ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ (ΤΕΙ)
ΠΕΛΟΠΟΝΝΗΣΟΥ
ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
(ΣΠΑΡΤΗ)
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Θέμα:

Παρουσίαση του πρωτοκόλλου Mobile IP

ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΣΠΟΥΔΑΣΤΗ: Λυμπερόπουλος Κωνσταντίνος
Αριθμός Μητρώου: 2010171

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: Μποζαντζής Βασίλης

ΣΠΑΡΤΗ, 2017

ΔΗΛΩΣΗ ΜΗ ΛΟΓΟΚΛΟΠΗΣ ΚΑΙ ΑΝΑΛΗΨΗΣ ΠΡΟΣΩΠΙΚΗΣ ΕΥΘΥΝΗΣ

"Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ενυπογράφως ότι είμαι αποκλειστικός συγγραφέας της παρούσας Πτυχιακής Εργασίας, για την ολοκλήρωση της οποίας κάθε βοήθεια είναι πλήρως αναγνωρισμένη και αναφέρεται λεπτομερώς στην εργασία αυτή. Έχω αναφέρει πλήρως και με σαφείς αναφορές, όλες τις πηγές χρήσης δεδομένων, απόψεων, θέσεων και προτάσεων, ιδεών και λεκτικών αναφορών, είτε κατά κυριολεξία είτε βάση επιστημονικής παράφρασης.

Αναλαμβάνω την προσωπική και ατομική ευθύνη ότι σε περίπτωση αποτυχίας στην υλοποίηση των ανωτέρω δηλωθέντων στοιχείων, είμαι υπόλογος έναντι λογοκλοπής, γεγονός που σημαίνει αποτυχία στην Πτυχιακή μου Εργασία και κατά συνέπεια αποτυχία απόκτησης του Τίτλου Σπουδών, πέραν των λοιπών συνεπειών του νόμου περί πνευματικών δικαιωμάτων.

Δηλώνω, συνεπώς, ότι αυτή η Πτυχιακή Εργασία προετοιμάστηκε και ολοκληρώθηκε από εμένα προσωπικά και αποκλειστικά και ότι, αναλαμβάνω πλήρως όλες τις συνέπειες του νόμου στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δε μου ανήκει διότι είναι προϊόν λογοκλοπής άλλης πνευματικής ιδιοκτησίας."

Όνομα και Επώνυμο Συγγραφέα: ΚΩΝΣΤΑΝΤΙΝΟΣ ΛΥΜΠΕΡΟΠΟΥΛΟΣ

Υπογραφή:

Ημερομηνία: 29 ΜΑΪΟΥ 2017

Ευχαριστίες

Καταρχάς αισθάνομαι την ανάγκη να ευχαριστήσω θερμά τον καθηγητή μου Μποζαντζή Βασίλη, για την ενθάρρυνση του καθώς και για την πολύτιμη καθοδήγηση του στον σχηματισμό της δομής της εργασίας.
Επίσης θα ήθελα να ευχαριστήσω τα μέλη της οικογένειας μου και τους φίλους που με στήριξαν ψυχολογικά στην προσπάθεια περάτωσης της εργασίας μου.

Περίληψη

Η παρούσα διπλωματική εργασία πραγματεύεται τεχνολογίες, που αφορούν το πρωτόκολλο Mobile IP. Δίνονται σταδιακά όλες οι απαραίτητες έννοιες που απαιτούνται για τον τρόπο λειτουργίας του και εφαρμογές του πρωτόκολλου.

Παραθέτονται τα κάτωθι στοιχεία αναλυτικά στα κεφάλαια της εργασίας:

- Περιγραφή της υποδομής που είναι αναγκαία για τα δίκτυα υπολογιστών, κατηγοριοποίηση των δικτύων σύμφωνα με την περιοχή την οποία καλύπτουν, την τοπολογία και τους τρόπους μετάδοσης.
- Αναφορά στο πρωτόκολλο ασύρματης επικοινωνίας 802.11.
- Αναφορά στο πρωτόκολλο Mobile IP, ανάλυση των εκδόσεων IPv4 και IPv6 του πρωτοκόλλου. Παρουσιάζονται υλοποιήσεις του πρωτοκόλλου σε λειτουργικό σύστημα Linux και αναλύονται επιπρόσθετες ανάγκες που καλύπτει η έκδοση αυτή.
- Αναφορά στο MDM, εφαρμογή του πρωτοκόλλου για τον απομακρυσμένο έλεγχο συσκευών, που καλύπτουν ανάγκες δικτύωσης πολλαπλών συσκευών.
- Δίνεται ένα πλήρες παράδειγμα χρήσης του MDM.

Abstract

This diploma study deals with technologies related to the Mobile IP protocol. All the necessary concepts required for its mode of operation and protocol applications are given gradually.

The following items are listed in detail in the chapters of the study:

- Description of infrastructure needed for computer networks, categorization of networks according to the area they cover, topology and modes of transmission.
- Reference to the 802.11 wireless communication protocol.
- Reference to the Mobile IP protocol, analysis of IPv4 and IPv6 versions of the protocol. Implementations of the protocol are presented on a Linux operating system and additional needs are covered in this release.
- Reference to MDM, application of protocol for remote control of mobile devices that meet multi-device networking needs.
- MDM Example.

Περιεχόμενα

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΔΙΑΓΡΑΜΜΑΤΩΝ

1 ΔΙΚΤΥΑ ΕΠΙΚΟΙΝΩΝΙΩΝ ΠΡΩΤΟΚΟΛΛΑ ΚΑΙ ΜΟΝΤΕΛΑ

1.1 Εισαγωγή

Τα δίκτυα υπολογιστών είναι ίσως η πιο σημαντική τεχνολογική εφεύρεση των τελευταίων 50 ετών στον πλανήτη. Τα δίκτυα υπολογιστών έχουν μεγάλη σημασία για την ανθρωπότητα καθώς έχουν αμέτρητες εφαρμογές. Χρησιμοποιούνται για επικοινωνία που είναι το κύριο χαρακτηριστικό τους. Είναι ιδιαίτερα σημαντικά για πολλούς τομείς όπως η εκπαίδευση, η υγεία, οι επιχειρηματικές δραστηριότητες και άλλα πολλά. Ένα σε όλους γνωστό δίκτυο είναι το Διαδίκτυο ή Internet που αποτελεί το μεγαλύτερο δίκτυο με αμέτρητες συνδεδεμένες συσκευές πάνω σε αυτό.

Στο κεφάλαιο αυτό αρχικά θα παρουσιαστούν πληροφορίες που αφορούν τα δίκτυα υπολογιστών, τις κατηγορίες δικτύων και τα πρωτόκολλα τους. Έπειτα θα παρατεθεί μια σύντομη ιστορική αναδρομή για να φανεί ο τρόπος με τον οποίο έφτασε η κατάσταση στην σημερινή εικόνα. Τέλος, θα παρουσιαστούν πρωτόκολλα δικτύων και μοντέλα όπως το TCP/IP και το μοντέλο OSI της ISO.

1.2 Ορισμός δικτύων και κατηγοριοποίηση τους

Γενικότερα τα δίκτυα θα μπορούσαν να χωριστούν σε δύο κατηγορίες τα υπολογιστικά και τα δίκτυα τηλεπικοινωνιών. Αντίστοιχα οι ορισμοί τους είναι:

- "Ένα τηλεπικοινωνιακό δίκτυο είναι μια συλλογή από τερματικούς κόμβους που είναι συνδεδεμένοι με τέτοιο τρόπο ώστε να εξασφαλίζουν την επικοινωνία μεταξύ των κόμβων αυτών. Οι κόμβοι χρησιμοποιούν τα κυκλώματα σύνδεσης για να μεταφέρουν το σήμα στον σωστό προορισμό."
- "Το υπολογιστικό δίκτυο ή δίκτυο δεδομένων είναι ένα τηλεπικοινωνιακό δίκτυο το οποίο επιτρέπει στους εμπλεκόμενους κόμβους να διαμοιραστούν δεδομένα μεταξύ τους μέσω ενός συνδέσμου δεδομένων. Η επικοινωνία μεταξύ των κόμβων δημιουργείται είτε μέσω καλωδιακών είτε μέσω ασύρματων συνδέσεων."

Τα δίκτυα των υπολογιστών μπορούν να διαχωριστούν σε διάφορες κατηγορίες ανάλογα με το κριτήριο που επιλέγεται σαν το εκάστοτε σημείο αναφοράς. Κάποιοι από αυτούς τους παράγοντες είναι η γεωγραφική έκταση της περιοχής που καλύπτουν, η τοπολογία τους και ο τρόπος μετάδοσης της πληροφορίας μεταξύ των κόμβων.

1.2.1 Διαχωρισμός με βάση την γεωγραφική έκταση που καλύπτουν:

- Τοπικά δίκτυα (LAN ή Local Area Network)

Ένα τοπικό δίκτυο ή LAN διασυνδέει διάφορες συσκευές που βρίσκονται έως λίγες δεκάδες χιλιομέτρων απόσταση μεταξύ τους. Η πιο ευρεία χρήση τους είναι για διασύνδεση ηλεκτρονικών υπολογιστών και τερματικών σε γραφεία εταιρειών, εργοστάσια, νοσοκομεία και άλλα.

- Μητροπολιτικά δίκτυα (MAN ή Metropolitan Area Network)

Ένα μητροπολιτικό δίκτυο ή MAN τυπικά διασύνδεει συσκευές που βρίσκονται μερικά εκατοντάδες χιλιόμετρα απόσταση μεταξύ τους καλύπτοντας μεγαλύτερες αποστάσεις σε σχέση με τα δίκτυα LAN. Τα μητροπολιτικά δίκτυα χρησιμοποιούνται για να διασυνδέουν τις εγκαταστάσεις μιας πόλης, για στρατιωτικούς σκοπούς και άλλα.

- Ευρείας περιοχής (WAN ή Wide Area Network)

Οι συσκευές ενός δικτύου ευρείας περιοχής ή WAN μπορούν να υπάρχουν σε οποιοδήποτε σημείο της γης και μπορούν να συνδέσουν από πόλεις ολόκληρες μέχρι και ηπείρους. Πολλές φορές ένα δίκτυο ευρείας περιοχής μπορεί να αποτελείται από ομάδες δικτύων LAN ή MAN. Συνήθως τα δίκτυα αυτά χρησιμοποιούν για την διασύνδεση τους τηλεφωνικές γραμμές ακόμα και δορυφόρους.

- Διαδίκτυα (Internets)

Τα διαδίκτυα είναι η μεγαλύτερη κατηγορία δικτύων που υπάρχουν. Διασυνδέουν ολόκληρο τον πλανήτη. Ένα τέτοιο γνωστό παράδειγμα είναι το "διαδίκτυο" γνωστό σε όλους ως Internet που χρησιμοποιείται σε όλο τον κόσμο.

1.2.2 Διαχωρισμός με βάση την τοπολογία τους:

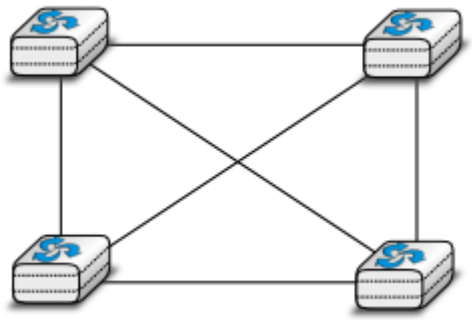
Ένας άλλος διαχωρισμός των δικτύων θα μπορούσε να είναι με βάση την φυσική τους τοπολογία. Στις εικόνες που θα παρατεθούν παρακάτω οι φυσικές συνδέσεις αναπαρίστανται με γραμμές οι συσκευές ή άλλος δικτυακός εξοπλισμός αναπαρίσταται με κουτιά. Οι κατηγορίες των δικτύων με βάση την τοπολογία τους είναι οι εξής:

- Τοπολογία πλέγματος (Meshtopology):

Τα δίκτυα υπολογιστών επιτρέπουν σε πολλά τερματικά να ανταλάσσουν πληροφορία μεταξύ τους. Για να στείλει μια συσκευή πληροφορία σε μία άλλη εντός του δικτύου ο ευκολότερος τρόπος για να οργανωθούν είναι σε διάταξη πλέγματος με έναν άμεσο και αποκλειστικό

σύνδεσμο να ενώνει κάθε ζεύγος τερματικών. Μία τέτοια διάταξη χρησιμοποιείται όταν το δίκτυο θέλει να δώσει έμφαση στην υψηλή απόδοση και άμεση ανταπόκριση σε μικρό αριθμό τερματικών. Ωστόσο παρά τα πλεονεκτήματα, που παρουσιάζει η διάταξη αυτή υπάρχουν και μερικά πλεονεκτήματα:

- Για ένα δίκτυο που περιέχει ν τερματικά ή hosts, το κάθε ένα από αυτά πρέπει να περιέχει ν-1 φυσικές συνδέσεις δηλαδή να συνδέεται με όλα τα υπόλοιπα εκτός από τον εαυτό του.
- Για ένα δίκτυο που περιέχει ν τερματικά ή hosts, απαιτούνται ν*(n-1)/2 συνδέσεις. Αυτό είναι δυνατόν εάν υπάρχουν λίγοι κόμβοι μέσα στον ίδιο χώρο αλλά δεν εξυπηρετεί καθόλου όταν βρίσκονται σε απόσταση μερικών χιλιομέτρων.



Εικόνα 1: Διάταξη τοπολογίας αστέρα

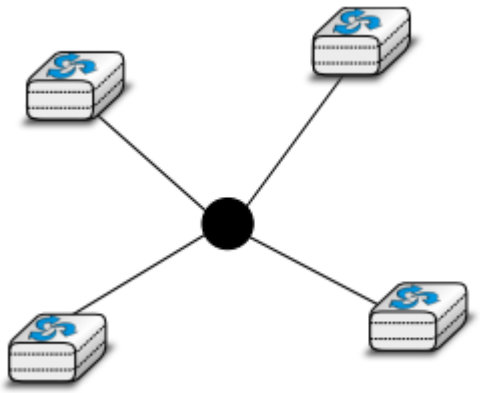
- Τοπολογία διαύλου (Bustopology):

Η δεύτερη δυνατή τοπολογία που χρησιμοποιείται εντός των ηλεκτρονικών υπολογιστών για να συνδεθούν διαφορετικές κάρτες επέκτασης είναι η τοπολογία διαύλου. Σε μια τοπολογία διαύλου όλα τα τερματικά συνδέονται σε ένα κοινό μέσο μετάδοσης που είναι συνήθως ένα και μόνο καλώδιο με μία μόνο διεπαφή (interface). Όταν ένα από τα host εκπέμπει ηλεκτρικό σήμα μέσα στο δίαυλο το σήμα μπορούν να λάβουν όλοι οι υπόλοιποι άμεσα. Το αρνητικό με αυτήν την τοπολογία είναι ότι εάν κοπεί ο κοινός δίαυλος επικοινωνίας τότε το δίκτυο κατακερματίζεται σε δύο απομονωμένα μεταξύ τους υποδίκτυα. Για αυτό το λόγο τα δίκτυα με τοπολογία διαύλου πολλές φορές θεωρούνται δύσκολα στην λειτουργία και συντήρηση ειδικά εάν ο δίαυλος έχει μεγάλο μήκος με αποτέλεσμα να αυξάνεται το ρίσκο αποκοπής σε κάποιο σημείο. Δίκτυα τέτοιας τοπολογίας χρησιμοποιήθηκαν ευρέως στις πρώιμες μορφές δικτύων Ethernet.

Εικόνα 2: Διάταξη τοπολογίας διαύλου

- Τοπολογία αστέρα (Star topology):

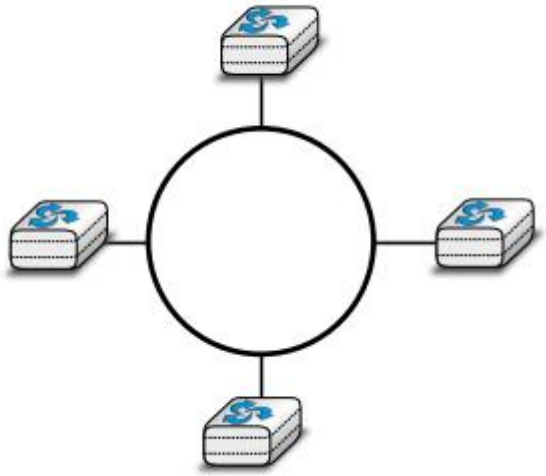
Η τρίτη δυνατή τοπολογία οργάνωσης δικτύων είναι η τοπολογία αστέρα. Σε αυτήν την τοπολογία οι hosts έχουν μια φυσική διεπαφή και έναν σύνδεσμο μεταξύ αυτών και της κεντρικής διεπαφής. Ο κόμβος στος κέντρο είτε θα είναι ένα τερματικό που ενισχύει το σήμα ή μια ενεργή συσκευή που αντιλαμβάνεται τα μηνύματα που ανταλάσσουν οι κόμβοι μεταξύ τους. Ωστόσο υπάρχει το μειονέκτημα ότι η αποτυχία του κεντρικού κόμβου θα οδηγήσει σε αποτυχία του δικτύου. Παρ' όλα αυτά εάν οποιοσδήποτε άλλος κόμβος αποτύχει να λειτουργήσει σωστά είναι ο μόνος που αποκόβεται από το δίκτυο χωρίς να επηρεάζει την λειτουργία των υπολοίπων. Πρακτικά τα δίκτυα με τοπολογία αστέρα είναι πιο εύκολα στην συντήρηση από τα δίκτυα με τοπολογία διαύλου. Επίσης, πολλοί διαχειριστές δικτύων εκτιμούν το γεγονός ότι με αυτήν την τοπολόγία δίνεται η δυνατότητα κεντρικής διαχείρισης του δικτύου. Είτε μέσω ενός δικτυακού περιβάλλοντος διεπαφής είτε μέσω κονσόλας (terminal) ο κεντρικός κόμβος των δικτύων αυτών είναι ένα ιδανικό σημείο ελέγχου (π.χ. για ενεργοποίηση ή απενεργοποίηση συσκευών) ή παρατήρησης (π.χ. για την εξαγωγή στατιστικών χρήσης ή και άλλων δεδομένων).



Εικόνα 3: Διάταξη τοπολογίας αστέρα

- Τοπολογία δακτυλίου (Ring topology):

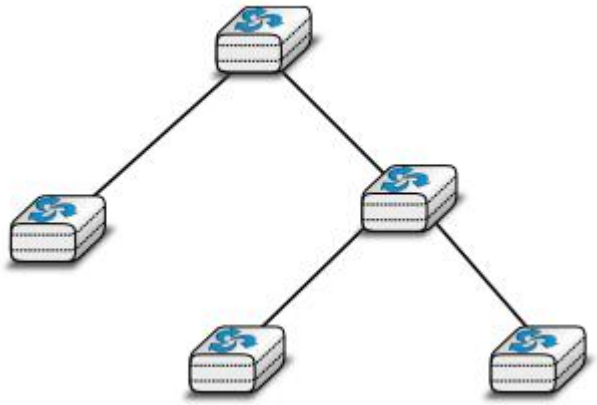
Ο τέταρτος τρόπος φυσικής οργάνωσης ενός δικτύου είναι η χρήση τοπολογίας δακτυλίου. Όπως και η τοπολογία διαύλου κάθε host έχει μια φυσική σύνδεση με τον κεντρικό δακτύλιο. Οποιοδήποτε σήμα σταλεί από κάποιο τερματικό θα είναι ορατό από όλες τις συσκευές που είναι συνδεδεμένες πάνω στον δακτύλιο. Με συγκεκριμένη οπτική γωνία ένας απλός δακτύλιος δεν είναι και η καλύτερη δυνατή επιλογή καθώς το σήμα ταξιδεύει προς μια κατεύθυνση με αποτέλεσμα ένα κομμάτι του δακτυλίου να κοπεί πέφτει ολόκληρο το δίκτυο. Πρακτικά τέτοιες τοπολογίες χρησιμοποιούνται περισσότερο σε LAN δίκτυα αλλά στις μέρες μας αντικαθίστανται από άλλα δίκτυα με τοπολογία αστέρα. Στα μητροπολιτικά δίκτυα οι δακτύλιοι συχνά χρησιμοποιούνται για να συνδέσουν διαφορετικές περιοχές του δικτύου. Σε αυτήν την περίπτωση εγκαθίστανται δύο παράλληλοι σύνδεσμοι αποτελούμενοι από διαφορετικά καλώδια. Με αυτό τον τρόπο εγκατάστασης αυτόματα όταν κάτι πάει στραβά στον ένα σύνδεσμο η κίνηση των δεδομένων δρομολογείται στον άλλο σύνδεσμο.



Εικόνα 4: Διάταξη τοπολογίας δακτυλίου

- Τοπολογία δένδρου (Tree topology):

Ο πέμπτος τρόπος οργάνωσης ενός δικτύου είναι η τοπολογία δένδρου. Αυτός ο τύπος δικτύου χρησιμοποιείται σε περιπτώσεις όπου απαιτείται μια μεγάλη εγκατάσταση πελατών με έναν αποδοτικό οικονομικά τρόπο. Τα δίκτυα καλωδιακής τηλεόρασης συνήθως εγκαθίστανται με αυτόν τον τρόπο.



Εικόνα 5: Διάταξη τοπολογίας δένδρου

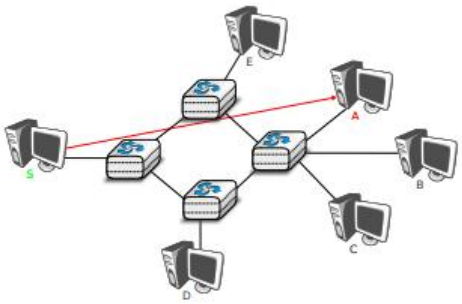
Πρακτικά τα περισσότερα δίκτυα συνδυάζουν κατά τμήματα περισσότερες από μία τοπολογίες. Για παράδειγμα ένα δίκτυο πανεπιστημίου θα μπορούσε να οργανωθεί σε τοπολογία δακτυλίου μεταξύ των σημαντικών του κτιρίων με τα μικρότερα κτίρια να είναι οργανωμένα σε τοπολογία δένδρου ή αστέρα. Ένα άλλο παράδειγμα θα ήταν ένας πάροχος επικοινωνίας που μπορεί να έχει τοπολογία πλέγματος συσκευών στο κέντρο του δικτύου του και τοπολογία δένδρου για να συνδέσει τους απόμακρους χρήστες του.

1.2.3 Διαχωρισμός των δικτύων με βάση τους τρόπους μετάδοσης:

Το τελευταίο κριτήριο διαχωρισμού δικτύων είναι ο τρόπος μετάδοσης της πληροφορίας. Όταν ανταλλάσσεται πληροφορία μέσα από ένα δίκτυο υπάρχουν τρεις διαφορετικοί τρόποι μετάδοσης. Στην τηλεόραση και στο ραδιόφωνο χρησιμοποιείται ο όρος ευρείας διανομής (broadcast) για να περιγράψει μια τεχνολογία που αποστέλλει σήμα σε όλους τους δέκτες εντός μιας συγκεκριμένης γεωγραφικής περιοχής. Η αναμετάδοση χρησιμοποιείται πολλές φορές σε τοπικά δίκτυα (LAN) σε περιπτώσεις που ο αριθμός των δεκτών είναι περιορισμένος.

- Μοναδικής διανομής (unicast)

Ο πρώτος και ο πιο διαδεδομένος τρόπος μετάδοσης πληροφορίας είναι ο μοναδικής διανομής (unicast). Σε αυτόν τον τρόπο μετάδοσης τα δεδομένα μεταβαίνουν από έναν αποστολέα σε έναν παραλήπτη. Οι περισσότερες διαδικτυακές εφαρμογές βασίζονται σε αυτόν τον τρόπο μετάδοσης. Στα παρακάτω διαγράμματα που θα παρουσιαστούν οι hosts αναπαρίστανται σαν υπολογιστές και οι ενδιάμεση κόμβοι σαν κύβοι. Οι hosts μεταδίδουν την πληροφορία μέσω των ενδιάμεσων κόμβων. Στο παράδειγμα που ακολουθεί ένας host S χρησιμοποιεί μετάδοση μοναδικής διανομής(unicast) για να στείλει πληροφορίες μέσω των τριών ενδιάμεσων κόμβων. Ο κάθε ένας από αυτούς τους κόμβους λαμβάνει την πληροφορία και την προωθεί στον επόμενο host ή κόμβο.



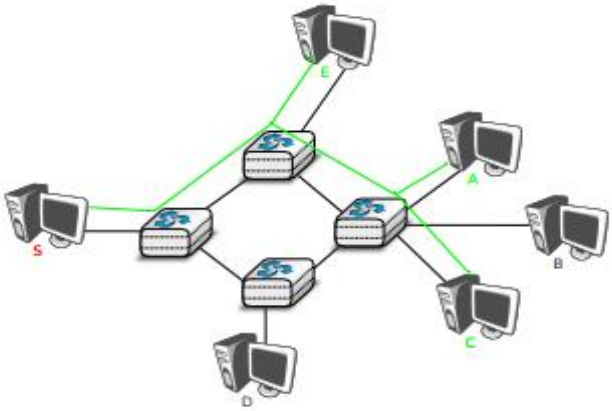
Εικόνα 6: Δίκτυο με μετάδοση μοναδικής διανομής (unicast)

- Πολλαπλής διανομής (multicast)

Ένας δεύτερος τρόπος μετάδοσης είναι ο πολλαπλής διανομής (multicast). Αυτός ο τρόπος μετάδοσης χρησιμοποιείται όταν η πληροφορία πρέπει να σταλεί σε ένα σύνολο παραληπτών. Αρχικά, χρησιμοποιήθηκε στα LAN δίκτυα και έπειτα εφαρμόστηκε και στα WAN. Όταν

ένας αποστολέας χρησιμοποιεί πολλαπλή μετάδοση για να στείλει πληροφορία σε ν παραλήπτες, ο αποστολέας στέλνει ένα και μοναδικό αντίγραφο της πληροφορίας και οι κόμβοι του δικτύου το αντιγράφουν όποτε αυτό είναι απαραίτητο ώστε να φτάσει σε όλους τους παραλήπτες.

Για να γίνει κατανοητή η σημασία της πολλαπλής διανομής, θα παρατεθεί ένα παράδειγμα. Ας γίνει η υπόθεση ότι έχουμε μια πηγή S που στέλνει την ίδια ακριβώς πληροφορία στους προορισμούς A,C και E. Με την μετάδοση μοναδικής διανομής (unicast) η ίδια πληροφορία περνά τρεις φορές από τους ενδιάμεσους κόμβους 1 και 2 και δύο φορές από τον κόμβο 4. Αυτό ουσιαστικά είναι μια σπατάλη πόρων τόσο στους ενδιάμεσους κόμβους όσο και στο μέσο που τους συνδέει. Με την μετάδοση πολλαπλής διανομής(multicast) ο host S στέλνει την πληροφορία στον κόμβο 1 ο οποίος με τη σειρά του την προωθεί στον κόμβο 2. Αυτός ο κόμβος δημιουργεί δύο αντίγραφα της πληροφορίας που έχει δεχτεί και στέλνει το ένα απευθείας στον host E και το άλλο στον κόμβο 4. Το ίδιο κάνει και ο κόμβος 4 που παράγει δύο αντίγραφα της πληροφορίας και στέλνει το ένα στον κόμβο A και το άλλο στον κόμβο C. Χάρη στην μετάδοση πολλαπλής διανομής (multicast) η ίδια πληροφορία μπορεί να φτάσει σε έναν μεγάλο αριθμό παραληπτών έχοντας σταλεί μόνο μια φορά από κάθε σύνδεσμο.

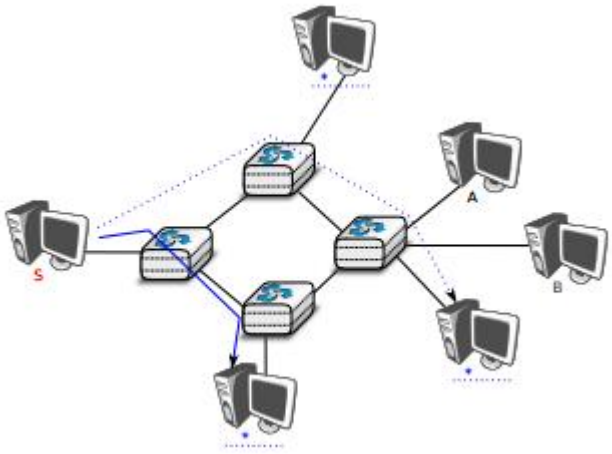


Εικόνα 7: Δίκτυο με μετάδοση πολλαπλής διανομής (multicast)

- Οποιασδήποτε διανομής (anycast)

Ο τελευταίος τρόπος μετάδοσης της πληροφορίας είναι ο οποιασδήποτε διανομής (anycast). Αρχικά ορίστηκε στο RFC 1542. Σε αυτόν τον τρόπο μετάδοσης αναγνωρίζεται μια ομάδα παραληπτών. Όταν η πηγή της πληροφορίας στέλνει την πληροφορία σε αυτήν την ομάδα παραληπτών το δίκτυο εξασφαλίζει ότι η πληροφορία θα φτάσει σίγουρα σε έναν παραλήπτη από αυτήν την ομάδα. Συνήθως ο παραλήπτης που λαμβάνει την πληροφορία είναι αυτός που

είναι πλησιέστερα στην πηγή. Αυτός ο τρόπος μετάδοσης είναι αξιόπιστος στον τομέα της διαθεσιμότητας καθώς εάν πέσει ο ένας κόμβος που επρόκειτο να δεχθεί την πληροφορία τότε το δίκτυο θα εξασφαλίσει ότι η πληροφορία θα πάει σε άλλο δέκτη που ανήκει στην ίδια ομάδα παραληπτών. Πρακτικά όμως η υποστήριξη δικτύων με αυτόν τον τρόπο μετάδοσης μπορεί να γίνει ιδιαίτερα δύσκολη.



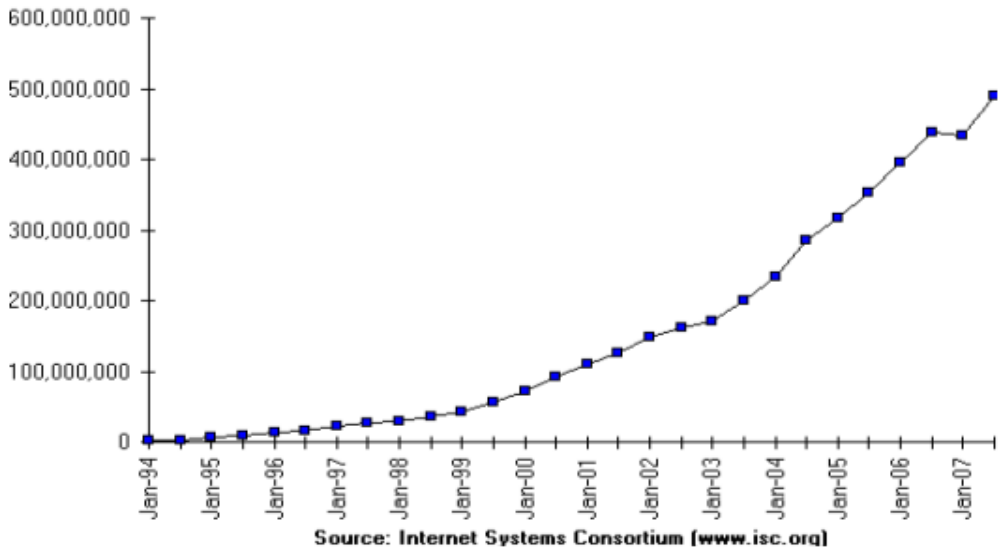
Εικόνα 8: Δίκτυο με μετάδοση πολλαπλής διανομής (anycast)

Στο παράδειγμα που φαίνεται από την παραπάνω εικόνα (Εικόνα 8), οι τρεις host που είναι σημαδεμένοι με * είναι μέρος της ίδιας ομάδας παραληπτών. Όταν ο host S (η πηγή της πληροφορίας) στέλνει πληροφορίες στην ομάδα το δίκτυο εξασφαλίζει ότι θα σταλεί σε όλους τους παραλήπτες της ομάδας. Οι διακεκομμένες γραμμές συμβολίζουν την πιθανή παράδοση της πληροφορίας μέσω των κόμβων 1,2 και 4. Μια μεταγενέστερη μετάδοση της πληροφορίας από την πηγή S στην ίδια ομάδα παραληπτών μπορεί να φτάσει στον host που είναι προσαρτημένος στον ενδιάμεσο κόμβο 3 όπως φαίνεται από την μπλε γραμμή. Μια μετάδοση οποιασδήποτε διανομής (anycast) φτάνει σε ένα μέλος της ομάδας παραληπτών που επιλέγεται από το δίκτυο σε συνάρτηση με τις συνθήκες που επικρατούν στο δίκτυο την δεδομένη χρονική στιγμή.

1.3 Σύντομη ιστορική αναδρομή στα δίκτυα και τα πρωτόκολλα τους

Όταν κατασκευάστηκαν οι πρώτοι υπολογιστές κατά τη διάρκεια του 2ου παγκοσμίου πολέμου ήταν ακόμα ακριβοί και απομονωμένοι. Ωστόσο, μετά από περίπου 20 χρόνια οι τιμές τους είχαν αρχίσει σταδιακά να μειώνονται. Την ίδια περίοδο περίπου χρονολογούνται

και τα πρώτα πειράματα που συνέδεαν υπολογιστές μεταξύ τους. Στις αρχές τις δεκαετίας του 1960 ερευνητές μεταξύ των οποίων και οι Paul Baran, Donald Davies, Joseph Licklider ανεξάρτητα δημοσίευσαν τα πρώτα τους συγγράμματα που περιέγραφαν την ιδέα της κατασκευής δικτύων υπολογιστών. Δεδομένου του κόστους των υπολογιστών η διασύνδεση τους και κατά επέκταση ο διαμοιρασμός τους ήταν μια ενδιαφέρουσα προοπτική. Στις Ηνωμένες Πολιτείες Αμερική το ARPANET ξεκίνησε το 1969 και συνέχισε μέχρι τα μέσα της δεκαετίας του 1980. Στην Γαλλία ο Louis Pouzin ανέπτυξε το δίκτυο Cyclades. Πολλά άλλα ερευνητικά δίκτυα δημιουργήθηκαν μέσα στη δεκαετία του 1970. Ταυτόχρονα η βιομηχανίες τηλεπικοινωνιών και ηλεκτρονικών υπολογιστών ξεκίνησαν να δείχνουν ενδιαφέρον για τα δίκτυα. Οι εταιρείες τηλεπικοινωνιών προσήλωσαν τις προσπάθειες τους στο δίκτυο X25. Αντίστοιχα, οι βιομηχανίες υπολογιστών ακολούθησαν εντελώς διαφορετική προσέγγιση χτίζοντας τα δίκτυα LAN (Local Area Networks). Πολλά LANs όπως το Ethernet και το Token Ring σχεδιάστηκαν τότε. Κατά τη διάρκεια της δεκαετίας του 1980 η ανάγκη για περισσότερες υπερσυνδέσεις οδήγησε σε μία ραγδαία ανάπτυξη δικτυακών πρωτοκόλλων επικοινωνίας. Η Xerox ανέπτυξε το XNS, η DEC διάλεξε το DECNet, η IBM ανέπτυξε το SNA, η Microsoft εισήγαγε το NetBIOS ενώ η Apple επένδυσε στο Appletalk. Στην ερευνητική κοινότητα το Arpanet έχασε την ισχύ του και αντικαταστάθηκε από το TCP/IP του οποίου η υλοποίηση έγινε για πρώτη φορά σε λειτουργικό σύστημα BSD Unix. Πανεπιστήμια τα οποία έτρεχαν Unix λειτουργικά συστήματα μπορούσαν εύκολα να κάνουν την μετάβαση στο νέο πρωτόκολλο. Επιπλέον οι πάροχοι σταθμών εργασίας που χρησιμοποιούσαν λειτουργικό Unix όπως η Sun ή η Silicon Graphics συμπεριέλαβαν στους σταθμούς αυτούς την χρήση του νέου πρωτοκόλλου. Παράλληλα η ISO με την υποστήριξη κυβερνήσεων εργάστηκε για την δημιουργία μιας ανοιχτής σουίτας από δικτυακά πρωτόκολλα. Στο τέλος το πρωτόκολλο TCP/IP έγινε αναντικατάστατο και η χρήση του εκτεινόταν πέρα από ερευνητικούς σκοπούς. Όπως φαίνεται από το διάγραμμα που ακολουθεί ο αριθμός των συνδεδεμένων συσκευών στο μεγαλύτερο δίκτυο (το Internet ή διαδίκτυο) συνεχίζει να αυξάνεται ραγδαία τα τελευταία 20 χρόνια.



Διάγραμμα 1: Υπολογισμός των συνδεδεμένων συσκευών στο διαδίκτυο

1.4 Μοντέλα δικτύων υπολογιστών

Έχοντας σαν δεδομένο την αύξηση της πολυπλοκότητας των δικτύων υπολογιστών κατά τη διάρκεια της δεκαετίας του 1970 οι ερευνητές πρότειναν διάφορα μοντέλα αναφοράς για να αναπαραστήσουν και να αποτυπώσουν την περιγραφή των πρωτοκόλλων και υπηρεσιών. Από αυτά το πιο δημοφιλές ήταν το μοντέλο OSI που είναι αποτέλεσμα της έρευνας της ISO που στόχευε στην ανάπτυξη των παγκοσμίων σταθερών που αφορούν τα δίκτυα υπολογιστών. Στη συνέχεια παρατίθεται η περιγραφή ενός μοντέλου σαν μια απλοποιημένη έκδοση του OSI μοντέλου.

1.4.1 Το μοντέλο των πέντε επιπέδων

Το μοντέλο που επρόκειτο να περιγραφεί παρακάτω χωρίζεται σε πέντε επίπεδα ή στρώματα που διακρίνονται ως εξής:

1. Φυσικό επίπεδο (Physical Layer):

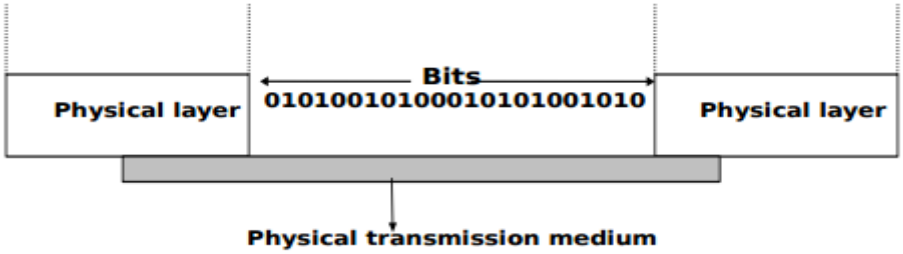
Ξεκινώντας από κάτω προς τα πάνω το πρώτο επίπεδο είναι το Φυσικό Επίπεδο (Physical Layer). Δύο συσκευές που επικοινωνούν συνδέονται μεταξύ τους με ένα φυσικό μέσο. Αυτό το φυσικό μέσο χρησιμοποιείται για να μεταφέρει ένα ηλεκτρικό ή οπτικό σήμα μεταξύ δύο άμεσα συνδεδεμένων συσκευών. Υπάρχουν διάφοροι τύποι φυσικών μέσων που χρησιμοποιούνται:

- *Ηλεκτρικό καλώδιο:* Η πληροφορία μπορεί να μεταδοθεί μέσα από διαφορετικούς τύπους ηλεκτρικών καλωδίων. Τα πιο συχνά είναι τα ζεύγη καλωδίων που χρησιμοποιούνται στα τηλεφωνικά και εταιρικά δίκτυα αλλά και τα ομοαξονικά καλώδια (coaxial cables). Τα δεύτερα χρησιμοποιούνται σε δίκτυα καλωδιακής τηλεόρασης αλλά δεν χρησιμοποιούνται πλέον σε εταιρικά δίκτυα.

- *Οπτική ίνα:* Οι οπτικές ίνες χρησιμοποιούνται συχνά σε δημόσια και εταιρικά δίκτυα συνήθως όταν οι αποστάσεις μεταξύ των συσκευών που επικοινωνούν είναι μεγαλύτερη από ένα χιλιόμετρο. Υπάρχουν δύο ειδών οπτικές ίνες η πολύτροπη (multi mode) και η μονότροπη(mono mode). Η πολύτροπη είναι αρκετά φθηνότερη καθώς απαιτείται ένα LED για να σταλεί το σήμα ενώ η μονότροπη θα πρέπει να διαθέτει τεχνολογία laser.

- *Ασύρματα:* Σε αυτήν την περίπτωση ένα εναέριο σήμα χρησιμοποιείται για να κωδικοποιήσει την πληροφορία που ανταλλάσσεται μεταξύ των συσκευών που επικοινωνούν. Υπάρχουν και άλλες ασύρματες τεχνολογίες που αντί για ένα εναέριο σήμα χρησιμοποιούν μικρούς παλμούς laser προς έναν απομακρυσμένο ανιχνευτή.

Το Φυσικό επίπεδο επιτρέπει δύο ή περισσότερες οντότητες που είναι άμεσα συνδεδεμένες στο ίδιο μέσο μετάδοσης να ανταλλάσσουν bits πληροφορίας. Η δυνατότητα ανταλλαγής bits είναι σημαντική καθώς οποιαδήποτε πληροφορία μπορεί να κωδικοποιηθεί σαν μια ακολουθία από bits. Το ίδιο ακριβώς ισχύει και για τις αποθήκες αρχείων και δεδομένων. Οι συσκευές αποθήκευσης όπως οι σκληροί δίσκοι αποθηκεύουν επίσης ροές από bits. Γενικότερα, τα υπολογιστικά δίκτυα χρησιμοποιούν μια παρόμοια προσέγγιση. Κάθε επίπεδο παρέχει υπηρεσίες που βασίζονται στο αμέσως προηγούμενο επίπεδο και είναι πιο κοντά στις ανάγκες των εφαρμογών.



Εικόνα 9: Ο τρόπος επικοινωνίας του φυσικού επιπέδου

2. Επίπεδο Διασύνδεσης Δεδομένων (Datalink Layer):

Το επίπεδο διασύνδεσης δεδομένων βασίζεται πάνω στις υπηρεσίες που προσφέρει το Φυσικό επίπεδο. Επιτρέπει σε δύο hosts που είναι άμεσα συνδεδεμένοι μεταξύ τους μέσω του Φυσικού Επίπεδου να ανταλλάξουν πληροφορία. Η μονάδα της πληροφορίας που ανταλλάσεται μεταξύ των δύο οντοτήτων ονομάζεται πλαίσιο (frame). Το πλαίσιο ουσιαστικά είναι μια ακολουθία από bits. Κάποια υποεπίπεδα του Επιπέδου Διασύνδεσης Δεδομένων χρησιμοποιούν πλαίσια μεταβλητού μήκους bits και άλλα σταθερού μήκους. Κάποια υποεπίπεδα του Επιπέδου Διασύνδεσης Δεδομένων παρέχουν υπηρεσίες προσανατολισμένες στην διασύνδεση ενώ άλλα παρέχουν υπηρεσίες χωρίς σύνδεση. Τέλος, άλλα υποεπίπεδα παρέχουν αξιόπιστη μεταφορά δεδομένων ενώ άλλα δεν εγγυώνται την σωστή μεταφορά της πληροφορίας.

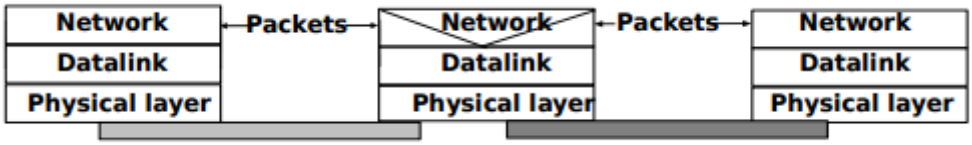
Το Επίπεδο Διασύνδεσης Δεδομένων επιτρέπει σε άμεσα συνδεδεμένους hosts να ανταλλάξουν πληροφορία αλλά πολλές φορές είναι απαραίτητη η ανταλλαγή πληροφορίας μεταξύ hosts που δεν είναι συνδεδεμένοι στο ίδιο φυσικό μέσο. Αυτό είναι δουλειά του Επιπέδου Δικτύου που θα αναλυθεί παρακάτω.

Εικόνα 10: Ο τρόπος επικοινωνίας του επιπέδου διασύνδεσης

3. Επίπεδο Δικτύου (Network Layer):

Το Επίπεδο Δικτύου χτίζει της διεργασίες του πάνω σε αυτές του Επίπεδου Διασύνδεσης Δεδομένων. Οι οντότητες του επιπέδου αυτού ανταλλάσσουν πακέτα πληροφορίας. Ένα πακέτο είναι μια πεπερασμένη ακολουθία από bytes που μεταφέρεται από το Επίπεδο Διασύνδεσης Δεδομένων μέσα σε ένα ή περισσότερα πλαίσια. Ένα πακέτο συνήθως μεταφέρει πληροφορίες σχετικά με την προέλευση του και τον προορισμό του και συνήθως περνά μέσα από πλήθος ενδιάμεσων συσκευών που ονομάζονται δρομολογητές (routers) μέχρι να φτάσει στον προορισμό του.

Οι περισσότερες εφαρμογές του Επιπέδου Δικτύου συμπεριλαμβανομένου και του διαδικτύου δεν εξασφαλίζουν αξιόπιστες υπηρεσίες. Ωστόσο, υπάρχουν εφαρμογές που απαιτούν την αξιόπιστη μεταφορά των δεδομένων γεγονός που έχει ως αποτέλεσμα να είναι δύσκολη η αξιοπιστία εάν χρησιμοποιούν το Επίπεδο Δικτύου. Το να εξασφαλιστεί η αξιόπιστη μεταφορά των δεδομένων είναι καθήκον του Επιπέδου Μεταφοράς.

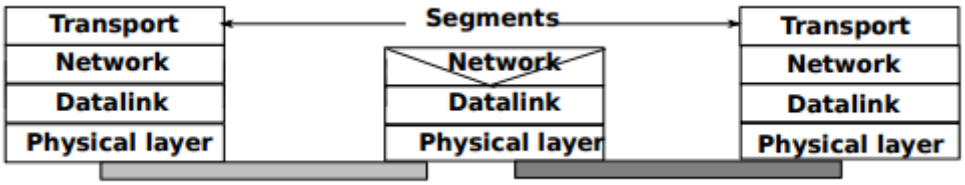


Εικόνα 11: Ο τρόπος επικοινωνίας του επιπέδου δικτύου

4. Επίπεδο Μεταφοράς (Transport Layer):

Οι οντότητες του Επιπέδου Μεταφοράς ανταλλάσσουν μεταξύ τους δομικά τμήματα που ονομάζονται τομείς (segments). Τα segments είναι πεπερασμένες ακολουθίες από bytes που μεταφέρονται μέσα σε ένα ή περισσότερο πακέτα του Επιπέδου Δικτύου.

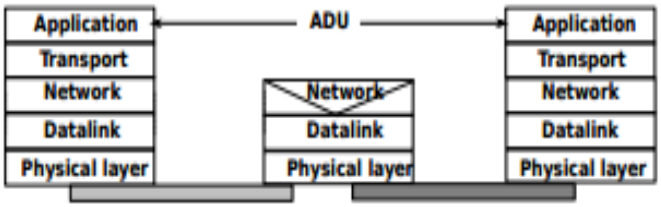
Υπάρχουν διάφορα είδη επιπέδων μεταφοράς. Το πιο ευρέως χρησιμοποιούμενο επίπεδο μεταφοράς είναι το TCP που παρέχει υπηρεσίες διασύνδεσης και το UDP που παρέχει υπηρεσίες μεταφοράς άνευ σύνδεσης.



Εικόνα 12: Ο τρόπος επικοινωνίας του επιπέδου μεταφοράς

5. Επίπεδο Εφαρμογής (Application Layer):

Το Επίπεδο Εφαρμογής περιλαμβάνει όλους τους μηχανισμούς και τις δομές δεδομένων που είναι απαραίτητες για τις εφαρμογές. Παρακάτω θα χρησιμοποιηθεί ο όρος Μονάδα Δεδομένων Εφαρμογής (Application Data Unit - ADA) για να οριστεί η μονάδα δεδομένων που ανταλλάσσονται μεταξύ δύο οντοτήτων του Επιπέδου Εφαρμογής.



Εικόνα 13: Ο τρόπος επικοινωνίας του επιπέδου εφαρμογής

2 ΠΡΩΤΟΚΟΛΛΟ IEEE 802.11

2.1 Ορισμός

"Το πρωτόκολλο IEEE 802.11 είναι ένα σύνολο από προδιαγραφές του ελέγχου πρόσβασης μέσων(MAC) και φυσικού επιπέδου (PHY) για την υλοποίηση ασύρματων τοπικών δικτύων (WLAN) επικοινωνίας υπολογιστών στα 900 Mhz και 2.4, 3.6, 5 και 60 GHz ζώνες συχνοτήτων."

Τα πρότυπα αυτά δημιουργήθηκαν και συντηρούνται από το Institute of Electrical and Electronics Engineers (IEEE) και πιο συγκεκριμένα από την LAN/MAN Standards Committee (IEEE 802). Η πρώτη και βασική έκδοση εκδόθηκε το 1997, και είχε αργότερα

αρκετές προσθήκες. Η βάση του προτύπου και οι προσθήκες παρέχουν την βάση για όλα τα δικτυακά προϊόντα που φέρουν την επωνυμία του ονόματος Wi-Fi.

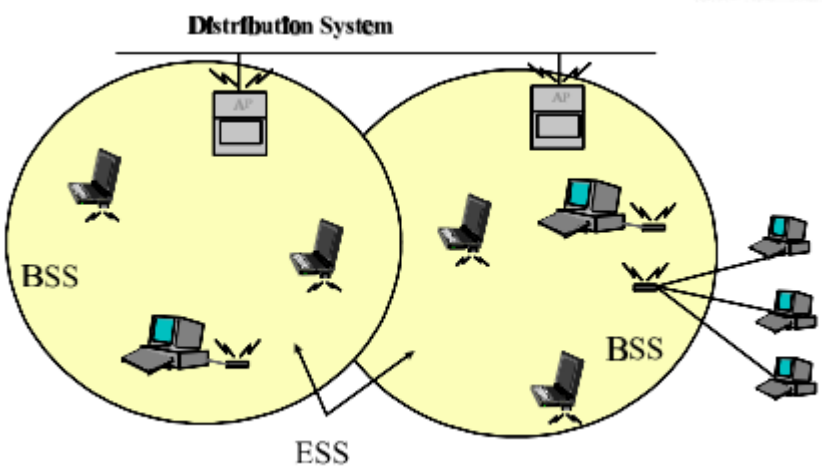
2.2 Σύντομη ιστορική αναδρομή

Η τεχνολογία που αφορά το πρότυπο 802.11 έχεις τις απαρχές της το 1985 ξεκινώντας από την Ομοσπονδιακή Επιτροπή Επικοινωνιών των Η.Π.Α.(U.S. Federal Communications Commission) που εξέδωσε την ζώνη ραδιοσυχνοτήτων ISM για χρήση χωρίς αδειοδότηση.
Το 1991 η NCR Corporation/AT&T εφηύρε έναν πρόγονο του 802.11 στο Nieuwegein της Ολλανδίας. Οι εφευρέτες του αρχικά σκόπευαν να χρησιμοποιήσουν την τεχνολογία σε συστήματα ταμειακών μηχανών. Τα πρώτα ασύρματα προϊόντα κυκλοφόρησαν στην αγορά με την επωνυμία WaveLAN με ταχύτητες μεταφοράς δεδομένων του 1 Mbit/s και 2 Mbit/s.
Ο VicHayes που ήταν πρόεδρος της επιτροπής του IEEE 802.11 για 10 χρόνια και αποκαλείται ως ο πατέρας το Wi-Fi, ενεπλάκη στον σχεδιασμό των αρχικών 802.11b και 802.11a προτύπων με την IEEE.
Το 1999 σχηματίστηκε η εμπορική ένωση Wi-FiAlliance για να διατηρήσει το εμπορικό σήμα Wi-Fi με τη χρήση του οποίου πωλούνται αρκετά ηλεκτρονικά προϊόντα και συσκευές στις μέρες μας.

2.3 Η αρχιτεκτονική του IEEE 802.11

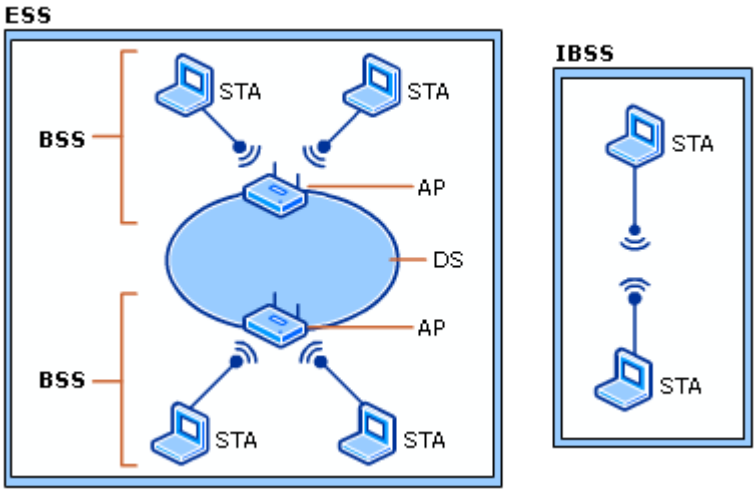
Ένα 802.11 δίκτυο LAN βασίζεται σε μία αρχιτεκτονική κυτταρικού τύπου όπου το όλο σύστημα διαιρείται σε κύτταρα. Κάθε κύτταρο ονομάζεται Σετ Βασικής Υπηρεσίας (Basic Service Set-BSS) ή/και Ανεξάρτητο Σετ Βασικών Υπηρεσιών (IndependentBasic Service Set-IBSS) και ελέγχεται από έναν βασικό σταθμό που ονομάζεται Σταθμός Βάση(BaseStation-BS ή Station-STA) ή Σημείο Πρόσβασης (Access Point) με συντομογραφία AP. Τα ασύρματα STA περιέχουν μια κάρτα δικτύου αφαιρούμενη ή μια ενσωματωμένη συσκευή για να παρέχουν ασύρματη συνδεσιμότητα.
Παρ' όλο που ένα ασύρματο δίκτυο LAN μπορεί να αποτελείται από ένα μόνο κύτταρο με ένα μόνο Σημείο Πρόσβασης(και όπως θα περιγραφεί παρακάτω μπορεί να δουλέψει και χωρίς σημείο πρόσβασης), οι περισσότερες εγκαταστάσεις σχηματίζονται από αρκετά κύτταρα όπου τα Σημεία Πρόσβασης συνδέονται μεταξύ τους με συνδέσεις που λειτουργούν σαν μια ραχοκοκαλιά και ονομάζονται Σύστημα Διανομής (Distribution System) με συντομογραφία DS. Συνήθως αυτή η ραχοκοκαλιά είναι Ethernet ενώ σε κάποιες περιπτώσεις είναι και αυτή ασύρματης σύνδεσης.

Όλο το διασυνδεδεμένο ασύρματο δίκτυο LAN, συμπεριλαμβανομένου των διαφορετικών κυττάρων, των AP και του συστήματος DS σχηματίζουν ένα απλό 802 δίκτυο στα ανώτατα επίπεδα του μοντέλου OSI και είναι γνωστό σαν Σετ Εκτεταμένων Υπηρεσιών (Extended Service Set) με συντομογραφία ESS.



Εικόνα 14: Παράδειγμα ενός 802.11 ασύρματου LAN

Ένα IBSS είναι ένα ασύρματο δίκτυο που αποτελείται τουλάχιστον από δύο STA που χρησιμοποιείται εκεί που δεν υπάρχει πρόσβαση σε DS. Ένα IBSS δίκτυο συχνά ακούγεται με την ονομασία "ad hoc" ασύρματο δίκτυο.
Ένα BSS είναι ένα ασύρματο δίκτυο που αποτελείται από απλά ασύρματα AP που υποστηρίζουν έναν ή περισσότερους ασύρματους κόμβους.
Ένα ESS είναι ένα σετ από δύο ή περισσότερα ασύρματα AP συνδεδεμένα στο ίδιο δίκτυο σταθερής καλωδίωσης που ορίζει έναν λογικό τομέα δικτύου συνδεδεμένο με έναν δρομολογητή που είναι γνωστό σαν υποδίκτυο (subnet).



Εικόνα 15: Η αρχιτεκτονική των ESS και IBSS ασυρμάτων δικτύων

Το παραπάνω πρότυπο που περιγράφηκε συμπεριλαμβάνει και την έννοια της Πύλης (Portal). Η Πύλη είναι μια συσκευή ένα 802.11 με ένα άλλο 802 LAN. Αυτή η έννοια είναι μια αφηρημένη περιγραφή τμήματος της λειτουργικότητας μιας "γέφυρας μετάφρασης".
Παρ' όλο που το πρότυπο δεν το καθορίζει οι κλασσικές εγκαταστάσεις έχουν το Portal και το AP σε μία φυσική οντότητα.

2.4 Οι τρόποι λειτουργίας του IEEE 802.11

Το πρωτόκολλο IEEE 802.11 ορίζει τους παρακάτω τρόπους λειτουργίας:

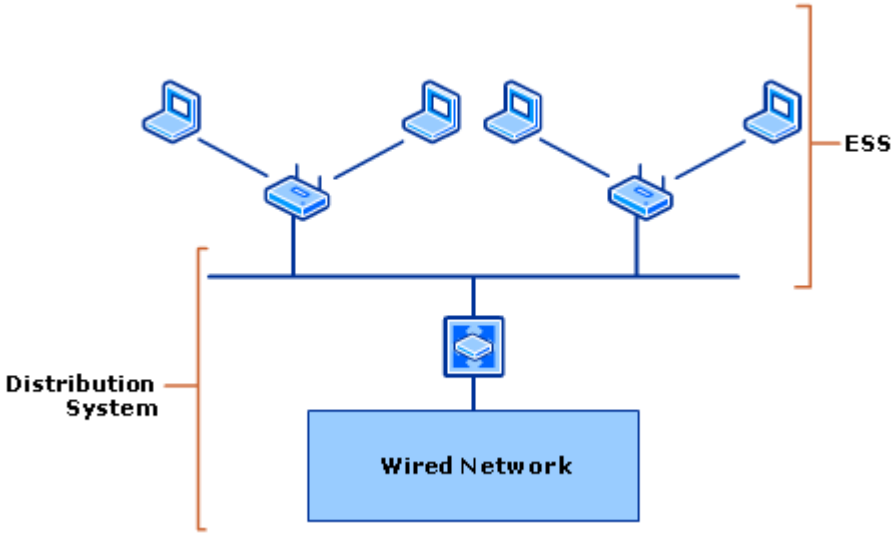
- Λειτουργία υποδομής (Infrastructure mode)
- Λειτουργία Ad hoc (Ad hoc mode)

Και στους δύο τρόπους λειτουργίας ένα Σετ Υπηρεσιών Αναγνώρισης (Service Set Identifier-SSID) που είναι γνωστό και σαν το όνομα του ασύρματου δικτύου, αναγνωρίζει το ασύρματο δίκτυο. Το SSID είναι ένα όνομα(αλφαριθμητικό) που στην Λειτουργία Υποδομής ορίζεται στο ασύρματο AP ή σε έναν αρχικό client για την λειτουργία ad-hoc που διαχωρίζει μοναδικά το δίκτυο. Το SSID εμφανίζεται περιοδικά από το ασύρματο AP χρησιμοποιώντας ένα ειδικό 802.11 MAC πλαίσιο διαχείρισης που είναι γνωστό και σαν beacon frame.

- Λειτουργία υποδομής (Infrastructure mode)

Στην Λειτουργία Υποδομής υπάρχουν τουλάχιστον ένα ασύρματο AP και ένας ασύρματος client. Ο ασύρματος client χρησιμοποιεί την ασύρματη σύνδεση με το AP για να αποκτήσει πρόσβαση σε ένα παραδοσιακό δίκτυο με καλωδίωση. Το δίκτυο με καλωδίωση μπορεί να

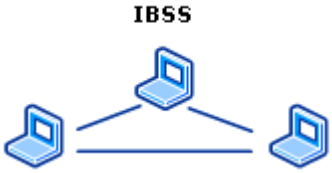
είναι ένα Intranet ή το ίδιο το διαδίκτυο γεγονός που εξαρτάται από την τοποθέτηση του ασύρματου AP.



Εικόνα 16: Λειτουργία υποδομής σε ασύρματο δίκτυο

- Λειτουργία Ad hoc (Ad hoc mode)

Η λειτουργία Ad hoc ονομάζεται επίσης λειτουργία παρόχου προς πάροχο (peer to peer). Οι ασύρματοι clients στην λειτουργία ad-hoc σχηματίζουν ένα ανεξάρτητο σετ βασικών υπηρεσιών (IBSS). Ένας από τους ασύρματους clients και πιο συγκεκριμένα ο πρώτος στο IBSS αναλαμβάνουν κάποια από τα καθήκοντα του ασύρματου AP. Μία από αυτές περιλαμβάνει την περιοδική διαδικασία αναμετάδοσης στίγματος και η πιστοποίηση νέων μελών στο δίκτυο (authentication). Ο ασύρματος client δεν δρα σαν γέφυρα για να εναποθέτει πληροφορία που μεταδίδεται μεταξύ άλλων ασύρματων clients. Η λειτουργία ad-hoc χρησιμοποιείται για να συνδέει τους ασύρματους clientsόταν δεν είναι διαθέσιμος το ασύρματο AP.Σε αυτόν τον τύπο λειτουργίας δικτύου οι ασύρματοι clients θα πρέπει να ρυθμιστούν ρητά για να χρησιμοποιούν την λειτουργία ad-hoc. Σε ένα 802.11 ad-hoc δίκτυο μπορούν να συνδεθούν μέχρι εννέα clients.



Εικόνα 17: Λειτουργία ad-hoc σε ασύρματο δίκτυο

2.5 802.11 πρωτόκολλα και τεχνολογίες

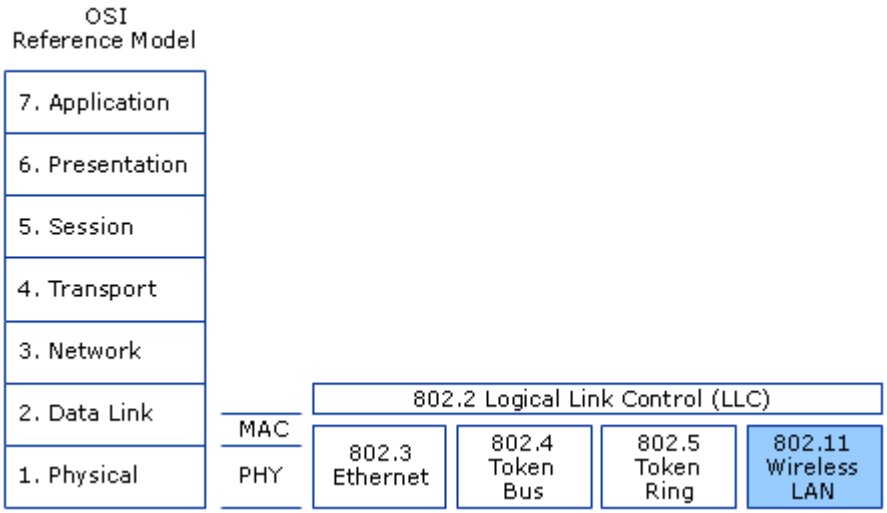
Τα σχετικά με το 802.11 πρωτόκολλα και τεχνολογίες θα αναλυθούν παρακάτω και είναι τα εξής:

1. 802.11: Το πρότυπο IEEE 802.11 ορίζει τις προδιαγραφές για το Φυσικό Επίπεδο (Physical Layer) και για τον έλεγχο των μέσων πρόσβασης (media access control-MAC)
2. 802.1X: Το πρότυπο IEEE 802.1X ορίζει βασισμένο σε πύλες έλεγχο πρόσβασης που χρησιμοποιείται για να παρέχει πιστοποιημένη πρόσβαση δικτύου στα δίκτυα Ethernet.
3. Extensible Authentication Protocol (EAP) over LAN (EAPOL): Το EAP είναι ένα πρωτόκολλο Σημείου προς Σημείο (Point-to-Point Protocol-PPP) που χρησιμοποιείται σαν μηχανισμός πιστοποίησης σε point-to-point τμήματα LAN δικτύων.
4. Wired Equivalent Privacy (WEP): Το γνωστό σε όλους πρωτόκολλο WEP παρέχει υπηρεσίες ασφάλειας των δεδομένων, κρυπτογραφώντας την πληροφορία που ανταλλάσσεται μεταξύ των ασύρματων κόμβων.
5. Wi-Fi Protected Access (WPA): Το WPA είναι ένα προσωρινό πρότυπο μέχρι να επικυρωθεί το IEEE 802.11i πρότυπο. Τα δύο αυτά πρότυπα σχεδιάστηκαν για να αντικαταστήσουν το WEP και προσφέρουν πιο εξελιγμένες μεθόδους κρυπτογράφησης δεδομένων και πιστοποίησης πρόσβασης στο δίκτυο.
6. Wireless Auto Configuration: Η λειτουργία Wireless Auto Configuration των Windows XP και Windows Server 2003 δυναμικά επιλέγει το δίκτυο που θα συνδεθεί με βάση διάφορους παράγοντες όπως οι προτιμήσεις του χρήστη ή οι αρχικές ρυθμίσεις.

2.5.1 Πρωτόκολλο 802.11

Η επιτροπή προτύπων του 802 πρωτοκόλλου ορίζει δύο διαφορετικά επίπεδα το Logical Link Control (LLC) και το Media Access Control (MAC) για το Επίπεδο Διασύνδεσης Δεδομένων του μοντέλου OSI. Το πρότυπο IEEE 802.11 για τα ασύρματα δίκτυα περιγράφει τις

προδιαγραφές για το Φυσικό Επίπεδο και το επίπεδο MAC που επικοινωνεί με το επίπεδο LLC όπως φαίνεται από την εικόνα που ακολουθεί.



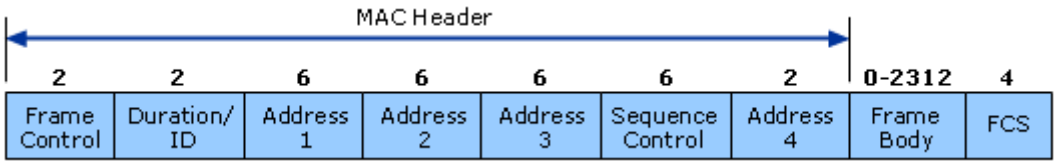
Εικόνα 18: OSI και 802.11

Όλα τα μέρη της 802.11 αρχιτεκτονικής οδηγούν είτε στο υποεπίπεδο MAC του επιπέδου διασύνδεσης ή του φυσικού επιπέδου.

- Πλαίσιο 802.11 MAC:

Το πλαίσιο 802.11 MAC όπως φαίνεται στην παρακάτω εικόνα (Εικόνα 18) αποτελείται από την κεφαλίδα MAC (MAC header), το κυρίως σώμα του πλαισίου και τον έλεγχο ακολουθίας του πλαισίου(Frame CheckSequence-FCS). Οι αριθμοί στην παρακάτω εικόνα αναπαριστούν τον αριθμό των bytes για κάθε πεδίο.

- Μορφοποίηση πλαισίου 802.11 MAC:

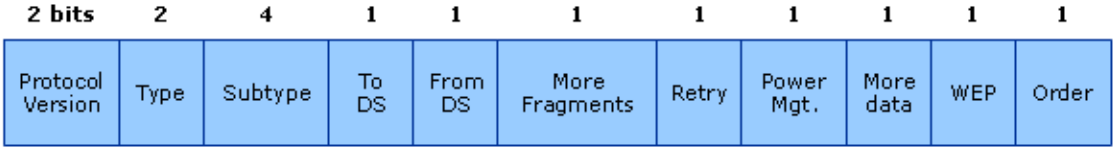


Εικόνα 19: Μορφοποίηση πλαισίου MAC

Η μορφοποίηση του πλαισίου 802.11 MAC φαίνεται ξεκάθαρα στην παραπάνω εικόνα που το πλαίσιο διαχωρίζεται σε πεδία.

Το πρώτο πεδίο, το Frame Control περιέχει πληροφορίες ελέγχουν για τον ορισμό του τύπου του 802.11 MAC πλαισίου και παρέχει πληροφορίες απαραίτητες για να κατανοήσουν τα

επόμενα πεδία τον τρόπο με τον οποίο θα γίνει η επεξεργασία του πλαισίου. Οι αριθμοί στην εικόνα που ακολουθεί συμβολίζουν των αριθμό των bits πάνω από κάθε πεδίο του πεδίου Frame Control.



Εικόνα 20: Το Frame Control πεδίο του πλαισίου 802.11 MAC

Πάνω στο Frame Control πεδίου του πλαισίου 802.11 ορίζονται διάφορα πεδία όπως φαίνεται από την παραπάνω εικόνα. Απαραίτητα στοιχεία όπως η έκδοση του πρωτοκόλλου, ο τύπος του πλαισίου, το αν το πλαίσιο επρόκειτο να εξέλθει από ένα DS, εάν θα ακολουθήσουν περισσότερα πακέτα πληροφορίας, η διαχείριση ενέργειας, εάν θα χρησιμοποιηθούν μέθοδοι πιστοποίησης και άλλα.

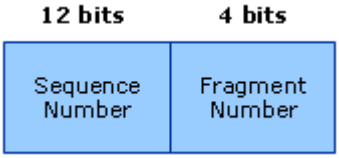
Το πεδίο Duration/ID δείχνει την απαιτούμενη διάρκεια για την μετάδοση του επόμενου πλαισίου.

Τα πεδία Address (4 σε αριθμό) θα περιέχουν έναν συνδυασμό από τις εξής επιλογές:

- BSS Identifier (BSSID): Είναι ένα αναγνωριστικό που ταυτοποιεί μοναδικά κάθε BSS.
- Destination Address (DA): Αυτή η πληροφορία δηλώνει την διεύθυνση MAC του παραλήπτη που θα παραλάβει το πλαίσιο.
- Source Address (SA): Αυτή η πληροφορία δηλώνει την διεύθυνση MAC της πηγής της πληροφορίας που αρχικά δημιούργησε και μετέδωσε το πλαίσιο.
- Receiver Address (RA): Αυτή η πληροφορία δηλώνει την διεύθυνση MAC του αμέσως επόμενου STA σταθμού στο ασύρματο μέσο που θα παραλάβει το πλαίσιο.
- Transmitter Address (TA): Αυτή η πληροφορία δηλώνει την διεύθυνση MAC του σταθμού STA που μετέδωσε το πλαίσιο στο ασύρματο μέσο.

Το πεδίο Sequence Control περιέχει δύο υποπεδία, το Fragment Number και το Sequence Number.Το πρώτο δηλώνει τον αριθμό κάθε πλαισίου που έχει αποσταλεί σαν κατακερματισμένο πλαίσιο. Έχει αρχική τιμή 0 και κάθε φορά προστίθεται 1 ανάλογα με τον αριθμό των υποπλαισίων. Το δεύτερο δηλώνει τον ακολουθιακό (αύξων αριθμό δηλαδή

αριθμό σειράς) κάθε πλαισίου. Αυτό είναι ίδιο για κάθε υποπλαίσιο ενός κατακερματισμένου πλαισίου. Διαφορετικά ο αριθμός αυξάνεται κατά ένα κάθε φορά για κάθε πλαίσιο που στέλνεται μέχρι να φτάσει το 4095 όπου και μηδενίζεται για να ξεκινήσει πάλι από την αρχή.



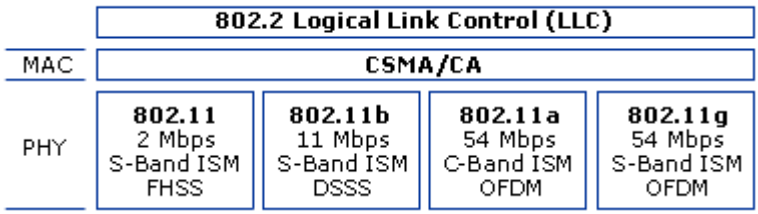
Εικόνα 21: Το Sequence Control πεδίο του πλαισίου 802.11 MAC

Το κύριο σώμα του πλαισίου (Frame Body) περιέχει δεδομένα τα οποία συμπεριλαμβάνονται είτε σε πλαίσια διαχείρισης είτε σε πλαίσια δεδομένων.

Ο σταθμός STA που μεταδίδει το πλαίσιο χρησιμοποιεί κυκλικό περιοδικό έλεγχο (Cyclic Redundancy Check-CRC) πάνω στα πεδία της κεφαλίδας MAC και στα πεδία του κυρίως σώματος του πλαισίου για να παράγει τον αριθμό FCS (Frame Check Sequence). Ο σταθμός STA αποδέκτης του πλαισίου χρησιμοποιεί τον ίδιο CRC υπολογισμό για να παράγει την τιμή του δικού του FCS πεδίου και να τα συγκρίνει με αυτό που μεταδόθηκε ώστε να συμπεράνει με αυτόν τον τρόπο τυχόν σφάλματα που έχουν συμβεί κατά την μετάδοσης του πλαισίου.

- Υποεπίπεδο 802.11 PHY(802.11 PHY Sublayer):

Στο φυσικό υποεπίπεδο (PHY),το IEEE 802.11 ορίζει μια σειρά από μοντέλα κωδικοποίησης και μετάδοσης για τις ασύρματες επικοινωνίες εκ των οποίων τα ποιο γνωστά μοντέλα μετάδοσης είναι τα Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS) και Orthogonal Frequency Division Multiplexing (OFDM). Η παρακάτω εικόνα δείχνει τα 802.11, 802.11b, 802.11a και 802.11g πρότυπα που υπάρχουν στο υποεπίπεδο PHY και θα αναλυθούν παρακάτω.



Εικόνα 22: Το υποεπίπεδο 802.11 PHY

- IEEE 802.11:

Ο ρυθμός μεταφοράς δεδομένων για το αρχικό IEEE 802.11 είναι 2 Mbps χρησιμοποιώντας τον FHSS τρόπο μετάδοσης με την ISM ζώνη συχνοτήτων που λειτουργεί στο εύρος

συχνοτήτων 2.4 με 2.5 GHz. Ωστόσο, σε μη ιδανικές συνθήκες χρησιμοποιείται ταχύτητα 1 Mbps.

- IEEE 802.11b:

Η κύρια βελτίωση από το IEEE 802.11 στο IEEE 802.11b είναι η προσθήκη της ικανότητας του Φυσικού Επιπέδου να δέχεται μεγαλύτερους ρυθμούς μεταφοράς δεδομένων. Το IEEE 802.11b υποστηρίζει δύο επιπλέον ταχύτητες μία στα 5.5 Mbps και μία στα 11 Mbps χρησιμοποιώντας το S-Band ISM. Το πρότυπο μετάδοσης DSSS χρησιμοποιείται για να υποστηρίξει μεγαλύτερες μεταφορές δεδομένων. Ο ρυθμός μεταφοράς δεδομένων των 11 Mbps είναι εφικτός σε ιδανικές συνθήκες. Σε κανονικές συνθήκες χρησιμοποιούνται οι ταχύτητες των 5.5 , 2 και 1 Mbps.

- IEEE 802.11a:

Το IEEE 802.11a ήταν το πρώτο πρότυπο που επικυρώθηκε αλλά μόλις στην εποχή μας χρησιμοποιείται σε τέτοιο μεγάλο εύρος.
Λειτουργεί σε ρυθμούς μεταφοράς της τάξης των 54 Mbps και χρησιμοποιεί το C-Band ISM το οποίο λειτουργεί σε συχνότητες μεταξύ 5.725 και 5.875 GHz.
Αντί για το DSSS το 802.11a χρησιμοποιεί το OFDM, που επιτρέπει στα δεδομένα να μεταδίδονται από υποσυχνότητες σε παραλληλία
και παρέχει μεγαλύτερη αντίσταση σε παρεμβολές και καλύτερη διακίνηση δεδομένων.
Επειδή(σε αντίθεση με το 802.11b) δεν είναι στις ίδιες συχνότητες με άλλες S-Band συσκευές(όπως φούρνοι μικροκυμάτων, συσκευές Bluetooth κ.λ.π.) το 802.11a
παρέχει και μεγαλύτερη μεταφορά δεδομένων και καθαρότερο σήμα.
Ο ρυθμός μεταφοράς δεδομένων των 54 Mbps είναι εφικτός σε ιδανικές συνθήκες. Σε κανονικές συνθήκες χρησιμοποιούνται οι ταχύτητες των 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps και 6 Mbps.

- IEEE 802.11g:

Το IEEE 802.11g λειτουργεί σε μεταφορές δεδομένων της τάξης των 54 Mbps, αλλά χρησιμοποιεί το S-Band ISM και OFDM.
Το 802.11g είναι συμβατό με το 802.11b και μπορεί να λειτουργήσει στις ταχύτητες του 802.11b και να χρησιμοποιήσει DSSS.

Όπως και το 802.11a,ο ρυθμός μεταφοράς δεδομένων των 54 Mbps είναι εφικτός σε ιδανικές συνθήκες. Σε κανονικές συνθήκες χρησιμοποιούνται οι ταχύτητες των 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps και 6 Mbps.

3 ΠΡΩΤΟΚΟΛΛΟ MOBILE IP

3.1 Εισαγωγή

Στο παρών κεφάλαιο, που αποτελεί το κύριο σώμα ανάλυσης του πρωτοκόλλου και της λειτουργικότητας του Mobile IP θα ακολουθηθεί συγκεκριμένη προσέγγιση σχετικά με την ανάλυση του περιεχομένου. Στο μεγαλύτερο κομμάτι του κεφαλαίου θα αναλυθούν οι συνιστάμενες του Mobile IP στις οποίες συμπεριλαμβάνονται η λειτουργίες, οι εφαρμογές, ορισμός και πλεονεκτήματα του πρωτοκόλλου. Στο τέλος του κεφαλαίου θα δοθούν πληροφορίες που αφορούν το πρωτόκολλο Mobile IPv4.

Το πρωτόκολλο Mobile IP επιτρέπει την δρομολόγηση των πακέτων IP στο διαδίκτυο ανεξάρτητα από την τοποθεσία τους. Ένας κινητός κόμβος αναγνωρίζεται με την βοήθεια της δικής του διεύθυνσης IP κρύβοντας την τρέχουσα θέση του στο διαδίκτυο. Οι υπηρεσίες διασύνδεσης φορητών συσκευών γνωρίζουν ιδιαίτερη ανάπτυξη τις τελευταίες δεκαετίες ενισχύουν την πρόσβαση στο διαδίκτυο από διάφορα κινητά τελικά σημεία (συσκευές) των οποίων οι χρήστες αυξάνονται ολοένα και περισσότερο στις μέρες μας. Όταν ο mobile κόμβος βρίσκεται εντός της εμβέλειας ενός ξένου δικτύου, συνοδεύεται από το COA (Care of Address) του που αναγνωρίζει τον κόμβο αυτό μοναδικά και περιέχει πληροφορίες σχετικά με την τρέχουσα θέση του και το αρχικό δίκτυο που ανήκει(home address).

Η μεγαλύτερη πρόκληση ήταν ο ολοένα και αυξανόμενος αριθμός χρηστών των mobile υπηρεσιών με ποικιλία υπηρεσιών και συσκευών με ασύρματη επικοινωνία και ειδικά στην περίπτωση που μετακινούνταν από το δίκτυο της περιοχής που κατοικούσαν σε ένα ξένο δίκτυο της περιοχής που επισκέπτονταν. Σε αυτήν την περίπτωση ο mobile κόμβος αλληλοεπιδρά και με το αρχικό δίκτυο.

Οι ερευνητές έπειτα από μελέτες κατέληξαν στο συμπέρασμα ότι μεγάλη σημασία στην φορητότητα διαδραματίζει το αρχιτεκτονικό επίπεδο της IP.

Εάν γίνει η υπόθεση ότι ένας mobile κόμβος εισέρχεται σε ένα ξένο δίκτυο με πληροφορίες σχετικά με το αρχικό του δίκτυο χωρίς να έχει πληροφορίες για το νέο σημείο προσκόλλησης του(στο νέο δίκτυο), τότε ο δρομολογητής δεν μπορεί αποστείλει ορθά τα απαραίτητα δεδομένα. Κατά συνέπεια ο mobile κόμβος θα πρέπει να επαναριθμήσει την διεύθυνση IP του πράγμα που είναι αρκετά δύσκολο στη διαχείριση. Έτσι εάν ο κόμβος αλλάξει τη θέση του

χωρίς να αλλάξει την διεύθυνση IP του, χάνει την δρομολόγηση του. Εάν αλλάξει την διεύθυνση IP του τότε χάνει την σύνδεση του.

3.2 Ορισμός

"Το Mobile IP είναι ένα IETF πρωτόκολλο επικοινωνίας που είναι σχεδιασμένο για να επιτρέπει στους χρήστες κινητής τηλεφωνίας να μετακινούνται από το ένα δίκτυο στο άλλο χωρίς να αλλάζει η διεύθυνση IP τους."
Το πρωτόκολλο αυτό βγαίνει σε δύο κύριες εκδόσεις την IPV4 που ορίστηκε στο IETF RFC 5944 και τις επεκτάσεις του που ορίστηκαν στο IETF RFC 4721. Η άλλη έκδοση του πρωτοκόλλου Mobile IP, η IPv6 υλοποιήθηκε για το IPv6 πρωτόκολλο του διαδικτύου και ορίστηκε στο RFC 6275.

3.3 Πλεονεκτήματα και εφαρμογές

Το πρωτόκολλο Mobile IP είναι ιδιαίτερα σημαντικό στις μέρες μας. Σε παλαιότερες εποχές γινόταν χρήση μόνο τηλεφώνων που συνδέονταν σε σταθερές τηλεφωνικές γραμμές οι οποίες δέσμευαν την φορητότητα των χρηστών. Αυτό είχε σαν αποτέλεσμα οι καταναλωτές να στραφούν σε μοντέρνα δίκτυα κινητής που ήταν στη φύση τους ασύρματα για να μετακινούνται εύκολα από το ένα δίκτυο στο άλλο.
Ωστόσο, οι ασύρματες τεχνολογίες συνοδεύονται και από αρνητικά όπως είναι η κάλυψη σήματος και το απαγορευτικό κόστος. Είναι σχεδόν ξεκάθαροι οι λόγοι για τους οποίους το mobile computing είναι στην εποχή μας τόσο δημοφιλές. Στις μέρες μας φορητές συσκευές με πρόσβαση στο διαδίκτυο χρησιμοποιούνται από πολλά εκατομμύρια καταναλωτές.

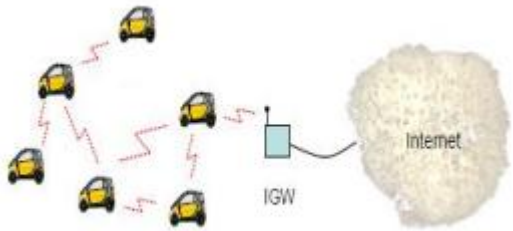
Κάποια από τα σημαντικά πλεονεκτήματα του πρωτοκόλλου Mobile IP είναι τα εξής:

- Οι συσκευές προσφέρουν τις υπηρεσίες τους ανεξάρτητα από την τοποθεσία τους.
- Οικονομία σε φυσικούς πόρους καθώς δεν υπάρχουν ανάγκες δημιουργίας και συντήρησης καλωδιώσεων.
- Ασύρματες δικτυακές υπηρεσίες.
- Αξιόπιστη και συνεχή συνδεσιμότητα.

Υπάρχουν μερικά παραδείγματα περιπτώσεων όπου η χρήση των Mobile IP τεχνολογιών ιδιαίτερα σημαντική:

- Σε θέματα συνεργατικότητας που αφορούν γραφεία εταιρειών ή οργανισμών. Μέσω αυτών των τεχνολογιών οι εργαζόμενοι μπορούν να αλληλεπιδρούν μεταξύ τους σε προσωπικό επίπεδο. Επιπλέον τους επιτρέπει να διαμοιράζονται μεταξύ τους πληροφορία.
- Σε νοσοκομεία όπου οι ασθενείς μπορούν να μοιράζονται αναφορές με τους γιατρούς χωρίς να χρειάζονται να τους επισκεφθούν σε περίπτωση έκτακτης ανάγκης.
- Σε στρατιωτικές επιχειρήσεις όπου η ανάγκη για μετάδοση πληροφοριών είναι αυξημένη.
- Σε δίκτυα οχημάτων που θα αναλυθεί παρακάτω.

Τα adhoc δίκτυα οχημάτων έχουν ιδιαίτερη σημασία για την επικοινωνία μεταξύ των οχημάτων επειδή επιτρέπουν την τοπική διασύνδεση μεταξύ των οχημάτων χωρίς κάποια υποδομή, φόρτο παραμετροποίησης και χωρίς το μεγάλο κόστος άλλων δικτύων. Πέρα από την ανταλλαγή τοπικά δεδομένων μεταξύ των αυτοκινήτων τα δίκτυα οχημάτων μπορούν να επεκταθούν έχοντας πρόσβαση σε υπηρεσίες του διαδικτύου. Υπάρχουν ειδικές θύρες που ονομάζονται IGW (Internet Gateways) που μπορούν να προσφέρουν προσωρινή πρόσβαση στο δίκτυο όπως φαίνεται στην εικόνα που υπάρχει παρακάτω.



Εικόνα 23: Ένα adhoc δίκτυο οχημάτων

3.4 Λειτουργικότητα

3.4.1 Εισαγωγή

Οι σύγχρονες εκδόσεις του πρωτοκόλλου διαδικτύου (IP) παίρνουν σαν δεδομένο ότι το σημείο στο οποίο ένας Η/Υ προσαρτάται στο διαδίκτυο ή σε ένα δίκτυο είναι σταθερό και η διεύθυνση IP του δηλώνει το δίκτυο στο οποίο έχει προσαρτηθεί. Τα δεδομενογράμματα

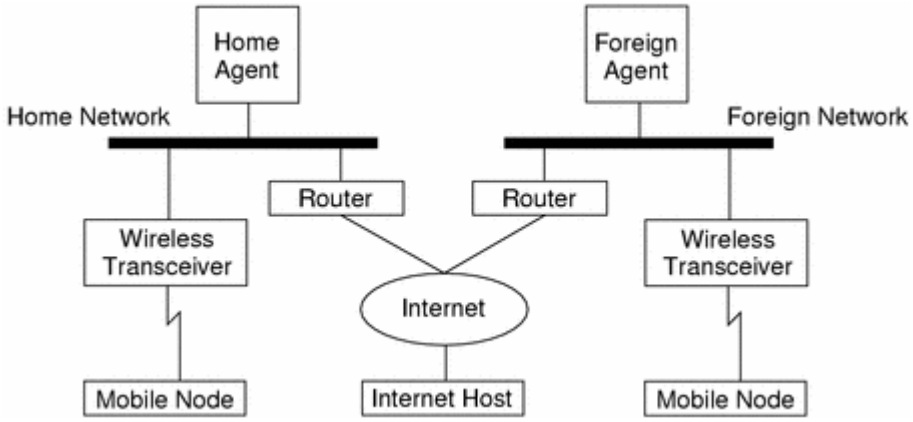
(datagrams) στέλνονται σε έναν υπολογιστή βάση της πληροφορίας για την τοποθεσία που υπάρχει στην διεύθυνση IP.

Εάν ένας φορητός υπολογιστής ή φορητός κόμβος μετακινηθεί σε ένα άλλο δίκτυο διατηρώντας την διεύθυνση IP του, η διεύθυνση αυτή δεν αντικατοπτρίζει πλέον το δίκτυο στο οποίο είναι προσαρτημένος. Κατά συνέπεια τα υπάρχοντα πρωτόκολλα δρομολόγησης δεν μπορούν να κατευθύνουν δεδομενογράμματα σε αυτόν τον κόμβο σωστά. Σε αυτήν την περίπτωση θα πρέπει να γίνει επαναπροσδιορισμός της διεύθυνσης IP του κόμβου με βάση την νέα του τοποθεσία γεγονός που είναι ένα φορτικό πρόβλημα. Έτσι με βάση το τωρινό πρωτόκολλο του διαδικτύου εάν ο κόμβος κινείται χωρίς να αλλάζει την διεύθυνση IP του χάνει την δρομολόγηση του και εάν την αλλάζει χάνει την σύνδεση του.

Το Mobile IP λύνει αυτό το πρόβλημα επιτρέποντας στον κόμβο να χρησιμοποιεί δύο διευθύνσεις IP. Η μία δηλώνει την διεύθυνση δικτύου που ανήκει (home address) και η άλλη δηλώνει μια προσωρινή διεύθυνση (Care Of Address-COA) που μεταβάλλεται ανάλογα με το δίκτυο στο οποίο προσαρτάται. Η Mobile IP επιτρέπει σε μία συσκευή να πλοηγείται ελεύθερα στο διαδίκτυο ή στο δίκτυο ενός οργανισμού διατηρώντας σταθερή την αρχική του διεύθυνση δηλαδή την home address. Με αυτόν δεν διακόπτονται οι δικτυακές λειτουργίες του υπολογιστή όταν μετακινείται από το ένα δίκτυο στο άλλο. Αντίθετα, το δίκτυο ενημερώνεται για την νέα θέση του φορητού κόμβου.

3.4.2 Παράδειγμα λειτουργίας

Με βάση την τοπολογία που φαίνεται στην παρακάτω εικόνα παρουσιάζεται ο τρόπος με τον οποίο κινείται ένα δεδομενόγραμμα στα πλαίσια του MobileIP.



Εικόνα 24: Παράδειγμα κίνησης ενός δεδομενογράμματος σε ένα Mobile IP δίκτυο

1. Ο host του διαδικτύου στέλνει ένα δεδομενόγραμμα χρησιμοποιώντας την αρχική διεύθυνση (home address) του φορητού κόμβου.
2. Εάν ο φορητός κόμβος (mobile node) βρίσκεται εντός του αρχικού δικτύου (home network) τότε το δεδομενόγραμμα παραδίδεται μέσω της κανονικής IP διαδικασίας. Διαφορετικά το δεδομενόγραμμα παραδίδεται στον agent του αρχικού δίκτυο (home agent).
3. Εάν ο φορητός κόμβος βρίσκεται εντός ξένου δικτύου ο agent του αρχικού δικτύου προωθεί το δεδομενόγραμμα στον agent του ξένου δικτύου.
4. Ο agent του ξένου δικτύου παραδίδει το δεδομενόγραμμα στον φορητό κόμβο.
5. Τα δεδομενογράμματα από τον φορητό κόμβο προς το διαδίκτυο στέλνονται χρησιμοποιώντας παραδοσιακές IP διαδικασίες δρομολόγησης. Εάν ο φορητός κόμβος βρίσκεται σε ξένο δίκτυο τα πακέτα παραδίδονται στον agent του ξένου δικτύου ο οποίος και τα προωθεί στο διαδίκτυο.

3.4.3 Βασικές οντότητες

Το Mobile IP εισάγει τις εξής λειτουργικές οντότητες:

- Mobile Node (MN) ή Φορητός Κόμβος: Είναι το host ή το router που μεταβάλει το σημείο προσάρτησης του από το ένα δίκτυο στο άλλο.

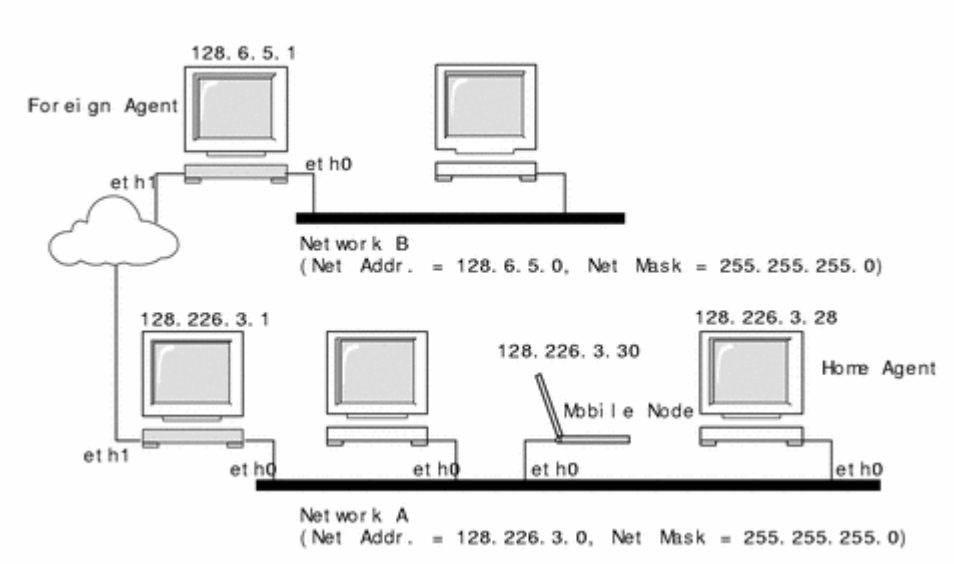
- Home Agent (HA) ή Αρχικό Μέσο: Είναι το router στο αρχικό δίκτυο ενός φορητού κόμβου που παρεμβάλλεται στα δεδομενογράμματα που προορίζονται για τον Φορητό Κόμβο και τα παραδίδει μέσω της προσωρινής διεύθυνσης (COA-Care Of Address). Επίσης διατηρεί και τις πληροφορίες που αφορούν την τρέχουσα τοποθεσία του φορητού κόμβου.
- Foreign Agent (FA) ή Ξένο Μέσο: Είναι το router στο δίκτυο που επισκέπτεται ο φορητός κόμβος και παρέχει υπηρεσίες δρομολόγησης στον φορητό κόμβο όταν αυτός είναι καταχωρημένος στο δίκτυο.

3.4.4 Τρόπος λειτουργίας

Οι τεχνολογίες Mobile IP ενεργοποιούν την δρομολόγηση δεδομενογραμμάτων σε φορητούς κόμβους. Η αρχική διεύθυνση του φορητού κόμβου πάντα διαχωρίζει μοναδικά τον κόμβο αυτό ανεξάρτητα από το τρέχων σημείο πρόσδεσης δηλαδή το τρέχων δίκτυο. Όταν ο κόμβος είναι μακριά από το αρχικό δίκτυο μια δεύτερη διεύθυνση (Care Of Address-COA) συσχετίζει τον κόμβο με την αρχική του διεύθυνση παρέχοντας πληροφορίες σχετικά με το υπάρχων σημείο πρόσδεσης του κόμβου είτε στο διαδίκτυο είτε στο δίκτυο κάποιου οργανισμού. Η Mobile IP χρησιμοποιεί μηχανισμούς καταχώρησης για να καταχωρήσει την COA διεύθυνση με τη χρήση του home agent.

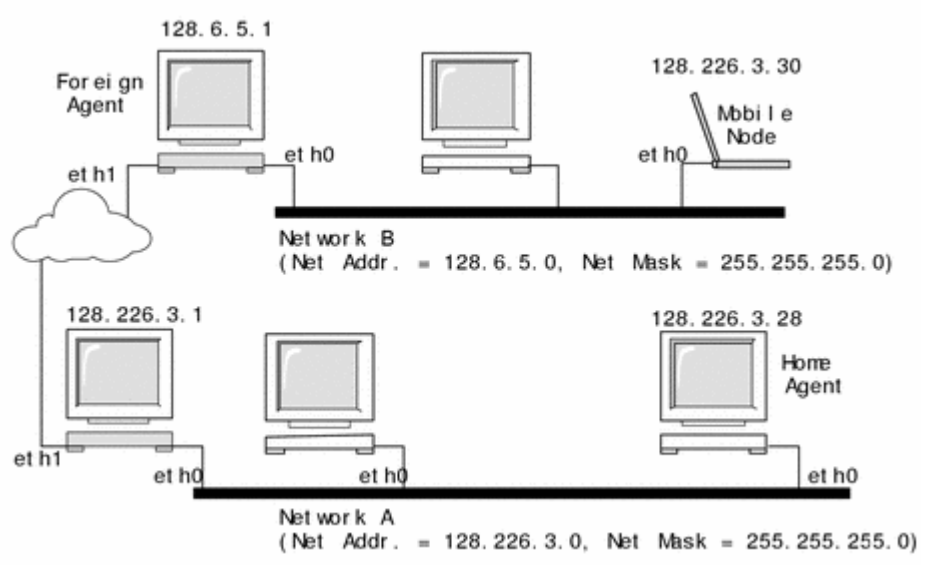
Ο home agent ανακατευθύνει δεδομενογράμματα από το αρχικό δίκτυο στην διεύθυνση COAδημιουργώντας μια νέα IP κεφαλίδα(header) που περιέχει την COA διεύθυνση του φορητού κόμβου σαν την IP διεύθυνση προορισμού. Αυτή η νέα κεφαλίδα ενθυλακώνει το αρχικό IP δεδομενόγραμμα αναιρώντας την επιρροή της αρχικής διεύθυνσης (home address) ώστε να μην έχει επιρροή στην δρομολόγηση του ενθυλακωμένου δεδομενογράμματος μέχρι να φτάσει στην διεύθυνση COA. Αυτός ο τρόπος ενθυλάκωσης ονομάζεται διοχέτευση (tunneling). Μετά την άφιξη στην διεύθυνση COA κάθε δεδομενόγραμμα αποθυλακώνεται και παραδίδεται στον φορητό κόμβο.

Η εικόνα που ακολουθεί απεικονίζει έναν φορητό κόμβο που έχει έδρα στο home network που ανήκει, το δίκτυο Α στην προκειμένη περίπτωση, πριν αυτός μεταβεί στο ξένο δίκτυο Β. Και τα δύο δίκτυα υποστηρίζουν Mobile IP. Ο φορητός κόμβος συσχετίζεται με το αρχικό του δίκτυο, μέσω της διεύθυνσης IP του που είναι η 128.226.3.30. Παρά το ότι το δίκτυο Α έχει δικό του agent, τα δεδομενογράμματα που προορίζονται για τον φορητό κόμβο μεταδίδονται μέσω της κανονικής IP διαδικασίας.



Εικόνα 25: Η ύπαρξη του φορητού κόμβου στο δίκτυο που ανήκει

Η εικόνα που ακολουθεί (Εικόνα 26) απεικονίζει τον φορητό κόμβο να μετακινείται σε ένα ξένο δίκτυο, το δίκτυο Β. Τα δεδομενογράμματα που προορίζονται για τον φορητό κόμβο ανακόπτονται από τον agent του αρχικού δικτύου(δικτύου Α) ενθυλακωμένα και αποστέλλονται στον foreign agent του δικτύου Β. Όταν ολοκληρώνεται η λήψη του ενθυλακωμένου δεδομενογράμματος ο foreign agent αποκολλά την εξωτερική κεφαλίδα και παραδίδει το δεδομενόγραμμα στον φορητό κόμβο που έχει επισκεφθεί το δίκτυο Β.



Εικόνα 26: Η ύπαρξη του φορητού κόμβου σε ένα ξένο δίκτυο

Η διεύθυνση COA μπορεί να ανήκει στον foreign agent, ή μπορεί να αποκτηθεί από τον φορητό κόμβο μέσω των πρωτοκόλλων Dynamic Host Configuration Protocol (DHCP) ή Point-to-Point Protocol (PPP).

Ο φορητός κόμβος χρησιμοποιεί μια ειδική διαδικασία καταχώρησης για να κρατήσει ενήμερο σχετικά με την θέση του τον home agent του αρχικού του δικτύου. Όποτε ο φορητός κόμβος μετακινείται από το αρχικό του δίκτυο σε ένα ξένο ή από ένα ξένο σε ένα άλλο ξένο δίκτυο, επιλέγει έναν foreign agent του δικτύου στο οποίο εισήλθε για να αποστείλει ένα μήνυμα καταχώρησης στον home agent του αρχικού του δικτύου.

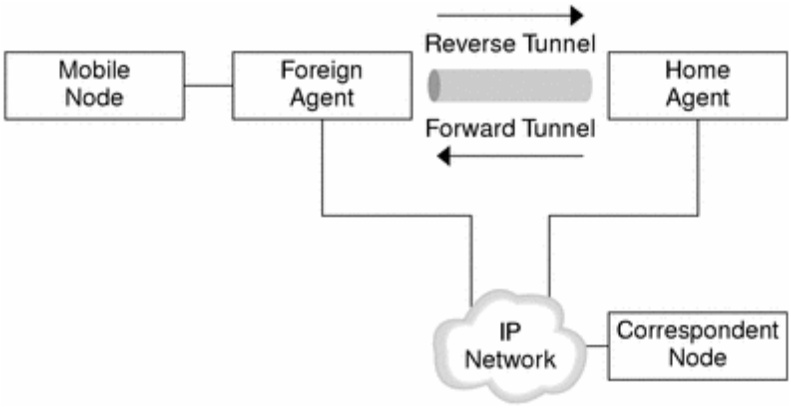
Γενικότερα οι agents (του αρχικού και των ξένων δικτύων) δηλώνουν την παρουσία τους μέσω μηνυμάτων.

Ένας φορητός κόμβος μπορεί προαιρετικά να ζητήσει το δηλωμένο μήνυμα ενός agent από κάποιους άλλους τοπικά τοποθετημένους agents του δικτύου. Ο φορητός κόμβος λαμβάνει αυτές τις δηλώσεις και ανάλογα αποφασίζει εάν βρίσκεται στο αρχικό του ή σε ξένο δίκτυο.

Όταν ο φορητός κόμβος ανιχνεύει ότι βρίσκεται εντός του αρχικού δικτύου, λειτουργεί χωρίς τις υπηρεσίες που αφορούν την φορητότητα. Όταν επιστρέφει στο αρχικό δίκτυο ενώ προηγουμένως είχε καταχωρηθεί αλλού, τότε αναιρεί την καταχώρηση στον home agent.

- Mobile IP με αντίστροφη διοχέτευση

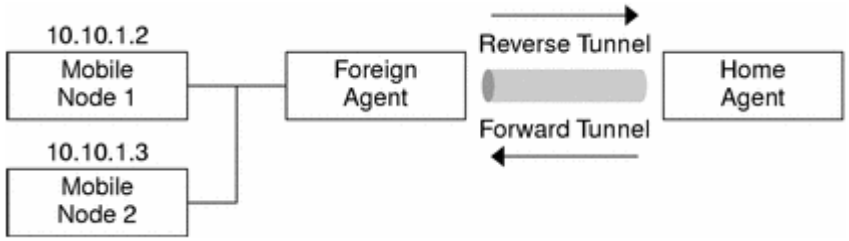
Η προηγούμενη περιγραφή της Mobile IP προϋποθέτει ότι η δρομολόγηση μέσα στο διαδίκτυο είναι ανεξάρτητη από την πηγαία διεύθυνση του πακέτου δεδομένων. Ωστόσο, οι ενδιάμεσοι δρομολογητές μπορεί να ελέγξουν για μια τοπολογικά σωστή πηγαία διεύθυνση. Εάν ένας ενδιάμεσος δρομολογητής κάνει τον έλεγχο, θα πρέπει να δημιουργηθεί μια αντίστροφη δίοδος. Δημιουργώντας μια αντίστροφη διοχέτευση από την διεύθυνση COA προς τον homeagent εξασφαλίζεται η ορθότητα της πηγαίας διεύθυνσης για το IP πακέτο δεδομένων. Ένας φορητός κόμβος μπορεί να ζητήσει μια αντίστροφη δίοδο μεταξύ των δύο agents του home και του foreign όταν ο καταχωρείται ο φορητός κόμβος.



Εικόνα 27: Mobile IP με χρήση αντίστροφης διοχέτευσης

- Όριο υποστήριξης ιδιωτικών διευθύνσεων

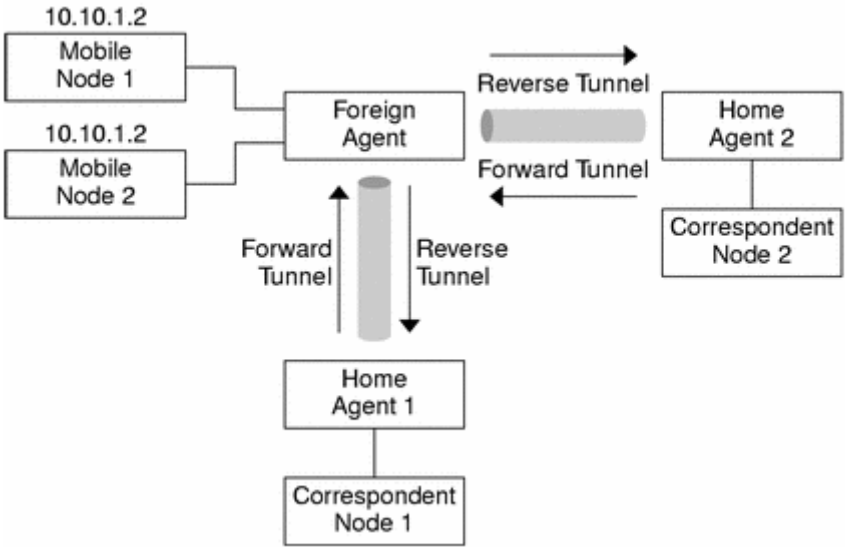
Οι φορητοί κόμβοι που έχουν ιδιωτικές διευθύνσεις που δεν είναι δρομολογήσιμοι μέσω του διαδικτύου απαιτούν αντίστροφες διόδους. Οι οργανισμοί και οι εταιρείες απασχολούν ιδιωτικές διευθύνσεις όταν δεν απαιτείται εξωτερική σύνδεση. Όταν ένας φορητός κόμβος έχει μια ιδιωτική διεύθυνση, τότε μπορεί να επικοινωνήσει με έναν αντίστοιχο κόμβο μόνο μέσω αντίστροφης διοχέτευσης. Στο διάγραμμα που ακολουθεί φαίνεται η τοπολογία ενός δικτύου με δύο φορητούς κόμβους που έχουν ιδιωτική διεύθυνση και χρησιμοποιούν την ίδια COA διεύθυνση όταν καταχωρούνται στον ίδιο foreignagent.



Εικόνα 28: Δύο φορητοί κόμβοι με ιδιωτικές διευθύνσεις καταχωρημένοι στον ίδιο foreign agent

Επειδή οι δύο κόμβοι ανήκουν στον ίδιο διαχειριστικό τομέα, ο homeagent γνωρίζει πως θα δρομολογήσει τα πακέτα δεδομένων στον κάθε ένα από τους δύο κόμβους. Επίσης, η COA διεύθυνση του foreign agent και η IP διεύθυνση του home agent θα πρέπει να είναι δρομολογήσιμες διευθύνσεις.

Υπάρχει η πιθανότητα να υπάρχουν δύο φορητοί κόμβοι με ιδιωτικές διευθύνσεις με την ίδια διεύθυνση IP ενώ βρίσκονται στο ίδιο ξένο δίκτυο. Αυτή η περίπτωση είναι δυνατή μόνο όταν κάθε ένας φορητός κόμβος έχει διαφορετικό home agent. Επίσης αυτό είναι δυνατόν να συμβεί όταν κάθε φορητός κόμβος είναι σε διαφορετικό υποδίκτυο ενός μόνο foreign agent. Στην ακόλουθη εικόνα φαίνεται αυτή η περίπτωση:



Εικόνα 29: Δύο φορητοί κόμβοι σε διαφορετικά ξένα δίκτυα

3.4.5 Πρωτόκολλο Mobile IPv4

Το πρωτόκολλο Mobile IPv4 προϋποθέτει ότι η διεύθυνση IP ενός κόμβου αναγνωρίζει το σημείο προσάρτησης του κόμβου στο διαδίκτυο. Δύο διαδικασίες υπάρχουν ώστε ο κόμβος να αλλάξει το σημείο προσάρτησης του:

- Ο κόμβος θα πρέπει να αλλάξει την διεύθυνση IP του για να αλλάξει το σημείο προσάρτησης.
- Το πλήθος των ειδικών διαδρομών θα πρέπει να πολλαπλασιαστεί σε ένα μεγάλο μέρος του υφάσματος δρομολόγησης του διαδικτύου.

Οι λειτουργίες του Mobile IPv4 περιλαμβάνουν 3 βασικά βήματα:

- *Ανακάλυψη του παράγοντα (Agent discovery):*Ο παράγοντας (agent) στέλνει περιοδικά πακέτα πληροφορίας για να ειδοποιήσει ότι είναι παρών σε κάθε διαδρομή που προσφέρει υπηρεσίες.
- *Καταχώρηση του παράγοντα (Agent Registration):*Όταν ο φορητός κόμβος απομακρύνεται μακριά από το αρχικό δίκτυο, θα πρέπει να καταχωρήσει την

διεύθυνση στον home agent για να εξασφαλισθεί ότι θα μπορεί ο δεύτερος να προωθήσει πακέτα σε αυτόν. Ανάλογα με τους τρόπους συσχετισμού του με τον foreign agent ο φορητός κόμβος μπορεί να καταχωρηθεί είτε άμεσα μέσω του home agent ή έμμεσα μέσω του foreign agent.

- *Μεταφορά δεδομένων (Datatransfer):* Μετά την καταχώρηση, ο home agent ενθυλακώνει κάθε πακέτο που περιέχει την διεύθυνση COA του φορητού κόμβου και τα προωθεί στην τοποθεσία του μέσω του foreign agent.

3.4.6 Προβλήματα του Mobile IPv4

Παρά τις αποτελεσματικές λύσεις το πρωτόκολλο Mobile IPv4 έχει κάποια προβλήματα τα οποία χρειαζόντουσαν επίλυση. Αυτά καθιστούσαν μη αποδοτική την επικοινωνία που ενέπλεκε γενικότερα το πρωτόκολλο Mobile IP. Υπάρχουν ζητήματα ασφαλείας, διπλοεγγραφές πεδίων και ζητήματα αξιοπιστίας. Τα ζητήματα που απασχολούν το Mobile IP είναι τα εξής:

1. *Ασφάλεια:* Η ασφάλεια είναι το πιο φλέγον ζήτημα του πρωτοκόλλου. Γίνεται εδώ και μεγάλο διάστημα προσπάθεια για τον παραλληλισμό της ασφάλειας του με τους κανόνες ασφαλείας που υπάρχουν για την χρήση εντός του διαδικτύου. Ειδικότερα, τα τείχη προστασίας προκαλούν προβλήματα στο πρωτόκολλο Mobile IPv4 καθώς απαγορεύουν την διέλευση όλων των εισερχομένων πακέτων που δεν πληρούν συγκεκριμένα κριτήρια. Τα τείχη προστασίας εταιρειών ή οργανισμών είναι ειδικά παραμετροποιημένα ώστε να εμποδίζουν πακέτα πληροφορίας που έρχονται από το διαδίκτυο που φαίνεται ότι έχουν βγει από συσκευές εντός του δικτύου. Παρ' όλο που αυτό επιτρέπει την διαχείριση των εντός δικτύου συσκευών(που έχουν πρόσβαση στο διαδίκτυο) με πολύ πιο εύκολο τρόπο, δημιουργεί προβλήματα στους φορητούς κόμβους μέσα στα δίκτυα αυτά. Τέτοιου είδους επικοινωνίες μεταφέρουν την αρχική διεύθυνση του φορητού κόμβου και κατά συνέπεια θα αποκλειστούν από το τείχος προστασίας.
2. *Προβλήματα τριγωνοποίησης:* Η τριγωνική δρομολόγηση είναι πιθανόν το δεύτερο μεγαλύτερο πρόβλημα του Mobile IP. Η κύρια ιδέα του προβλήματος ξεκινά από έναν φορητό κόμβο που θέλει να στείλει ένα πακέτο σε έναν κόμβο που βρίσκεται εντός του ίδιου δικτύου. Ο κόμβος δέκτης μπορεί την συγκεκριμένη χρονική στιγμή να βρίσκεται μακριά από το διαδίκτυο ή το αρχικό κοινό δίκτυο. Όταν συμβαίνει αυτό ο κόμβος αποστολέας κατευθύνει όλα τα πακέτα στο αρχικό

δίκτυο. Αυτά περνούν μέσα από το διαδίκτυο για να φτάσουν στον home agent και μετά διοχετεύονται προς τα πίσω ώστε να φτάσουν στον foreign agent. Θα ήταν βέλτιστο εάν ο κόμβος αποστολέας μπορούσε να αντιληφθεί ότι ο κόμβος δέκτης βρίσκεται στο ίδιο δίκτυο και να του τα στείλει απευθείας. Ο στόχος είναι να παραδοθούν τα πακέτα όσο πιο άμεσα γίνεται χωρίς να περάσει μέσα από τον home agent. Αυτός ο τρόπος ονομάζεται τριγωνική δρομολόγηση και αποτελεί πρόβλημα καθώς η διαδρομή από τον αποστολέα στον παραλήπτη γίνεται με ενδιάμεσο σταθμό και όχι άμεσα.

3. *Η διπλοεγγραφή της IP:* Για να γίνει αυτό κατανοητό είναι σαν να τοποθετείται το δεδομενόγραμμα μέσα σε έναν άλλο IP φάκελο. Έτσι το πακέτο περιλαμβάνει την εξωτερική IP κεφαλίδα συν το αρχικό δεδομενόγραμμα. Τα πεδία στην εξωτερική κεφαλίδα προσθέτουν μεγάλο φόρτο στο τελικό δεδομενόγραμμα καθώς αντιγράφονται αρκετά πεδία. Αυτή η σπατάλη χώρου δεν παράγει κάποιο όφελος.
4. *Ζητήματα αξιοπιστίας:* Ένα άλλο ζήτημα είναι η αντίληψη της αξιοπιστίας που αναφέρεται στην προϋπόθεση ότι οι συνδέσει του Mobile IPv4 βασίζονται στις αλλαγές των κελιών TCP. Μία άλλη ανησυχία αφορά ζητήματα στην διευθυνσιοδότηση της IP. Το Mobile IPv4 δημιουργεί μια αντίληψη ότι είναι μονίμως συνδεδεμένο στο αρχικό του δίκτυο. Από αυτό μπορεί να προκύψουν μη αποδοτικές συνθήκες.

4 ΠΡΩΤΟΚΟΛΛΟ MOBILE IPv6

4.1 Εισαγωγή

Το Mobile IPv6 είναι το πρωτόκολλο επόμενης γενιάς και στο εγγύς μέλλον που οι δρομολογητές (routers) θα γίνουν ακόμα πιο γρήγοροι και οι νέες τεχνολογίες θα μειώσουν τους χρόνους απόκρισης στο διαδίκτυο θα γνωρίσει ακόμα μεγαλύτερη απήχηση. Η υποστήριξη φορητότητας στο IPv6 είναι ιδιαίτερα σημαντική, καθώς οι φορητές συσκευές πλέον εξυπηρετούν την πλειοψηφία των χρηστών του διαδικτύου. Το πρωτόκολλο Mobile IPv6 είναι απολύτως κατάλληλο για φορητότητα τόσο ανάμεσα σε ομογενοποιημένα μέσα όσο και ανάμεσα σε ετερογενή μέσα. Για παράδειγμα το MobileIPV6 υποστηρίζει την κίνηση των κόμβων από έναν τομέα Ethernet σε έναν άλλο καθώς και την κίνηση του κόμβου από έναν Ethernet τομέα σε ένα ασύρματο LAN διατηρώντας την διεύθυνση IP ίδια παρά την αλλαγή αυτή.

Το Mobile IPv4 δεν χρησιμοποιήθηκε τόσο ευρέως για να παρέχει πολύ φορητότητα και έχει πολλούς σημαντικούς περιορισμούς, στους οποίους συμπεριλαμβάνονται και η διαδικασία της επικοινωνίας και ο περιορισμός στον αριθμό των διευθύνσεων IP. Το τελευταίο είναι ένα ιδιαίτερα σημαντικό πρόβλημα επειδή ο αριθμός των συσκευών που πρέπει να διαθέτουν την δική τους διεύθυνση IP για να έχουν πρόσβαση στο διαδίκτυο αυξάνεται ραγδαία. Για να ξεπεραστούν αυτοί οι περιορισμοί ο IETF σχεδίασε το Mobile IPv6. Η νέα αυτή έκδοση του πρωτοκόλλου υποστηρίζει περισσότερα διαθέσιμες διευθύνσεις IP και επιτρέπει στους χρήστες φορητών συσκευών να παραμείνουν συνδεδεμένοι στο διαδίκτυο όσο αυτοί μετακινούνται μεταξύ δικτύων. Το Mobile IPv6 σχεδιάστηκε με γνώμονα τις εμπειρίες που είχαν αποκτηθεί από το IPv4 και για αυτό το λόγο η νέα αυτή έκδοση του πρωτοκόλλου επιδιορθώνει τα προβλήματα που είχαν εντοπιστεί στην παλιά έκδοση. Το μεγαλύτερο πλεονέκτημα του Mobile IPv6 είναι ότι βασίζεται στο αντίστοιχο νέο IPv6 πρωτόκολλο του διαδικτύου. Στο Mobile IPv6 οι διευθύνσεις IP έχουν μήκος 128 bits ακεραίων όπως και στο IPV6 ενώ πολλά από τα βασικά προβλήματα του Mobile IP (φίλτρα εισόδου, διοχέτευση)επιλύονται με αυτήν την έκδοση του πρωτοκόλλου.

4.2 Επιπρόσθετη ορολογία Mobile IPv6

Σε αυτήν την παράγραφο θα γίνει αναφορά σε κάποιους όρους που είχαν αναφερθεί και στην ανάλυση του Mobile IPv4 και σε κάποιους άλλους που αφορούν αποκλειστικά και μόνο το Mobile IPv6. Οι όροι που θα αναλυθούν είναι οι εξής:

- *Φορητός Κόμβος-Mobile Node (MN)*: Ο φορητός κόμβος είναι ένας κόμβος που μεταβάλλει την τοποθεσία του εντός της τοπολογίας του διαδικτύου. Η φορητότητα ενός κόμβου μπορεί να είναι το αποτέλεσμα φυσικής κίνησης ή αλλαγών εντός της τοπολογίας του διαδικτύου. Αυτό σημαίνει ότι κίνηση μπορεί να υπάρξει εξαιτίας του γεγονότος ότι μια συσκευή μετακινείται από την μία σύνδεση στην άλλη (όπως μια συσκευή από το αυτοκίνητο στο τρένο) ή από αλλαγές στην τοπολογία που επιβάλλουν στην συσκευή αυτή να συνδεθεί σε διαφορετικό δρομολογητή ενώ η συσκευή βρίσκεται φυσικά στο ίδιο ακριβώς σημείο.
- *Κόμβος Ανταποκριτής- Correspondent Node (CN):* Ως κόμβος ανταποκριτής ορίζεται οποιοσδήποτε κόμβος επικοινωνεί με τον φορητό κόμβο. Οι όροι φορητός και ανταποκριτής αναφέρονται σε συγκεκριμένες λειτουργίες εντός ενός IPV6 κόμβου. Συνεπώς, ένας φορητός κόμβος μπορεί να είναι και κόμβος ανταποκριτής και το αντίθετο ανάλογα με την περίπτωση που περιγράφεται. Για παράδειγμα ένας διακομιστής μπορεί να αναφερθεί σαν κόμβος ανταποκριτής από τον φορητό κόμβος με τον οποίο επικοινωνεί. Την ίδια στιγμή ένας κόμβος ανταποκριτής μπορεί να βρίσκεται σε κατάσταση κίνησης γεγονός που τον καθιστά φορητό κόμβο(επειδή κινείται) ενώ σε σχέση με τον πάροχο του θα είναι ένας κόμβος ανταποκριτής.
- *Διεύθυνση Οικίας (Home address):* Είναι μια σταθερή διεύθυνση που ανήκει τον φορητό κόμβο και χρησιμοποιείται από τους κόμβους ανταποκριτές για να έχουν πρόσβαση στους φορητούς κόμβους. Όπως όλες οι IPv6 διευθύνσεις, έτσι και αυτή η διεύθυνση βασίζεται στο πρόθεμα μήκους 64 bit που ανατίθεται στον οικιακό σύνδεσμο (homelink) που συνδυάζεται με το αναγνωριστικό διεπαφής του φορητού κόμβου. Ένας φορητός κόμβος μπορεί να έχει πάνω από μία τέτοιου είδους διευθύνσεις. Τα πακέτα IP που δρομολογούνται στην home address περνούν στον οικιακό σύνδεσμο (homelink)με τη χρήση κλασσικών πρωτοκόλλων δρομολόγησης.

- *Οικιακός Σύνδεσμος (Homelink):* Είναι ένας σύνδεσμος στον οποίο ανατίθεται το πρόθεμα της διεύθυνσης οικίας που περιγράφηκε ακριβώς παραπάνω.
- *Οικιακός Πράκτορας – Home Agent (HA):* Ένας δρομολογητής που βρίσκεται στον οικιακό σύνδεσμο και δρα εκ μέρους του φορητού κόμβου όταν είναι μακριά από το οικιακό σύνδεσμο. Ο οικιακός πράκτορας έχει σαν ρόλο την ανακατεύθυνση των πακέτων πληροφορίας (που προορίζονται για την διεύθυνση οικίας του φορητού κόμβου) στην τρέχουσα τοποθεσία (με χρήση της COA διεύθυνσης) χρησιμοποιώντας IP διοχέτευση.
- Ξένος Σύνδεσμος (ForeignLink): Οποιοσδήποτε σύνδεσμος (εκτός από τον οικιακό σύνδεσμο) που επισκέπτεται ο φορητός κόμβος.
- *Διεύθυνση COA (Care-of address):* Είναι μια διεύθυνση που ανατίθεται στον φορητό κόμβο όταν βρίσκεται σε ξένο σύνδεσμο. Αυτή η διεύθυνση βασίζεται στο πρόθεμα του ξένου συνδέσμου σε συνδυασμό με το αναγνωριστικό της διεπαφής του φορητού κόμβου. Δεν υπάρχει ειδική μορφοποίηση για την διεύθυνση COA. Είναι μια κανονική IPV6 διεύθυνση που προσδιορίζει την τρέχουσα τοποθεσία του φορητού κόμβου.
- *Δέσιμο (Binding):* Ως δέσιμο ορίζεται η συσχέτιση μεταξύ της διεύθυνσης οικίας και της διεύθυνσης COA για ένα συγκεκριμένο χρονικό διάστημα. Αυτό επιτρέπει στον οικιακό πράκτορα να προωθεί πακέτα στην τρέχουσα τοποθεσία του φορητού κόμβου. Το δέσιμο ανανεώνεται (εάν λήξει ο χρονομετρητής που υπάρχει) ή ενημερώνεται όταν ο φορητός κόμβος λάβει νέα διεύθυνση COA (λόγω της μετακίνησης του σε νέο σύνδεσμο).
- *Κρυφή Μνήμη Δεσίματος (Binding Cache):* Είναι μια κρυφή μνήμη που αποθηκεύεται στην δυναμική μνήμη που περιέχει ένα πλήθος από δεσίματα για έναν ή περισσότερους φορητούς κόμβους. Η μνήμη αυτή διατηρείται τόσο από τον κόμβο ανταποκριτή όσο και από τον οικιακό πράκτορα. Κάθε εγγραφή (καταχώρηση) στην κρυφή μνήμη δεσίματος περιέχει την διεύθυνση οικίας και την διεύθυνση COA ενός φορητού κόμβου καθώς επίσης και τον χρόνο ζωής που δηλώνει την εγκυρότητα της εγγραφής. Όταν η κρυφή μνήμη δεσίματος κρατείται από τους κόμβους ανταποκριτές περιέχει επίσης και κάποιες παραμέτρους ασφαλείας.
- *Λίστα Ενημέρωσης Δεσίματος-Binding Update List (BUL):*Είναι μια λίστα που διατηρείται από τον φορητό κόμβο στην δυναμική μνήμη. Αυτή η λίστα

περιέχει όλα τα δεσίματα που στάλθηκαν στον οικιακό πράκτορα του φορητού κόμβου και στους κόμβους ανταποκριτές. Αυτή η λίστα υπάρχει για να γνωρίζει ο φορητός κόμβος πότε πρέπει να ανανεωθεί ένα δέσιμο και χρησιμοποιείται επίσης για να επιλεχθεί η σωστή διεύθυνση COA όταν υπάρχει άμεση επικοινωνία με έναν κόμβο ανταποκριτή.

4.3 Βασικές λειτουργίες MobileIPv6

Το πρωτόκολλο Mobile IP σχεδιάστηκε για να επιτρέπει στους κόμβους να είναι προσβάσιμους και να διατηρούν τις τρέχουσες συνδέσεις τους ενώ μεταβάλλουν την θέση τους εντός της τοπολογίας του δικτύου. Για να εξασφαλισθούν διάφορες απαιτήσεις και κυρίως η διαφάνεια στα υψηλότερα επίπεδα του μοντέλου το πρωτόκολλο χρησιμοποιεί σταθερή διεύθυνση IP, που ανατίθεται στους κόμβους και είναι διεύθυνση οικείας (home address). Η διεύθυνση αυτή χρησιμοποιείται κυρίως για δύο λόγους: αρχικά για να επιτρέψει στον φορητό κόμβο να είναι προσβάσιμος διαθέτοντας μια σταθερή εγγραφή στα DNS και δεύτερον για να κρύψει την φορητότητα του επιπέδου IP από τα ανώτερα επίπεδα. Η ύπαρξη μνήμης DNS υπαινίσσεται ότι ένας κόμβος που αλλάζει συχνά την διεύθυνση IP του δεν θα έχει την ίδια διεύθυνση σε όλους τους εξυπηρετητές DNS επειδή κάποιοι από αυτούς θα έχουν κρατήσει στην μνήμη τους την παλιά διεύθυνση μέχρι να φτάσει η λήξη της περιόδου αποθήκευσης. Συνεπώς, για να είναι οι κόμβοι προσβάσιμοι στη σωστή διεύθυνση, θα πρέπει αυτή να είναι σταθερή και όχι να αλλάζει κάθε φορά που κόμβος μετακινείται. Ως εκ τούτου το πρωτόκολλο IPV6 παρέχει την οικεία διεύθυνση. Μια συνέπεια της διατήρησης σταθερής διεύθυνσης ανεξάρτητα από την τοποθεσία του κόμβου είναι ότι όλοι οι κόμβοι ανταποκριτές προσπαθούν να φτάσουν τον φορητό κόμβο στην διεύθυνση αυτή, χωρίς να γνωρίζουν την πραγματική του τοποθεσία. Είτε ο φορητός κόμβος είναι συνδεδεμένος στον οικείο σύνδεσμο είτε όχι τα πακέτα της πληροφορίας προωθούνται σε αυτόν. Εάν ο φορητός κόμβος δεν βρίσκεται στον οικείο σύνδεσμο του, ο οικείος πράκτορας είναι αρμόδιος για να διοχετεύει τα πακέτα στην διεύθυνση COA του φορητού κόμβου.

Από τη στιγμή που ο κόμβος ανταποκριτής προσπαθεί να συνδεθεί με την οικεία διεύθυνση του φορητού κόμβου, ειδικοί υποδοχείς (τόσο στον φορητό κόμβο όσο και στους κόμβους ανταποκριτές) χρησιμοποιούν την οικεία διεύθυνση για να καταγράψουν τέτοιες συνδέσεις, ώστε οι εφαρμογές και στις δύο πλευρές να βλέπουν μόνο την οικεία διεύθυνση για τον φορητό κόμβο. Επομένως το επίπεδο IP σε εφαρμογές που εκτελούνται στον φορητό κόμβο

είναι αρμόδιο να παρουσιάζει την οικεία διεύθυνση σαν πηγαία ανεξάρτητα από την τοποθεσία του φορητού κόμβου. Ουσιαστικά, το επίπεδο IP κρύβει την φορητότητα (αλλαγή διευθύνσεων) από τα ανώτερα στρώματα ώστε να διατηρηθούν οι τρέχουσες συνδέσεις για όσο ο φορητός κόμβος αλλάζει διευθύνσεις. Εάν άλλαζε η πραγματική διεύθυνση του φορητού κόμβου οι υποδοχείς θα γίνονταν μη έγκυροι και οι συνδέσεις θα τερματίζονταν αυτόματα.

Η οικεία διεύθυνση σχηματίζεται προσαρτώντας ένα αναγνωριστικό διεπαφής στο πρόθεμα που υπάρχει στον οικείο σύνδεσμο. Όπως κάθε IPv6 κόμβος, στον φορητό κόμβο μπορούν να ανατεθούν διευθύνσεις από διαφορετικά πεδία. Αυτό εφαρμόζεται και στην οικεία και στην διεύθυνση COA.

Όταν ο φορητός κόμβος είναι στο οικείο δίκτυο λειτουργεί σαν οποιοδήποτε άλλο IPv6 κόμβο. Δέχεται πακέτα που έχουν διευθυνσιοδοτηθεί για οποιαδήποτε από τις οικείες διευθύνσεις του και παραδίδονται μέσω απλής δρομολόγησης. Το πρωτόκολλο Mobile IPv6 ουσιαστικά καλείται και αξιοποιείται όταν ένας φορητός κόμβος δεν είναι στο οικείο του δίκτυο, δηλαδή όταν βρίσκεται σε έναν ξένο σύνδεσμο.

Όταν ο φορητός κόμβος μετακινείται από τον οικείο σε έναν ξένο σύνδεσμο, πρώτα σχηματίζει μια διεύθυνση COA βασιζόμενος στο πρόθεμα του ξένου συνδέσμου. Μετά τον σχηματισμό της διεύθυνσης αυτής ο φορητός κόμβος ενημερώνει τον οικείο πράκτορα για την ενέργεια αυτή στέλνοντας ένα μήνυμα ενημέρωσης δεσίματος (Binding Update - BU). Το μήνυμα αυτό είναι ένα από τα διάφορα μηνύματα του πρωτοκόλλου IPV6 που κωδικοποιούνται σαν επιλογές σε μια νέα κεφαλίδα που ονομάζεται κεφαλίδα κινητικότητας. Η κεφαλίδα αυτή είναι και η τελευταία στην αλυσίδα των κεφαλίδων επέκτασης και εμφανίζεται σαν ένα πρωτόκολλο των άνω στρωμάτων.

Το μήνυμα ενημέρωσης δεσίματος περιέχει την οικεία διεύθυνση και τη διεύθυνση COA του φορητού κόμβου. Η οικεία διεύθυνση συμπεριλαμβάνεται σε μια νέα επιλογή που ονομάζεται επιλογή της οικείας διεύθυνσης και η διεύθυνση COA συμπεριλαμβάνεται είτε στην πηγαία διεύθυνση της κεφαλίδας IP ή σε μια νέα επιλογή που ονομάζεται εναλλακτική διεύθυνση COA. Η επιλογή οικείας διεύθυνσης είναι μέρος της κεφαλίδας επέκτασης με τις επιλογές προορισμού, ενώ η επιλογή της οικείας διεύθυνσης συμπεριλαμβάνεται στην κεφαλίδα κινητικότητας. Ο σκοπός της ενημέρωσης δεσίματος είναι να ενημερώνει τον οικείο πράκτορα για την τρέχουσα διεύθυνση του φορητού κόμβου δηλαδή την διεύθυνση COA. Ως εκ τούτου ο οικείος πράκτορας έχει ανάγκη να αποθηκεύει αυτήν την πληροφορία ώστε να προωθεί τα πακέτα που προορίζονται για την οικεία διεύθυνση του φορητού κόμβου. Ο

οικείος πράκτορας περιέχει μια μνήμη δεσίματος στην οποία αποθηκεύονται όλα τα δεσίματα του φορητού κόμβου τον οποίο υπηρετεί. Κάθε εγγραφή της μνήμης αυτής αποθηκεύει ένα δέσιμο για μια οικεία διεύθυνση. Όταν ο οικείος πράκτορας λαμβάνει την ενημέρωση δεσίματος, κάνει διάφορες ενέργειες για να επικυρώσει το μήνυμα. Εάν η ενημέρωση δεσίματος περάσει την διαδικασία επικύρωσης και γίνει αποδεκτή, ο οικείος πράκτορας ψάχνει την μνήμη δεσίματος του εάν υπάρχει εγγραφή με την οικεία διεύθυνση του φορητού κόμβου. Εάν βρει εγγραφή ο οικείος πράκτορας ενημερώνει αυτήν την εγγραφή με τις νέες πληροφορίες που έλαβε στην ενημέρωση δεσίματος. Διαφορετικά, εάν δεν βρει εγγραφή δημιουργεί μια νέα. Από αυτό το σημείο και μετά, ο οικείος πράκτορας δρα σαν διαμεσολαβητής για τον φορητό κόμβο στον οικείο σύνδεσμο. Ουσιαστικά εκπροσωπεί τον φορητό κόμβο στον οικείο σύνδεσμο και προσφέρει σε αυτόν υπηρεσίες προώθησης. Για να εξασφαλισθεί ότι αυτή η αναπαράσταση είναι κατανοητή από όλους τους κόμβους στον οικείο σύνδεσμο ο οικείος πράκτορας στέλνει ένα μήνυμα ενημέρωσης στην κοινή διεύθυνση για όλους τους κόμβους που υπάρχει στον σύνδεσμο. Το μήνυμα αυτό περιλαμβάνει την οικεία διεύθυνση του φορητού κόμβου και την διεύθυνση του επιπέδου σύνδεσης του οικείου πράκτορα. Με αυτόν τον τρόπο ο οικείος πράκτορας εξασφαλίζει ότι οποιοδήποτε IP πακέτο που προορίζεται για τον φορητό κόμβο προωθείται στην διεύθυνση στην διεύθυνση του επιπέδου σύνδεσης του οικείου πράκτορα. Επειδή οι παραλήπτες του μηνύματος δεν μπορούν να επιβεβαιώσουν ότι το παρέλαβαν, το μήνυμα αυτό μπορεί να σταλεί πάνω από μία φορά για να μειωθεί η πιθανότητα μη παράδοσης σε κάποιο παραλήπτη. Ο οικείος πράκτορας επίσης προστατεύει με αυτόν τον τρόπο τις διευθύνσεις του φορητού κόμβου ειδικά στην περίπτωση που ένας άλλος κόμβος διαμορφώσει μια διεύθυνση που συγκρούεται με την οικεία διεύθυνση (ή διευθύνσεις) του φορητού κόμβου. Σε αυτήν την περίπτωση εάν ένας άλλος κόμβος δοκιμαστικά διαμορφώσει μία από τις διευθύνσεις του φορητού κόμβου και επιχειρήσει να την χρησιμοποιήσει, ο οικείος πράκτορας απαντά στο μήνυμα καταδεικνύοντας ότι η διεύθυνση είναι ανατεθειμένη σε άλλο κόμβο.

Σε αυτό το στάδιο ο οικείος πράκτορας ξεκινά να λαμβάνει όλα τα πακέτα που προορίζονται για τον φορητό κόμβο. Κατά την διάρκεια λήψης ενός πακέτου που προορίζεται για την οικεία διεύθυνση του φορητού κόμβου, ο οικείος πράκτορας ελέγχει την μνήμη δεσίματος του για διαπιστώσει εάν υπάρχει καταχώρηση για τον φορητό κόμβο. Ο οικείος πράκτορας αναζητά την μνήμη του χρησιμοποιώντας την οικεία διεύθυνση του φορητού κόμβου (που είναι η διεύθυνση προορισμού στο ληφθέν πακέτο πληροφορίας) σαν κλειδί αναγνώρισης των εγγραφών. Όταν βρεθεί μια εγγραφή το πακέτο διοχετεύεται στην διεύθυνση COA του

φορητού κόμβου που εμπεριέχεται στην συγκεκριμένη εγγραφή μνήμης. Το σημείο εισόδου είναι ο οικείος πράκτορας και το σημείο εξόδου είναι η διεύθυνση COA του φορητού κόμβου. Η διοχέτευση είναι διπλής κατεύθυνσης. Αυτό σημαίνει ότι όταν ο φορητός κόμβος στείλει με τη σειρά του IP πακέτα, τα διοχετεύει πρώτα στον οικείο πράκτορα, ο οποίος αποθηλακώνει το πακέτο και στέλνει το αρχικό στον προορισμό του.

Οι προδιαγραφές του πρωτοκόλλου Mobile IPv6 απαγορεύουν στον οικείο πράκτορα την διοχέτευση πακέτων που προορίζονται για την τοπική σύνδεση του φορητού κόμβου. Επιπλέον οι προδιαγραφές συνιστούν ότι η κανονική συμπεριφορά του οικείου πράκτορα θα πρέπει να ρυθμιστεί ώστε να μην διοχετεύει πακέτα που προορίζονται για κάποια από τις τοπικές διευθύνσεις του φορητού κόμβου. Η μόνη εξαίρεση για αυτούς τους κανόνες που επιβάλλονται από τις προδιαγραφές είναι πακέτα Multicast Listener Discovery (MLD).

Η διοχέτευση απαιτεί να εξασφαλισθεί η διαφάνεια των υπηρεσιών που προσφέρονται από τον οικείο πράκτορα. Αυτό χρειάζεται για να διατηρηθεί η φιλοσοφία της κίνησης των πακέτων από άκρη σε άκρη μεταξύ του φορητού κόμβου και των κόμβων ανταποκριτών. Αυτό σχετίζεται με το ότι οι δρομολογητές δεν θα πρέπει να τροποποιήσουν το περιεχόμενο της πηγής ή τις διευθύνσεις προορισμού στην κεφαλίδα IP και ως εκ τούτου διατηρώντας την ακεραιότητα του πακέτου και επιτρέποντας τους από άκρη σε άκρη ελέγχους ακεραιότητας. Επιπρόσθετα, η διοχέτευση είναι σημαντική για την διατήρηση της διαφάνειας για τα υψηλότερα επίπεδα. Αυτό εξηγείται εάν αναλογιστεί κανείς ότι αντί για διοχέτευση ο οικείος πράκτορας επανεγγράφει την διεύθυνση προορισμού του πακέτου για παράδειγμα αντικαθιστά την οικεία διεύθυνση με την COA. Μία άμεση συνέπεια αυτής της ενέργειας είναι ότι έχει εκτεθεί η ακεραιότητα του πακέτου προκαλώντας το σφάλμα της Κεφαλίδας Πιστοποίησης (Authentication Header). Επιπλέον έστω ότι ο φορητός κόμβος λαμβάνει το πακέτο και το προωθεί στα ανώτερα επίπεδα όπως για παράδειγμα το TCP το οποίο θα επεξεργαζόταν το πακέτο παίρνοντας σαν δεδομένο ότι χρησιμοποιείται η διεύθυνση COA για να αναγνωριστεί η σύνδεση. Ωστόσο, ο κόμβος ανταποκριτής αναγνωρίζει την σύνδεση από την διεύθυνση, το αριθμό θύρας της πηγής, την οικεία διεύθυνση του φορητού κόμβου, τον αριθμό θύρας του και τον αριθμό πρωτοκόλλου. Ως εκ τούτου εάν ο φορητός κόμβος απαντήσει στον κόμβο ανταποκριτή άμεσα, χρησιμοποιώντας την διεύθυνση COA, ο κόμβος ανταποκριτής θα ήταν αδύνατο να εντοπίσει την σύνδεση και συνεπώς θα έριχνε τα πακέτα.

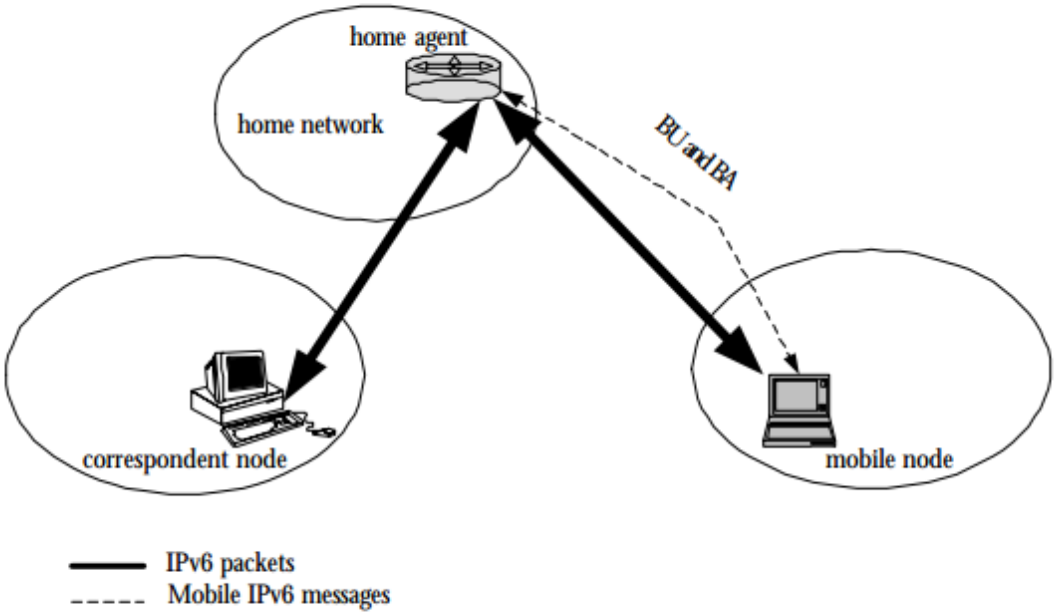
Ο οικείος πράκτορας έχει την δυνατότητα να ασφαλίσει τη δίοδο προς τον φορητό κόμβο χρησιμοποιώντας μια Κεφαλίδα Πιστοποίησης (Authentication Header) ή ESP, πράγμα που εξαρτάται από την πολιτική του οικείου δικτύου. Για παράδειγμα μέσα σε ένα εταιρικό

δίκτυο που έχει έναν οικείο πράκτορα, άλλοι κόμβοι μέσα στην εταιρεία μπορεί να μην είναι ενήμεροι για την απομάκρυνση του φορητού κόμβου από τον οικείο σύνδεσμο, καθώς συνεχίζουν να αποστέλλουν πακέτα στην οικεία διεύθυνση του φορητού κόμβου.

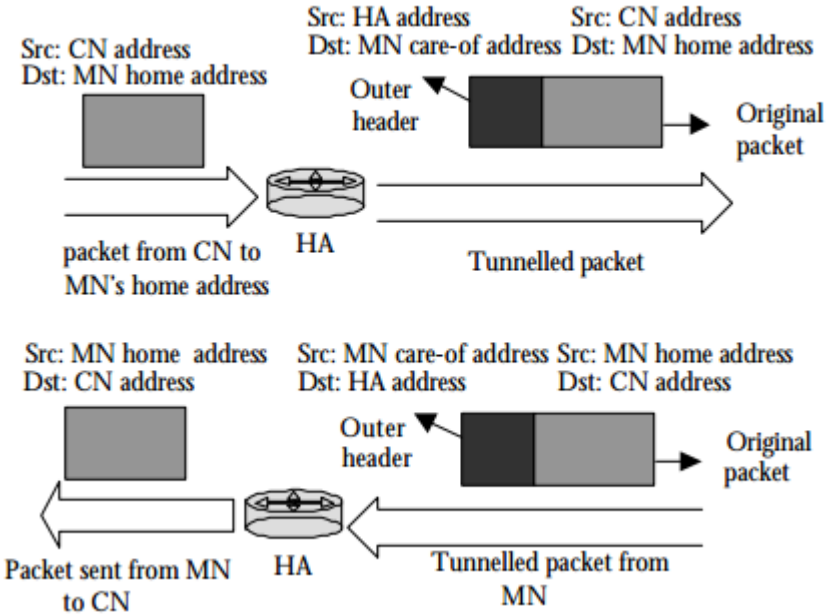
Οι επιλογές προορισμού διαφοροποιούν το πρωτόκολλο Mobile IPv6 και επιτρέπουν στους πράκτορες και στους κόμβους ανταποκριτές να ενημερώνονται για το δέσιμο του φορητού κόμβου. Οι επιλογές αυτές είναι οι εξής:

- *Ενημέρωση δεσίματος(Binding Update)*: Η διαδικασία αυτή χρησιμοποιείται από τον φορητό κόμβο για να ενημερώσει έναν κόμβο ανταποκριτή ή τον οικείο πράκτορα του φορητού κόμβου για το τρέχων δέσιμο. Η ενημέρωση δεσίματος που αποστέλλεται στον οικείο πράκτορα του φορητού κόμβου για την καταχώρηση της κύριας COA διεύθυνσης ονομάζεται οικεία καταχώρηση (home registration).
- *Αναγνώριση δεσίματος (Binding Acknowledgement)*: Αυτή η επιλογή χρησιμοποιείται για την αναγνώριση της λήψης της ενημέρωσης δεσίματος εάν είχε ζητηθεί κατά την διαδικασία αίτησης της.
- *Αίτηση δεσίματος(Binding Request)*: Αυτή η επιλογή χρησιμοποιείται για να αποστείλει ο φορητός κόμβος στον κόμβο που το ζητά μια ενημέρωση δεσίματος που περιέχει το υπάρχον δέσιμο του φορητού κόμβου. Αυτή η επιλογή συνήθως χρησιμοποιείται από έναν κόμβο ανταποκριτή για να ανανεώσει την μνήμη δεσίματος του για έναν φορητό κόμβο όταν αυτή είναι ενεργή αλλά ο χρόνος ζωής της εγγραφής είναι κοντά στην λήξη του.
- *Οικεία διεύθυνση (Home Address)*: Αυτή η επιλογή χρησιμοποιείται σε ένα πακέτο που στέλνεται από τον φορητό κόμβο ώστε να ενημερώσει τον παραλήπτη για την οικεία του διεύθυνση. Όταν ο φορητός κόμβος αποστέλλει ένα πακέτο ενώ βρίσκεται μακριά από το οικείο δίκτυο θα ορίσει σαν πηγαία διεύθυνση στην κεφαλίδα IPv6 του πακέτου μια από τις τρέχουσες COA διευθύνσεις. Επίσης θα συμπεριλάβει μια επιλογή προορισμού οικείας διεύθυνσης στο πακέτο, δίνοντας την οικεία του διεύθυνση. Βάζοντας αυτήν την επιλογή σε κάθε πακέτο ο φορητός κόμβος αποστολέας μπορεί να επικοινωνεί μέσω της οικείας του διεύθυνσης με τους κόμβους ανταποκριτές κάνοντας γνωστή τη διεύθυνση COA στα ανώτερα επίπεδα (π.χ. μεταφοράς) του πρωτοκόλλου IPv6. Το γεγονός ότι στο πακέτο συμπεριλαμβάνεται η

επιλογή οικείας διεύθυνσης επηρεάζει την παραλαβή μόνο του συγκεκριμένου πακέτου από τον κόμβο ανταποκριτή.



Εικόνα 30: Ενημέρωση δεσίματος στο πρωτόκολλο MobileIPV6



Εικόνα 31: Προώθηση πακέτων δεδομένων στο πρωτόκολλο Mobile IPv6

4.4 Σύγκριση πρωτοκόλλων Mobile IPv4 και Mobile IPv6

Η σύγκριση των δύο πρωτοκόλλων (IPV4 και IPV6) συνοψίζεται στα εξής σημεία:

- Τα πακέτα της πληροφορίας που στέλνονται σε έναν φορητό κόμβο που βρίσκεται μακριά από το οικείο δίκτυο στο Mobile IPv6 διοχετεύονται με τη χρήση μιας κεφαλίδας δρομολόγησης και όχι μέσω IP ενθυλάκωσης όπως συμβαίνει στην έκδοση IPv4 που πρέπει να χρησιμοποιεί ενθυλάκωση για όλα τα πακέτα πληροφορίας. Η χρήση της κεφαλίδας δρομολόγησης απαιτεί λιγότερο όγκο πληροφορίας (bytes στην κεφαλίδα) γεγονός που μειώνει την επιβάρυνση της παράδοσης των πακέτων.
- Δεν υπάρχει η ανάγκη ανάπτυξης ειδικών δρομολογητών όπως οι ξένοι πράκτορες (foreign agents) που χρησιμοποιούνται στο Mobile IPv4. Στο Mobile IPv6 οι φορητοί κόμβοι χρησιμοποιούν επαυξημένες λειτουργίες όπως είναι η ανακάλυψη των γειτονικών κόμβων και η αυτόματη διαμόρφωση της διεύθυνσης.
- Η διαδικασία εύρεσης βέλτιστης δρομολόγησης είναι υλοποιημένη στο Mobile IPv6 σε αντίθεση με το IPv4 που προστίθεται προαιρετικά σαν επέκταση και δεν υποστηρίζεται από όλα τα είδη κόμβων. Αυτή η διαδικασία επιτρέπει άμεση δρομολόγηση από οποιοδήποτε κόμβο ανταποκριτή στον φορητό κόμβο, χωρίς να χρειάζεται να περάσει στο οικείο δίκτυο του φορητού κόμβου (και να προωθηθεί από τον οικείο πράκτορα αυτού του δικτύου) και επιπλέον εξουδετερώνει το πρόβλημα της τριγωνικής δρομολόγησης από το οποίο πάσχει το Mobile IPv4.
- Την στιγμή που ένας φορητός κόμβος είναι μακριά από το οικείο δίκτυο, ο οικείος πράκτορας του παρεμβάλλεται σε πακέτα που καταφθάνουν στο οικείο δίκτυο χρησιμοποιώντας την μέθοδο ανακάλυψης γειτνίασης που διαθέτει η έκδοση IPv6 του πρωτοκόλλου και όχι την μέθοδο ARP που διαθέτει η IPv4.
- Η έκδοση IPv6 χρησιμοποιεί επιλογές προορισμού που επιτρέπει στον έλεγχο της κίνησης να ενσωματωθεί στα πακέτα, ενώ το IPv4 και οι μέθοδοι βελτιστοποίησης της δρομολόγησης που διαθέτει χρειάζονται ξεχωριστό UDP πακέτο για κάθε μήνυμα ελέγχου.
- Η έκδοση IPv6 επιτρέπει στο Mobile IP και στους φορητούς κόμβους να συνυπάρχουν αποδοτικά με τους δρομολογητές που πραγματοποιούν το φιλτράρισμα εισόδου. Ένας φορητός κόμβος πλέον χρησιμοποιεί την διεύθυνση

COA του σαν την πηγαία διεύθυνση στα πακέτα που στέλνει, επιτρέποντας στα πακέτα να περάσουν κανονικά μέσα από τα φίλτρα εισόδου των δρομολογητών. Ο φορητός κόμβος κρατεί την οικεία διεύθυνση του σε ένα σημείο, επιτρέποντας την χρήση της διεύθυνσης COA ώστε να υπάρχει διαφάνεια για τα ανώτερα IP στρώματα.

- Η έκδοση IPv6 υλοποιεί όλες τις προϋποθέσεις ασφαλείας IP (IP Security-IPsec) (όπως είναι η ταυτοποίηση αποστολέα και η προστασία ακεραιότητας και επανάληψης των δεδομένων) για τις ενημερώσεις δεσίματος(που στο IPv4 καλύπτουν το ρόλο τόσο της καταχώρησης όσο και της βελτιστοποίησης δρομολόγησης), σε αντίθεση με την έκδοση IPv4 όπου η ασφάλεια εναπόκειται σε στατικά διαμορφωμένους συσχετισμούς ασφαλείας.
- Παρ' όλο που το IPv6 δίνει την δυνατότητα υλοποίησης φορητότητας σε ευρεία περιοχή στο επίπεδο IP δεν έχει χαρακτηριστικές λειτουργίες των ασύρματων δικτύων πρόσβασης όπως λειτουργίες ταχείας παράδοσης και σελιδοποίησης.
- Μία από τις βασικές λειτουργίες της έκδοσης IPv4 ήταν να υποστηρίζει φιλοξενία φορητότητας στο δίκτυο χωρίς να επιβάλλει αλλαγές σε κάθε κόμβο, ενώ η IPV6 έκδοση δίνει σαφή υποστήριξη σε αυτές τις περιπτώσεις.
- Το Mobile IPv6 και το Mobile IPv4 με βελτιστοποίηση δρομολόγησης μπορούν θεωρητικά να υποστηρίξουν δίκτυα με τον ίδιο τρόπο. Η διαφορά έγκειται στο ότι η έκδοση IPV6 δεν μπορεί να χρησιμοποιηθεί χωρίς να γίνουν σημαντικές αλλαγές όταν έχουμε ως στόχο να προσφέρουμε βέλτιστη υποστήριξη φορητότητας. Πιο συγκεκριμένα το Mobile IPv6 δεν προσαρμόζεται στο μέγεθος του δικτύου.
- Το πρωτόκολλο Mobile IP ακόμα είναι σαν μια ανοιχτή πόρτα προς επιθέσεις ασφαλείας όλων των ειδών καθώς δεν υπάρχουν στοιχεία όπως η ισχυρή ταυτοποίηση ενός επισκεπτόμενου χρήστη, η ακεραιότητα και ιδιωτικότητα των δεδομένων μεταξύ του φορητού κόμβου και του οικείου δικτύου του.

4.5 Η αναγκαιότητα και οι εφαρμογές του πρωτοκόλλου Mobile IPv6

Σε πολλές εφαρμογές (όπως VPN, VOIP τεχνολογίες), οι ξαφνικές αλλαγές στην συνδεσιμότητα του δικτύου και στην διεύθυνση IP μπορούν να προκαλέσουν προβλήματα. Το πρωτόκολλο Mobile IP σχεδιάστηκε κατά τέτοιο τρόπο που ώστε να προσφέρει αδιάλειπτη σύνδεση στο διαδίκτυο.

Το πρωτόκολλο Mobile IP συναντάται τόσο σε ενσύρματα όσο και σε ασύρματα δίκτυα που υπάρχουν φορητές συσκευές που κινούνται μέσα σε πολλαπλά υποδίκτυα. Παραδείγματα τέτοιας χρήσης είναι η πλοήγηση μεταξύ επικαλυπτόμενων ασύρματων δικτύων όπως τα WLAN, WiMAX και BWA.

Το πρωτόκολλο Mobile IP δεν είναι απαραίτητο μεταξύ συστημάτων κινητών τηλεφώνων όπως το 3G, για να παρέχει διαφάνεια όταν οι χρήστες μετακινούνται μεταξύ πύργων κινητής τηλεφωνίας, αφού αυτά τα συστήματα παρέχουν τους δικούς τους μηχανισμούς παράδοσης και περιαγωγής. Ωστόσο, χρησιμοποιείται συχνά σε συστήματα 3G ώστε να επιτρέψει αδιάλειπτη φορητότητα IP μεταξύ διαφορετικών PDSN (Packet Data Serving Node) διευθύνσεων.

Ένα καλό παράδειγμα για το Mobile IP είναι η ανάπτυξη και η εξέλιξη των κινητών τηλεφώνων την τελευταία δεκαετία. Πολλοί πελάτες και χρήστες τηλεφώνων έχουν μεταβεί από τα παραδοσιακά ενσύρματα τηλέφωνα(που χρειάζονται μια σταθερή πρίζα στον τοίχο για να συνδεθούν στο δίκτυο) στα κινητά τηλέφωνα που επιτρέπουν στον χρήστη να είναι σε κίνηση όσο συνομιλεί με κάποιον στο τηλέφωνο του. Αυτή η φορητότητα επιτυγχάνεται χρησιμοποιώντας τεχνολογία που επιτρέπει την δημιουργία και διατήρηση μια σταθερής σύνδεση μεταξύ του χρήστη και του δέκτη και το αντίστροφο.

Μια καλή παρατήρηση είναι ότι πήρε αρκετό χρονικό διάστημα για να γίνουν αποδεκτά τα κινητά τηλέφωνα στην ευρεία καταναλωτική αγορά. Το αρχικά απαγορευτικό κόστος των τεχνολογιών κινητής τηλεφωνίας και η αρχικά περιορισμένη κάλυψη στις υπηρεσίες της αποθάρρυνες πολλούς χρήστες από το να χρησιμοποιούν κινητά τηλέφωνα. Η χρήση φορητών υπολογιστικών συσκευών είναι δεδομένο ότι θα βρίσκεται στο επίκεντρο των τεχνολογικών εξελίξεων, καθώς η αποδοχή φορητών συσκευών που χρησιμοποιούν το διαδίκτυο είναι ιδιαίτερα ευρεία στις μέρες μας.

Όπως αναφέρθηκε παραπάνω ένα από τα μεγαλύτερα πλεονεκτήματα του Mobile IP είναι ότι ο χρήστης μπορεί να μετακινείται αδιάλειπτα χωρίς να χρειάζεται να συνδέεται ή να παραμετροποιεί ξανά τις ρυθμίσεις δικτύου του σε κάθε σημείο πρόσδεσης. Ο κύριος στόχος του Mobile IP με την βοήθεια των πρωτοκόλλων που το απαρτίζουν είναι να παρέχει αυτόματα και μη διαδραστική επανασύνδεση στις δικτυακές δραστηριότητες σε οποιοδήποτε σημείο πρόσδεσης.

Από αυτήν την οπτική γωνία τα σημαντικά πλεονεκτήματα του Mobile IP είναι τα ακόλουθα:

1. Πρόσβαση σε υπολογιστικούς πόρους ανεξάρτητα από την τοποθεσία
2. Ασύρματη πρόσβαση στο δίκτυο

3. Ευκολία και άνεση στην λειτουργία καθώς ο χρήστης μπορεί να κάνει χρήση των υπηρεσιών σχεδόν από παντού
4. Οικονομία καθώς τα περιβάλλοντα αυτά δεν απαιτούν σχεδόν καθόλου καλωδιακές εγκαταστάσεις και τα κόστη συντήρησης που έχουν αυτές.
5. Εύκολη επαναχρησιμοποίηση του λογισμικού καθώς υπάρχουσες υποδομές (σε λογισμικό) μπορούν να δουλεύουν σε αυτά χωρίς αλλαγές.
6. Διαρκή συνδεσιμότητα.

Κάποιες από τις εφαρμογές του πρωτοκόλλου Mobile IPv6 στις οποίες είναι ιδιαίτερα χρήσιμο είναι:

- *Συνεργατικά περιβάλλοντα γραφείου*: Οι εργαζόμενοι σε τέτοια γραφεία μπορούν να μετακινούνται ελεύθερα με τη χρήση φορητών συσκευών, να μπορούν να αλληλοεπιδρούν να συζητούν και να διαμοιράζονται δεδομένα στις συσκευές τους. Η κατασκευαστική εταιρεία αεροπλάνων Airbus, διαθέτει στην Witchita των Η.Π.Α συνεργατικές εγκαταστάσεις μηχανικής που χρησιμοποιούν επιτυχώς το πρωτόκολλο Mobile IPv6.
- *Σε νοσοκομεία*: Οι γιατροί μπορούν να λάβουν άμεσες πληροφορίες για τους ασθενείς τους στις φορητές τους συσκευές χωρίς να χρειάζεται να προσέλθουν στα τερματικά τους ή να είναι παρών οι ασθενείς τους. Η απόκτηση τέτοιων δεδομένων με αυτόν τον τρόπο μπορεί να είναι ιδιαίτερα σημαντική σε επείγοντα περιστατικά.
- *Σε στρατιωτικές επιχειρήσεις*: Η ασύρματη μετάδοση δεδομένων ήχου ήταν για πολλές δεκαετίες μονόδρομος σε στρατιωτικές επιχειρήσεις. Με τις νέες στρατιωτικές τεχνολογίες που αναπτύχθηκαν τα τελευταία χρόνια παρουσιάστηκε η ανάγκη για χρήση συσκευών που μπορούν να λάβουν και να μεταδώσουν σημαντικές στρατιωτικού περιεχομένου πληροφορίες από και προς έναν κεντρικό υπολογιστή.
- *Σε πανεπιστήμια και κολλέγια*: Τα πανεπιστημιακά περιβάλλοντα επωφελούνται πολύ σημαντικά από τις εφαρμογές του πρωτοκόλλου Mobile IPv6 δίνοντας ενιαία και αδιάλειπτη πρόσβαση σε δίκτυο και σε δεδομένα που αφορούν φοιτητές δημιουργώντας με αυτόν τον τρόπο τις απαραίτητες αυτοματοποιήσεις που επιταχύνουν την πρόσβαση σε διδακτικό υλικό και απαραίτητους εκπαιδευτικούς πόρους.

4.6 Υλοποιήσεις Mobile IP σε λειτουργικό σύστημα Linux

Υπάρχει πολύ έρευνα και υλοποιήσεις του Mobile IP σε λειτουργικό σύστημα Linux, οι οποίες είναι οι εξής:

- *MosquitoNet* (https://mosquitto.org/): Είναι μια ανοιχτού κώδικα υλοποίηση που υλοποιεί το πρωτόκολλο MQTT στις εκδόσεις 3.1 και 3.1.1. Ουσιαστικά είναι ένας διακομιστής μηνυμάτων που χρησιμοποιεί τις έννοιες της εγγραφής και μετάδοσης. Αυτό το γεγονός κάνει κατάλληλη την υλοποίηση για το γνωστό σε όλους "Διαδίκτυο των Αντικειμένων" (Internet of Things) καθώς επιτρέπει την ανταλλαγή μηνυμάτων χρησιμοποιώντας αισθητήρες χαμηλής ισχύος ή φορητές συσκευές όπως έξυπνα τηλέφωνα.
- *Dynamics – HUT Mobile IP* (http://dynamics.sourceforge.net/): Το σύστημα Dynamics Mobile IP, αρχικά αναπτύχθηκε από το πανεπιστήμιο τεχνολογίας του Ελσίνκι (Helsinki University of Technology-HUT) και είναι ένα προσαρμόσιμο, δυναμικό και ιεραρχικό Mobile IP λογισμικό για λειτουργικά συστήματα Linux ενώ εισήχθει και σε κάποιες εκδόσεις των Windows (98SE, ME, NT4, 2000).
- Lancaster Mobile IPv6 Package (www.research.lancs.ac.uk): Αφορά μια υλοποίηση για παιχνίδια μέσα σε ασύρματα MAN δίκτυα χρησιμοποιώντας τεχνολογίες και πρωτόκολλα όπως το GPRS και IEEE 802.11 βασισμένα στο Mobile IPv6.
- *Portland State University Secure Mobile Networking Project-SMN* (http://www.cs.pdx.edu/research/SMN/): Το έργο αυτό περιλαμβάνει την υλοποίηση ενός ασφαλούς και υψηλών επιδόσεων δίκτυο mobile με στόχο την ενσωμάτωση του στην υπάρχουσα υποδομή εθνικών πληροφοριών. Η υλοποίηση περιελάμβανε μια αυστηρή προσέγγιση των Mobile IP και IPSEC πρωτοκόλλων ώστε όλα τα πακέτα που προέρχονται από έναν ασύρματο φορητό κόμβο να μπορούν να προστατευθούν κάτω από την ομπρέλα του IPSEC είτε ο κόμβος βρίσκεται στο οικεί δίκτυο είτε σε άλλο.

Όπως φαίνεται από τα παραπάνω υπάρχουν αρκετές υλοποιήσεις του Mobile IP για Linux. Ένα κοινό στοιχείο των υλοποιήσεων στις μέρες μας είναι ότι στρέφονται στο Mobile IPv6 λόγω της ενσωμάτωσης του πρωτοκόλλου Mobile IPv6 στον πυρήνα του λειτουργικού στις τελευταίες εκδόσεις του.

4.7 Άλλες ανάγκες που υποστηρίζουν οι τεχνολογίες Mobile IP

Οι εταιρίες που κατασκευάζουν συσκευές όπως φορητούς υπολογιστές, τάμπλετ, έξυπνα τηλέφωνα, PDA και άλλες παρόμοιες συσκευές δείχνουν ιδιαίτερο ενδιαφέρον στο Mobile IP καθώς επιθυμούν να παρέχουν αξιόπιστες και πάντα σε λειτουργία υπηρεσίες όπως η πλοήγηση στο διαδίκτυο και το ηλεκτρονικό ταχυδρομείο.

Διενεργείται πολύ έρευνα σε εργαστήρια από εταιρείες και οργανισμούς που είναι πλήρως ικανές για ασύρματη επικοινωνία σε συνεργατικότητα πάντα με υποδομές που πρέπει να υπάρχουν για να υποστηριχθούν οι παραπάνω τεχνολογίες IPv6. Τέτοιες εταιρείες είναι η Hewlett Packard, η Earthlink, η Palm και η Sony. Σε περιοχές και πόλεις που οι παραπάνω υποδομές υπάρχουν έχει αποδειχθεί ότι οι ασύρματες επικοινωνίες είναι ανεκτίμητες.

Η αξία των τεχνολογιών αυτών δοκιμάστηκε κατά την τρομοκρατική επίθεση στις Η.Π.Α. την 11η Σεπτεμβρίου. Μετά την επίθεση αυτή εκατοντάδες εργαζόμενοι γραφείων που βρέθηκαν χωρίς χώρο εργασίας γύρισαν σε ασύρματες Mobile IPv6 τεχνολογίες για να μπορέσουν να ανταπεξέλθουν στις απαιτήσεις του εργασιακού τους χώρου. Οι τεχνολογίες Mobile IPv6 επέτρεψαν επίσης την εκπλήρωση διασώσεων και άλλων διεργασιών με αξιοπιστία εν μέσω μιας τρομερής καταστροφής για τις Η.Π.Α και τις εταιρείες που στεγάζονταν στο συγκρότημα.

5 ΣΥΝΟΨΗ ΓΙΑ ΤΟ MOBILE DEVICE MANAGEMENT (MDM)

Εικόνα 32: Κύκλος διαχείρισης φορητών συσκευών

Στην παραπάνω εικόνα, φαίνεται η σειρά που ακολουθείται για την διαχείριση των φορητών συσκευών. Συγκεκριμένα:

- Εγγραφή χρήστη/συσκευής
- Σάρωση συσκευής
- Διαχείριση πληροφοριών συσκευής
- Ρυθμίσεις συσκευής
- Εφαρμογή πολιτικής
- Διαχείριση ασφάλειας συσκευής
- Διαχείριση εφαρμογών

- Απομάκρυνση συσκευής από την πλατφόρμα ή Απομακρυσμένη επαναφορά συσκευής στις ρυθμίσεις του κατασκευαστή (remote wipe) σε περίπτωση απώλειας συσκευής.

Υποστηριζόμενα λειτουργικά φορητών συσκευών:

- IOS (Apple)
- Android
- Windows mobile

Η διαχείριση των κινητών συσκευών (MDM) είναι ένας όρος, που χρησιμοποιείται για τη διαχείριση κινητών συσκευών, όπως smartphones, υπολογιστές tablet, φορητούς υπολογιστές και επιτραπέζιους υπολογιστές.

Το MDM υλοποιείται συνήθως με τη χρήση προϊόντος τρίτου μέρους, που διαθέτει λειτουργίες διαχείρισης για συγκεκριμένους προμηθευτές κινητών. Πολλοί οργανισμοί ελέγχουν τις δραστηριότητες των υπαλλήλων τους χρησιμοποιώντας υπηρεσίες MDM διότι είναι ένας τρόπος διασφάλισης ότι οι εργαζόμενοι παραμένουν παραγωγικοί και δεν παραβιάζουν την εταιρική πολιτική ή την ταυτότητα τους.

Με τον κατακλυσμό των Smartphone και των tablet να χτυπούν την αγορά, σχεδόν όλοι έχουν ένα Smartphone και tablet. Τώρα, με όλους να έχουν πρόσβαση στα μηνύματα ηλεκτρονικού ταχυδρομείου και επίσημα δεδομένα στις κινητές τους συσκευές, η εντολή των επιχειρήσεων είναι να εστιάζουν και να φέρνουν όλες τις κινητές συσκευές κάτω από το ραντάρ για τον έλεγχο της ροής δεδομένων και την πρόληψη της κατάχρησης των επίσημων δεδομένων.

Το MDM ασχολείται πρωτίστως, με τον διαχωρισμό των εταιρικών δεδομένων, την εξασφάλιση μηνυμάτων ηλεκτρονικού ταχυδρομείου, την εξασφάλιση εταιρικών εγγράφων σε διάφορες συσκευές, την επιβολή εταιρικών πολιτικών, την ενσωμάτωση και διαχείριση φορητών συσκευών, συμπεριλαμβανομένων φορητών υπολογιστών και έξυπνων τηλεφώνων.

Στο MDM οι υλοποιήσεις μπορεί να είναι είτε τοπικά είτε σε cloud τεχνολογίες. Η λειτουργικότητα του MDM μπορεί να περιλαμβάνει τη διανομή εξ αποστάσεως εφαρμογών, δεδομένων και ρυθμίσεις παραμέτρων για όλους τους τύπους φορητών συσκευών, συμπεριλαμβανομένου των κινητών τηλεφώνων, smartphones, υπολογιστών tablet, δικτυακών εκτυπωτών, κινητών συσκευών POS, κλπ.

Οι περισσότερες εταιρείες, λόγω κόστους εφαρμόζουν την πολιτική «Φέρτε τη δική σας συσκευή» (BYOD - Bring your own device), όπου επιτρέπεται οι εργαζόμενοι να φέρουν συσκευές της επιλογής τους (φορητοί υπολογιστές, ταμπλέτες και έξυπνα τηλέφωνα) στο χώρο εργασίας τους, και να χρησιμοποιούν τις εν λόγω συσκευές για πρόσβαση στα εσωτερικά δίκτυα, εταιρικές πληροφορίες και εφαρμογές.

Με το MDM δύναται ο έλεγχος και η προστασία στις ρυθμίσεις δεδομένων και γενικότερα τις ρυθμίσεις όλων των κινητών συσκευών, παρέχοντας τη δυνατότητα μείωσης του κόστους υποστήριξης και περιορισμού των επιχειρηματικών κινδύνων. Η πρόθεση του MDM είναι η βελτιστοποίηση της λειτουργικότητας και της ασφάλειας ενός δικτύου κινητής τηλεφωνίας με ταυτόχρονη ελαχιστοποίηση του κόστους και του χρόνου.

Με τις κινητές συσκευές να γίνονται πανταχού παρόντες και οι εφαρμογές να πλημμυρίζουν την αγορά, η παρακολούθηση και η ασφάλεια των δεδομένων αποκτά όλο και μεγαλύτερη σημασία. Επομένως, οι κατασκευαστές και οι προγραμματιστές κινητών συσκευών, τεστάρουν και παρακολουθούν την παράδοση του περιεχομένου, τις εφαρμογές και τις υπηρεσίες. Αυτή η δοκιμή του περιεχομένου γίνεται σε πραγματικό χρόνο προσομοιώνοντας τις ενέργειες χιλιάδων πελατών και παράλληλα ανιχνεύοντας και διορθώνοντας σφάλματα στις εφαρμογές.

5.1 Υλοποίηση

Τυπικές λύσεις περιλαμβάνουν ένα εξυπηρετητή (server), ο οποίος στέλνει τις εντολές διαχείρισης στις κινητές συσκευές και ένα στοιχείο client (διεπαφής), το οποίο τρέχει στη διαχειριζόμενη συσκευή λαμβάνοντας και εφαρμόζοντας τις εντολές διαχείρισης. Σε ορισμένες περιπτώσεις, ο μεμονωμένος προμηθευτής παρέχει τόσο το λογισμικό της διεπαφής όσο και τον εξυπηρετητή, ενώ σε άλλες περιπτώσεις η διεπαφή και ο εξυπηρετητής προέρχονται από διαφορετικές πηγές.

Η διαχείριση των κινητών συσκευών έχει εξελιχθεί με την πάροδο του χρόνου. Αρχικά ήταν απαραίτητη είτε η σύνδεση μέσω φορητού ακουστικού είτε η εγκατάσταση μιας κάρτας SIM για να γίνουν αλλαγές και ενημερώσεις. Η επεκτασιμότητα επίσης ήταν ένα πρόβλημα. Ένα από τα επόμενα βήματα ήταν να επιτραπούν ενημερώσεις που ξεκινούν από τον client, παρόμοιες με εκείνες του χρήστη των Windows που ζητά ένα Windows Update. Η κεντρική απομακρυσμένη διαχείριση, χρησιμοποιώντας τις εντολές που στέλνονται στον αέρα, είναι το

επόμενο βήμα. Ο διαχειριστής στο φορέα εκμετάλλευσης κινητής τηλεφωνίας, είναι ένα κέντρο δεδομένων πληροφορικής επιχείρησης ή ένας φορητός υπολογιστής, με τη χρήση μιας κονσόλας διαχείρισης για να ενημερωθεί ή να διαμορφωθεί ένα ακουστικό, ομάδα ή ομάδες των φορητών ακουστικών. Αυτό παρέχει πλεονεκτήματα επεκτασιμότητας ιδιαίτερα χρήσιμα όταν ο στόλος των διαχειριζόμενων συσκευώνείναι μεγάλου μεγέθους. Οι πλατφόρμες λογισμικού διαχείρισης συσκευών εξασφαλίζουν ότι οι τελικοί χρήστες επωφελούνται από την απλότητα και αμεσότητα ενεργοποίησης και λειτουργίας. Μια τέτοια πλατφόρμα μπορεί να εντοπίζει αυτόματα συσκευές στο δίκτυο, στέλνοντας τις ρυθμίσεις της για άμεση και συνεχιζόμενη χρηστικότητα. Η διαδικασία είναι πλήρως αυτοματοποιημένη, διατηρεί ιστορικό χρησιμοποιημένων συσκευών και αποστέλλει ρυθμίσεις μόνο σε συσκευές συνδρομητών που δεν έχουν οριστεί προηγουμένως, σε ταχύτητες που φτάνουν τα 50 αρχεία ενημέρωσης ρυθμίσεων ανά δευτερόλεπτο.

5.2 Προδιαγραφές MDM

- οργανισμός Open Mobile Alliance (OMA) καθόρισε ένα πρωτόκολλο ανεξάρτητο από την πλατφόρμα του πρωτόκολλου διαχείρισης κινητών συσκευών, που ονομάζεται διαχείριση συσκευών OMA(OMA Device Management). Η προδιαγραφή πληροί τους κοινούς ορισμούς ενός ανοικτού προτύπου, δηλαδή η προδιαγραφή είναι ελεύθερα διαθέσιμη και εφαρμόσιμη. Υποστηρίζεται από πολλές κινητές συσκευές, όπως PDA και κινητά τηλέφωνα.
- Τα έξυπνα μηνύματα είναι πρωτόκολλο παροχής πρωτότυπων μηνυμάτων SMS (κουδουνίσματα, καταχωρήσεις ημερολογίου αλλά και ρυθμίσεις που υποστηρίζονται επίσης όπως: ftp, telnet, αριθμός SMSC, ρυθμίσεις email κ.λ.π.)
- Το OMA Client Provisioning είναι μια δυαδική παροχή υπηρεσιών με βάση τις υπηρεσίες του πρωτοκόλλου SMS.
- Το Nokia-Ericsson OTA (Over-the-air programming) είναι δυαδικό πρωτόκολλο παροχής υπηρεσιών για τις ρυθμίσεις υπηρεσιών με βάση το SMS, σχεδιασμένο κυρίως για παλαιότερα κινητά τηλέφωνα Nokia και Ericsson.

Οι δυνατότητες προγραμματισμού χωρίς φυσική πρόσβαση στη συσκευή θεωρούνται βασικό στοιχείο του κινητού φορέα εκμετάλλευσης δικτύου και του λογισμικού διαχείρισης μιας κινητής συσκευής για επιχειρήσεις. Αυτά τα περιλαμβάνουν τη δυνατότητα ρύθμισης από

απόσταση μιας κινητής συσκευής, ενός ολόκληρου στόλου κινητών τηλεφώνων, συσκευών ή οποιοδήποτε σύνολο κινητών συσκευών. Επίσης δίνεται η δυνατότητα αποστολής λογισμικού και ενημερώσεων λειτουργικού συστήματος, το κλείδωμα και η εκκαθάριση μιας συσκευής, η οποία προστατεύει τα δεδομένα που είναι αποθηκευμένα στη συσκευή σε περίπτωση που αυτή χαθεί ή κλαπεί καθώς επίσης και την απομακρυσμένη αντιμετώπιση προβλημάτων. Οι εντολές OTA αποστέλλονται ως δυαδικό μήνυμα SMS. Το δυαδικό SMS είναι ένα μήνυμα που περιλαμβάνει δυαδικά δεδομένα. Το λογισμικό διαχείρισης κινητών συσκευών επιτρέπει στα εταιρικά τμήματα πληροφορικής να διαχειρίζονται πλήθος από κινητές συσκευές που χρησιμοποιούνται σε ολόκληρη την επιχείρηση. Επιχειρήσεις που χρησιμοποιούν OTA SMS ως μέρος της υποδομής MDM απαιτούν υψηλή ποιότητα στην αποστολή μηνυμάτων OTA, η οποία επιβάλλει την από την πύλη SMS την παροχή υπηρεσιών υψηλού επιπέδου ποιότητας και αξιοπιστίας.

5.3 Το MDM και η ασφάλεια φορητών συσκευών

Όλα τα προϊόντα που σχετίζονται με το MDM κατασκευάζονται με μια ιδέα δημιουργίας δοχείων (containers). Το δοχείο MDM είναι εξασφαλισμένο με τις τελευταίες κρυπτογραφικές τεχνικές όπως ο αλγόριθμος AES-256.Τα εταιρικά δεδομένα όπως τα μηνύματα ηλεκτρονικού ταχυδρομείου, τα έγγραφα και οι επιχειρηματικές εφαρμογές είναι κρυπτογραφημένα και επεξεργάζονται μέσα στο δοχείο. Αυτό εξασφαλίζει ότι τα εταιρικά δεδομένα διαχωρίζονται από το χρήστη και τα προσωπικά δεδομένα που υπάρχουν στη συσκευή. Επιπλέον, κρυπτογράφηση για ολόκληρη τη συσκευή και / ή την κάρτα SD μπορεί να εφαρμοστεί ανάλογα με την ικανότητα του προϊόντος MDM.

Επιπλέον δυνατότητες που σχετίζονται με την ασφάλεια είναι οι εξής:

- **Ασφαλής ηλεκτρονική αλληλογραφία**: Τα προϊόντα MDM επιτρέπουν στους οργανισμούς να εισάγουν το υπάρχων σύστημα ηλεκτρονικού ταχυδρομείου ώστε να ενσωματωθεί εύκολα στο περιβάλλον MDM. Σχεδόν όλα τα προϊόντα MDM υποστηρίζουν εύκολη ενσωμάτωση με τον Exchange Server (2003/2007/2010), Office365, BlackBerry Enterprise Server (BES) και άλλα. Αυτό παρέχει την ευελιξία στην διαμόρφωση του μηνύματος ηλεκτρονικού ταχυδρομείου.
- **Ασφαλή έγγραφα:** Οι υπάλληλοι συχνά αντιγράφουν συνημμένα των οποίων η λήψη γίνεται από το εταιρικό ηλεκτρονικό ταχυδρομείο στις προσωπικές τους συσκευές και

έπειτα μπορεί να υπάρχει κατάχρηση τους. Το MDM μπορεί να περιορίσει ή να απενεργοποιήσει τη χρήση της αντιγραφής μέσα ή έξω από το ασφαλές δοχείο, ώστε να περιοριστεί η προώθηση των συνημμένων σε εξωτερικούς τομείς ή να αποτραπεί η αποθήκευση συνημμένων σε κάρτα SD. Αυτό διασφαλίζει την ασφάλεια των εταιρικών δεδομένων.

- **Ασφαλής πλοήγηση:** Η χρήση ασφαλούς προγράμματος περιήγησης μπορεί να αποτρέψει πολλούς πιθανούς κινδύνους ασφαλείας. Κάθε λύση MDM έρχεται με ενσωματωμένο προσαρμοσμένο πρόγραμμα περιήγησης. Ένας διαχειριστής μπορεί να απενεργοποιήσει το αρχικό πρόγραμμα περιήγησης για να αναγκάσει τους χρήστες να χρησιμοποιήσουν το ασφαλές πρόγραμμα περιήγησης στο εσωτερικό του container MDM. Επίσης σαν πρόσθετο μέτρο ασφαλείας μπορούν να φιλτράρονται οι διευθύνσεις πλοήγησης (URL) από το MDM ώστε να επιλέγεται από το σύστημα σε ποιες μπορούν να μεταβαίνουν οι χρήστες και σε ποιες όχι.
- **Λίστα ασφαλών εφαρμογών**: Οι οργανισμοί μπορούν να διανέμουν, να διαχειριστούν και να αναβαθμίσουν εφαρμογές στη συσκευή ενός υπαλλήλου χρησιμοποιώντας έναν κατάλογο εφαρμογών. Αυτό επιτρέπει την προώθηση των εφαρμογών στη συσκευή χρήστη απευθείας από το App Store ή πιέζοντας μια ιδιωτική εφαρμογή που έχει αναπτυχθεί ή αγοραστεί από την επιχείρηση μέσω του καταλόγου εφαρμογών. Αυτό παρέχει μια επιλογή για τον έλεγχο των συσκευών και την ανάγκη ενεργοποίησης της λειτουργίας κλειδώματος.

5.4 Παράδειγμα χρήσης MDM

5.4.1 Μετατροπή ενός Android tablet σε kiosk

Το SureLock μετατρέπει οποιοδήποτε Android tablet ή Smartphone σε kiosk. Πρόκειται για μια εφαρμογή Android kiosk που αντικαθιστά την προεπιλεγμένη Αρχική οθόνη ή οθόνη Εκκίνησης και περιορίζει την πρόσβαση του χρήστη σε μία μόνο εφαρμογή ή σε κάποιες επιτρεπόμενες εφαρμογές.

Δύναται να χρησιμοποιηθεί όταν υπάρχει ανησυχία για ανεπιθύμητη κακή χρήση των συσκευών Android που ανήκουν στην εταιρεία. Η χρήση φορητών συσκευών εκτός λειτουργίας έχει γίνει συνηθισμένη για την εκτέλεση επιχειρηματικών εφαρμογών ή Kiosk

αυτοεξυπηρέτησης. Ωστόσο, η κακή χρήση της συσκευής μπορεί να επηρεάσει την παραγωγικότητα των χρηστών, να αυξήσει το κόστος συντήρησης της συσκευής και να προκαλέσει άλλα προβλήματα, όπως αύξηση της χρήσης δεδομένων κινητής τηλεφωνίας κ.λπ.

Μπορούμε να χρησιμοποιήσουμε το SureLock για να κλειδώσουμε τα Android tablet και Smartphone και να περιορίσουμε την πρόσβαση μόνο σε επιλεγμένες εφαρμογές και λειτουργίες συσκευών. Παιχνίδια όπως το Angry Birds, οι εφαρμογές κοινωνικών μέσων όπως το Facebook και το Twitter, οι ρυθμίσεις του συστήματος ή οποιεσδήποτε άλλες εφαρμογές μπορούν να κρυφτούν εντελώς από το χρήστη.

Το SureLock επιτυγχάνει τέλειο κλείδωμα σε όλα τα είδη συσκευών Android και δεν απαιτεί πρόσβαση σε ρίζα. Προτείνεται για ενισχυμένη ασφάλεια και έλεγχο πρόσβασης στις συσκευές

5.4.1.1 Χαρακτηριστικά - Λειτουργίες

- Κλείνει τα Android Smartphone & Tablets
- Περιορίζει την πρόσβαση σε επιλεγμένες εφαρμογές
- Εμφανίζει widgets στην αρχική οθόνη
- Προβάλει συντομεύσεων εφαρμογής
- Αποτρέπει τον χρήστη να αλλάξει τις ρυθμίσεις συστήματος
- Ρυθμίζει τους κωδικούς πρόσβασης για επιλεγμένες εφαρμογές
- Έχει αυτόματες εκκινήσεις εφαρμογών κατά την εκκίνηση
- Ελέγχει την πρόσβαση σε περιφερειακά (Wifi, Bluetooth, Κάμερα, Προσανατολισμός οθόνης, Λειτουργία πτήσης, Ήχος, GPS, κ.λπ.)
- Προσαρμόζει την αρχική οθόνη (Διάταξη, Λεζάντες εφαρμογών, Ταπετσαρία κ.λπ.)
- Μπορεί να επιτευχθεί απομακρυσμένη εγκατάσταση της ρύθμισης SureLock από το Cloud ή χρησιμοποιώντας το SureMDM

5.4.1.2 Προηγμένα χαρακτηριστικά - Λειτουργιές

- Λειτουργία μίας μόνο εφαρμογής
- Ομαδοποίηση εφαρμογών σε φακέλους
- Απόκρυψη του εικονιδίου μιας επιτρεπόμενης εφαρμογής
- Χρονικό όριο αναμονής της εφαρμογής

- Λειτουργία εξοικονόμησης οθόνης
- Απενεργοποίηση της γραμμής κατάστασης και του πίνακα ειδοποιήσεων
- Απενεργοποίηση του κουμπιού τροφοδοσίας
- Έναρξη καθυστερημένης εφαρμογής
- Επιλεκτικά επιτρέπει ή μπλοκάρει μεμονωμένα παράθυρα για παιδιά
- Πολλαπλές μικροεπεξεργασίες
- Περιορίζει την ευχρηστία της συσκευής κατά την οδήγηση
- Συλλέγει τα δεδομένα χρήσης της εφαρμογής (χρόνος εκκίνησης, διάρκεια χρήσης, κ.λπ.)
- Ρυθμίζει την εξοικονόμηση ενέργειας (έλεγχος φωτεινότητας βάσει της κατάστασης φόρτισης και αδράνειας του χρήστη)
- Διαχειρίζεται τη μνήμη (κλείσιμο εφαρμογών εάν επιτευχθεί κατώτατο όριο χρήσης μνήμης)

5.4.2 Προσεγγίσεις της ManageEngine: Επιτραπέζιοι υπολογιστές και Διαχείριση κινητών συσκευών

Σήμερα, οι φορητές συσκευές παρέχονται ως συμπληρωματικές εκτός από την επιφάνεια εργασίας και τους φορητούς υπολογιστές ενός υπαλλήλου. Το βάρος της διαχείρισης των κινητών συσκευών εμπίπτει κυρίως στο διαχειριστή της επιφάνειας εργασίας. Αυτός είναι ο λόγος για τον οποίο η ManageEngine κατασκευάζει το Mobile Device Management για να αποτελεί μέρος του ManageEngine Desktop Central.

5.4.2.1 Λειτουργιές Διαχείρισης

Εργασίες ρύθμισης παραμέτρων συσκευών Over-The-Air, όπως π.χ.:

- Ενεργοποίηση κωδικού πρόσβασης
- Επιβολή περιορισμών
- Ρύθμιση μηνυμάτων ηλεκτρονικού ταχυδρομείου
- Ενεργοποίηση του Exchange ActiveSync
- Webclips
- Ρυθμίσεις VPN και Wi-Fi
- Εκτέλεση εντολών ασφαλείας όπως το κλείδωμα της συσκευής

- Διαγραφή των δεδομένων της συσκευής
- Διαγραφή των εταιρικών ρυθμίσεων
- Διαγραφή του κωδικού πρόσβασης

Στοιχεία ενεργητικού που περιλαμβάνουν:

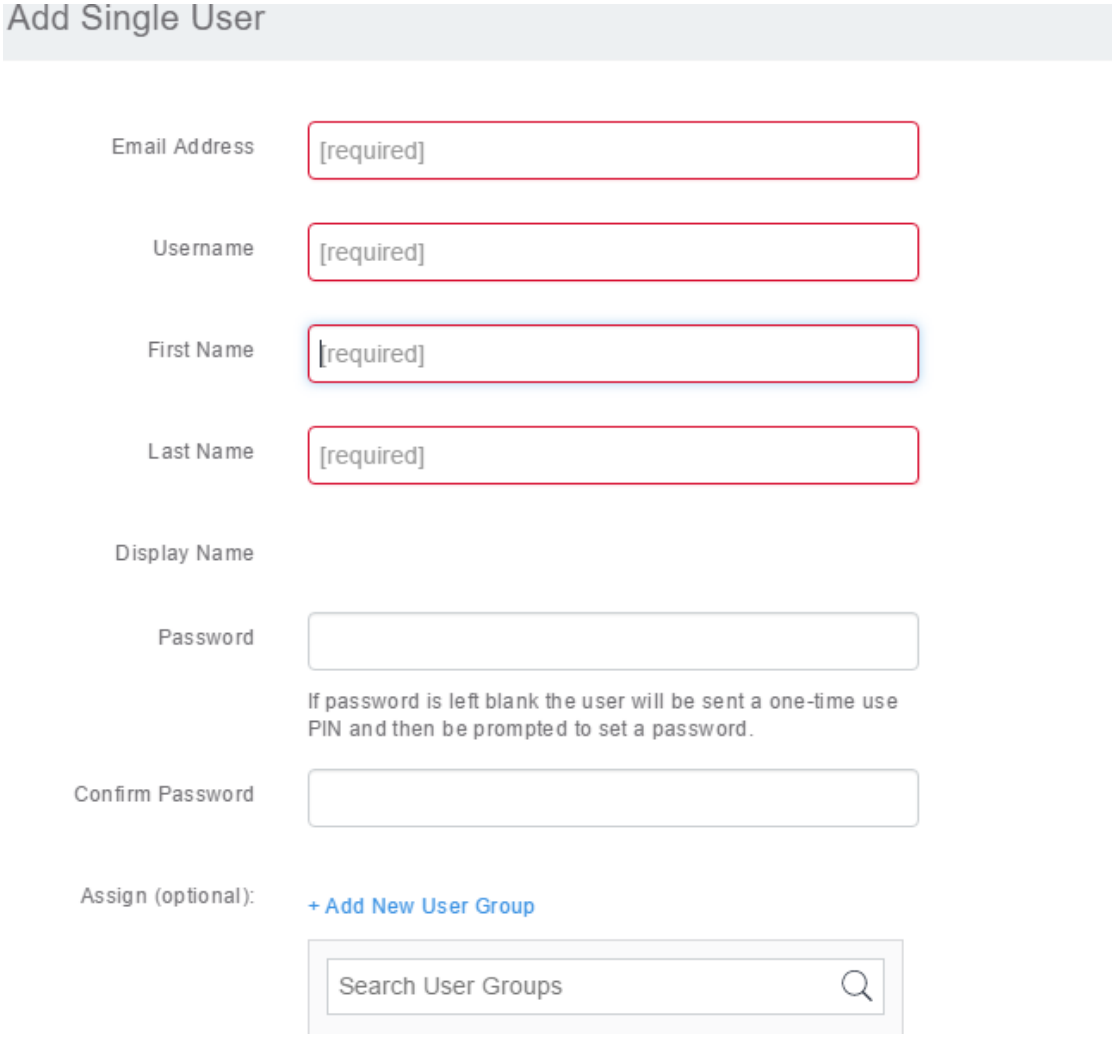
- Εγκατεστημένο πιστοποιητικό
- Εγκατεστημένο προφίλ
- Στοιχεία Περιορισμού
- Πληροφορίες ασφαλείας
- Εφαρμογές απογραφής
- Πληροφορίες συσκευής

Διαχείριση εφαρμογών:

- Διανομή εσωτερικών εφαρμογών και εφαρμογών π.χ. App Store
- Apple VPP ολοκλήρωση
- Κατάργηση εφαρμογών

5.5 Παράδειγμα εγγραφής φορητών συσκευών ή χρηστών φορητών συσκευών

Η εγγραφή των συσκευών σε πλατφόρμες διαχείρισης φορητών συσκευών μπορεί να γίνεται είτε ανά συσκευή είτε ανά χρήστη στον οποίο ανήκουν εγγεγραμμένες συσκευές



5.5.1 Παράδειγμα πληροφοριών συσκευής που εποπτεύεται διασχίζεται απομακρυσμένα

General

Manufacturer	samsung
Wi-Fi MAC Address	b4:74:43:4a:18:3d
Serial Number	R58H41NRWKH
OS/Version	Android 6.0.1
OS Build Version	N/A

Settings

Device Name	N/A
Device Identifier	N/A
Device Groups	2
Language	el_GR
Client App Version	43.0.0.5
Client App Bundle ID	com.mobileiron.anyware.android
EAS Device Identifiers	SEC18DE356AA7637, bccbdba49b69f577
Terms of Service	Internal Demo Accepted on December 22, 2016
Ownership	Not Set
Android ID	3d618a344dc3195d
Kiosk Mode	Not supported on device.
Android for Work Capable	Yes
Android for Work Enabled	No
Samsung SAFE Capable	Yes
Device Owner Mode	No
Android for Work App Enabled	No

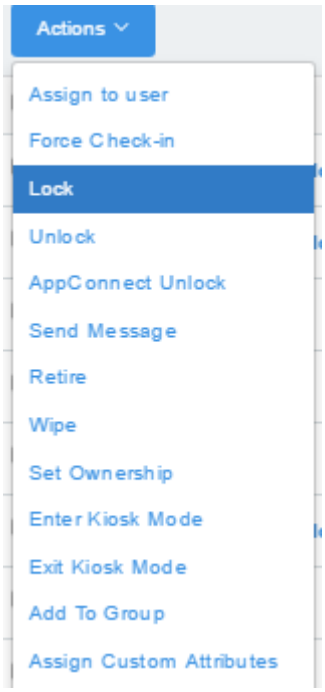
5.5.2 Παράδειγμα πολιτικής για την εφαρμογή σε συσκευές android της κατάστασης kiosk mode.

Η λειτουργία Περίπτερο (kioskMode) για συσκευές Android σας επιτρέπει να περιορίσετε τη χρήση μιας συσκευής σε συγκεκριμένες εφαρμογές. Μπορείτε να χρησιμοποιήσετε τη λειτουργία Kiosk για να ρυθμίσετε συσκευές για υπαλλήλους που θα χρησιμοποιούν μόνο εφαρμογές για συγκεκριμένες εφαρμογές.
Κατά την προετοιμασία συσκευών Android για λειτουργία Περίπτερο ή Χειριστής Συσκευής με Περίπτερο, θα χρειαστεί να δημιουργήσετε μια λίστα με τις εφαρμογές που θέλετε να είναι διαθέσιμες στους χρήστες σε λειτουργία Περίπτερο. Για συσκευές που χρησιμοποιούν τον Κάτοχο της Συσκευής, μπορείτε να προσθέσετε εφαρμογές στη λίστα εφαρμογών που έχετε επιλέξει, μεταφέροντας και αποθέτοντας τις παραμέτρους των εφαρμογών με τη σειρά που θα εμφανίζονται στη λειτουργία εκκίνησης του Kiosk Mode κατά τη διαμόρφωση της εφαρμογής. Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα "Ρύθμιση κλειδώματος & περίπτερο".

Πριν ξεκινήσετε :

- Πριν να διαμορφώσετε τη λειτουργία Kiosk για συσκευές Android, βεβαιωθείτε ότι έχετε κάνει τις ακόλουθες εργασίες:
- Εγκαταστήσατε την εφαρμογή στις συσκευές.
- Διαμορφώσατε τον κατάλογο εφαρμογών με τις εφαρμογές που χρειάζονται οι ρυθμίσεις παραθύρων.
- Διανέμεται ο κατάλογος των εφαρμογών στις συσκευές που θα εκτελούνται σε λειτουργία Kiosk.
- Εγκαταστήσατε τις εφαρμογές που χρειάζονται οι ρυθμίσεις παραθύρων.
- Προαιρετικά: Ρυθμίστε την επωνυμία του kiosk Android.

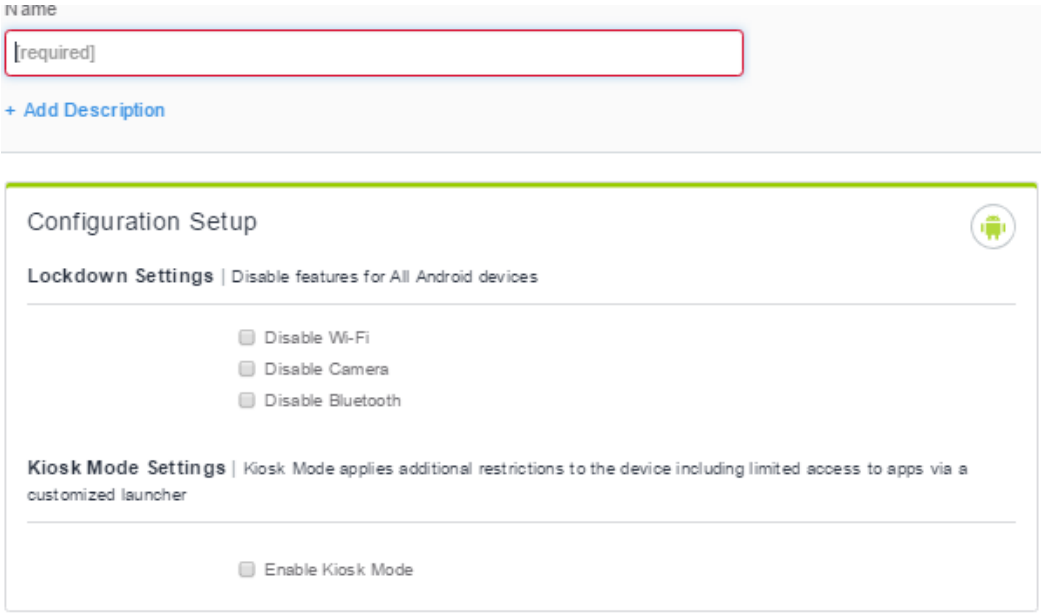
- Βήματα
    - Μεταβείτε στις Ρυθμίσεις.
    - Κάντε κλικ στο κουμπί Προσθήκη +.
    - Κάντε κλικ στο κουμπί Lockdown & Kiosk: Android.
    - Στην οθόνη Δημιουργία ρυθμίσεων της ρύθμισης Lockdown & Kiosk, συμπληρώστε τουλάχιστον την ενότητα "Ρυθμίσεις λειτουργίας κιβωτίων".
    - Στην οθόνη "Διανομή", επιλέξτε τις ομάδες συσκευών για να λάβετε αυτήν τη διαμόρφωση.
    - Κάντε κλικ στο κουμπί Ολοκληρώθηκε.
    - Για συσκευές που δεν είναι Samsung, συνεχίστε με τα παρακάτω βήματα:
    - Μεταβείτε στην επιλογή Συσκευές> Συσκευές.
    - Επιλέξτε τις συσκευές που θέλετε να ενεργοποιήσετε για λειτουργία κιβωτίου.
    - Επιλέξτε Ενέργειες> Έλεγχος δύναμης.
    - Στις συσκευές, ξεκινήστε την εφαρμογή.
    - Πατήστε το πλήκτρο λειτουργίας Περίπτερο.
    - Πατήστε το κουμπί Αρχική σελίδα της συσκευής.
    - Εάν εμφανιστεί ένα παράθυρο διαλόγου Επιλογή εκκίνησης, πατήστε Kiosk Launcher και επιλέξτε Πάντα.
    - Αυτό το βήμα είναι απαραίτητο για να διασφαλιστεί ότι θα χρησιμοποιηθεί ο κατάλληλος εκτοξευτής για αυτό το χαρακτηριστικό. Διαφορετικά, ο χρήστης θα σας ζητηθεί να επιλέξετε έναν εκκινητή.
- Εκκίνηση της Λειτουργίας Kiosk από απόσταση
    - Μεταβείτε στην επιλογή Συσκευές> Συσκευές.
    - Προσθέστε τη στήλη "Λειτουργία περίσφιξης" στην οθόνη.
    - Επιλέξτε συσκευές που έχουν ενεργοποιημένη τη λειτουργία Kiosk, αλλά δεν βρίσκονται αυτήν τη στιγμή σε λειτουργία Kiosk.
    - Επιλέξτε Ενέργειες> Εισαγωγή λειτουργίας κιβωτίων.



- Απενεργοποίηση γρήγορων ρυθμίσεων σε κατάσταση λειτουργίας περίπτωσης

Η λειτουργία Γρήγορες ρυθμίσεις είναι ενεργοποιημένη στις συσκευές Android από προεπιλογή. Τώρα μπορείτε να ενεργοποιήσετε ή να απενεργοποιήσετε τη λειτουργία Γρήγορες ρυθμίσεις για μια μόνο συσκευή ή μια ομάδα συσκευών.

1. Μεταβείτε στην επιλογή Πολιτικές> Διαμορφώσεις
2. Κάντε κλικ στο κουμπί + Προσθήκη
3. Κάντε κλικ στο Lockdown & Kiosk
4. Επιλέξτε τύπο κλειδώματος
5. Ενεργοποιήστε τη λειτουργία Kiosk. Όταν ενεργοποιείτε τη λειτουργία Kiosk, έχετε τώρα τις ακόλουθες επιλογές:
   - Απενεργοποιήστε τις γρήγορες ρυθμίσεις
   - Να επιτρέπεται στο χρήστη η πρόσβαση στις ρυθμίσεις Wi-Fi
   - Να επιτρέπεται στο χρήστη η πρόσβαση στις ρυθμίσεις Bluetooth
   - Να επιτρέπεται στο χρήστη η πρόσβαση στις ρυθμίσεις τοποθεσίας
   - Να επιτρέπεται στον χρήστη να καθυστερεί τις ενημερώσεις εφαρμογών
6. Προαιρετικά, μπορείτε να δημιουργήσετε έναν κωδικό PIN για έξοδο από τη λειτουργία Kiosk.


Name
[required]
+ Add Description
Configuration Setup
Lockdown Settings | Disable features for All Android devices
Disable Wi-Fi
Disable Camera
Disable Bluetooth
Kiosk Mode Settings | Kiosk Mode applies additional restrictions to the device including limited access to apps via a customized launcher
Enable Kiosk Mode

- Έξοδος από τη λειτουργία Kiosk

Μπορείτε να πραγματοποιήσετε έξοδο από τη λειτουργία Kiosk στη συσκευή εάν ορίσετε έναν κωδικό PIN στη διαμόρφωση:

- Αγγίξτε το εικονίδιο Ρυθμίσεις.
- Επιλέξτε Exit Kiosk Mode.
- Αγγίξτε το πεδίο PIN Περίπτερο όταν σας ζητηθεί.
- Εισαγάγετε το PIN του περίπτερο.
- Μπορείτε να πραγματοποιήσετε έξοδο από τη λειτουργία Kiosk για μια συγκεκριμένη συσκευή από την πύλη:

- Μεταβείτε στην επιλογή Συσκευές> Συσκευές.
- Εμφάνιση των στοιχείων της συσκευής.
- Επιλέξτε Ενέργειες> Κατάσταση εξόδου από το περίπτερο.
- Μπορείτε επίσης να χρησιμοποιήσετε τις ακόλουθες μεθόδους για να εξέλθετε από την λειτουργία Kiosk:
- Διαγράψτε τη διαμόρφωση
- Απενεργοποιήστε τη διαμόρφωση
- Καταργήστε την ομάδα συσκευών από τη διαμόρφωση

ΒΙΒΛΙΟΓΡΑΦΙΑ

- Bonaventure Olivier 'Computer Networking : Principles, Protocols and Practice Release 0.25', διαθέσιμο σε: https://www.saylor.org/site/wp-content/uploads/2012/02/Computer-Networking-Principles-Bonaventure-1-30-31-OTC1.pdf, προσπέλαση στις 5/3/17, 2011
- Breeze Wireless Communications Ltd 'IEEE 802.11 Technical Tutorial', διαθέσιμο σε: https://classes.soe.ucsc.edu/cmpe257/Spring03/papers/802_11tut.pdf, προσπέλαση στις 16/3/17, χ.χ
- Dynamics group 'Dynamics Mobile IP', διαθέσιμο σε: http://dynamics.sourceforge.net/, προσπέλαση στις 10/5/17, χ.χ
- Fayza Nada 'Performance Analysis of Mobile IPv4 and Mobile IPv6' *The International Arab of Information Technology,* Vol. 4, No 2, pp. 153_160, 2007
- Hazarika Barenya Bikash and Sharma Bobby 'Survey on Design and Analysis of Mobile IP', διαθέσιμο σε: http://www.ijcaonline.org/research/volume139/number2/hazarika-2016-ijca-909111.pdf, προσπέλαση στις 13/4/17, 2016
- Laurie Victor 'Computer Protocols- TCP/IP, POP, SMTP, HTTP, FTP and More', διαθέσιμο σε: http://vlaurie.com/computers2/Articles/protocol.htm, προσπέλαση στις 11/3/17, χ.χ
- Microsoft, "How 802.11 Wireless Works", διαθέσιμο σε: https://technet.microsoft.com/en-us/library/cc757419(v=ws.10).aspx, προσπέλαση στις 21/3/17, 2003
- Oracle, 'Mobile IP Administration Guide', διαθέσιμο σε: https://docs.oracle.com/cd/E19455-01/806-7600/6jgfbep13/, προσπέλαση στις 28/3/17, χ.χ
- PORTAL IPv6 CUBA 'MOBILE IPv6', διαθέσιμο σε: http://www.cu.ipv6tf.org/literatura/0201788977_ch03.pdf, προσπέλαση στις 8/4/17, χ.χ
- Prachi and Nikita Jora 'Mobile IP and Comparison between Mobile IPv4 and IPv6' *Journal of Network Communications and Emerging Technologies* , Vol. 2, No 1, pp. 72_77, 2015
- Seyedeh Masoumeh Ahmadi 'Analysis towards Mobile IPv4 and Mobile IPV6 in Computer Networks' *Intelligent Systems and Applications,* Vol. 4, pp 33_39, 2012

- http://web.cecs.pdx.edu/~jrb/SMN/ προσπέλαση στις 10-05-2017
- https://en.wikipedia.org/wiki/Computer_network προσπέλαση στις 22/2/17
- https://en.wikipedia.org/wiki/Mobile_device_management#Device_management_specifications προσπέλαση στις 6/5/17
- https://en.wikipedia.org/wiki/Mobile_IP προσπέλαση στις 11-05-2017
- https://en.wikipedia.org/wiki/Telecommunications_network προσπέλαση στις 28/2/17
- https://mosquitto.org/ προσπέλαση στις 10/5/17

- https://www.manageengine.com/mobiledevicemanagement/register.htm προσπέλαση στις 12/5/17