο και στον αντίστοιχο του home agent.

i) Παραμετροποίηση του home agent

Αντιγράφουμε το directory scripts/etc/had.conf στο directory /etc και δίνουμε ιδιαίτερη έμφαση στα παρακάτω σημεία:

- Ο αριθμός των υποστηριζόμενων κινητών κόμβων (όπως αυτός ορίζεται από το keyword ***MOBILE_HOSTS*** το οποίο βρίσκεται στα παραπάνω αρχεία) θα πρέπει να είναι ακριβώς ίδιος με τον αριθμό των γραμμών κώδικα που ακολουθούν και καθορίζουν τους συσχετισμούς ασφάλειας μεταξύ του κινητού κόμβου και του home agent.
- Ο συσχετισμός ασφάλειας μεταξύ ενός κινητού κόμβου και του home agent καθορίζεται από την IP διεύθυνση του κινητού κόμβου, τον υπάρχοντα SPI (Security Parameter Index) και τον αλγόριθμο ασφαλείας που χρησιμοποιείται. Ο SPI είναι ένας ακέραιος αριθμός που επιλέγεται τυχαία με μόνη προϋπόθεση να είναι ίδιος με αυτόν που υπάρχει στα configuration files του κινητού κόμβου.

ii) Παραμετροποίηση του κινητού κόμβου

Αντιγράφουμε το directory scripts/etc/mhd.conf στο directory /etc και ελέγχουμε ότι ισχύουν οι παραπάνω απαιτήσεις. Συνεχίζουμε αντιγράφοντας το directory scripts/etc/mpt.conf στο directory /etc. Τα αρχεία αυτά είναι υπεύθυνα για την επιλογή των κατάλληλων, για κάθε περίπτωση (ανάλογα με την care-of address που χρησιμοποιεί ο κινητός κόμβος) τακτικών που θα ακολουθήσει ο κινητός κόμβος.

Ακολουθεί ένα παράδειγμα των όσων προαναφέραμε:

1) Care-of address=171.64.0.0
2) Netmask=255.255.0.0
3) Entries=2
4) 0.0.0.0 0.0.0.0 80 0 0
5) 0.0.0.0 0.0.0.0 0 1 0

6) Care-of address=0.0.0.0
7) Netmask=0.0.0.0
8) 0.0.0.0 0.0.0.0 80 0 0
9) 171.64.0.0 255.255.0.0 1.1
10) 0.0.0.0 0.0.0.0 0 1 0

Η συγκεκριμένη διαμόρφωση υποδηλώνει ότι έχουμε καθορίσει δυο πιθανές τακτικές, με τις οποίες μπορεί να αντιμετωπιστεί μια care-of address στο δίκτυο **171.64.0.0** με Netmask **255.255.0.0.**

Η πρώτη εγγραφή δηλώνει ότι με προορισμό κάθε δίκτυο (η πρώτη σειρά μηδενικών με τη δεύτερη να είναι η Netmask – γραμμή 4) και χρησιμοποιώντας την port 80 δεν θα πρέπει να χρησιμοποιείται το Mobile IP (η τιμή μηδέν μετά το port) και συνεπώς η αμφίδρομη δρομολόγηση datagrams (η δεύτερη μηδενική τιμή).

Η δεύτερη εγγραφή δηλώνει ότι μπορούμε να χρησιμοποιήσουμε τριγωνική δρομολόγηση με το Mobile IP όταν χρησιμοποιούμε μια care-of address η οποία βρίσκεται εντός των προκαθορισμένων ορίων.

Για όλες τις άλλες πιθανές care-of address υπάρχουν τρεις τακτικές αντιμετώπισης. Η μόνη διαφορά μεταξύ τους είναι ότι τα πακέτα δεδομένων που δεν χρησιμοποιούν την port 80 μπορούν να χρησιμοποιήσουν το Mobile IP με αμφίδρομη δρομολόγηση όταν προορίζονται για το καθορισμένο δίκτυο ενώ διαφορετικά θα πρέπει να χρησιμοποιήσουν την τριγωνική δρομολόγηση σε συνδυασμό με το πρωτόκολλο.

ΕΦΑΡΜΟΓΗ ΤΟΥ ΠΡΩΤΟΚΟΛΛΟΥ

Μετά την ολοκλήρωση των παραπάνω διαδικασιών επανεκκινούμε το σύστημα μας και εκτελούμε τους διαμορφωμένους daemons.

i) Εκκίνηση του home agent

Ο διαμορφωμένος, πλέον, home agent daemon εκτελείται πληκτρολογώντας την εντολή:

/sbin/had-d-v ενώ για debugging πληκτρολογούμε:
/sbin/had-d-d

Εάν θέλουμε ο συγκεκριμένος daemon να ξεκινά κατά την εκκίνηση του υπολογιστή πληκτρολογούμε:

/etc/rc.d/rc.local

ii) Εκκίνηση του κινητού κόμβου

Ο συγκεκριμένος daemon εκτελείται με τη βοήθεια του script mip_start. Κατά τη λειτουργία του παραμένει ενεργός στο background αναμένοντας τη λήψη σημάτων.

Για να εξασφαλίσουμε ότι ο daemon του κινητού κόμβου διατηρεί την έγγραφη με κάποιο home agent θα πρέπει να εκτελέσουμε μια από τις παρακάτω διαδικασίες:

- Εάν ο κινητός κόμβος χρησιμοποιεί μια co-located care-of address, τόσο το interface όσο και ο κατάλογος των διαθέσιμων δρομολογητών θα πρέπει να έχουν ρυθμιστεί σαν να πρόκειται για κάποιο συνηθισμένο host. Στη συνέχεια αφήνουμε τον daemon να αναλάβει δουλεία πληκτρολογώντας mip_start ή mip_restart.
- Εάν θέλουμε να αναζητήσουμε ένα foreign agent απομακρύνουμε τον κατάλογο των διαθέσιμων δρομολογητών (ως ένα είδος απόδειξης ότι ο κινητός κόμβος δεν γνωρίζει το σημείο πρόσβασης του στο Διαδίκτυο) πριν εκτελέσουμε τον daemon. Αυτός θα ξεκινήσει την αναζήτηση και, όταν βρει κάποιον foreign agent, θα δημιουργήσει εκ νέου ένα κατάλογο διαθέσιμων δρομολογητών.

Στο συνοδευτικό cd περιέχονται, εκτός της πτυχιακής και της παρουσίασης (αρχεία Mobile IP.doc και **Mobile IP.ppt** αντίστοιχα) και ο kernel για την έκδοση RedHat 6.1 (αρχείο ***linux-2.4.8.tar.gz*** και το patch με τις απαραίτητες μετατροπές (αρχείο ***MosquitoNet-MIP-2.0.2beta.tar.gz***).Υπάρχει, επίσης, το αρχείο ***Checkv4.exe*** για κάποιον που επιθυμεί να πειραματιστεί με τα Windows.

Βιβλιογραφία

http://MosquitoNet.Stanford.edu/mip

http://www.ietf.org

http://www.cisco.com

http://www.linuxhq.com

http://www.computer.org/internet/v2n1/perkins.htm

http://playground.sun.com/pub/mobile-ip/

http://mip.ee.nus.edu.sg/

http://www.cis.ohio-state.edu/~jain/refs/wir_refs.htm

http://www.acm.org/crossroads/xrds7-2/mobileip.html

http://www.birdstep.com/wireless_infrastructure/mobile_ip.php3

http://www.iprg.nokia.com/~charliep/txt/commag97/paper.ps

http://www.tiaonline.org

RFC 2002
RFC 2003
RFC 2005
RFC 2344

"Supporting Mobility in MosquitoNet"
Mary G.Baker, Stuart Cheshire, Xinhua Zhao
"Flexible Network Support for Mobility"
Xinhua Zhao, Claude Castellucia, Mary G.Baker

Η συγκεκριμένη εργασία είναι αφιερωμένη στην οικογένεια μου για την υλική και, κυρίως, για την ηθική υποστήριξη που μου παρείχαν και συνεχίζουν να μου προσφέρουν απλόχερα.