



ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ, ΗΛΕΚΤΡΟΝΙΚΗΣ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ

ΠΛΗΡΟΦΟΡΙΚΗΣ

Δυναμικός διαμοιρασμός κίνησης σε οικιακούς δρομολογητές

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Σοφία Π. Χατζή

Επιβλέπων : Ευστάθιος Συκάς

Καθηγητής Ε.Μ.Π

Αθήνα, Ιούνιος 2016



ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΕΠΙΚΟΙΝΩΝΙΩΝ, ΗΛΕΚΤΡΟΝΙΚΗΣ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ

ΠΛΗΡΟΦΟΡΙΚΗΣ

Δυναμικός διαμοιρασμός κίνησης σε οικιακούς δρομολογητές

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Σοφία Π. Χατζή

Επιβλέπων : Ευστάθιος Συκάς

Καθηγητής Ε.Μ.Π

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την

.....
Ευστάθιος Συκάς

Καθηγητής Ε.Μ.Π

.....
Μιχαήλ Θεολόγου

Καθηγητής Ε.Μ.Π

.....
Γεώργιος Στασινόπουλος

Καθηγητής Ε.Μ.Π

Αθήνα, Ιούνιος 2016

.....
Σοφία Π. Χατζή

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Copyright © Σοφία Π. Χατζή, 2016.

Με επιφύλαξη παντός δικαιώματος. All rights reserved.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα.

Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Εθνικού Μετσόβιου Πολυτεχνείου.

Περίληψη

Σκοπός της παρούσας διπλωματικής εργασίας είναι ο δυναμικός διαμοιρασμός της κίνησης μεταξύ δύο διεπαφών δικτύου ευρείας περιοχής(wide area network) σε οικιακούς δρομολογητές. Η υλοποίηση αυτή πραγματοποιήθηκε με τη χρήση ενός Raspberry pi , μίας Ethernet διεπαφής αλλά και ενός USB 3G dongle. Ουσιαστικά δημιουργήθηκε ένας οικιακός δρομολογητής με επιπρόσθετες δυνατότητες από αυτές που διαθέτει σήμερα ένας τυπικός δρομολογητής.

Πέραν των δύο διεπαφών WAN που χρησιμοποιήθηκαν έγινε και η προσθήκη ενός ασύρματου προσαρμογέα (wi-fi dongle) στο Raspberry pi.Ο βασικός στόχος της παρούσας εργασίας είναι η ανάπτυξη μηχανισμού μετάβασης σε μια από τις δύο WAN διεπαφές (Ethernet και 3G) σε περίπτωση απώλειας κάποιας εξ αυτών. Επιπλέον εφαρμόσαμε μια πολιτική δρομολόγησης δεδομένων με βάση την IP διεύθυνση πηγής (source based routing) ώστε υπολογιστές του οικιακού δικτύου να χρησιμοποιούν μια συγκεκριμένη διεπαφή του δικτύου ευρείας περιοχής για την εξερχόμενη κίνηση, ανάλογα με τις ρυθμίσεις που θα κάνει ο διαχειριστής του οικιακού δικτύου. Επιπρόσθετα καταστήσαμε εφικτή την παράλληλη χρήση και των δύο διεπαφών, δηλαδή του Ethernet και του 3G dongle με σκοπό τον διαμοιρασμό της εξερχόμενης κίνησης (load sharing).

Χρησιμοποιήθηκε το Quagga που αποτελεί ένα λογισμικό δρομολόγησης και το Cacti σε συνδυασμό με το πρωτόκολλο SNMP για την καταγραφή της κίνησης του δικτύου. Τέλος έγινε χρήση και του μηχανισμού των iptables των Linux ώστε ο χρήστης να μπορεί να ορίσει τους δικούς του κανόνες δρομολόγησης.

Λέξεις κλειδιά: Raspberry pi, Raspbian, home-gateway, 3G dongle, wi-fi dongle, NAT, Quagga ,Cacti ,SNMP, πολιτική δρομολόγησης (policy based routing),iptables

Abstract

The purpose of the present thesis is the dynamic sharing of the traffic between two WAN (Wide Area Network) interfaces. The implementation of this was carried out with the use of a Raspberry pi, an Ethernet interface and a USB 3G dongle. Essentially, we created a home gateway with additional abilities compared to a typical – as of today – home gateway.

In addition to the two interfaces used we also added a wi-fi dongle on Raspberry pi. There are three main objectives achieved hereby: first, in case of failure in any of the two interfaces (Ethernet and 3G dongle) a fallback to the other one is possible. Furthermore we applied a data policy based routing from a specific client of the local network to a specific interface of the WAN. Last, we have enabled the parallel usage of two interfaces, namely Ethernet and 3G dongle.

All the above were implemented using Quagga, a routing software, and Cacti in combination with SNMP protocol for network traffic recording. Last, we used iptables, through which the users can create their own routing rules.

Key words: Raspberry pi, Raspbian, home-gateway, 3G dongle, wi-fi dongle, NAT, Quagga, Cacti, SNMP, policy based routing, iptables

Ευχαριστίες

Η παρούσα διπλωματική εργασία εκπονήθηκε κατά το ακαδημαϊκό έτος 2015-2016 στον τομέα Επικοινωνιών, Ηλεκτρονικής και Συστημάτων Πληροφορικής της Σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Εθνικού Μετσόβιου Πολυτεχνείου.

Υπεύθυνος κατά την εκπόνηση της διπλωματικής ήταν ο καθηγητής κ. Ευστάθιος Συκάς στον οποίο οφείλω ιδιαίτερες ευχαριστίες τόσο για την ανάθεση της διπλωματικής όσο και για την βοήθεια ,την στήριξη αλλά και την καθοδήγηση που μου παρείχε σε όλη τη διάρκεια της διπλωματικής εργασίας. Επιπλέον θα ήθελα να τον ευχαριστήσω θερμά για την δυνατότητα που μου παρείχε να ασχοληθώ με ένα τόσο ενδιαφέρον θέμα μέσα από το οποίο εμπλούτισα τις τεχνικές μου γνώσεις. Ακόμη θα ήθελα να ευχαριστήσω τον κ. Γιώργο Λυμπερόπουλο για την βοήθεια που μου δόθηκε κατά την συγγραφή της εργασίας. Τέλος θα ήθελα επίσης να ευχαριστήσω τον υποψήφιο διδάκτορα κ. Πάρη Χαραλάμπου για την υποστήριξη και την βοήθεια που μου παρείχε κατά την εκπόνηση της παρούσας διπλωματικής.

Τέλος θα ήταν παράλειψη να μην ευχαριστήσω όλους τους δικούς μου ανθρώπους για την αμέριστη υποστήριξη και την κατανόηση που επέδειξαν σε όλη την πορεία μου.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

1.Εισαγωγή

- 1.1 Σκοπός διπλωματικής εργασίας.....16
- 1.2 Οργάνωση κειμένου.....18

2.Οικιακός δρομολογητής

- 2.1 Ο ρόλος.....19
- 2.2 Τα δομικά συστατικά.....21
- 2.3 Η εξέλιξη.....22

3.Το υλικό

- 3.1 Raspberry Pi.....24
- 3.2 Προσαρμογή του Raspberry Pi ως οικιακός δρομολογητής.....29
 - 3.2.1 USB 3G Dongle.....29
 - 3.2.2 USB Ethernet.....36
 - 3.2.3 Χρήση του wi-fi dongle για wi-fi access.....44

4.Λογισμικό

- 4.1 Quagga.....54
- 4.2 SNMP και Cacti στο Raspberry Pi.....59

5.Δρομολόγηση

- 5.1 Μετάβαση στο 3G δίκτυο σε περίπτωση απώλειας της ζεύξης.....75
- 5.2 Πολιτική δρομολόγησης.....81
- 5.3 Παράλληλη χρήση δύο διεπαφών.....87

6.Συμπεράσματα.....89

Βιβλιογραφία.....91

ΠΕΡΙΕΧΟΜΕΝΑ ΕΙΚΟΝΩΝ

Εικόνα 2.1.1 DSL modem.....	20
Εικόνα 2.2.1 Οι θύρες ενός router.....	21
Εικόνα 2.3.1 Λειτουργία ADSL σύνδεσης.....	23
Εικόνα 3.1.1 Raspberry Pi Model B+.....	24
Εικόνα 3.1.2 Σύγκριση του Raspberry Pi Model A, Model B και Model B+..	25
Εικόνα 3.1.3 GPIO Model B.....	26
Εικόνα 3.2.1.1 USB 3G Dongle.....	31
Εικόνα 3.2.1.2 Αρχιτεκτονική USB dongle.....	32
Εικόνα 3.2.1.3 Έξοδος της εντολής lsusb.....	33
Εικόνα 3.2.1.4 usb_modeswitch config file.....	34
Εικόνα 3.2.1.5 ppp0 interface.....	35
Εικόνα 3.2.2.1 Δομή πλαισίου Ethernet.....	36
Εικόνα 3.2.2.2 USB Ethernet.....	38
Εικόνα 3.2.2.3 eth1 interface.....	39
Εικόνα 3.2.2.4 iptables.....	43
Εικόνα 3.2.3.1 IEEE 802.11 Standards.....	46
Εικόνα 3.2.3.2 wi-fi dongle.....	47
Εικόνα 3.2.3.3 network interfaces.....	48
Εικόνα 3.2.3.4 ifconfig wlan0.....	48
Εικόνα 3.2.3.5 Αρχείο /etc/dhcp/dhcpd.conf.....	49
Εικόνα 3.2.3.6 Αρχείο /etc/dhcpd.conf.....	50
Εικόνα 3.2.3.7 Αρχείο /etc/hostapd.hostapd.conf.....	51
Εικόνα 3.2.3.8 wlan0 interface.....	52
Εικόνα 3.2.3.9 Σύνδεση στο wi-fi μέσω του raspberry pi.....	53

Εικόνα 4.1.1	Αρχείο με τους daemons.....	55
Εικόνα 4.1.2	Πίνακας δρομολόγησης πριν την σύνδεση του 3G.....	57
Εικόνα 4.1.3	Πίνακας δρομολόγησης μετά την σύνδεση του 3G.....	57
Εικόνα 4.2.1	Μοντέλο διαχειριστή – αντιπροσώπου.....	59
Εικόνα 4.2.2	Μοντέλο διαχείρισης SNMP.....	61
Εικόνα 4.2.3	Αρχείο snmpd.conf.....	64
Εικόνα 4.2.4	Είσοδος του χρήστη στο cacti.....	65
Εικόνα 4.2.5	Προσθήκη της συσκευής ri-cosmo.....	66
Εικόνα 4.2.6	Παράμετροι ri-cosmo.....	66
Εικόνα 4.2.7	Προσθήκη γραφημάτων στο ri-cosmo.....	67
Εικόνα 4.2.8	Εισαγωγή διεπαφών στο ri-cosmo.....	67
Εικόνα 4.2.9	Προσθήκη graph trees.....	68
Εικόνα 4.2.10	Γραφήματα διαδικασιών του raspberry-pi.....	69
Εικόνα 4.2.11	Γραφήματα της κίνησης της διεπαφής eth0.....	70
Εικόνα 4.2.12	Γραφήματα της κίνησης της διεπαφής lo.....	71
Εικόνα 4.2.13	Γραφήματα της κίνησης της διεπαφής rrr0.....	72
Εικόνα 4.2.14	Γραφήματα της κίνησης της διεπαφής wwan0.....	73
Εικόνα 4.2.15	Γραφήματα της κίνησης της διεπαφής wlan0.....	74
Εικόνα 5.1.1	Αρχείο results.txt.....	79
Εικόνα 5.2.1	Σύνδεση πριν την εφαρμογή πολιτικής δρομολόγησης.....	83
Εικόνα 5.2.2	ip tables του πυρήνα kernel.....	83
Εικόνα 5.2.3	ip table local.....	84
Εικόνα 5.2.4	ip table main.....	84

Εικόνα 5.2.5 Αρχείο /etc/iproute2/route_tables.....	85
Εικόνα 5.2.6 Σύνδεση μετά την εφαρμογή πολιτικής δρομολόγησης.....	86
Εικόνα 5.3.1 Αρχείο ip_route.txt.....	88

1 Εισαγωγή

1.1 Σκοπός διπλωματικής εργασίας

Στη σύγχρονη εποχή η τεχνολογία εξελίσσεται με ραγδαίους ρυθμούς και η χρήση του διαδικτύου αποτελεί πλέον αναπόσπαστο κομμάτι της καθημερινότητας του ανθρώπου. Το διαδίκτυο παρέχει μια αστείρευτη πηγή γνώσεων σε όλους τους ανθρώπους, εκμηδενίζει τις αποστάσεις και οι χρήστες αποκτούν ολοένα και περισσότερο την ιδιότητα του παγκόσμιου πολίτη. Οι νέες τεχνολογικές συσκευές και το ευρύ φάσμα των διαδικτυακών εφαρμογών έχουν ως αποτέλεσμα την εκπληκτική αύξηση των χρηστών σε παγκόσμια κλίμακα. Το γεγονός αυτό επιφέρει ως συνέπεια την δημιουργία νέων αναγκών που αφορούν στη σχεδίαση καινοτόμων συσκευών για την ευκολότερη και ταχύτερη διασύνδεση στο παγκόσμιο ιστό. Οι λύσεις στο πρόβλημα αυτό μπορούν να αναζητηθούν σε διαφορετικά επίπεδα δομής του δικτύου κάτι το οποίο μελετάται έντονα τόσο σε ερευνητικό όσο και σε πρακτικό επίπεδο.

Η έννοια του διαδικτύου ξεκίνησε στις ΗΠΑ κατά τη διάρκεια του ψυχρού πολέμου. Στη συνέχεια δημιουργήθηκε το πρώτο είδος διαδικτύου γνωστό ως ARPANET και έπειτα με τη σύνδεση του ARPANET με το NSFNet (διαδικτυακή πανεπιστημιακή ραχοκοκαλιά) προέκυψε ο όρος διαδίκτυο (internet). Στην ουσία Internet σήμαινε οποιοδήποτε δίκτυο χρησιμοποιούσε το πρωτόκολλο TCP/IP. Η μεγάλη άνθιση του διαδικτύου ξεκίνησε με την εφαρμογή της υπηρεσίας του Παγκόσμιου Ιστού στο CERN το 1989, η οποία αποτελεί μια πλατφόρμα για την διευκόλυνση της πρόσβασης στο Internet κάτι που είναι γνωστό ακόμα και σήμερα.

Η υποδομή του διαδικτύου αποτελείται από ένα σύνολο συσκευών που συνδέονται μεταξύ τους, όπως είναι οι δρομολογητές (routers), οι μεταγωγείς (switches), οι επαναλήπτες (hub), οι εξυπηρετητές (servers) και οι πελάτες. Σήμερα ένας οικιακός ή εταιρικός χρήστης (home/business user) χρησιμοποιεί συνήθως για την επικοινωνία του με το διαδίκτυο μια xDSL σύνδεση. Για να

πραγματοποιηθεί αυτή η σύνδεση είναι απαραίτητη η χρήση ενός DSL modem/router. Λόγω του μεγάλου πλήθους χρηστών , η γρήγορη αλλά και η συνεχής σύνδεση στο διαδίκτυο απαιτεί τη συνεχή εξέλιξη της τεχνολογίας και του υλικού των routers που χρησιμοποιούνται καθημερινά.

Στόχος της παρούσας διπλωματικής είναι η υλοποίηση μιας τεχνικής εκμετάλλευσης δύο (2) διεπαφών δικτύου ευρείας περιοχής (Wide Area Network interfaces xDSL,3G) σε ένα Raspberry pi ώστε να παρέχεται η δυνατότητα για δρομολόγηση του συνόλου της κίνησης προς μια διεπαφή δικτύου ευρείας περιοχής (WAN interface)σε περίπτωση απώλειας της άλλης διεπαφής δικτύου ευρείας περιοχής. Πιο συγκεκριμένα στο raspberry pi υπάρχει παράλληλη διασύνδεση με ενσύρματο και ασύρματο δίκτυο πρόσβασης. Η σύνδεση στο ενσύρματο δίκτυο παρέχεται μέσω του Ethernet και στο ασύρματο μέσω της χρήσης ενός 3G/4G USB dongle. Έτσι σε περίπτωση απώλειας της ενσύρματης σύνδεσης, ανάλογα με το τύπο του DSL modem που χρησιμοποιείται, υπάρχει η δυνατότητα μετάβασης στο 3G/4G δίκτυο μέσω του USB dongle το οποίο συνδέεται σε USB θύρα του DSL modem/router. Αντίστοιχα, σε περίπτωση απώλειας της ασύρματης διασύνδεσης υπάρχει η δυνατότητα μετάβασης στην ενσύρματη μέσω του Ethernet. Επιπλέον παρέχεται και η δυνατότητα για δρομολόγηση δεδομένων από συγκεκριμένο χρήστη του τοπικού δικτύου προς συγκεκριμένη διεπαφή του δικτύου ευρείας περιοχής καθώς και η παράλληλη χρήση και των δύο διεπαφών.

1.2 Οργάνωση κειμένου

Η διπλωματική εργασία αποτελείται από συνολικά έξι (6) κεφάλαια. Στο πρώτο (1) κεφάλαιο αναλύονται οι ανάγκες και οι εξελίξεις που οδήγησαν στην δημιουργία αυτής της διπλωματικής εργασίας.

Στο δεύτερο (2) κεφάλαιο παρουσιάζεται η έννοια του οικιακού δρομολογητή (home-gateway). Πιο συγκεκριμένα αναλύονται ο ρόλος, τα δομικά του συστατικά καθώς και η εξέλιξη του στο πέρασμα του χρόνου.

Στο τρίτο (3) κεφάλαιο περιγράφεται το υλικό που χρησιμοποιήσαμε δηλαδή το Raspberry Pi , το USB 3G dongle, ο Ethernet adapter καθώς και το wi-fi dongle. Πιο συγκεκριμένα περιγράφουμε τις συνδέσεις που δημιουργήσαμε μεταξύ των μηχανημάτων ώστε να καταστήσουμε το Raspberry pi ως ένα home-gateway.

Στο τέταρτο (4) κεφάλαιο περιγράφεται το λογισμικό quagga που χρησιμοποιήθηκε για την πραγματοποίηση του back-up μεταξύ του Ethernet και του 3G. Επιπλέον περιγράφεται το πρωτόκολλο SNMP και το λογισμικό Cacti που χρησιμοποιούνται για την γραφική αναπαράσταση των διεπαφών και της συσκευής.

Στο πέμπτο (5) κεφάλαιο παρουσιάζεται η διαδικασία δρομολόγησης (routing) ώστε να πετύχουμε τη δυνατότητα μετάβασης από το ασύρματο 3G/4G δίκτυο στο ενσύρματο και αντίστροφα (3G/4G-Ethernet back-up) .Επιπρόσθετα αναλύεται η διαδικασία που ακολουθήθηκε για την επίτευξη της δρομολόγησης από συγκεκριμένο χρήστη προς συγκεκριμένη διεπαφή (policy based routing) αλλά και η παράλληλη χρήση του ενσύρματου και του ασύρματου δικτύου (parallel link usage) για την επίτευξη καλύτερων αποτελεσμάτων.

Τέλος στο έκτο(6) κεφάλαιο αναφέρονται τα αποτελέσματα που προέκυψαν από την παρούσα διπλωματική και τα συμπεράσματα που εξήχθησαν κατά την μελέτη του δυναμικού διαμοιρασμού κίνησης μεταξύ δύο (2) διεπαφών WAN .

2. Οικιακός δρομολογητής

2.1 Ο ρόλος

Στη σημερινή εποχή για να είναι εφικτή η σύνδεση του χρήστη με το διαδίκτυο είναι απαραίτητη η χρήση μια συσκευής γνωστής ως home-gateway. Στην ουσία επιτρέπει την σύνδεση ενός τοπικού δικτύου (LAN) σε ένα δίκτυο ευρείας περιοχής (WAN), δηλαδή τη σύνδεση ετερογενών δικτύων μεταξύ τους με χρήση IP τεχνολογίας. Ως τοπικό δίκτυο (LAN) ορίζεται ένα σύνολο συνδεδεμένων υπολογιστών που εκτείνεται σε μια περιορισμένη γεωγραφική περιοχή. Αντίστοιχα το δίκτυο ευρείας ζώνης αποτελείται από ένα σύνολο υπολογιστών που εκτείνονται σε μια ευρεία γεωγραφική περιοχή και δημιουργούν μεταξύ τους ένα δίκτυο επικοινωνίας. Ένας home-gateway πρέπει να είναι ικανός να προσαρμόζεται σε μεταβλητές παραμέτρους και συνθήκες και να αλληλεπιδρά έξυπνα τόσο με εσωτερικές συσκευές και δίκτυα όσο και με εξωτερικά δίκτυα.

Μέσω του home-gateway δίνεται η δυνατότητα στους χρήστες να έχουν πρόσβαση σε διαφορετικές υπηρεσίες χάρη στην λειτουργία των «έξυπνων συσκευών» που υπάρχουν σήμερα σε μια οικεία. Στην ουσία ο home-gateway χρησιμοποιώντας πρωτοκόλλα δρομολόγησης και επίλυσης διευθύνσεων επιτυγχάνει την επικοινωνία μεταξύ των τοπικών δικτύων και του διαδικτύου. Ακόμα προσφέρει ένα τοίχος προστασίας στον οικιακό χρήστη μέσω του κατάλληλου λογισμικού και συγκεκριμένα του NAT (Network Address Translation).

Βέβαια η συσκευή που χρησιμοποιείται κατά κόρον σήμερα ως οικιακός δρομολογητής και δίνει τη δυνατότητα διασύνδεσης χιλιάδων οικιακών και όχι μόνο συσκευών στο παγκόσμιο ιστό είναι το DSL modem, το οποίο φαίνεται παρακάτω:

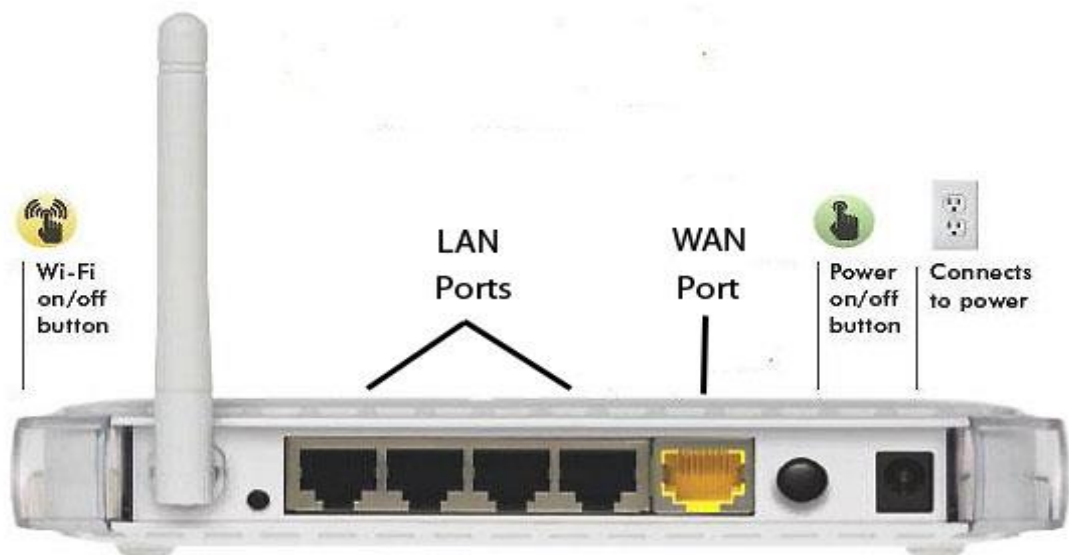


Εικόνα 2.1.1 DSL modem

Ο όρος ψηφιακή γραμμή συνδρομητή (Digital Subscriber Line) αναφέρεται συνολικά στα διάφορα είδη ψηφιακής συνδρομητικής τεχνολογίας, η οποία παρέχει πρόσβαση υψηλής ταχύτητας στο διαδίκτυο χρησιμοποιώντας ως μέσο τις κοινές τηλεφωνικές γραμμές. Συνεπώς με την τεχνολογία DSL επιτυγχάνεται ο συνδυασμός της υψηλής ταχύτητας μεταφοράς δεδομένων και της ταυτόχρονης μετάδοσης φωνής πάνω από την ίδια γραμμή. Το "x" στη συντομογραφία xDSL προκύπτει από την ύπαρξη πολλών διαφορετικών και ασύμβατων προδιαγραφών, οι οποίες καλύπτουν διαφορετικές ανάγκες. Ανάλογα με τον τρόπο διαμόρφωσης του σήματος και την ικανότητα συμμετρικής ή ασύμμετρης μετάδοσης, υπάρχουν διαφορετικά είδη xDSL τεχνολογιών που επιτυγχάνουν διαφορετικούς ρυθμούς μετάδοσης και μέγιστες αποστάσεις κυκλώματος και αναφέρονται με το όνομα ads .

2.2 Τα δομικά συστατικά

Ένας τυπικός router, ο οποίος αποτελεί σήμερα την πιο συνηθισμένη μορφή home-gateway, έχει μια(1) WAN διεπαφή και ένα πλήθος LAN διεπαφών. Η WAN διεπαφή συνδέει τον χρήστη με το δίκτυο πρόσβασης που υπάρχει εκτός του τοπικού του δικτύου. Υπάρχουν διαφορετικοί τύποι WAN διεπαφών αλλά μόνο ένας μπορεί να υποστηριχθεί κάθε φορά. Αντίστοιχα οι LAN διεπαφές συνδέονται με τους κόμβους που υπάρχουν στο τοπικό οικιακό δίκτυο. Οι διεπαφές αυτές είναι ανεξάρτητες μεταξύ τους όπως φαίνεται στην παρακάτω εικόνα :



Εικόνα 2.2.1 Οι θύρες ενός router

Οι συνδέσεις του δρομολογητή δεν περιορίζονται σε μια δεδομένη τεχνολογία δικτύου. Ένας δρομολογητής μπορεί να συνδέει δυο LAN ,ένα LAN με ένα WAN ή δύο WAN.Ακόμα όταν ένας δρομολογητής συνδέει δυο δίκτυα της ίδιας γενικής κατηγορίας αυτά δεν είναι απαραίτητο να είναι της ίδιας τεχνολογίας .

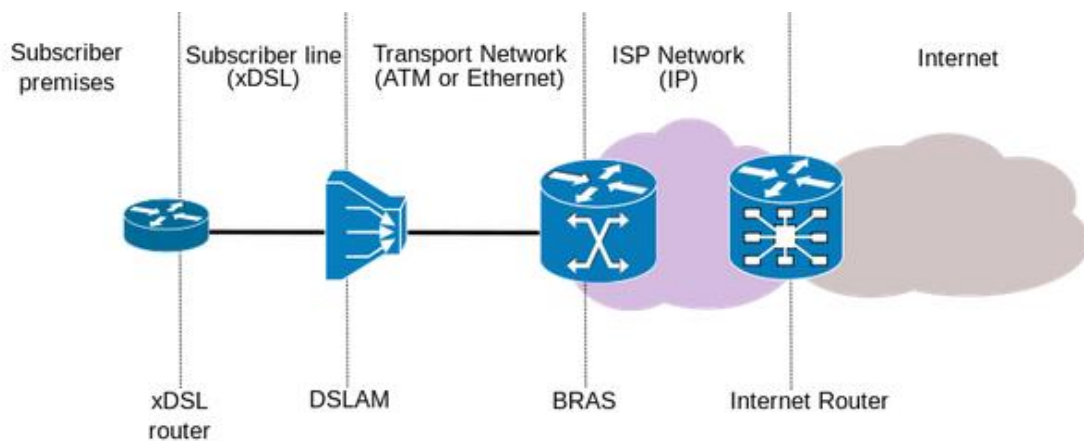
2.3 Η εξέλιξη

Ο όρος customer-premises equipment ή customer-provided equipment (CPE) αποτελεί κάθε τερματικό και συναφές εξοπλισμό που βρίσκεται στις εγκαταστάσεις του συνδρομητή και συνδέεται με τηλεπικοινωνιακά κανάλια στο σημείο οριοθέτησης(demarcation point). Το demarcation point είναι ένα σημείο που είναι εγκατεστημένο σε ένα κτήριο και διαχωρίζει τον εξοπλισμό του πελάτη από τον εξοπλισμό που βρίσκεται στην κεντρική υπηρεσία του παρόχου υπηρεσιών επικοινωνιών. Το CPE αναφέρεται γενικά σε συσκευές όπως τηλέφωνα ,δρομολογητές διακόπτες, οικιακές πύλες (home gateways),προσαρμογείς οικιακού δικτύου και πύλες πρόσβασης στο διαδίκτυο ,μέσω όλων αυτών επιτρέπει στους καταναλωτές να έχουν πρόσβαση στις υπηρεσίες των παρόχων υπηρεσιών επικοινωνίας .Επιπλέον ένας CPE μπορεί να περιλαμβάνει έναν ενεργό εξοπλισμό όπως των συσκευών που αναφέρθηκαν παραπάνω ή ένα παθητικό εξοπλισμό όπως οι προσαρμογείς του αναλογικού τηλεφώνου ή οι xDSL διαχωριστές.

Μια από τις πιο διαδεδομένες μορφές CPE σήμερα αποτελεί ο home gateway η λειτουργία του οποίου αναλύθηκε παραπάνω. Είναι ένας γενικός όρος που χρησιμοποιείται για την κάλυψη των πολλαπλών λειτουργιών που έχουν οι συσκευές δικτύωσης που χρησιμοποιούνται σε μια οικεία, το οποίο μπορεί να είναι ο συνδυασμός ενός DSL modem ή ενός καλωδιακού modem ,ενός διακόπτη δικτύου, ενός δρομολογητή και ενός σημείου ασύρματης πρόσβασης. Στο παρελθόν οι λειτουργίες αυτές παρέχονταν από ξεχωριστές συσκευές αλλά τα τελευταία χρόνια η τεχνολογική σύγκλιση επέτρεψε την συγχώνευση αυτών των πολλαπλών λειτουργιών σε μία μόνο συσκευή. Μια από τις πρώτες συσκευές οικιακής πύλης που κυκλοφόρησε επιλέχθηκε από την Telecom Italia το 2002 και μπορούσε να προσφέρει στον χρήστη υπηρεσίες triple play.Μαζί με μία συσκευή SIP VoIP για την πραγματοποίηση φωνητικών κλήσεων επέτρεψε στους συνδρομητές να έχουν πρόσβαση σε υπηρεσίες φωνής ,βίντεο και δεδομένων μέσω μίας 10MB συμμετρικής σύνδεσης ADSL ινών.

Σήμερα βέβαια έχουν αυξηθεί οι ταχύτητες των ADSL συνδέσεων ,πιο συγκεκριμένα στην Ελλάδα η μικρότερη σύνδεση ADSL είναι 2 Mbps και η

μέγιστη φτάνει έως και 24 Mbps ενώ στο πρωτόκολλο VDSL οι ταχύτητες φτάνουν μέχρι και τα 50 Mbps. Για να πραγματοποιηθεί η σύνδεση στο διαδίκτυο μέσω μια γραμμής ADSL η τηλεφωνική γραμμή που ξεκινάει από μια οικεία καταλήγει με μια συσκευή δικτύου που ονομάζεται Digital Subscriber Line Access Multiplexer (DSLAM). Ο ρόλος του DSLAM είναι να συγκεντρώσει τη κίνηση (traffic) των δεδομένων αλλά και της φωνής από πολλαπλούς συνδρομητές, και να τα συνδυάσει σε ένα περίπλοκο "σήμα", με τη διαδικασία της πολυπλεξίας (multiplexing). Από εκεί και πέρα, το σήμα από το DSLAM μεταφέρεται μέσω του πρωτοκόλλου Asynchronous Transfer Mode (PPP over ATM, PPPoA) ή Ethernet (PPP over Ethernet, PPPoE) στο δίκτυο του ISP, που μας δίνει πρόσβαση στο Internet όπως φαίνεται στην εικόνα που ακολουθεί.



Εικόνα 2.3.1 Λειτουργία ADSL σύνδεσης

3.Το υλικό

3.1 Raspberry Pi

Το raspberry pi αποτελεί μια σειρά από υπολογιστές σε μέγεθος μιας πιστωτικής κάρτας. Δημιουργήθηκαν στο Ηνωμένο Βασίλειο από το Raspberry pi ίδρυμα με στόχο την προώθηση της διδασκαλίας της επιστήμης των υπολογιστών στις αναπτυσσόμενες χώρες. Τα βασικά μοντέλα παραγωγής είναι δύο, το Model A και το Model B ενώ πλέον είναι διαθέσιμη και μια βελτιωμένη έκδοση του Model B που είναι το Model B+. Το αρχικό raspberry pi βασίζεται στο σύστημα Broadcom BCM2835 σε ένα chip το οποίο περιλαμβάνει ARM1176JZF - S 700 MHz επεξεργαστή και αρχικά είχε εξοπλιστεί με μνήμη RAM 256 MB που αργότερα στα μοντέλα B και B+ αναβαθμίστηκε στα 512 MB. Επιπλέον το σύστημα τους περιλαμβάνει υποδοχές SD(Secure Digital) ή MicroSD για την εκκίνηση και την μόνιμη αποθήκευση δεδομένων. Το μοντέλο B+ που χρησιμοποιήθηκε στην παρούσα διπλωματική φαίνεται στην παρακάτω εικόνα:



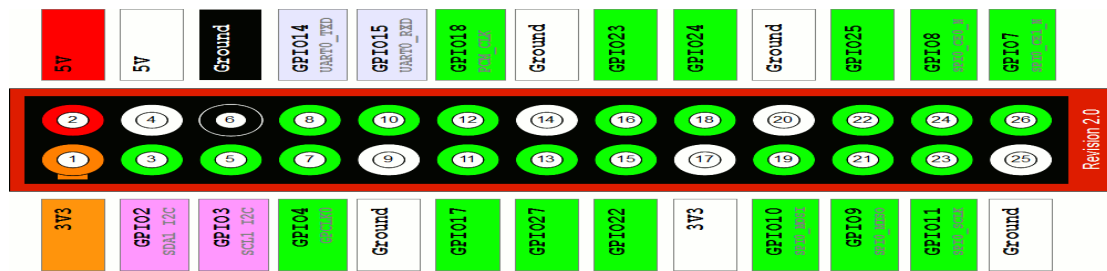
Εικόνα 3.1.1 Raspberry Pi Model B+

Οι διαφορές που υπάρχουν μεταξύ του Model A, του Model B και του Model B + παρουσιάζονται στον πίνακα που ακολουθεί :

	Model A	Model B	Model B+
Target price:	US\$25	US\$35	
SoC:	Broadcom BCM2835(CPU,GPU,DSP,SDRAM and single USB port)		
CPU:	700 MHz ARM1176JZF-S core(ARM11 family,ARMv6 instruction set)		
GPU:	Broadcome VideoCore IV@250MHz OpenGL ES 2.0(24GFLOPS) MPEG-2 and VC-1(with license),1080p30 h.264/MPEG-4 AVC high-profile decoder and encoder		
Memory(SDRAM)	256 MB (shared with GPU)	512 MB(shared with GPU) as of 15 October 2012	
USB 2.0 ports:	1 (direct from BCM2835 chip)	2(via the on-board 3 port USB hub)	4(via the on-board 5 port USB hub)
Video input:	15-pin MIPI camera interface(CSI) connector, used with the Raspberry pi camera or Raspberry pi NOIR camera		
Video outputs:	Composite video(PAL and NTSC)(in models A and B via RCA jack: in Model B+,via 3.5mmTRRS jack shared with audio out).HDMI,DSI for raw LCD panels.14 HDMI resolutions from 640x350 to 1920x1200 plus various PAL and NTSC standars		
Audio outputs:	Analog audio via 3.5mm phone jack,HDMI, and as of revision 2boards		
Onboard storage:	SD/MMC/SDIO card slot(3.3 V with card power only)		
Onboard network:	none	10/100 Mbits Ethernet USB adapter on the third/fifth port of the USB hub	
Low-level peripherals:	8xGPIO plus the following which can also be used as GPIO:UART,IC bus,SPI bus with two chips selects		17xGPIO plus the same specific functions and HAT ID bus
Power ratings:	300 mA(1.5W)	700mA(3.5W)	600mA(3.0W)
Power source:	5V via MicroUSB or GPIO header		
Size:	85.60mm x 56mm(3.370 in x 2.205 in)-not including protruding connectors		
Weight:	45g (1.6oz)		

Εικόνα 3.1.2 Σύγκριση του Raspberry Pi Model A, Model B και Model B+

Τα Raspberry Pi Model A και Model B έχουν 26 pins ενώ το Model B+ έχει 40 pins τα οποία ονομάζονται GPIO(General Purpose Input Output) και αποτελούν μια φυσική διασύνδεση του raspberry pi με τον έξω κόσμο. Μπορούν να θεωρηθούν ως διακόπτες που μπορούν να ενεργοποιηθούν ή να απενεργοποιηθούν. Επιπλέον τα pins μπορούν να προγραμματιστούν ώστε να επιδρούν με τον πραγματικό κόσμο εκπληκτικά επιτρέποντας τη διασύνδεση του raspberry pi με άλλες συσκευές που είτε χρησιμοποιούνται ως είσοδοι είτε ως έξοδοι. Παρακάτω παρουσιάζεται η μορφολογία του GPIO για το Model B.



Εικόνα 3.1.3 GPIO Model B

Το raspberry πi στην έκδοση Model B+ έχει τέσσερις(4) USB θύρες σε αντίθεση με το Model A που περιλαμβάνει δύο(2).Πέρα από τις τέσσερις(4) θύρες είναι εξοπλισμένο και με μια θύρα Ethernet καθώς και μία έξοδο HDMI.Επιπρόσθετα η βελτιωμένη έκδοση του raspberry πi προσφέρει χαμηλότερη κατανάλωση ενέργειας αφού πλέον έχουν αντικατασταθεί οι γραμμικοί ρυθμιστές με ρυθμιστές μεταγωγής μειώνοντας έτσι την κατανάλωση ισχύος μεταξύ 0.5W και 1W.Τέλος παρέχεται καλύτερος ήχος αφού στο νέο μοντέλο είναι ενσωματωμένη μια παροχή ρεύματος χαμηλού θορύβου.

Με όλα αυτές τις δυνατότητες που περιλαμβάνει το raspberry πi μπορεί να χρησιμοποιηθεί στην υλοποίηση ενός μεγάλου εύρους εφαρμογών όπως : Media Center, Arcade Machine, Smart TV, Robotics, RPi cloud server, RPi Μετεωρολογικός Σταθμός, για αυτοματισμούς σπιτιού, για αποθήκευση δικτύου, Streaming internet radio, Mini web server, FTP server, Proxy server, Firewall και πολλά άλλα. Επομένως γίνεται κατανοητό ότι με τη χρήση του raspberry πi η τεχνολογία προάγεται αφού μέρα με τη μέρα χρησιμοποιείται όλο και περισσότερο, δίνοντας στην δυνατότητα στο χρήστη να εφαρμόζει ένα μεγάλο εύρος εφαρμογών αλλά και να ανακαλύπτει νέες που στόχο θα έχουν την συνεχή βελτίωση του σύγχρονου επιπέδου ζωής.

Όσον αναφορά το λειτουργικό σύστημα του raspberry πi είναι γνωστό ότι λόγω της τροφοδοσίας του από τον ARM επεξεργαστή δεν μπορεί να «τρέξει» το ίδιο λειτουργικό σύστημα με τον υπολογιστή του χρήστη. Για αυτό το λόγο πρέπει να χρησιμοποιηθεί ένα από τα διαθέσιμα λειτουργικά συστήματα τα οποία βασίζονται στον πυρήνα Linux.Το Raspbian “Weezy” αποτελεί το

πρότυπο λειτουργικό σύστημα που «τρέχει» στο raspberry pi, το οποίο είναι πολύ εύχρηστο για μη έμπειρους χρήστες των linux .Το Soft-float Debian “Weezy” αποτελεί ένα άλλο λειτουργικό σύστημα το οποίο είναι χρήσιμο κυρίως για java εφαρμογές. Το Arch Linux ARM αποτελεί την τρίτη επιλογή και απευθύνεται κυρίως σε πιο έμπειρους χρήστες.

Στη παρούσα διπλωματική πραγματοποιήθηκε η εγκατάσταση του λογισμικού raspbian Jessie που είναι βασισμένο σε debian linux.Γενικά υπάρχουν πολλές αλλαγές μεταξύ του Weezy και του Jessie.Στην έκδοση του Jessie έχουν γίνει πολλές βελτιώσεις ως προς την επίδοση και την ευελιξία των διαδικασιών του συστήματος αλλά και ως προς την διόρθωση διαφόρων σφαλμάτων. Για την εγκατάσταση λοιπόν του λογισμικού αρχικά έγινε η λήψη ενός συμπιεσμένου αρχείου που περιείχε την εικόνα της έκδοσης που επιθυμούσαμε να εγκαταστήσουμε. Την εικόνα αυτή την αποθηκεύσαμε στην micro sd κάρτα που χρησιμοποιείται από το raspberry pi.Για να επιτευχθεί βέβαια αυτό ήταν απαραίτητη πρώτα η εγκατάσταση του προγράμματος Win 32 Disk Imager στην έκδοση 0.9.5.Μέσω αυτού του προγράμματος είναι δυνατή η εγγραφή της εικόνας του λογισμικού σε μια micro sd κάρτα. Η ελάχιστη μνήμη μιας sd κάρτας για το raspberry pi είναι 2GB ωστόσο προτείνονται να χρησιμοποιούνται κάρτες των 4GB και άνω. Αφού πραγματοποιηθούν όλα τα παραπάνω βήματα εισάγουμε την κάρτα στο raspberry pi και αφού το συνδέσουμε με μια οθόνη και ένα πληκτρολόγιο εγκαθιστούμε το λογισμικό και έπειτα μπορούμε να εισέλθουμε στην επιφάνεια εργασίας του. Εκεί μετά την είσοδο μας στο τερματικό ανοίγουμε το αρχείο /etc/network/interfaces στο οποίο ορίζουμε τη στατική διεύθυνση 147.102.7.60 στη διεπαφή eth0 αλλά και τις διευθύνσεις των υπόλοιπων διεπαφών που χρησιμοποιούνται στο raspberry pi.Μέσω της στατικής διεύθυνσης ip και αφού έχει ενεργοποιηθεί η λειτουργία SSH καθίσταται δυνατή η απομακρυσμένη χρήση του raspberry pi μέσω του προγράμματος putty. Το SSH (Secure Shell) είναι ένα ασφαλές δικτυακό πρωτόκολλο το οποίο επιτρέπει τη μεταφορά δεδομένων μεταξύ δύο υπολογιστών. Το SSH όχι μόνο κρυπτογραφεί τα δεδομένα που ανταλλάσσονται κατά τη συνεδρία, αλλά προσφέρει ένα ασφαλές σύστημα αναγνώρισης καθώς και άλλα

χαρακτηριστικά όπως ασφαλή μεταφορά αρχείων (SSH File Transfer Protocol, SFTP).

3.2 Προσαρμογή του Raspberry Pi ως οικιακός δρομολογητής

Όπως προαναφέρθηκε το Raspberry pi χρησιμοποιείται ευρέως για την κατασκευή διαφόρων εφαρμογών. Μια από τις γνωστότερες είναι η χρήση του Raspberry pi για την δημιουργία ενός οικιακού δρομολογητή (home gateway). Για την υλοποίηση του είναι απαραίτητη η χρήση Ethernet και ενός USB 3G dongle.

3.2.1 USB 3G Dongle

Λόγω της αυξανόμενης χρήσης του διαδικτύου οι χρήστες επιζητούν ολοένα και περισσότερο την ασύρματη πρόσβαση σε αυτό από οποιαδήποτε τοποθεσία. Έτσι μπορούν να συνδεθούν ασύρματα μέσω ενός WLAN hotspot, ενός κινητού τηλεφώνου, ενός φορητού modem, ή μέσω κάποιων συσκευών όπως ένα 3G USB(Universal Serial Bus) dongle. Μια από τα πιο διαδεδομένες μορφές ασύρματων δικτύων είναι τα κυψελοειδή δίκτυα ευρείας περιοχής. Το βασικό χαρακτηριστικό συστημάτων 3^{ης} γενιάς είναι η υποστήριξη εφαρμογών πολυμέσων και η δυνατότητα πρόσβασης σε πληροφορίες και υπηρεσίες από δημόσια ή ιδιωτικά δίκτυα ,με υψηλούς ρυθμούς μετάδοσης. Βρίσκουν εφαρμογή στην ασύρματη φωνητική τηλεφωνία, την κινητή πρόσβαση στο διαδίκτυο, την σταθερή ασύρματη πρόσβαση στο διαδίκτυο, τις κλήσεις βίντεο και την κινητή τηλεόραση.

Η Διεθνής Ένωση Τηλεπικοινωνιών όρισε τα πρότυπα της τρίτης γενιάς (3G) κινητής τηλεφωνίας το 2000 για να διευκολύνει την ανάπτυξη ,την αύξηση του εύρους ζώνης και την υποστήριξη ενός ευρύτερου φάσματος εφαρμογών. Για να είναι όμως εφικτή η μετάβαση από το 2G στο 3G δίκτυο οι φορείς εκμετάλλευσης κινητών επικοινωνιών πραγματοποίησαν μεγάλες αλλαγές των υφιστάμενων δικτύων ενώ παράλληλα σχεδίασαν νέα κινητά ευρυζωνικά δίκτυα. Αυτό είχε ως αποτέλεσμα τη δημιουργία δύο νέων 3G τη 3GPP και την 3GPP2. Η 3GPP(3rd Generation Partnership Project) ιδρύθηκε το 1998 για την προώθηση της ανάπτυξης των δικτύων 3G που προέρχονταν από το σύστημα για κινητές τηλεπικοινωνίες γνωστό ως GSM(Global System for Mobile Communications). Η τεχνολογία 3GPP εξελίχθηκε ως εξής :

- Το GSM αρχικά παρείχε δυνατότητα μετάδοσης δεδομένων με ρυθμούς 9.6 kbps. Στη συνέχεια η αναβάθμιση του GSM με την υποστήριξη υπηρεσιών δεδομένων με τεχνολογία μεταγωγής πακέτων οδήγησε στο GPRS (General Packet Radio Service) το οποίο πλέον παρέχει ταχύτητες μεγαλύτερες των 114 kbps.
- Η τεχνολογία EDGE (Enhanced Data for Global Evolution) η οποία θεωρείται μετεξέλιξη του GPRS μπορεί να υποστηρίξει ρυθμούς πάνω από 384 kbps.
- Το σύστημα ευρείας ζώνης CDMA (Wideband CDMA-WCDMA) προσφέρει ταχύτητες downlink πάνω από 1.92 Mbps.
- Το δίκτυο LTE είναι ένα δίκτυο βασισμένο εξ ολοκλήρου στη μεταγωγή πακέτων με μια από τις βασικές δομικές μονάδες του το δίκτυο ράδιο-πρόσβασης (Evolved UMTS Terrestrial Radio Access Network –E-UTRAN) .Στην ανερχόμενη ζεύξη (uplink) ο υψηλότερος ρυθμός μετάδοσης δεδομένων φτάνει τα 75 Mbps και στην κάτω ζεύξη (down link) ο ρυθμός αυτός μπορεί να φτάσει τα 300 Mbps.

Η τεχνολογία 3GPP2 εξελίχθηκε ως εξής :

- Η τεχνολογία 1xRTT (Radio Transmission Technology) προσφέρει ταχύτητες πάνω από 144 kbps.
- Το EV-DO (Evolution Data Optimized) είναι ένα πρότυπο δεδομένων ασύρματης ευρυζωνικότητας 3G που επιτρέπει μεγαλύτερες ταχύτητες από ότι είναι διαθέσιμες στα υφιστάμενα δίκτυα CDMA ή άλλες 2G υπηρεσίες. Στην τεχνολογία 3GPP2 το EV-DO αύξησε την ταχύτητα downlink πάνω από 2.4 Mbps.

Όλη η τεχνολογία 3G καθώς και τα χαρακτηριστικά της χρησιμοποιούνται στο 3G USB dongle το οποίο παρουσιάζεται στην παρακάτω εικόνα.



Εικόνα 3.2.1.1 USB 3G Dongle

Κάθε USB dongle περιέχει ένα μικρό modem και έναν πομποδέκτη που επιτρέπει στη συσκευή να συνδέεται στο 3G/4G δίκτυο. Για να αποκτηθεί η πρόσβαση στο διαδίκτυο μέσω του δικτύου της κινητής τηλεφωνίας το λειτουργικό σύστημα χρησιμοποιεί το dongle σαν ένα modem που συνδέεται σε έναν τερματικό διακομιστή μέσω του πρωτοκόλλου PPP. Το PPP είναι ένα πρωτόκολλο σύνδεσης δεδομένων που χρησιμοποιείται για να δημιουργήσει μια άμεση σύνδεση μεταξύ δύο κόμβων. Μπορεί να παρέχει πιστοποίηση της σύνδεσης, κρυπτογράφηση μετάδοσης (χρησιμοποιώντας ECP, RFC 1968) και τη συμπίεση. Χρησιμοποιείται σε πολλά είδη των φυσικών δικτύων, συμπεριλαμβανομένων του σειριακού καλωδίου, της τηλεφωνικής γραμμής, της γραμμής κορμού, του κινητού τηλεφώνου, των εξειδικευμένων ραδιοζεύξεων, και τις συνδέσεις οπτικών ινών όπως το SONET. Το PPP χρησιμοποιείται επίσης πάνω από τις συνδέσεις στο διαδίκτυο. Οι πάροχοι υπηρεσιών διαδικτύου (ISP) έχουν χρησιμοποιήσει το πρωτόκολλο PPP για dial-up συνδέσεις αφού τα πακέτα IP δεν μπορούν να μεταδοθούν μέσω μιας γραμμής modem χωρίς τη χρήση κάποιου πρωτοκόλλου ζεύξης δεδομένων. Υπάρχουν δύο παράγωγα του PPP πρωτοκόλλου, το Point-to-Point Protocol over Ethernet (PPPoE) και το Point-to-Point Protocol over ATM (PPPoA) που χρησιμοποιούνται πιο συχνά από τους παρόχους υπηρεσιών διαδικτύου (ISP) για τη δημιουργία μίας ψηφιακής συνδρομητικής γραμμής (DSL). Έτσι λοιπόν το USB dongle συνδέεται με έναν «διακομιστή τερματικού (terminal server)» μέσω του PPP και διαπραγματεύεται ποια οικογένεια πρωτοκόλλου πρόκειται να χρησιμοποιήσει, εκχωρείται έπειτα μια διεύθυνση IP και τότε μπορούν να αρχίσουν να ενθυλακώνονται τα πακέτα IP και να διαβιβάζονται στον

προορισμό. Σε περίπτωση απώλειας της σύνδεσης η διαδικασία αυτή θα πρέπει να επαναληφθεί από την αρχή. Αυτό το είδος της dial up υπηρεσίας υποστηρίζεται από την υπηρεσία απομακρυσμένης πρόσβασης (RAS) η οποία αποτελεί μια τεχνική που δημιουργήθηκε από την Microsoft. Η RAS συνδέει απομακρυσμένους πελάτες σε έναν κεντρικό υπολογιστή που είναι γνωστός ως διακομιστής(server) απομακρυσμένης πρόσβασης. Μέσω αυτού του διακομιστή οι πελάτες μπορούν να έχουν πρόσβαση σε ένα τοπικό δίκτυο (LAN) ή στο διαδίκτυο. Η RAS χρησιμοποιεί το πρωτόκολλο PPP για να εγκαταστήσει μια σύνδεση μεταξύ του απομακρυσμένου πελάτη και του διακομιστή. Το αποτέλεσμα που προκύπτει είναι το ίδιο όπως στην περίπτωση όπου ο πελάτης θα συνδεόταν σειριακά στον διακομιστή. Η αρχιτεκτονική ενός USB dongle φαίνεται στην παρακάτω εικόνα :



Εικόνα 3.2.1.2 Αρχιτεκτονική USB dongle

Η αρχιτεκτονική RNDIS χρησιμοποιείται για την διασύνδεση της Rm διεπαφής του USB dongle. Η RNDIS είναι ένα πρωτόκολλο USB στενά συνδεδεμένο με τους NDIS οδηγούς το οποίο παρέχει εικονικό Ethernet μέσω USB. Για τις Um διεπαφές το dongle θα πρέπει να είναι σε θέση να υποστηρίξει τόσο κινητές ευρυζωνικές υπηρεσίες όσο και WLAN και το dongle θα πρέπει αυτόματα να χρησιμοποιήσει την καλύτερη διεπαφή ώστε να παρέχει στο χρήστη την βέλτιστη ποιότητα. Για αυτό το λόγο είναι αναγκαία η διεπαφή για κυψελοειδές δίκτυο και για WLAN. Επιπλέον δεδομένου ότι πολλοί κινητοί κόμβοι χρησιμοποιούν USB dongles είναι απαραίτητη η μετάφραση διευθύνσεων δικτύου (NAT), έτσι μια δημόσια διεύθυνση IP στο dongle μπορεί να αντιστοιχεί σε διαφορετικές ιδιωτικές διευθύνσεις IP στους κινητούς κόμβους. Επιπλέον το dongle περιλαμβάνει έναν DHCP server, έναν DNS server καθώς και ένα τοίχος προστασίας (firewall). Μέσω του DHCP

server το dongle παρέχει τοπικές διευθύνσεις στις συνδεδεμένες συσκευές, με τον DNS server επιτυγχάνεται ταχύτερη περιήγηση στο διαδίκτυο και σε άλλες υπηρεσίες. Τέλος με το τείχος προστασίας μειώνεται η ανεπιθύμητη ροή δεδομένων.

Όπως προαναφέρθηκε και παραπάνω το USB 3G dongle μπορεί να συνδεθεί σε ένα μεγάλο εύρος συσκευών ,μια από αυτές είναι και το raspberry pi.Για την εγκατάσταση του USB 3G dongle στο raspberry pi ακολουθείται η εξής διαδικασία. Αρχικά πραγματοποιείται μια ανανέωση των πακέτων που είναι διαθέσιμα μέσω της εντολής που ακολουθεί, η οποία εισάγεται στο command line του raspberry pi :

- **sudo apt-get update**

Τα USB modems κατασκευάζονται συχνά ως ολοκληρωμένες συσκευές οι οποίες πολλές φορές εμποδίζουν τα linux από την αυτόματη ανίχνευση του modem.Για να καταχωρηθεί το modem ως μια συσκευή linux είναι απαραίτητο να ρυθμιστεί η κατάλληλη ID τιμή του προϊόντος που επιλέγεται όταν το dongle είναι συνδεδεμένο. Κάτι τέτοιο επιτυγχάνεται με την εντολή:

- **sudo apt-get install ppp usb-modeswitch wvdial.**

Έπειτα λαμβάνονται οι κωδικοί ενεργοποίησης του 3G μέσω της εντολής:

- **lsusb**

```
root@RPi:~# lsusb
Bus 001 Device 002: ID 0424:9514 Standard Microsystems Corp.
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 003: ID 0424:ec00 Standard Microsystems Corp.
Bus 001 Device 004: ID 0fe6:9700 Kontron (Industrial Computer Source / ICS Advent)
DM9601 Fast Ethernet Adapter
Bus 001 Device 005: ID 19d2:2000 ZTE WCDMA Technologies MSM MF627/MF628/MF628+/MF636+
HSDPA/HSUPA
```

Εικόνα 3.2.1.3 Έξοδος της εντολής lsusb

Στη συνέχεια πραγματοποιείται μια επανεκκίνηση του Raspberry pi και εισάγεται ξανά η εντολή lsusb.Η εντολή lsusb δείχνει αν το chipset αναγνωρίστηκε από τον πυρήνα USB και αποτελεί την πρώτη προϋπόθεση ώστε μια συσκευή να είναι έγκυρη. Η έξοδος της εντολής lsusb μας δίνει το Vendor ID και το Product ID δυο αριθμούς που χωρίζονται με άνω και κάτω

Επομένως κάθε φορά για την ενεργοποίηση του 3G dongle είναι απαραίτητη η εκτέλεση των εντολών :

- **sudo usb_modeswitch -c /etc/usb_modeswitch.conf**
- **wvdial 3gconnect**

Το wvdial αποτελεί ένα point-to-point πρωτόκολλο που στόχο έχει να καλέσει ένα modem και να ξεκινήσει ένα rppd (Point-to-Point Protocol daemon) για να είναι εφικτή η σύνδεση με το διαδίκτυο. Κατά την εκκίνηση του το wvdial φορτώνει τη διαμόρφωση του από το αρχείο **/etc/wvdial.conf** . Έπειτα από την εκτέλεση της εντολής wvdial 3gconnect είναι απαραίτητη και η εκτέλεση της εντολής **bg** η οποία επιτρέπει στη σύνδεση του 3g dongle να παραμένει ενεργή στο background δίνοντας την δυνατότητα στο χρήστη να συνεχίζει με την εκτέλεση άλλων εντολών. Στην πορεία όταν επιτυγχάνεται η σύνδεση στο τερματικό του raspberry pi και μέσω της εντολής ifconfig βλέπουμε ότι το 3G dongle λειτουργεί και εμφανίζεται η διεπαφή ppp0 η οποία έχει λάβει πλέον ip διεύθυνση όπως φαίνεται στην παρακάτω εικόνα :

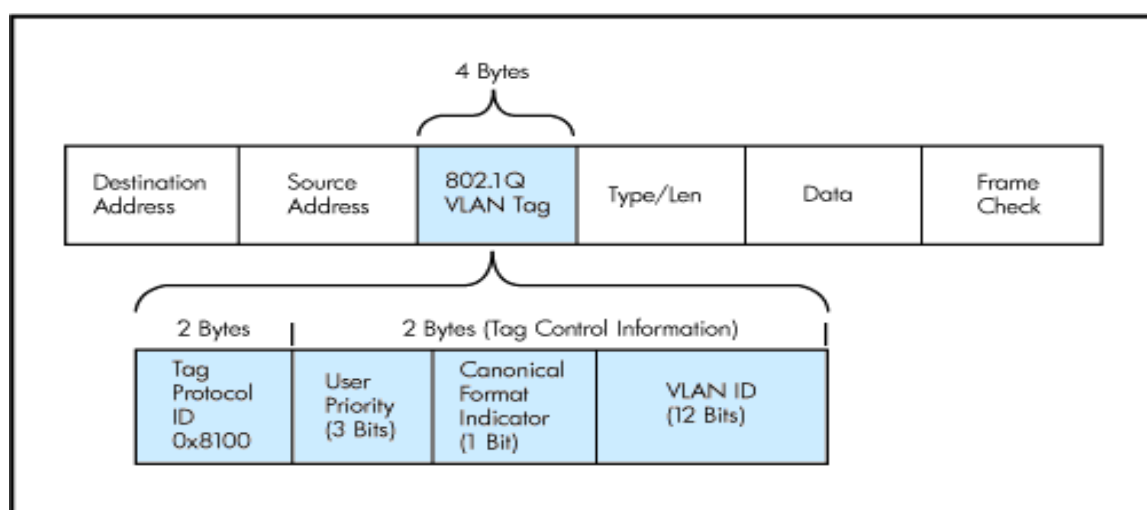
```
ppp0      Link encap:Point-to-Point Protocol
          inet addr:5.203.231.189 P-t-P:10.64.64.64 Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1500 Metric:1
          RX packets:6 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:102 (102.0 B)  TX bytes:141 (141.0 B)
```

Εικόνα 3.2.1.5 ppp0 interface

3.2.2 USB Ethernet

Το Ethernet είναι ένα πρότυπο δικτύωσης για τοπικά δίκτυα που επιτρέπει στους χρήστες να συνδεθούν στο διαδίκτυο μέσω συσκευών όπως προσωπικοί υπολογιστές, δρομολογητές, modem με την χρήση των πυλών που διαθέτουν και του καλωδίου Ethernet. Ενώ η τεχνολογία Ethernet δεν αποτελεί τον μόνο τρόπο δικτύωσης μέσω μιας φυσικής σύνδεσης, είναι η πιο δημοφιλής και υλοποιείται στις περισσότερες συσκευές. Επιπλέον, η τεχνολογία Ethernet χρησιμοποιείται κατά κύριο λόγο για τη δημιουργία μιας σύνδεσης διαδικτύου μεταξύ ενός σημείου πρόσβασης και ενός υπολογιστή. Μπορεί επίσης να χρησιμοποιηθεί για τη μεταφορά δεδομένων μεταξύ δύο συσκευών .

Η δομή του πλαισίου Ethernet αποτελεί ένα πολύ σημαντικό στοιχείο για την κατανόηση της λειτουργίας του και παρουσιάζεται στην παρακάτω εικόνα :



Εικόνα 3.2.2.1 Δομή πλαισίου Ethernet

Υπάρχουν έξι πεδία του πλαισίου Ethernet:

- Πεδίο δεδομένων (46 ως 1.500 bytes). Αυτό το πεδίο μεταφέρει δεδομένογραμμα IP. Το ελάχιστο μέγεθος του πεδίου είναι 46 bytes και το μέγιστο 1.500 bytes.
- Διεύθυνση προορισμού (6 bytes). Αυτό το πεδίο περιέχει τη διεύθυνση MAC του προσαρμογέα προορισμού.

- Διεύθυνση προέλευσης (6 bytes). Αυτό το πεδίο περιέχει την διεύθυνση MAC του προσαρμογέα, που εκπέμπει το πλαίσιο επάνω στο LAN.
- Πεδίο τύπου (2 bytes). Το πεδίο τύπου επιτρέπει στο Ethernet να κάνει πολύπλεξη πρωτοκόλλων επιπέδου δικτύου (εκτός του IP).
- Κυκλικός έλεγχος πλεονασμού (CRC) (4 bytes). Ο σκοπός του πεδίου CRC είναι να επιτρέπει στον προορισμό λήψης, να ανιχνεύει αν έχουν εισαχθεί σφάλματα μέσα στο πλαίσιο, δηλαδή αν κάποια bits μέσα στο πλαίσιο έχουν αλλαχθεί.
- Προοίμιο (8 bytes). Το πλαίσιο Ethernet αρχίζει με ένα πεδίο προοιμίου 8 bytes. Τα πρώτα 7 bytes του προοιμίου εξυπηρετούν για να αφυπνίσουν τους προσαρμογείς λήψης και για να συγχρονίσουν τα ρολόγια τους με το ρολόι του αποστολέα.

Η ικανότητα σύνδεσης των Ethernet συσκευών μέσω USB θυρών είναι γνωστή ως Ethernet over USB. Υπάρχει μια μεγάλη ποικιλία συσκευών USB Ethernet στην αγορά χαμηλού κόστους. Ένα τυπικό USB Ethernet παρουσιάζεται στην παρακάτω εικόνα :



Εικόνα 3.2.2.2 USB Ethernet

Όπως προαναφέρθηκε το raspberry pi δεν διαθέτει αρκετές θύρες Ethernet για αυτό το λόγο γίνεται η χρήση του USB Ethernet adapter. Μέσω αυτού δίνεται η δυνατότητα στο οικιακό δίκτυο να συνδέεται με το raspberry pi χρησιμοποιώντας το ως ένα κοινό δρομολογητή για τη διασύνδεση του με το διαδίκτυο. Τα τεχνικά χαρακτηριστικά ενός USB Ethernet adapter είναι τα εξής :

- 10/100/1000 Mbps ταχύτητα Ethernet
- Ολοκληρωμένη διεύθυνση ελέγχου πρόσβασης (MAC) για γρήγορο Ethernet, φυσικό chip και πομποδέκτη.
- Είναι συμβατό με USB 1.1/2.0/3.0.
- Περιλαμβάνει 18KB μνήμη SRAM.
- Υποστηρίζει το IEEE 802.3x έλεγχο ροής (flow control).

Έτσι λοιπόν με τη χρήση του USB Ethernet adapter στο raspberry pi εισήχθη μια επιπλέον διεπαφή (interface) το eth1 πέρα από τις διεπαφές του Ethernet και του USB 3G dongle που είναι αντίστοιχα οι eth0 και η rrr0. Πληκτρολογώντας την εντολή ifconfig eth1 λαμβάνεται η διαμόρφωση

(configuration) της διεπαφής eth1 ,τα στοιχεία της οποίας φαίνονται στην παρακάτω εικόνα :

```
root@RPi:~# ifconfig eth1
eth1      Link encap:Ethernet  HWaddr 00:e0:4c:53:44:58
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:1 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Εικόνα 3.2.2.3 eth1 interface

Από την εντολή ifconfig μπορούν να ληφθούν σημαντικές πληροφορίες για την διεπαφή όπως ποια είναι η ip διεύθυνση της διεπαφής ,η broadcast διεύθυνση, η MAC διεύθυνση καθώς και η μάσκα της. Επίσης φαίνονται διάφορες πληροφορίες σχετικά με τα πακέτα που λαμβάνονται και εκπέμπονται.

Για να μπορέσει λοιπόν ένας υπολογιστής του οικιακού δικτύου να συνδεθεί στην διεπαφή eth1 του raspberry pi και μέσω αυτού να συνδεθεί στο διαδίκτυο είναι απαραίτητη η εγκατάσταση της μετάφρασης διευθύνσεων δικτύου (Network Address Translation-NAT). Το NAT σχεδιάστηκε για την απλοποίηση και την διατήρηση των IP διευθύνσεων αφού αυτό που κάνει είναι να επιτρέπει σε ιδιωτικά δίκτυα που χρησιμοποιούν μη εγγεγραμμένες IP διευθύνσεις να έχουν σύνδεση με το Internet. Το σύστημα NAT λειτουργεί σε κάποιον δρομολογητή, ο οποίος συνδέει συνήθως δύο δίκτυα και μεταφράζει τις ιδιωτικές (μη μοναδικές στον παγκόσμιο ιστό) διευθύνσεις του εσωτερικού δικτύου σε νόμιμες διευθύνσεις προτού τα πακέτα προωθηθούν σε άλλο δίκτυο. Σαν μέρος αυτής της λειτουργίας το NAT μπορεί να ρυθμιστεί ώστε να κάνει γνωστή μόνο μία διεύθυνση στον έξω κόσμο για ολόκληρο το δίκτυο που συνδέει με αυτόν. Αυτό το χαρακτηριστικό παρέχει επιπλέον ασφάλεια αφού κρύβει ολόκληρο το εσωτερικό δίκτυο από το κόσμο πίσω από μία διεύθυνση. Πιο συγκεκριμένα το NAT δουλεύει ως εξής: κάθε υπολογιστής ενός ιδιωτικού δικτύου που ζητάει να συνδεθεί με κάποιον εκτός δικτύου κάνει αίτηση στον Network Address Translator (που υπάρχει στη πύλη(gateway ή firewall)) για να πάρει μια νέα διεύθυνση. Το NAT διαθέτει ένα σύνολο IP διευθύνσεων («address pool») και μία από αυτές τις αναθέτει στον

υπολογιστή. Ταυτόχρονα, κρατάει μία βάση δεδομένων στην οποία καταγράφει τη διεύθυνση που απέδωσε σε κάθε υπολογιστή ,γνωστή ως διαδικασία MAP. Έτσι, κάθε πακέτο που φεύγει από τον υπολογιστή του ιδιωτικού δικτύου και «ταξιδεύει» στο Internet έχει σαν διεύθυνση αποστολέα τη νέα αυτή διεύθυνση. Αντίστροφα, κάθε υπολογιστής που θέλει να στείλει δεδομένα στον συγκεκριμένο υπολογιστή του ιδιωτικού δικτύου, στέλνει πακέτα με διεύθυνση παραλήπτη τη νέα διεύθυνση. Το NAT είναι πάλι υπεύθυνος σε αυτήν την περίπτωση για να παραλάβει ο υπολογιστής τα πακέτα που προορίζονται για αυτόν: συγκεκριμένα, το NAT κοιτάει τη βάση δεδομένων και βλέπει ποια είναι η πραγματική IP διεύθυνση του υπολογιστή (δηλαδή η διεύθυνση που έχει στο ιδιωτικό του δίκτυο) και, με βάση αυτήν την πληροφορία, δρομολογεί τα εισερχόμενα πακέτα. Το NAT άρχισε να χρησιμοποιείται όλο και περισσότερο από το 1990 και μετά λόγω της προβλεπόμενης εξάντλησης διευθύνσεων IP σε παγκόσμιο επίπεδο.

Έτσι λοιπόν σύμφωνα με τα παραπάνω γίνεται κατανοητό ότι είναι απαραίτητη η εγκατάσταση του NAT στο raspberry pi καθώς χωρίς αυτή ένας υπολογιστής του τοπικού δικτύου είναι αδύνατον να συνδεθεί στο διαδίκτυο. Για την εγκατάσταση του ακολουθήθηκαν τα παρακάτω βήματα :

Βήμα 1^ο

Αρχικά θα πρέπει να είναι δυνατή η προώθηση ip πακέτων (ip forwarding). Η προώθηση ip είναι γνωστή ως μια διαδικασία δρομολόγησης του διαδικτύου που χρησιμοποιείται για να προσδιορίσει μέσω ποιας διαδρομής μπορεί να σταλεί ένα πακέτο δεδομένων. Έτσι η διαδικασία αυτή κάνει χρήση των πληροφοριών δρομολόγησης για την λήψη αποφάσεων και έχει σχεδιαστεί ώστε να είναι εφικτή η αποστολή ενός πακέτου σε πολλαπλά δίκτυα. Για να γίνει δυνατή λοιπόν η προώθηση ip είναι αναγκαίο να εκτελεστεί η εντολή :

- **echo 1 > /proc/sys/net/ipv4/ip_forward** μέσω της οποίας γίνεται μόνιμη η προώθηση ip,

έπειτα μέσω της εντολής :

- **/etc/init.d/procps restart** εκτελείται επανεκκίνηση της δικτύωσης,

τέλος μέσω της εντολής :

- **cat /proc/sys/net/ipv4/ip_forward** μπορεί να ελεγχθεί αν τροποποιήθηκε η προώθηση ip από την τιμή που δίνει ως αποτέλεσμα η εντολή. Σε περίπτωση που είναι η τιμή 1(ένα) σημαίνει ότι είναι δυνατή η προώθηση ip ,ενώ δεν είναι δυνατή όταν παρουσιαστεί 0 (μηδέν).

Βήμα 2^ο

Αφού λοιπόν τροποποιήθηκε η προώθηση ip και διαμέσου αυτής το raspberry pi έχει την δυνατότητα να λειτουργήσει ως δρομολογητής(router) το επόμενο στάδιο αποτελεί η εγκατάσταση του NAT. Για την επίτευξη αυτού του στόχου είναι αναγκαία η δημιουργία κάποιων «κανόνων» γνωστοί ως iptables. Τα iptables χρησιμοποιούνται για να επιθεωρήσουν, τροποποιήσουν, προωθήσουν, ανακατευθύνουν ή απορρίψουν IPv4 πακέτα. Ο κώδικας για το φιλτράρισμα των IPv4 πακέτων είναι ήδη ενσωματωμένος στον πυρήνα και οργανώνεται σε μία συλλογή από πίνακες (*tables*), ο καθένας με ένα συγκεκριμένο σκοπό. Οι πίνακες είναι φτιαγμένοι από ένα σύνολο προκαθορισμένων αλυσίδων (*chains*), και οι αλυσίδες περιέχουν κανόνες οι οποίοι διασχίζονται κατά σειρά. Κάθε κανόνας αποτελείται από ένα κατηγορημα με πιθανά matches και μία αντίστοιχη δράση (που ονομάζεται στόχος (*target*)) η οποία εκτελείται αν το κατηγορημα είναι αληθές, πχ. οι καταστάσεις ταιριάζουν. Τα iptables αποτελούν το εργαλείο του χρήστη που του επιτρέπει να δουλέψει με αυτές τις αλυσίδες/κανόνες. Τα iptables περιέχουν πέντε πίνακες:

- raw χρησιμοποιείται μόνο για τη ρύθμιση πακέτων έτσι ώστε να εξαιρούνται από την παρακολούθηση της σύνδεσης.
- filter είναι ο default πίνακας, και είναι εκεί όπου λαμβάνουν μέρος όλες οι δράσεις που συνήθως συνδέονται με ένα firewall.
- nat χρησιμοποιείται για το network address translation.
- mangle χρησιμοποιείται για ειδικές μετατροπές πακέτων.

- security χρησιμοποιείται για το Mandatory Access Control κανόνες δικτύου.

Επομένως χρησιμοποιήθηκε ο πίνακας nat για την εγκατάσταση του NAT στο raspberry pi. Οι πίνακες όμως αποτελούνται από αλυσίδες, λίστες κανόνων που ακολουθούνται διαδοχικά. Ο πίνακας nat περιέχει τις αλυσίδες **PREROUTING**, **POSTROUTING**, και **OUTPUT**. Αρχικά, καμία αλυσίδα δεν περιέχει κανόνες. Ο χρήστης γράφει κανόνες στις επιθυμητές του αλυσίδες, οι οποίες έχουν μια προεπιλεγμένη πολιτική, συνήθως ρυθμισμένη στο **ACCEPT**, η οποία μπορεί να επαναφερθεί στο **DROP** ώστε να εξασφαλιστεί ότι τίποτα δεν ξεφεύγει από το σύνολο κανόνων. Η προεπιλεγμένη πολιτική πάντοτε εφαρμόζεται στο τέλος, μόνο, της κάθε αλυσίδας, και έτσι το πακέτο πρέπει να περάσει από όλους τους υπάρχοντες κανόνες στην αλυσίδα προτού αυτή να εφαρμοστεί. Προσθέτοντας αλυσίδες που καθορίζονται από το χρήστη, τα σύνολα κανόνων είναι πιο αποτελεσματικά ή τροποποιούνται ευκολότερα. Το φιλτράρισμα των πακέτων βασίζεται σε κανόνες, που καθορίζονται από πολλαπλές ζεύξεις, προϋποθέσεις που πρέπει να τηρεί το πακέτο για να εφαρμοστεί ο κανόνας, έναν στόχο αλλά και τη δράση που λαμβάνεται όταν το πακέτο ταιριάζει με όλες τις προϋποθέσεις. Τυπικές περιπτώσεις ζεύξης κανόνα είναι η εύρεση της επιφάνειας απ' όπου προέρχεται το πακέτο (όπως eth0 ή eth1), τι τύπου πακέτο είναι (ICMP, TCP ή UDP) ή η θύρα για την οποία προορίζεται το πακέτο. Οι στόχοι καθορίζονται με την επιλογή **-j** ή **--jump**. Μπορούν να είναι είτε αλυσίδες που ορίζει ο χρήστης είτε ένας από τους ενσωματωμένους στόχους ή κάποια επέκταση αυτών. Οι ενσωματωμένοι στόχοι είναι: **ACCEPT**, **DROP**, **QUEUE** και **RETURN**. Παραδείγματα επεκτάσεων στόχων είναι οι **REJECT** και **LOG**. Επιπλέον υπάρχει και η επιλογή του **MASQUERADE** η οποία δίνει την δυνατότητα σε εσωτερικούς υπολογιστές που είναι συνδεδεμένοι με linux δρομολογητές μέσω rpp, ethernet ή wi-fi συνδέσεων να αποκτούν σύνδεση με το διαδίκτυο χωρίς να έχουν επίσημα εκχωρημένες ip διευθύνσεις αλλά εσωτερικές. Γενικά εάν ο στόχος ανήκει στους ενσωματωμένους, η μοίρα του πακέτου αποφασίζεται άμεσα και η επεξεργασία του στον τρέχον πίνακα σταματά. Όταν ο στόχος είναι αλυσίδα που ορίστηκε από τον χρήστη και το πακέτο περάσει επιτυχώς από τη δεύτερη αλυσίδα, θα προχωρήσει στον

επόμενο κανόνα της αυθεντικής αλυσίδας. Οι επεκτάσεις στόχων χωρίζονται σε "τερματικές" (ως ενσωματωμένοι στόχοι) και "μη-τερματικές" (ως αλυσίδες που ορίστηκαν από τον χρήστη).

Σύμφωνα λοιπόν με τα παραπάνω στο raspberry pi δημιουργήθηκαν οι παρακάτω κανόνες:

- **iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE**
- **iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE**
- **iptables -A FORWARD -i eth0 -o eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT**
- **iptables -A FORWARD -i ppp0 -o eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT**
- **iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT**
- **iptables -A FORWARD -i eth1 -o ppp0 -j ACCEPT**

Για να επιβεβαιωθεί ότι οι παραπάνω κανόνες καταχωρήθηκαν σωστά χρησιμοποιείται η εντολή :

- **iptables -L -t nat**

το αποτέλεσμα της οποίας φαίνεται στην εικόνα που ακολουθεί:

```
root@RPi:~# iptables -L -t nat
Chain PREROUTING (policy ACCEPT)
target     prot opt source                destination

Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source                destination
MASQUERADE all  -- anywhere             anywhere
MASQUERADE all  -- anywhere             anywhere
```

Εικόνα 3.2.2.4 iptables

3.2.3 Χρήση του wi-fi dongle για wi-fi access

Ένα ασύρματο τοπικό δίκτυο (Wireless Local Area Network) επιτυγχάνει αμφίδρομη μετάδοση δεδομένων ,με φυσικό μέσο μετάδοσης τον αέρα. Η μετάδοση πραγματοποιείται είτε στην περιοχή των ραδιοσυχνοτήτων είτε με υπέρυθρη ακτινοβολία. Τα τοπικά ασύρματα δίκτυα χρησιμοποιούνται εκτεταμένα τόσο σε κοινόχρηστους χώρους όσο και σε κατοικίες καθώς ,εμφανίζουν σημαντικά πλεονεκτήματα στην εγκατάσταση, λειτουργία και χρήση τους

Η εγκατάσταση ενός ασύρματου τοπικού δικτύου είναι γρήγορη και εύκολη ενώ το συνολικό κόστος λειτουργίας του μπορεί να είναι σημαντικά χαμηλότερο σε σχέση με άλλες τεχνολογίες πρόσβασης. Παράλληλα τα ασύρματα τοπικά δίκτυα παρέχουν στους χρήστες τη δυνατότητα πρόσβασης σε ευρυζωνικές υπηρεσίες για το διάστημα που αυτοί παραμένουν σε σημεία περιοχής κάλυψης των εν λόγω δικτύων.

Αναφορικά με την αρχιτεκτονική των wi-fi δικτύων ,η βασική δομική τους μονάδα είναι οι βασικές ομάδες υπηρεσίας (Basic Service Set)ένα σύνολο από συσκευές-σταθμούς με δυνατότητα πρόσβασης στο ασύρματο μέσο(STAtions), οι οποίες επικοινωνούν μέσω του ίδιου καναλιού στην ίδια περιοχή. Αντίστοιχα οι εκτεταμένες ομάδες υπηρεσίας (Extended Service Set) αποτελούν ένα σύνολο από BSSs και ενσύρματα τοπικά δίκτυα πρόσβασης. Το δίκτυο μεταφοράς διασυνδέει τα σημεία πρόσβασης μεταξύ τους καθώς και με τα υπόλοιπα ενσύρματα τοπικά δίκτυα και ονομάζεται σύστημα διανομής (Distribution System). Το πρότυπο δεν ορίζει την μορφή του, έτσι μπορεί να είναι είτε ένα ενσύρματο δίκτυο(για παράδειγμα Ethernet) είτε κάποιο ασύρματο.

Όσον αναφορά την τοπολογία τους τα δίκτυα αυτά εμφανίζονται με δύο βασικές δομές , τη δομημένη(Infrastructure),την τυχαία (Ad-hoc) ή συνδυασμό των παραπάνω. Με την χρήση δομημένης τοπολογίας πολλαπλά σημεία πρόσβασης (Access Points) συνδέονται με ενσύρματο δίκτυο , αυξάνοντας την κάλυψη και την χωρητικότητα του δικτύου πρόσβασης. Με τη χρήση τυχαίας διάταξης στο ασύρματο τοπικό δίκτυο, οι χρήστες συνδέονται απευθείας μεταξύ τους ,χωρίς τη μεσολάβηση σημείων πρόσβασης.

Προφανώς ένα ασύρματο τοπικό δίκτυο μπορεί να περιλαμβάνει οποιονδήποτε συνδυασμό των παραπάνω τοπολογιών.

Τον Ιούνιο του 1977 η IEEE οριστικοποίησε το πρώτο πρότυπο για τα ασύρματα τοπικά δίκτυα με την ονομασία 802.11. Σκοπός του προτεινόμενου προτύπου αποτέλεσε η ανάπτυξη μιας προδιαγραφής για την ασύρματη διασύνδεση σταθερών, φορητών και κινητών σταθμών μέσα σε μια τοπική περιοχή. Το τελικό πρότυπο ,που δημοσιεύθηκε τον Νοέμβριο του 1997, καθορίζει τη λειτουργία πρωτοκόλλων ικανών να υποστηρίξουν την ασύρματη δικτύωση μιας τοπικής περιοχής. Η κύρια υπηρεσία του 802.11 είναι η μεταφορά των M-SDU(MAC Service Data Unit) μεταξύ ομότιμων στρωμάτων ζεύξης δεδομένων. Παράλληλα περιλαμβάνει βασικές υπηρεσίες όπως διασύνδεση με τα εξωτερικά δίκτυα, συσχέτιση ενός σταθμού με ένα σημείο πρόσβασης, επανασυσχέτιση ενός σταθμού σε περίπτωση μετακίνησης, τερματισμός της συσχέτισης ,πιστοποίηση, ασφάλεια και διαχείριση ισχύος τερματικού σταθμού.

Η IEEE802.11 συνεπώς είναι μια οικογένεια πρωτοκόλλων που περιγράφουν τη λειτουργία ασύρματων τοπικών δικτύων. Στο πρότυπο 802.11 προδιαγράφονται τα δύο πρώτα επίπεδα του OSI,δηλαδή το φυσικό επίπεδο(PHYsical) και το επίπεδο ζεύξης δεδομένων (υποεπίπεδο Medium Access Control),γεγονός το οποίο επιτρέπει σε οποιαδήποτε δικτυακή εφαρμογή να «τρέχει» σε τοπικά δίκτυα που υποστηρίζουν το IEEE 802.11 όπως ακριβώς θα «έτρεχε» και σε τοπικό δίκτυο Ethernet(IEEE 802.3).

Το πρωτόκολλο 802.11 υποστηρίζει ρυθμούς μετάδοσης δεδομένων της τάξεως των 1Mbps και 2Mbps.Η μετάδοση του σήματος γίνεται είτε στην ISM ζώνη συχνοτήτων(2.4GHz-2.4835GHZ),είτε σε υπέρυθρη ακτινοβολία μήκους κύματος 850-950 nm.Για μεγαλύτερη ανθεκτικότητα στον θόρυβο στενής ζώνης το σήμα κωδικοποιείται με μεθόδους απλωμένου φάσματος. Το πρωτόκολλο υποστηρίζει την τεχνική εξάπλωσης φάσματος με εναλλαγή συχνότητας και την τεχνική εξάπλωσης φάσματος ευθείας ακολουθίας. Για την μετάδοση του σήματος στην ISM ζώνη χρησιμοποιείται(στην περίπτωση εξάπλωσης φάσματος με εναλλαγή συχνότητας)διαμόρφωση με μετατόπιση συχνότητας (FSK) δύο συχνοτήτων για ρυθμούς 1Mbps και τεσσάρων

συχνοτήτων για ρυθμούς 2 Mbps. Αντίστοιχα στην περίπτωση εξάπλωσης φάσματος ευθείας ακολουθίας χρησιμοποιείται δυαδική διαμόρφωση με μετατόπιση φάσης BPSK για ρυθμούς 1 Mbps και τετραφασική PSK για ρυθμούς 2 Mbps. Για την επικοινωνία μέσω υπέρυθρων χρησιμοποιείται διαμόρφωση θέσης παλμών (Pulse Position Modulation).

Το πρωτόκολλο 802.11 συνέβαλε ουσιαστικά στην ευρεία εξάπλωση των ασύρματων δικτύων, καθώς η προτυποποίηση κατέστησε δυνατή τη διαλειτουργικότητα μεταξύ των συσκευών που το υλοποιούσαν. Ωστόσο οι ταχύτητες των 1Mbps και 2 Mbps που υποστήριζε ήταν πολύ μικρές για τα 10 Mbps αρχικά και τώρα 100 Mbps που δίνει το ενσύρματο Ethernet. Πολύ γρήγορα λοιπόν εμφανίσθηκαν παραλλαγές του 802.11 που αύξησαν την ταχύτητα του και διόρθωσαν διάφορα εγγενή προβλήματα. Οι παραλλαγές μαζί με τις μεταξύ τους διαφορές φαίνονται στον παρακάτω πίνακα:

Standard	Frequency band	Bandwidth	Modulation	Maximum data rate
802.11	2.4GHz	20MHz	DSS,FHSS	2Mb/s
802.11b	2.4GHz	20MHz	DSSS	11Mb/s
802.11a	5GHz	20MHz	OFDM	54Mb/s
802.11g	2.4GHz	20MHz	DSSS,OFDM	54Mb/s
802.11n	2.4GHz,5GHz	20MHz,40 MHz	OFDM	600Mb/s
802.11ac	5GHz	20,40,80,80 +80,160 MHz	OFDM	6.93Gb/s
802.11ad	60GHz	2.16GHz	SC,OFDM	6.76Gb/s

Εικόνα 3.2.3.1 IEEE 802.11 Standards

Όμως για να είναι εφικτή η wi-fi πρόσβαση σε ένα raspberry pi είναι απαραίτητη η χρήση ενός nano wi-fi dongle το οποίο φαίνεται στην παρακάτω εικόνα :



Εικόνα 3.2.3.2 wi-fi dongle

Ο συγκεκριμένος wi-fi προσαρμογέας (adapter) παρά το μικρό του μέγεθος υποστηρίζει μέγιστο εύρος ,ταχύτητα και ρυθμό μετάδοσης που φτάνει έως τα 150 Mbps μέσω της σύνδεσης 802.11 n που είναι τρεις φορές γρηγορότερη από την σύνδεση 11g.Είναι συμβατό με τις IEEE 802.11 b/g/n παραλλαγές και έχει προσαρμοστεί σε αυτό ένα «έξυπνο» πρωτόκολλο ελέγχου της ισχύος μετάδοσης δημιουργώντας το λεγόμενο Green WLAN. Μέσω της τεχνολογίας Green WLAN η μείωση της κατανάλωσης ενέργειας του προσαρμογέα μπορεί να φτάσει το 20% έως 50%.

Για την εγκατάσταση του wi-fi dongle αρχικά πρέπει να συνδεθεί σε μια από τις θύρες usb που υπάρχουν στο raspberry pi.Στην συνέχεια για να δούμε εάν το raspberry pi αναγνώρισε το wi-fi εκτελούμε την εντολή :

- **dmesg | more .**

Έπειτα πρέπει να διαμορφώσουμε τις ρυθμίσεις του δικτύου στο αρχείο /etc/network/interfaces μέσω της εντολής :

- **sudo nano /etc/network/interfaces,**

ανοίγουμε το αρχείο και αφού το τροποποιήσουμε κατάλληλα βάζοντας στατική ip διεύθυνση το 192.168.1.1 στη διεπαφή wlan0, netmask τη 255.255.255.0 και ορίζοντας ως σχόλια τις τρεις επόμενες γραμμές που ακολουθούν:

- **iface wlan0 manual,**
- **wpa-roam/etc/wpa_supplicant/wpa_supplicant.conf,**

- **iface default inet dhcp**, παρατηρούμε την παρακάτω εικόνα :

```

auto lo

iface lo inet loopback
#iface eth0 inet dhcp

#auto eth0
iface eth0 inet static
    address 147.102.7.60
    netmask 255.255.255.0
    network 147.102.7.0
    broadcast 147.102.7.255
    gateway 147.102.7.200
    dns-nameservers 8.8.8.8
    dns-search telecom.ece.ntua.gr telecom.ntua.gr

allow-hotplug wlan0

iface wlan0 inet static
    address 192.168.1.1
    netmask 255.255.255.0
#iface wlan0 inet manual
#wpa-roam /etc/wpa_supplicant/wpa_supplicant.conf
#iface default inet dhcp

allow-hotplug wwan0
iface wwan0 inet dhcp

auto eth1
iface eth1 inet static
    address 192.168.2.1
    netmask 255.255.255.0
    network 192.168.2.0
    broadcast 192.168.2.255
#    gateway 192.168.2.1

```

Εικόνα 3.2.3.3 network interfaces

Ύστερα μέσω της εντολής **ifconfig wlan0** μπορούμε πλέον να δούμε και το wlan0 που αφορά το wi-fi όπως φαίνεται και στην εικόνα που ακολουθεί :

```

root@RPi:~# ifconfig wlan0
wlan0      Link encap:Ethernet  HWaddr 80:1f:02:fd:9a:93
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1935940 errors:0 dropped:1689 overruns:0 frame:0
          TX packets:16760 errors:0 dropped:8 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2497545 (2.3 MiB)  TX bytes:13495290 (12.8 MiB)

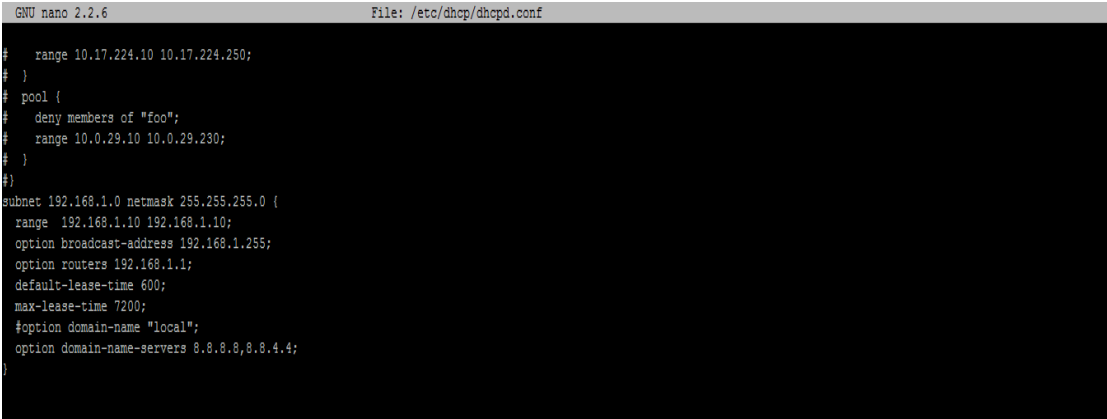
```

Εικόνα 3.2.3.4 ifconfig wlan0

Αφού έχουν επιτευχθεί όλα τα παραπάνω βήματα σειρά έχει η εγκατάσταση του dhcp(*Dynamic Host Configuration Protocol*) server. Το dhcp είναι μια υπηρεσία δικτύου που επιτρέπει να εκχωρηθούν αυτόματα οι ρυθμίσεις στους κεντρικούς υπολογιστές από έναν διακομιστή(server) και ουσιαστικά αποτελεί ένα μηχανισμό διαχείρισης πρωτοκόλλων TCP/IP. Οι υπολογιστές οι οποίοι έχουν ρυθμιστεί ώστε να είναι πελάτες dhcp δεν έχουν κανένα έλεγχο πάνω στις ρυθμίσεις που λαμβάνουν από το dhcp διακομιστή. Για την εγκατάσταση του dhcp server πληκτρολογούμε την εντολή :

- **sudo apt-get install isc-dhcp-server** στο τερματικό εντολών του raspberry pi.

Έπειτα στο αρχείο **/etc/default/isc-dhcp-server** γίνεται η τροποποίηση του πεδίου INTERFACES="" σε INTERFACES="wlan0" έτσι ώστε ο ασύρματος προσαρμογέας να αποτελεί την προεπιλογή για το αίτημα dhcp. Επιπλέον πραγματοποιήθηκε κατάλληλη τροποποίηση του αρχείου **/etc/dhcp/dhcpd.conf** στο οποίο προστέθηκαν τα δεδομένα που παρουσιάζονται στην παρακάτω εικόνα και αφορούν το δίκτυο και τους dns διακομιστές.



```
GNU nano 2.2.6 File: /etc/dhcp/dhcpd.conf
#       range 10.17.224.10 10.17.224.250;
#     }
# pool {
#   deny members of "foo";
#   range 10.0.29.10 10.0.29.230;
# }
#}
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.10 192.168.1.10;
  option broadcast-address 192.168.1.255;
  option routers 192.168.1.1;
  default-lease-time 600;
  max-lease-time 7200;
  #option domain-name "local";
  option domain-name-servers 8.8.8.8,8.8.4.4;
}
```

Εικόνα 3.2.3.5 Αρχείο /etc/dhcp/dhcpd.conf

Μετά την εκτέλεση όλων των παραπάνω βημάτων γίνεται η επανεκκίνηση του dhcp server μέσω της εντολής:

- **sudo service isc-dhcp-server restart.**

Πολλές φορές όμως ο δαίμονας `dhcpcd` ο οποίος αποτελεί ένα DHCP πελάτη (client) τρέχει πριν την εκτέλεση του αρχείου `/etc/network/interfaces`. Αυτό έχει ως αποτέλεσμα οι διεπαφές που έχουμε ορίσει να παίρνουν στατικές διευθύνσεις και συγκεκριμένα το `eth0` και το `eth1` να λαμβάνουν αρχικά δυναμικές διευθύνσεις στην εκκίνηση του `raspberrypi`. Για να διορθωθεί αυτό το πρόβλημα είναι απαραίτητη η μορφοποίηση του αρχείου `/etc/dhcpcd.conf` όπως φαίνεται στην εικόνα που ακολουθεί .

```
GNU nano 2.2.6 File: /etc/dhcpcd.conf
# on the server to actually work.
option rapid_commit

# A list of options to request from the DHCP server.
option domain_name_servers, domain_name, domain_search, host_name
option classless_static_routes
# Most distributions have NTP support.
option ntp_servers
# Respect the network MTU.
# Some interface drivers reset when changing the MTU so disabled by default.
#option interface_mtu

# A ServerID is required by RFC2131.
require dhcp_server_identifier

# Generate Stable Private IPv6 Addresses instead of hardware based ones
slaac private

# A hook script is provided to lookup the hostname if not set by the DHCP
# server, but it should not be run by default.
nohook lookup-hostname
# Custom static IP address for eth0.
interface eth0
static ip_address=147.102.7.0/24
static routers=147.102.7.60
static domain_name_servers=8.8.8.8

interface eth1
static ip_address=147.102.40.0/24
static routers=147.102.40.60
static domain_name_servers=8.8.8.8
```

Εικόνα 3.2.3.6 Αρχείο `/etc/dhcpcd.conf`

Το επόμενο βήμα προς την επίτευξη του στόχου είναι η εγκατάσταση του απαραίτητου λογισμικού στο `Raspberrypi` ώστε να λειτουργεί σαν `host access point (hostapd)`. Το `hostapd` στην ουσία αποτελεί έναν «δαίμονα (daemon)» ο οποίος είναι υπεύθυνος για τη μετατροπή μιας συσκευής `wi-fi` σε ένα σημείο πρόσβασης (access point). Μέσω της μετατροπής του `raspberrypi` σε ένα `access point` ο χρήστης μπορεί να επιτύχει ένα μεγάλος εύρος εφαρμογών. Μέσω των εντολών:

- **`sudo apt-get update`** με την οποία πραγματοποιείται η ενημέρωση της λίστας των πακέτων σχετικά με νέες εκδόσεις τους και
- **`sudo apt-get install hostapd`** είναι εφικτή η εγκατάσταση του `daemon`.

Για να δημιουργηθεί βέβαια το σημείο πρόσβασης (access point) μετά την εγκατάσταση του `hostapd` είναι απαραίτητη η διαμόρφωση του αρχείου

του **hostapd.conf**. Μέσω την εντολής **sudo nano /etc/hostapd/hostapd.conf** που μας επιτρέπει την εισαγωγή μας στο αρχείο ρυθμίσεων (configuration file) μπορεί να επιτευχθεί αυτό όπως φαίνεται στην παρακάτω εικόνα.

```
#created by ./install-rtl8188cus.sh
interface=wlan0
#bridge=br0
driver=rtl871xdrv
country_code=GR
ctrl_interface=wlan0
ctrl_interface_group=0
ssid=RPiAP
hw_mode=g
channel=1
wpa=3
wpa_passphrase=PASSWORD
wpa_key_mgmt=WPA-PSK
wpa_pairwise=TKIP
rsn_pairwise=CCMP
beacon_int=100
auth_algs=3
macaddr_acl=0
wmm_enabled=1
eap_reauth_period=360000000
```

Εικόνα 3.2.3.7 Αρχείο /etc/hostapd.hostapd.conf

Σύμφωνα με την παραπάνω εικόνα ως driver πρέπει να χρησιμοποιηθεί ο **rt1871xdrv**. Πριν την εγκατάσταση όμως του driver είναι απαραίτητη η εκτέλεση της εντολής **sudo apt-get install iw** . Το πακέτο **iw** μας δίνει την δυνατότητα να δούμε και να διαμορφώσουμε τις πληροφορίες σχετικά με την ασύρματη δικτύωση. Έπειτα πραγματοποιείται η εκτέλεση της εντολής **iw list** το αποτέλεσμα της οποίας είναι : **nl80211 not found** . Τα chips όπως το RT8188C και RT8192C αναγνωρίζονται ως RTL 8188CUS τα όποια όμως δεν υποστηρίζουν τον οδηγό nl80211 του hostapd έτσι προέκυψε το αποτέλεσμα της παραπάνω εντολής. Για την σωστή λειτουργία αυτού του τύπου chip είναι αναγκαία η εγκατάσταση του οδηγού **rt1871xdrv** . Για την λήψη του αρχικά εκτελείται η εντολή:

- **wget <https://dl.dropboxusercontent.com/u/1663660/scripts/install-rtl8188cus.sh>** , μέσω της οποίας πραγματοποιείται η λήψη ενός κώδικα που περιέχει ένα πρόγραμμα οδήγησης του πυρήνα και του

hostapd τον οδηγό δηλαδή rt1871xdrv που είναι απαραίτητος για αυτή την κατηγορία chip. Στην πορεία εκτελείται η εντολή :

- **sudo chown root:root install-rtl8188cus.sh** με την οποία είναι εφικτή η αλλαγή του ιδιοκτήτη του αρχείου και οι πληροφορίες της ομάδας ώστε να αναφέρονται στο root.

Τέλος πληκτρολογείται η εντολή:

- **sudo chmod 755 install-rtl8188cus.sh** για να αλλάξουν τα δικαιώματα πρόσβασης του αρχείου όπως η γραφή και η ανάγνωση και με την εντολή **sudo ./install-rtl8188cus.sh** είναι πλέον εφικτή η εκτέλεση του κώδικα και η εγκατάσταση του driver μέσω του οποίου θα πραγματοποιηθεί η wi-fi σύνδεση στο raspberry pi.

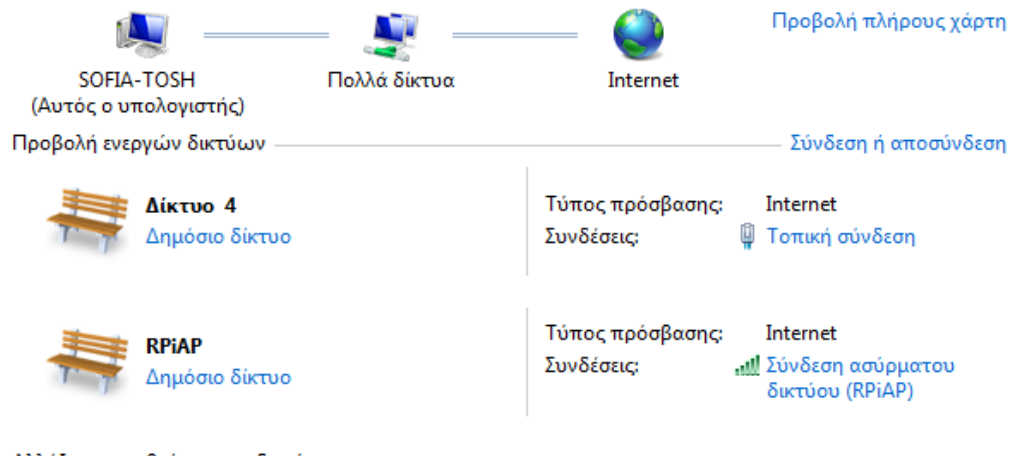
Αφού πραγματοποιηθούν τα παραπάνω βήματα για την εγκατάσταση του wi-fi adapter σειρά έχει η εκκίνηση του. Αρχικά πρέπει να εκκινήσει ο dhcp server μέσω της εντολής **service isc-dhcp-server start** και στη συνέχεια με την εντολή **/etc/init.d/hostapd start** συνδεόμαστε στο wi-fi. Όπως φαίνεται και στην εικόνα που ακολουθεί το interface wlan0 έχει λάβει πλέον την ip 192.168.1.1 .

```
wlan0    Link encap:Ethernet  HWaddr 80:1f:02:fd:9a:93
         inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
         UP BROADCAST MULTICAST  MTU:1500  Metric:1
         RX packets:0 errors:0 dropped:0 overruns:0 frame:0
         TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Εικόνα 3.2.3.8 wlan0 interface

Έαν λοιπόν συνδεθεί και ένας υπολογιστής στο raspberry pi θα μπορεί πλέον μέσω του wifi adapter να συνδέεται στο διαδίκτυο όπως φαίνεται και παρακάτω.

Προβολή των βασικών πληροφοριών δικτύου και ρύθμιση συνδέσεων



Εικόνα 3.2.3.9 Σύνδεση στο wi-fi μέσω του raspberry pi

4 ΛΟΓΙΣΜΙΚΟ

4.1 Quagga

Το Quagga αποτελεί ένα εξειδικευμένο λογισμικό δρομολόγησης ανοικτού κώδικα για λειτουργικά συστήματα τύπου UNIX. Περιλαμβάνει υλοποιήσεις διαφόρων δυναμικών πρωτοκόλλων (OSPF, RIP, BGP, IS-IS) καθώς και πολλές δυνατότητες στατικής και δυναμικής δρομολόγησης με περιβάλλον εντολών παρόμοιο με αυτό των δρομολογητών της εταιρίας Cisco. Το Quagga είναι εξέλιξη του παλαιότερου Zebra το οποίο έχει σταματήσει να εξελίσσεται από το 2005. Η αρχιτεκτονική του Quagga περιλαμβάνει τον πυρήνα (zebra daemon), όπου μεταφέρει τις εντολές από και προς το λειτουργικό σύστημα και τα διάφορα προγράμματα πελάτες που υλοποιούν τα πρωτόκολλα δρομολόγησης :

- OSPFd, Open Shortest Path First v2
- OSPF6d, Open Shortest Path First v3 για IPv6
- RIPd, Router Information Protocol v1 και v2
- RIPNGd, Router Information Protocol New Generation για IPv6
- BGPd, Border Gateway Protocol v4 (IPv4 και IPv6)
- ISISd, Intermediate System to Intermediate System
- BABELd, Babel Routing Protocol

Ένα σύστημα με εγκατεστημένο το Quagga λειτουργεί ως ένας δρομολογητής. Οπότε μέσω του Quagga μπορούν να πραγματοποιηθούν ανταλλαγές πληροφοριών δρομολόγησης με άλλους δρομολογητές με την εφαρμογή διαφόρων πρωτοκόλλων. Το Quagga χρησιμοποιεί αυτές τις πληροφορίες για την ενημέρωση του πίνακα δρομολόγησης του πυρήνα έτσι ώστε να είναι σωστή η ροή των δεδομένων. Επιπλέον το Quagga μπορεί να χρησιμοποιηθεί είτε για τη στατική δρομολόγηση μικρών δικτύων μέσω της χρήσης εύκολων εντολών , είτε για τη δυναμική δρομολόγηση δικτύων ευρύτερων περιοχών με την βοήθεια των πρωτοκόλλων που αναφέρθηκαν παραπάνω.

Για την εγκατάσταση του Quagga στο raspberry pi ακολουθήθηκαν τα παρακάτω βήματα :

- Αρχικά εγκαταστάθηκε το απαραίτητο λογισμικό με την εντολή :
apt-get install quagga quagga-doc.
- Στη συνέχεια τροποποιήθηκε το αρχείο με τους daemons των πρωτοκόλλων δρομολόγησης μέσω της εντολής:**nano /etc/quagga/daemons**.Γενικά ανάλογα με το πρωτόκολλο που χρησιμοποιείται σε κάθε περίπτωση τροποποιείται κατάλληλα το αρχείο θέτοντας yes ή no στο αντίστοιχο πρωτόκολλο. Στην παρούσα διπλωματική το αρχείο έλαβε την παρακάτω μορφή:

```
root@RPi:~# nano /etc/quagga/daemons
GNU nano 2.2.6 File: /etc/quagga/daemons
# The watchquagga daemon is always started. Per default in monitoring-only but
# that can be changed via /etc/quagga/debian.conf.
#
zebra=yes
bgpd=no
ospfd=no
ospf6d=no
ripd=no
ripngd=no
isisd=no
babeld=no
```

Εικόνα 4.1.1 Αρχείο με τους daemons

- Έπειτα δημιουργήθηκε ένα κενό αρχείο παραμετροποίησης για το Quagga μέσω της εντολής :
cp /usr/share/doc/quagga/examples/zebra.conf.sample /etc/quagga/zebra.conf . touch /etc/quagga/zebra.conf
- Στην πορεία πραγματοποιήθηκε μια αλλαγή της ταυτότητα του ιδιοκτήτη και της ομάδας του αρχείου με τις εντολές :
chown quagga:quaggavty /etc/quagga/*.conf
chmod 640 /etc/quagga/*.conf .
- Ύστερα από όλα τα παραπάνω βήματα ήταν εφικτή η εκκίνηση των daemons ως εξής : **/etc/init.d/quagga start .**
- Τέλος συνδέθηκε το Quagga μέσω της εντολής :**telnet localhost zebra .**

Το Quagga χρησιμοποιεί περιβάλλον γραμμής εντολών (CLI-Command Line Interface) μέσω του περιβάλλοντος **vtys** για την παραμετροποίηση του raspberry pi ως δρομολογητή. Το περιβάλλον διαχείρισης του δρομολογητή έχει τρία διακριτά επίπεδα με διαφορετικές δυνατότητες ως προς τον χρήστη. Στο πρώτο επίπεδο (**User EXEC mode**) ο χρήστης έχει τη δυνατότητα να εκτελέσει ένα υποσύνολο των διαθέσιμων εντολών της συσκευής και κυρίως εντολές εμφάνισης στατιστικών και πληροφορίες σχετικά με την έκδοση του λογισμικού. Στο δεύτερο επίπεδο (**Privileged EXEC mode**) ο χρήστης έχει πλήρη δικαιώματα στη συσκευή και μπορεί να εκτελέσει το σύνολο των εντολών. Στο τελευταίο επίπεδο (**Configuration mode**) ο χρήστης μπορεί να μεταβάλει την παραμετροποίηση του δρομολογητή. Οι μετατροπές μπορούν να γίνουν στα γενικά στοιχεία του δρομολογητή (**Global configuration mode**), στον τρόπο υλοποίησης των αλγορίθμων δρομολόγησης (**router configuration mode**) και στις διεπαφές δικτύου της συσκευής (**interface configuration mode**). Κανείς μπορεί εύκολα να καταλάβει σε τι επίπεδο βρίσκεται από την προτροπή (prompt) που εμφανίζεται στην γραμμή εντολών. Στο επίπεδο **User EXEC mode** εμφανίζεται η προτροπή : **routername >**, στο επίπεδο **Privileged EXEC mode** είναι : **routername#**, τέλος στο επίπεδο **Global configuration mode** παρουσιάζεται : **routername(config)#** ,στο **Interface configuration mode** : **routername(config-if)#** και στο **Router configuration mode** είναι : **routername(config-router)#**.

Έτσι λοιπόν σύμφωνα με τα παραπάνω γίνεται κατανοητή η σημασία του Quagga ως λογισμικό δρομολόγησης αλλά και το μεγάλο εύρος δυνατοτήτων που προσφέρει στον χρήστη για την υλοποίηση διαφόρων εφαρμογών. Στην παρούσα διπλωματική εργασία έγινε χρήση του Quagga έτσι ώστε μέσω αυτού να επιτευχθεί η επιτυχής δρομολόγηση στο ενσύρματο είτε στο ασύρματο 3G/4G δίκτυο. Για να πραγματοποιηθεί αυτό χρειάστηκε να εισαχθούμε στο τελευταίο επίπεδο του Quagga και συγκεκριμένα στο global configuration mode αφού μέσω αυτού μπορούν να υλοποιηθούν διάφορες αλλαγές στα στοιχεία του δρομολογητή. Κάθε επίπεδο όπως είναι λογικό έχει τις δικές του εντολές για τις διάφορες λειτουργίες που εκτελεί. Οπότε αρχικά μέσω της εντολής **configure terminal** εισερχόμαστε από το επίπεδο Privileged EXEC mode στο global configuration mode και έπειτα με τη χρήση

της εντολής **ip route** τροποποιήσαμε τη δρομολόγηση του raspberry pi. Οι εντολές αυτές εισήχθησαν σε ένα κώδικα (shell script) ο οποίος θα παρουσιαστεί σε επόμενο κεφάλαιο. Μέσω της χρήσης των εντολών του quagga μας δόθηκε να τροποποιήσουμε τη δρομολόγηση κατάλληλα όπως εμείς επιθυμούμε. Όπως φαίνεται και στις που ακολουθούν όταν εκτελείται ο κώδικας που δημιουργήσαμε ο πίνακας δρομολόγησης διαμορφώνεται κατάλληλα. Αρχικά χωρίς να συνδέσουμε το 3G dongle ο πίνακας δρομολόγησης είναι ο εξής, φυσικά έχουμε εισέλθει στο quagga με την εντολή **vttysh** και έχουμε πληκτρολογήσει **show ip route** :

```
show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, A - Babel,
       > - selected route, * - FIB route

K>* 0.0.0.0/0 via 147.102.7.200, eth0
C>* 127.0.0.0/8 is directly connected, lo
C>* 147.102.7.0/24 is directly connected, eth0
C>* 192.168.1.0/24 is directly connected, wlan0
```

Εικόνα 4.1.2 Πίνακας δρομολόγησης πριν την σύνδεση του 3G

Όπως φαίνεται και από την παραπάνω εικόνα η δρομολόγηση πραγματοποιείται μέσω του gateway της διεπαφής eth0 που είναι το 147.102.7.200. Στη συνέχεια παρουσιάζεται ο πίνακας δρομολόγησης έπειτα από την σύνδεση του 3G dongle.

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, A - Babel,
       > - selected route, * - FIB route

K>* 0.0.0.0/0 via 147.102.7.200, eth0
C>* 10.64.64.64/32 is directly connected, ppp0
C>* 127.0.0.0/8 is directly connected, lo
C>* 147.102.7.0/24 is directly connected, eth0
C>* 192.168.1.0/24 is directly connected, wlan0
```

Εικόνα 4.1.3 Πίνακας δρομολόγησης μετά την σύνδεση του 3G

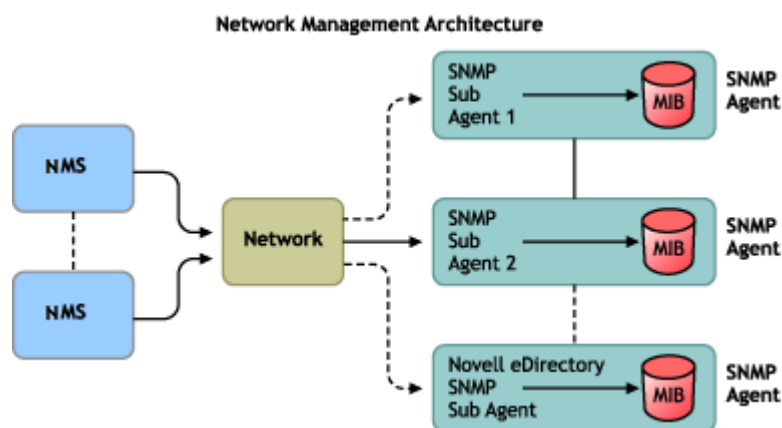
Σύμφωνα με την εικόνα που προηγείται η δρομολόγηση συνεχίζει να πραγματοποιείται μέσω του eth0 (φαίνεται από το K>*) διότι έτσι έχει οριστεί

στον κώδικα μας. Επιπλέον όμως βλέπουμε και την εγγραφή που αφορά το rrr0.

Γενικά το qmagga αποτελεί ένα πολύ εύχρηστο λογισμικό δρομολόγησης μέσω του οποίου μπορεί να επιτευχθεί ένα μεγάλο εύρος εφαρμογών στους δρομολογητές. Βελτιώνοντας έτσι την απόδοσή τους καλύπτονται ολοένα και περισσότερες ανάγκες των σύγχρονων χρηστών.

4.2 SNMP και Cacti στο Raspberry pi

Το Simple Network Management Protocol (SNMP) είναι μέρος της σουίτας πρωτοκόλλων Internet (IP - Internet Protocol), όπως έχει ορισθεί από το Internet Engineering Task Force (IETF). Χρησιμοποιείται στα συστήματα διαχείρισης δικτύων στη διαχείριση και παρακολούθηση δικτυακών συσκευών που απαιτούν παρέμβαση του διαχειριστή δικτύου. Αποτελείται από μια ομάδα προτύπων για τη διαχείριση δικτύου και περιλαμβάνει ένα πρωτόκολλο επιπέδου εφαρμογών (application layer), ένα σχήμα βάσης δεδομένων και μια ομάδα από σύνολα δεδομένων. Το SNMP συμπληρώνεται με τις προδιαγραφές για τη δομή της πληροφορίας διαχείρισης (Structure of Management Information – SMI) και με τη βάση πληροφορίας διαχείρισης (Management Information Base – MIB). Το SNMP βασίζεται στο μοντέλο διαχείρισης δικτύων που φαίνεται στην παρακάτω εικόνα :



Εικόνα 4.2.1 Μοντέλο διαχειριστή – αντιπροσώπου

Η αρχιτεκτονική του μοντέλου αυτού είναι η γνωστή αρχιτεκτονική πελάτη – εξυπηρετητή (client – server), που στην προκειμένη περίπτωση ονομάζεται αρχιτεκτονική διαχειριστή – αντιπροσώπου (manager – agent). Ο agent είναι μια οντότητα που εκτελείται σε κάθε έναν υπό διαχείριση κόμβο του δικτύου. Κάθε διαχειριζόμενος κόμβος πρέπει να εκτελεί τις παρακάτω λειτουργίες:

- Υλοποίηση στοίβας πρωτοκόλλων για την παροχή επικοινωνιακών υπηρεσιών (για παράδειγμα TCP/IP).

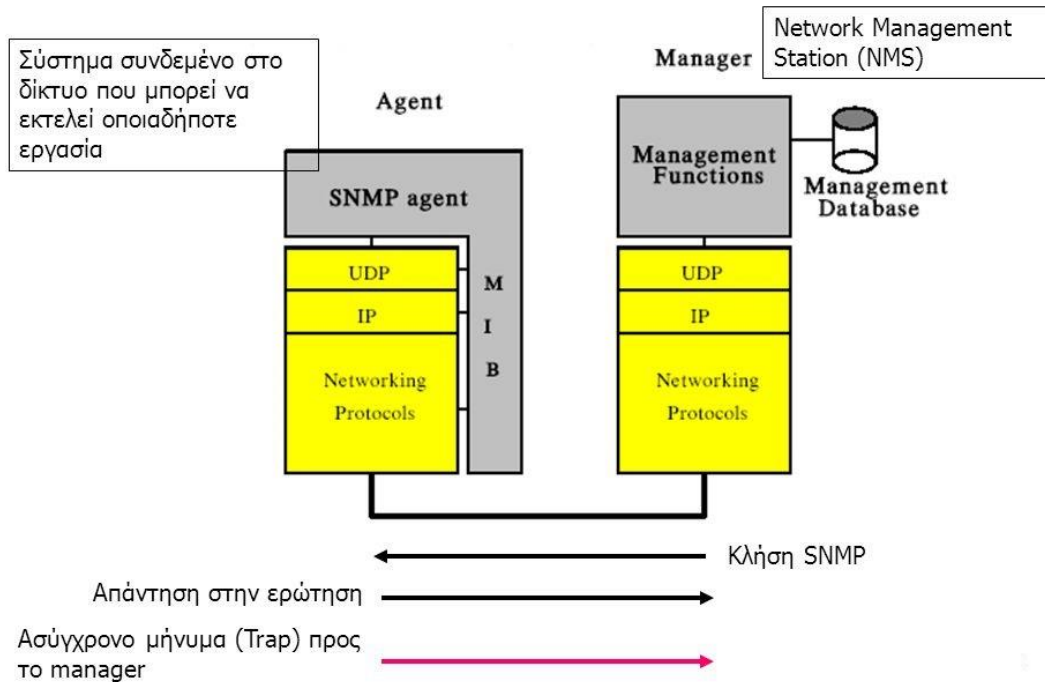
- Υλοποίηση κάποιου πρωτοκόλλου διαχείρισης δικτύων (για παράδειγμα SNMP).
- Υλοποίηση ενός σχήματος αλληλεπίδρασης μεταξύ των διαχειριζομένων αντικειμένων του κόμβου και του πρωτοκόλλου διαχείρισης.

Ο agent είναι ουσιαστικά ο συνδυασμός του σχήματος αλληλεπίδρασης, που αναφέρεται παραπάνω, και του πρωτοκόλλου διαχείρισης. Σκοπός του είναι η αλληλεπίδραση με διάφορες δομές δεδομένων του διαχειριζόμενου κόμβου, έχοντας τη δυνατότητα είτε να διαβάσει είτε να γράψει πληροφορία σε αυτές, και η επικοινωνία του, μέσω του πρωτοκόλλου διαχείρισης, με την οντότητα του manager.

Αυτές οι δομές δεδομένων αποτελούν ουσιαστικά την MIB του υπό διαχείριση κόμβου, η οποία αποτελείται από διαχειριζόμενα αντικείμενα (managed objects) οργανωμένα σε μία δενδρική και ιεραρχική δομή. Υπάρχουν τυποποιημένα διαχειριζόμενα αντικείμενα που πρέπει να περιλαμβάνει η MIB, αλλά υπάρχει η δυνατότητα να προστεθούν κι άλλα από τον εκάστοτε κατασκευαστή. Πρέπει να σημειωθεί εδώ ότι η MIB είναι ουσιαστικά ένα σύνολο δεικτών προς τα διαχειριζόμενα αντικείμενα. Το πως αυτά αποθηκεύονται στον κόμβο είναι επίσης θέμα του κατασκευαστή.

Το πρωτόκολλο SNMP ακολουθεί το διαχειριστικό μοντέλο που παρουσιάστηκε στην προηγούμενη παράγραφο. Στην εικόνα που ακολουθεί φαίνεται καλύτερα το μοντέλο του SNMP.

ΜΟΝΤΕΛΛΟ ΔΙΑΧΕΙΡΙΣΗΣ SNMP



Εικόνα 4.2.2 Μοντέλο διαχείρισης SNMP

Στη διαχείριση με το SNMP το NMS ζητάει από τον agent του διαχειριζόμενου κόμβου τις απαραίτητες πληροφορίες από τη MIB του ή αλλάζει κάποιες από αυτές τις πληροφορίες. Ακολουθείται λοιπόν ένα rolling – based μοντέλο διαχείρισης. Η μόνη περίπτωση που ο agent μπορεί να στείλει πληροφορία στο NMS με δική του πρωτοβουλία είναι τα μηνύματα TRAPs. Αυτά είναι αυτόκλητα μηνύματα που συνήθως αναφέρονται σε συγκεκριμένα γεγονότα που συμβαίνουν στον agent, για παράδειγμα reset του αντίστοιχου διαχειριζόμενου κόμβου.

Οι πληροφορίες που αντλεί ο agent από τη MIB του διαχειριζόμενου κόμβου παριστάνονται σύμφωνα με το συντακτικό ASN.1 (Abstract Syntax Notation 1), που προσφέρει τη δυνατότητα κωδικοποίησης κάθε είδους πληροφορίας μεταξύ των οντοτήτων που θέλουν να επικοινωνήσουν. Συγκεκριμένα προσφέρει τη δυνατότητα ορισμού αφηρημένων δομών καθώς και κάποιους βασικούς τύπους, χωρίς να υπάρχουν περιορισμοί στην

πολυπλοκότητα των δομών που μπορούν να οριστούν. Για τη μεταφορά αυτών των δομών μέσα από το δίκτυο χρησιμοποιούνται οι BER (Basic Encoding Rules), βάσει των οποίων γίνεται η κωδικοποίηση. Έτσι, οι διάφορες δομές πληροφοριών κωδικοποιούνται σε πλαίσια συγκεκριμένης μορφής και μεταφέρονται στο δίκτυο.

Τρία είναι τα μηνύματα που μπορεί να στείλει το NMS σε έναν SNMP agent. Αυτά είναι τα εξής:

- **Get – Request:** Με το μήνυμα αυτό ζητείται η τιμή ενός συγκεκριμένου διαχειριζόμενου αντικειμένου από τη MIB του agent.
- **Get – Next – Request:** Με αυτό το μήνυμα ζητείται η τιμή του αμέσως επόμενου αντικειμένου στην δομή της MIB.
- **Set – Request:** Με το μήνυμα αυτό το NMS μπορεί να ζητήσει από τον agent να μεταβάλει την τιμή ενός συγκεκριμένου στιγμιότυπου ενός αντικειμένου.

Ο agent απαντάει στις αιτήσεις του NMS με το μήνυμα Get – Response, επιστρέφοντας κάποιο αντικείμενο της MIB που του είχε ζητηθεί. Επιπλέον υπάρχει και ένας μικρός αριθμός TRAPs, που μπορεί να στείλει αυτόκλητα ο agent στο NMS. Αυτά είναι τα coldStart και warmStart για τις αρχικοποιήσεις του agent, linkDown και linkUp για τις μεταβολές στα interfaces του agent, authenticationFailure για τις χωρίς δικαίωμα προσπάθειες πρόσβασης στον agent, egrNeighborLoss για τη παύση λειτουργίας ενός EGP gateway γειτονικού και enterpriseSpecific για τον ορισμό TRAP από κάθε κατασκευαστή.

Είναι προφανής η προσπάθεια να διατηρηθεί η λειτουργία του SNMP όσο το δυνατόν απλούστερη. Παρόλα αυτά με τα παραπάνω μηνύματα μπορεί να υλοποιηθεί οποιαδήποτε εφαρμογή διαχείρισης. Ενώ το NMS φαινομενικά δεν μπορεί να μεταφέρει κάποια εντολή στον agent, αυτό μπορεί να γίνει ουσιαστικά με την αλλαγή της τιμής του κατάλληλου αντικειμένου της MIB.

Τα μηνύματα που ανταλλάσσονται κατά τη λειτουργία του SNMP αποτελούνται από ένα αναγνωριστικό της έκδοσης (version) του πρωτοκόλλου, ένα όνομα κοινότητας (community name) του SNMP και ένα PDU που περιέχει το SNMP μήνυμα ή το TRAP. Το SNMP χρησιμοποιεί, όντας ασύγχρονο, το πρωτόκολλο UDP. Η επιλογή αυτή είναι λογική εφόσον ο NMS δεν χρειάζεται να περιμένει απάντηση σε μία αίτησή του προς τον agent, αλλά μπορεί να συνεχίσει να στέλνει κι άλλες αιτήσεις. Επιπλέον, η εγκατάσταση σύνδεσης και η διαδικασία επιβεβαιώσεων του TCP θα επιβάρυνε ιδιαίτερα το διαχειριζόμενο δίκτυο, ενώ η απώλεια ενός πακέτου δεν είναι τόσο σημαντική ώστε να δικαιολογεί το επιπλέον φορτίο. Φυσικά αυτό δεν σημαίνει ότι το SNMP δεν μπορεί να χρησιμοποιήσει το TCP ή και άλλα πρωτόκολλα μεταφοράς (του OSI για παράδειγμα), ενώ μπορεί να υλοποιηθεί και κατευθείαν πάνω στο 802.3, με περιορισμένη χρησιμότητα βέβαια εντός του τοπικού δικτύου.

Όπως γίνεται κατανοητό σύμφωνα με όλα τα παραπάνω το SNMP χρησιμοποιείται για τη συλλογή δεδομένων σχετικά με το τι συμβαίνει στο εσωτερικό μιας συσκευής όπως για παράδειγμα το φορτίο της ,τις δηλώσεις του σκληρού δίσκου αλλά και το εύρος ζώνης. Έπειτα όλα αυτά τα δεδομένα χρησιμοποιούνται από εργαλεία παρακολούθησης του δικτύου όπως είναι το cacti έτσι ώστε να δημιουργηθούν γραφήματα που αφορούν την κίνηση του δικτύου. Στην παρούσα διπλωματική πραγματοποιήθηκε η εγκατάσταση του cacti που παρακολουθεί και καταγράφει τα δεδομένα με τη μορφή γραφικών παραστάσεων. Για να επιτευχθεί βέβαια αυτό είναι απαραίτητη αρχικά η εγκατάσταση του πρωτοκόλλου SNMP που παρουσιάστηκε παραπάνω. Έτσι λοιπόν για να υλοποιηθεί η εγκατάσταση του ακολουθήθηκαν τα παρακάτω βήματα :

- Πληκτρολογούμε **sudo apt-get install snmpd** έτσι ώστε να εγκαταστήσουμε το SNMP.
- Στη συνέχεια είναι απαραίτητη η διαμόρφωση του αρχείου snmpd.conf ,μέσω της εντολής **nano /etc/snmp/snmpd.conf** ανοίγουμε το αρχείο και το διαμορφώνουμε κατάλληλα. Το τμήμα του αρχείου που έχει τροποποιηθεί φαίνεται στην εικόνα που ακολουθεί.

```

# ACCESS CONTROL
#
# system + hrSystem groups only
view systemonly included .1.3.6.1.2.1.1
view systemonly included .1.3.6.1.2.1.25.1

# Full access from the local host
rocommunity public localhost
# Default access to basic system info
rocommunity public default -V systemonly
# rocommunity public CN-n7ua-pi -V systemonly

rocommunity n7ua-cN-pi
sysLocation CN Lab
sysContact Paris <pchara@cn.ntua.gr>
sysServices 72
querySecName spud

# Full access from an example network
# Adjust this network address to match your local
# settings, change the community string,
# and check the 'agentAddress' setting above
rocommunity secret 10.0.0.0/16

# Full read-only access for SNMPv3
rocommunity authOnlyUser

# Full write access for encrypted requests
# Remember to activate the 'createUser' lines above
rwcommunity authPrivUser priv

```

Εικόνα 4.2.3 Αρχείο snmpd.conf

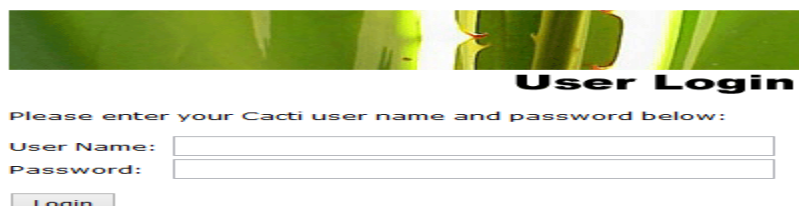
Το snmpd υποστηρίζει το View-Based Access Control Model (VACM) όπως ορίζεται στο RFC 2575 έτσι ώστε να ελέγχει ποιος μπορεί να ανακτήσει ή να ενημερώσει πληροφορίες. Για το σκοπό αυτό χρησιμοποιεί διάφορα μέσα που σχετίζονται με τον έλεγχο πρόσβασης. Κάτι τέτοιο επιτυγχάνεται με την χρήση των directives rocommunity/rwcommunity. Η σύνταξη τους είναι **rocommunity COMMUNITY [SOURCE [OID | -V VIEW [CONTEXT]]]**. Μέσω αυτών καθορίζεται μια SNMP κοινότητα στην οποία θα επιτρέπεται μόνο ανάγνωση (read-only, GET και GETNEXT) ή μόνο εγγραφή αντίστοιχα (write only, GET, GETNEXT και SET). Από προεπιλογή αυτή θα παρέχει πρόσβαση στο πλήρες δέντρο OID για τέτοια αιτήματα ανεξάρτητα από το που προήρθαν. Το διακριτικό SOURCE χρησιμοποιείται ώστε να περιορίσει την πρόσβαση σε αιτήσεις πέρα των προκαθορισμένων από το σύστημα. Τέλος το πεδίο OID περιορίζει την πρόσβαση για την εν λόγω κοινότητα στο υπόδεντρο του δεδομένου OID.

Στη συνέχεια πρέπει να διαμορφωθεί κατάλληλα το **system group**, στο οποίο αναφέρουμε το **sysLocation** που στην περίπτωση μας είναι το CN Lab, το **sysContact**, το **sysServices** δίπλα στο οποίο αναφέρεται ένας αριθμός που αφορά τη τιμή του αντικειμένου δηλαδή **sysServices.0**. Για

συστήματα υποδοχής (host systems) εισάγεται η τιμή 72 όπως φαίνεται και στην παραπάνω εικόνα. Οι ρυθμίσεις που προαναφέρθηκαν αφορούν το access control και το system information του αρχείου snmpd. Αφού πραγματοποιηθούν όλες οι προηγούμενες τροποποιήσεις εκτελούμε την εντολή **service snmpd restart** έτσι ώστε να αποθηκευτούν όλες οι αλλαγές στο σύστημα.

Έπειτα σειρά έχει η εγκατάσταση και διαμόρφωση του cacti το οποίο όπως έχει προαναφερθεί αποτελεί ένα λογισμικό ανοιχτού κώδικα παρέχοντας στο χρήστη ένα μεγάλο πλήθος γραφημάτων παρακολούθησης της συσκευής που αφορούν το εύρος ζώνης, τη χρήση του σκληρού δίσκου, τη χρήση της κεντρικής μονάδας επεξεργασίας (CPU), διάφορα στατιστικά της RAM και πολλά άλλα. Επιπλέον ο κάθε χρήστης μπορεί να δημιουργήσει τα δικά του γραφήματα ανάλογα με τις ανάγκες του, κάτι τέτοιο φυσικά είναι υλοποιήσιμο λόγω του ότι το cacti όπως αναφέρθηκε πρωτίτερα είναι λογισμικό ανοιχτού κώδικα.

Για την εγκατάσταση του αρχικά πληκτρολογείται η εντολή **apt-get install cacti** μέσω της οποίας εγκαθίσταται το απαραίτητο λογισμικό και στη συνέχεια επιλέγεται ο διακομιστής (server) που θα χρησιμοποιηθεί. Στην παρούσα διπλωματική ο server είναι ένα μηχάνημα ubuntu 12.04 LTS και το όνομα του είναι voip επιπλέον έχει ip διεύθυνση 147.102.7.6. Για να εισαχθούμε στο cacti πληκτρολογούμε τη διεύθυνση <http://voip.telecom.ntua.gr/cacti> και εμφανίζεται η παρακάτω εικόνα στην οποία εισάγουμε το username και το password που έχουμε επιλέξει.



User Login

Please enter your Cacti user name and password below:

User Name:

Password:

Εικόνα 4.2.4 Είσοδος του χρήστη στο cacti

Στη συνέχεια αφού έχουμε δικαιώματα διαχειριστή(admin) μπορούμε να προσθέσουμε την συσκευή (device) που επιθυμούμε. Αρχικά πατάμε πάνω στο console και στην συνέχεια στο devices.Στην παρακάτω εικόνα φαίνεται ότι έχει προστεθεί το raspberry pi με την ονομασία pi-cosmo.

Description**	ID	Graphs	Data Sources	Status	In State	Hostname	Current (ms)	Average (ms)	Availability
alderaan.cn.ntua.gr	10	2	2	Up	-	alderaan.cn.ntua.gr	1.03	2.16	99.86
atlas.telecom.ntua.gr	36	44	44	Up	-	atlas.telecom.ntua.gr	45.72	42.26	99.99
ats-net.telecom.ntua.gr	22	3	9	Up	-	147.102.7.245	91.44	63.02	98.43
ats-srv.telecom.ntua.gr	23	3	8	Up	-	147.102.7.243	94.89	64.21	98.59
bellerefon.cn.ntua.gr	14	6	8	Up	-	147.102.40.29	0.45	1.05	99.92
callisto.telecom.ntua.gr	37	29	29	Up	-	147.102.7.207	48.99	34.42	99.98
dagobah.cn.ntua.gr	9	2	2	Up	-	dagobah.cn.ntua.gr	0.75	1.22	99.93
dell-ups.cn.ntua.gr	30	7	10	Up	-	147.102.40.242	0.82	1.02	99.97
dragon.cn.ntua.gr	39	68	68	Up	-	dragon.cn.ntua.gr	55.25	39.66	99.96
hoth.cn.ntua.gr	19	28	29	Up	-	hoth.cn.ece.ntua.gr	1.8	2.21	99.95
iraklis.cn.ntua.gr	8	8	8	Down	82d 10h 12m	iraklis.cn.ece.ntua.gr	27.57	2.34	70.28
iraklis.telecom.ntua.gr	34	44	44	Up	-	iraklis.telecom.ntua.gr	0.45	0.77	99.97
localhost	1	4	5	Up	-	127.0.0.1	0.04	0.03	100
mustafar.cn.ntua.gr	20	28	29	Up	-	147.102.40.223	1.8	2.32	99.96
naboo.cn.ntua.gr	15	29	32	Up	-	naboo.cn.ntua.gr	2.71	1.22	99.97
Netbotz	2	6	6	Up	-	147.102.40.247	3.97	5.21	99.78
pi-cosmo	38	8	8	Up	-	147.102.7.60	53.97	57.08	81.39

Εικόνα 4.2.5 Προσθήκη της συσκευής pi-cosmo

Έπειτα σειρά έχει η τοποθέτηση των παραμέτρων που αφορούν την συσκευή όπως φαίνεται στην εικόνα που ακολουθεί.

pi-cosmo (147.102.7.60)

SNMP Information
 System: Linux 3.13.0+ ARMv7l GNU/Linux 3.13.0+ ARMv7l
 Uptime: 6209776 (0 days, 17 hours, 13 minutes)
 Hostname: RPi
 Location: Sitting on the Dock of the Bay
 Contact: Me me@example.org

Devices [edit: pi-cosmo]

General Host Options

Description
Give this host a meaningful description.

Hostname
Fully qualified hostname or IP address for this device.

Host Template
Choose the Host Template to use to define the default Graph Templates and Data Queries associated with this Host.

Number of Collection Threads
The number of concurrent threads to use for polling this device. This applies to the Spine poller only.

Disable Host
Check this box to disable all checks for this host.

Availability/Reachability Options

Downed Device Detection
The method Cacti will use to determine if a host is available for polling. NOTE: It is recommended that, at a minimum, SNMP always be selected.

Ping Timeout Value
The timeout value to use for host ICMP and UDP ping. This host SNMP timeout value applies for SNMP pings.

Ping Retry Count
After an initial failure, the number of ping retries Cacti will attempt before failing.

SNMP Options

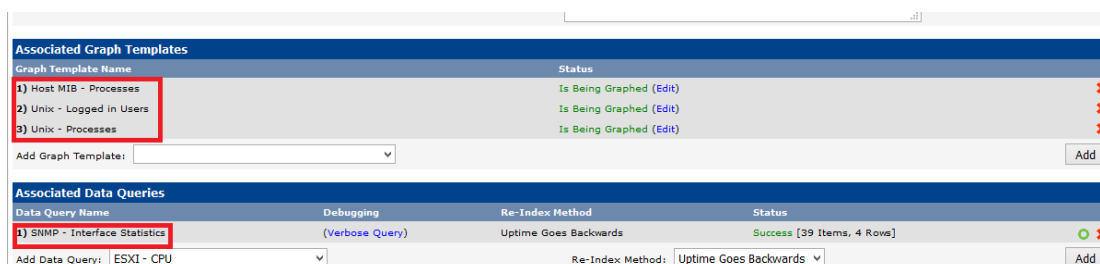
SNMP Version
Choose the SNMP version for this device.

SNMP Community
SNMP read community for this device.

SNMP Port
Enter the UDP port number to use for SNMP (default is 161).

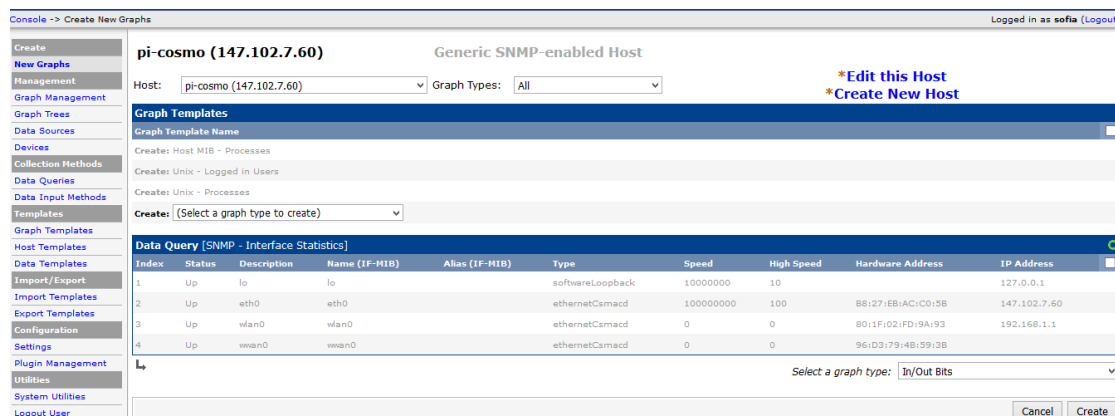
Εικόνα 4.2.6 Παράμετροι pi-cosmo

Στην παραπάνω εικόνα μέσα στο κόκκινο πλαίσιο απεικονίζονται οι αλλαγές που πραγματοποιήθηκαν για την συσκευή μας. Επόμενο βήμα αποτελεί η προσθήκη των γραφημάτων που επιθυμούμε να παρουσιάζονται στο cacti και αυτό το βήμα φαίνεται αναλυτικά στην παρακάτω εικόνα .



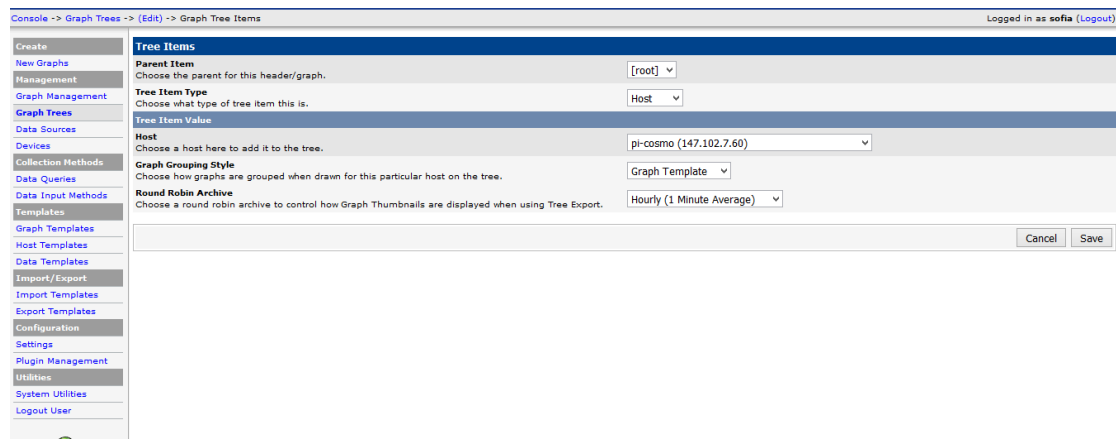
Εικόνα 4.2.7 Προσθήκη γραφημάτων στο ri-cosmo

Όπως φαίνεται παραπάνω έχουν προστεθεί να δημιουργούνται τρία γραφήματα καθώς και ο τύπος των δεδομένων που θα συλλέγονται. Έπειτα επιλέγοντας το **create graphs for this host** εισάγουμε τις διεπαφές(interfaces) του raspberry pi όπως φαίνεται στην εικόνα που ακολουθεί.



Εικόνα 4.2.8 Εισαγωγή διεπαφών στο ri-cosmo

Τέλος προσθέτουμε graph trees όπως παρουσιάζεται παρακάτω και στο cacti. Ύστερα από όλες αυτές τις ρυθμίσεις μπορεί και δημιουργεί όλα τα γραφήματα για το ίδιο το raspberry pi αλλά και τις διεπαφές του.



Εικόνα 4.2.9 Προσθήκη graph trees

Έπειτα από όλες αυτά τα βήματα που προηγήθηκαν στο cacti και αφορούσαν την παραμετροποίηση του μπορούν πλέον να πραγματοποιηθούν καταγραφές για όλες τις διεπαφές όπως παρουσιάζονται και στις εικόνες που ακολουθούν.

Το πρώτο γράφημα αφορά τις διαδικασίες που αφορούν το raspberry pi. Γενικά όλα τα γραφήματα παρουσιάζονται για ημερήσια βάση, εβδομαδιαία, μηνιαία αλλά και όλου του χρόνου.



Εικόνα 4.2.10 Γραφήματα διαδικασιών του raspberry-pi

Συνέχεια έχουν τα γραφήματα που αφορούν την κίνηση στη διεπαφή eth0 της σύνδεσης Ethernet.



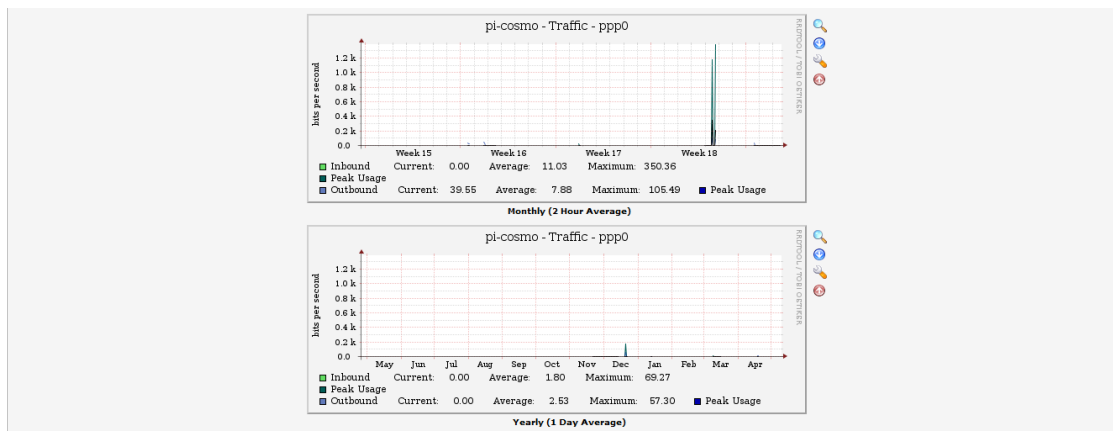
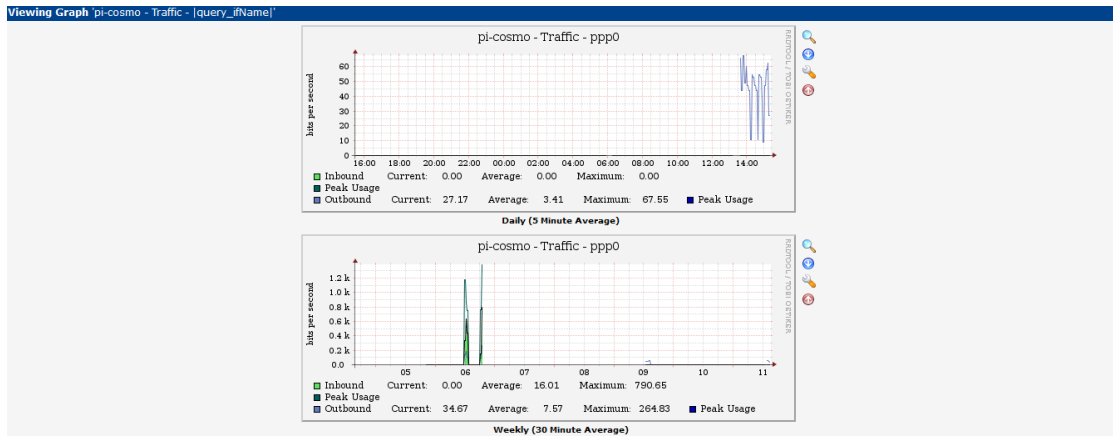
Εικόνα 4.2.11 Γραφήματα της κίνησης της διεπαφής eth0

Έπειτα ακολουθούν οι εικόνες για τη διεπαφή Io. Ουσιαστικά το Io(Ioorbak) αποτελεί διεύθυνση ειδικού σκοπού που προορίζεται για χρήση σε κάθε υπολογιστή. Το λογισμικό δικτύου και τα βοηθητικά προγράμματα μπορούν να χρησιμοποιήσουν την ip διεύθυνση 127.0.0.1 για να αποκτήσουν πρόσβαση σε πόρους του TCP/IP δικτύου του τοπικού υπολογιστή. Τα μηνύματα που αποστέλλονται στην 127.0.0.1 δεν φθάνουν έξω από το τοπικό δίκτυο (LAN), αλλά, αντίθετα δρομολογούνται αυτόματα από τον προσαρμογέα δικτύου του υπολογιστή πίσω στο άκρο λήψης του TCP/IP stack.



Εικόνα 4.2.12 Γραφήματα της κίνησης της διεπαφής lo

Ύστερα σειρά έχουν οι διεπαφές rrr0 και wwan0. Με τη διεπαφή wwan0 γνωρίζουμε ότι λειτουργεί το modeswitch σωστά, δηλαδή ότι το usb 3G dongle αναγνωρίζεται ως modem πλέον από το raspberry pi και όχι ως συσκευή usb. Μόνο όμως η διεπαφή rrr0 είναι αυτή που επιτρέπει τη σύνδεση του 3G dongle με το internet και μέσω αυτής διέρχονται τα πακέτα της σύνδεσης.



Εικόνα 4.2.13 Γραφήματα της κίνησης της διεπαφής ppp0



Εικόνα 4.2.14 Γραφήματα της κίνησης της διεπαφής wwan0

Τέλος στην εικόνα που ακολουθεί φαίνεται και η επαφή wlan0 που αφορά την ασύρματη (wi-fi) σύνδεση του raspberry pi.



Εικόνα 4.2.15 Γραφήματα της κίνησης της διεπαφής wlan0

5 Δρομολόγηση

5.1 Μετάβαση στο 3G δίκτυο σε περίπτωση απώλειας της ζεύξης

Στα προηγούμενα κεφάλαια της παρούσας διπλωματικής εργασίας αναλύθηκαν τόσο τα χαρακτηριστικά του 3g dongle και του ethernet όσο και η διαδικασία που ακολουθήθηκε για την σύνδεση τους στο raspberry pi. Έχοντας λοιπόν συνδεδεμένα το 3g dongle και το ethernet στις διεπαφές (interfaces) `ppp0` και `eth0` αντίστοιχα υλοποιήσαμε την εξής λειτουργία :όταν είναι συνδεδεμένα και τα δύο και λειτουργούν χωρίς προβλήματα όλη η κίνηση του δικτύου μας διέρχεται από την διεπαφή `eth0`,σε περίπτωση όμως απώλειας της ethernet συνδέσεως όλη η κίνηση του δικτύου θα διέρχεται πλέον από την διεπαφή `ppp0` που είναι του 3g dongle. Αυτό βέβαια λειτουργεί και αντίστροφα δηλαδή σε περίπτωση απώλειας της 3g συνδέσεως όλη η κίνηση διέρχεται από την διεπαφή `eth0` κάτι βέβαια που ισχύει ούτως ή άλλως. Έτσι με αυτό τον τρόπο καταφέραμε να υλοποιήσουμε ένα backup δηλαδή μια εφεδρική διαδρομή σε περίπτωση απώλειας της μιας από τις δύο συνδέσεις, παρέχοντας έτσι στο raspberry pi την δυνατότητα να λειτουργεί ως ένας οικιακός δρομολογητής ο οποίος θα παρέχει στο χρήστη συνεχή σύνδεση στο διαδίκτυο ακόμα και όταν θα συμβεί κάποιο σφάλμα σε μία από τις δύο συνδέσεις. Παρακάτω παρουσιάζεται ο κώδικας που δημιουργήσαμε έτσι ώστε να επιτευχθεί η παραπάνω λειτουργία. Ο κώδικας βρίσκεται στο αρχείο `fallback.sh` και στο φάκελο `root`.

fallback.sh

```
#!/bin/bash

intef=1

ping -c 1 -I eth0 147.102.7.200 > /dev/null

check_one=$?

if [[ $check_one -eq 0 ]]
then
    status1=1
else
    status1=0
fi

ping -c 1 -I ppp0 147.102.40.13 > /dev/null

check_two=$?

if [[ $check_two -eq 0 ]]
then
    status2=1
else
    status2=0
fi

while [ $intef -le 5 ]
do

Logfile="results.txt"
eth0=1
ppp0=1

ping -c 1 -I eth0 147.102.7.200 > /dev/null

check_one=$?
```

```

ping -c 1 -I ppp0 147.102.40.13 > /dev/null

check_two=$?

if [[ $check_one -eq 0 ]]
then
    eth0=1
    echo "eth0 is up and routing exists" >> $Logfile
    if [[ $status1 -eq 0 ]]
    then
        vtysh -c "show run" -c "conf t" -c "no ip route 0.0.0.0/0
10.64.64.64" -c "ip route 0.0.0.0/0 147.102.7.200 " -c "end"
-c "show run"
    fi
else
    eth0=0
    echo "Eth0 is down" >> $Logfile
fi

if [[ $check_two -eq 0 ]]
then
    ppp0=1
    echo "Ppp0 is up and routing exists" >> $Logfile
else
    ppp0=0
    echo "Ppp0 is down." >> $Logfile
fi

if [[ $eth0 -eq 0 ]] && [[ $ppp0 -eq 1 ]]
then
    if [[ $status1=1 ]] && [[ $status2=0 ]]
    then
        echo "eth0 is down routing via ppp0" >> $Logfile
        vtysh -c "show run" -c "conf t" -c "no ip route 0.0.0.0/0
147.102.7.200" -c "ip route 0.0.0.0/0 10.64.64.64" -c "end" -c
"show run"
    else

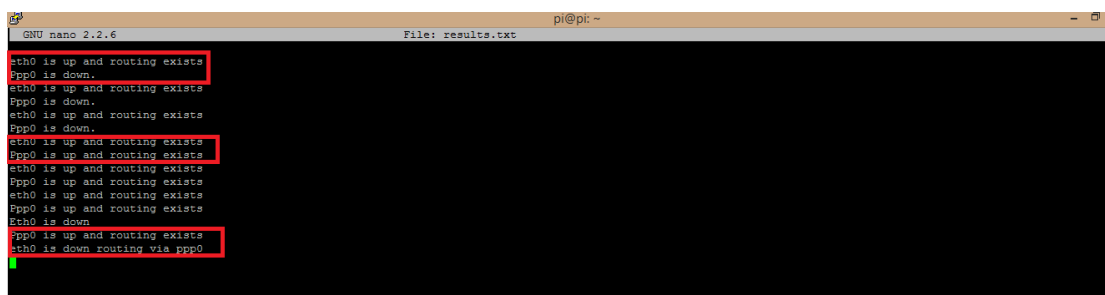
```

```
    echo "not doing anything" >> $Logfile
fi
fi

sleep 10
status1=eth0
status2=ppp0

done
```

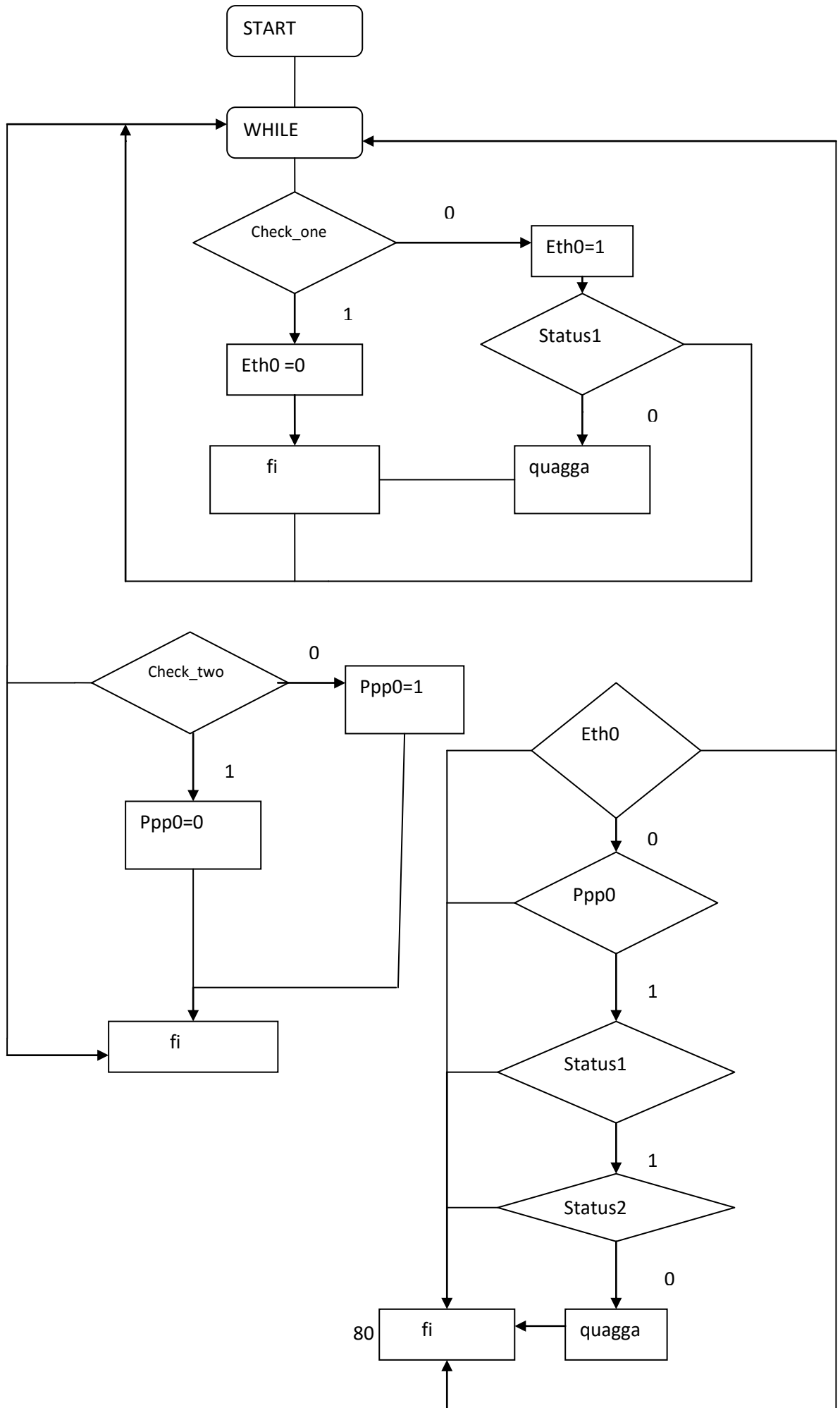
Όπως προαναφέρθηκε και παραπάνω ο κώδικας υλοποιεί το επιθυμητό fallback μεταξύ των δύο διεπαφών eth0 και ppp0. Η λογική του κώδικα είναι η εξής αρχικά εκτελείται η εντολή ping ώστε να ελέγξει αν οι δύο διεπαφές είναι ενεργές και στην συνέχεια αποθηκεύονται σε δύο μεταβλητές status1 και status2 οι τιμές 1 σε περίπτωση που είναι ενεργές και 0 όταν δεν λειτουργούν. Έπειτα πραγματοποιείται η είσοδος σε ένα βρόχο επανάληψης στον οποίο ελέγχεται ξανά μέσω ping η κατάσταση των δυο διεπαφών και αν η διεπαφή eth0 προηγουμένως ήταν μη ενεργή και η δρομολόγηση πραγματοποιούνταν μέσω του ppp0 και πλέον είναι ενεργή τότε η δρομολόγηση αλλάζει και πραγματοποιείται πλέον από το eth0. Αντίθετα εάν η διεπαφή eth0 ήταν πριν ενεργή και η δρομολόγηση υλοποιούνταν μέσω του eth0 και πλέον η διεπαφή eth0 δεν λειτουργεί τότε η δρομολόγηση θα γίνεται μέσω του ppp0. Όλα τα μηνύματα που εμφανίζει ο κώδικας αποθηκεύονται στο αρχείο results.txt το οποίο φαίνεται στην παρακάτω εικόνα όπου εμφανίζονται και οι τρεις περιπτώσεις. Δηλαδή η περίπτωση να λειτουργούν και οι δυο διεπαφες το eth0 και το ppp0 ,η περίπτωση να λειτουργεί μόνο η διεπαφή eth0 και όχι η ppp0 και τέλος όταν λειτουργεί η ppp0 και όχι η eth0. Φυσικά οι αλλαγές στη δρομολόγηση πραγματοποιούνται μέσω του quagga το οποίο αναλύθηκε σε προηγούμενο κεφάλαιο.



```
GNU nano 2.2.6 File: results.txt pi@pi: ~
eth0 is up and routing exists
ppp0 is down.
eth0 is up and routing exists
ppp0 is down.
eth0 is up and routing exists
ppp0 is down.
eth0 is up and routing exists
ppp0 is up and routing exists
eth0 is up and routing exists
ppp0 is up and routing exists
eth0 is up and routing exists
ppp0 is up and routing exists
eth0 is down
ppp0 is up and routing exists
eth0 is down routing via ppp0
```

Εικόνα 5.1.1 Αρχείο results.txt

Παρακάτω παρουσιάζεται και ένα λογικό διάγραμμα του κώδικα.



5.2 Πολιτική δρομολόγησης

Στη σημερινή εποχή όπου η χρήση του διαδικτύου αποτελεί αναπόσπαστο κομμάτι της καθημερινής ζωής και οι επιδόσεις των δικτύων είναι υψηλές καθίσταται επιτακτική η ελευθερία όσο αναφορά την προώθηση και την χρήση των πακέτων σύμφωνα με τις ανάγκες του χρήστη πέρα από τις παραδοσιακές πολιτικές δρομολόγησης. Με την χρήση της πολιτικής δρομολόγησης (Policy-based routing) ο χρήστης μπορεί να εφαρμόσει πολιτικές για να επιτύχει τους στόχους του. Τα οφέλη λοιπόν που προσφέρει η πολιτική δρομολόγησης είναι πολλά, τέσσερα όμως είναι τα πιο βασικά :

- Αρχικά πολλοί πάροχοι και οργανισμοί μπορούν να δρομολογήσουν την δικτυακή κίνηση που προέρχεται από διαφορετικές ομάδες χρηστών σε διαφορετικές συνδέσεις στο διαδίκτυο μέσω των δρομολογητών που έχουν προγραμματιστεί ώστε να ακολουθούν πολιτικές δρομολόγησης.
- Επιπλέον οι οργανισμοί μπορούν να παρέχουν QOS(Quality Of Service) σε διαφοροποιημένες δικτυακές κυκλοφορίες τοποθετώντας τον τύπο της υπηρεσίας (TOS) στις επικεφαλίδες των ip πακέτων και χρησιμοποιώντας μηχανισμούς κινητοποίησης ουρών έτσι ώστε να δίνουν προτεραιότητα στην κυκλοφορία του πυρήνα ή του κορμού του δικτύου αντίστοιχα.
- Ακόμη επιτυγχάνεται εξοικονόμηση κόστους μέσω της διανομής της κυκλοφορίας μεταξύ του χαμηλού εύρους και του χαμηλού κόστους μονοπατιών και αντίστοιχα του υψηλού εύρους και του υψηλού κόστους μονοπατιών.
- Τέλος παρέχεται ο διαμοιρασμός της κίνησης (load sharing) μέσω της διανομής της κυκλοφορίας μεταξύ των πολλαπλών διαδρομών με βάση τα χαρακτηριστικά της κυκλοφορίας.

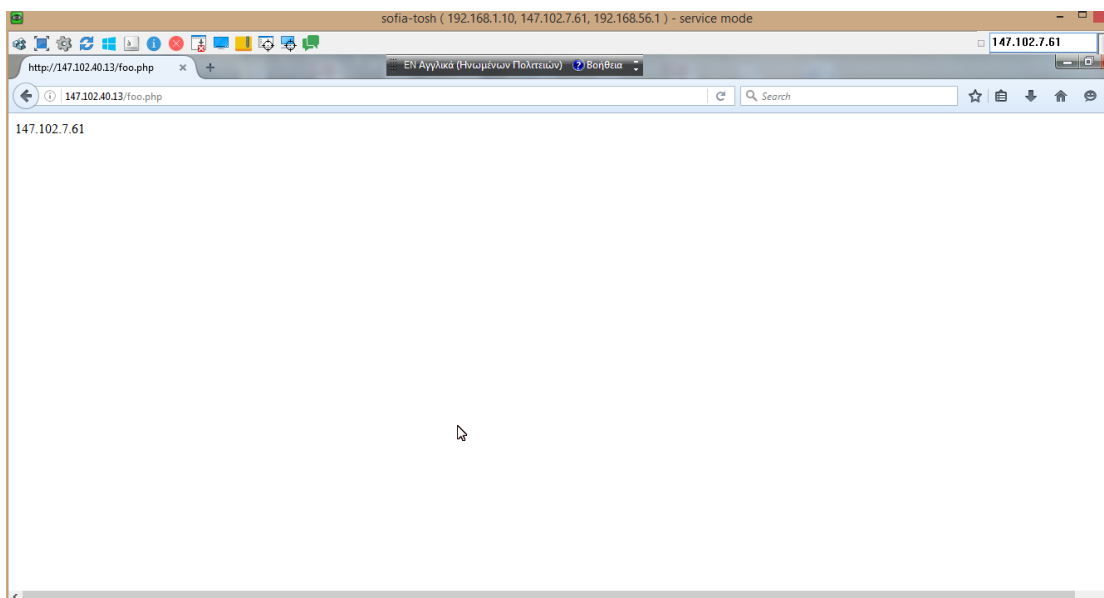
Στη παρούσα διπλωματική στόχος μας είναι η εφαρμογή της πολιτικής δρομολόγησης μεταξύ των διεπαφών Ethernet και συγκεκριμένα της eth0 και eth1. Όπως έχει αναφερθεί και σε προηγούμενα κεφάλαια η διεπαφή eth0 έχει λάβει στατική ip διεύθυνση την 147.102.7.60. και στην eth1 δόθηκε η διεύθυνση 147.102.40.60. Παράλληλα συνδέθηκε στο raspberry pi μέσω του

wi-fi dongle ένας φορητός υπολογιστής, η διαδικασία για την σύνδεση ενός υπολογιστή με το wi-fi του raspberry pi παρουσιάστηκε στο τρίτο κεφάλαιο. Επιπλέον ο υπολογιστής διαθέτει και σύνδεση Ethernet με την στατική διεύθυνση 147.102.7.61 έτσι ώστε να είναι εφικτή η απομακρυσμένη σύνδεση σε αυτόν.

Βέβαια για την υλοποίηση της απομακρυσμένης επιφάνειας εργασίας χρειάστηκαν να εκτελεστούν κάποια βήματα. Αρχικά εγκαταστάθηκε στο raspberry pi το πακέτο **wake-on-lan (wol)** με την εντολή **sudo apt-get install wol**. Το wake-on-lan αποτελεί ένα πρότυπο δικτύωσης Ethernet που επιτρέπει σε έναν διακομιστή ή σε έναν υπολογιστή να ενεργοποιηθεί με ένα μήνυμα δικτύου. Έτσι λοιπόν αποστέλλεται ένα «μαγικό» πακέτο (magic packet) το οποίο ενεργοποιεί τους προσαρμογείς Ethernet και τις μητρικές πλακέτες προκειμένου να εκκινήσουν τα συστήματα. Στη διπλωματική όταν επιθυμούμε να εκκινήσουμε το φορητό υπολογιστή εκτελείται η εντολή **wakeonlan -i 147.102.7.255 00:26:6C:6E:D9:65** στην οποία εισάγεται η broadcast ip διεύθυνση του δικτύου 147.102.7.0 και η MAC διεύθυνση του υπολογιστή. Βέβαια για να είναι κάτι τέτοιο εφικτό αποτελεί απαραίτητη προϋπόθεση να βρίσκονται και τα δύο μηχανήματα στο ίδιο τοπικό δίκτυο (LAN), δηλαδή και το μηχάνημα που αποστέλλει το «μαγικό» πακέτο αλλά και το μηχάνημα που επιθυμούμε να ενεργοποιήσουμε. Επειδή ο υπολογιστής που χρησιμοποιήσαμε έχει ως λειτουργικό σύστημα τα Windows 7 Home Premium δεν υποστηρίζει την απομακρυσμένη επιφάνεια εργασίας για αυτό το λόγο πραγματοποιήθηκε η λήψη του προγράμματος **Ultra VNC Viewer**. Μέσω αυτού δίνεται η δυνατότητα στο χρήστη να χρησιμοποιήσει απομακρυσμένα οποιονδήποτε υπολογιστή εισάγοντας μόνο κατά την έναρξη του προγράμματος την διεύθυνση ip του υπολογιστή.

Ακολουθώντας όλα τα βήματα που αναλύθηκαν παραπάνω είναι πλέον εφικτή η απομακρυσμένη σύνδεση μας στον φορητό υπολογιστή. Αφού εισαχθούμε σε αυτόν επιλέγουμε να συνδεθούμε στο raspberry pi μέσω του της ασύρματης σύνδεσης. Σύμφωνα με ένα κώδικα σε γλώσσα php ο οποίος χρησιμοποιεί ως διακομιστή (server) την διεύθυνση 147.102.40.13 δημιουργήσαμε την ιστοσελίδα <http://147.102.40.13/foo.php> στην οποία όταν εισαγάμαστε μας εμφανίζει σε ποία διεύθυνση ip είμαστε συνδεδεμένοι.

Αρχικά λοιπόν μόλις επισκεφτούμε την ιστοσελίδα μας λαμβάνουμε ως αποτέλεσμα ότι είμαστε συνδεδεμένοι από την ip διεύθυνση 147.102.7.61 δηλαδή μέσω του Ethernet. Αυτό φαίνεται και στην εικόνα που ακολουθεί.



Εικόνα 5.2.1 Σύνδεση πριν την εφαρμογή πολιτικής δρομολόγησης

Στόχος μας είναι στην παρούσα διπλωματική να εφαρμόσουμε πολιτικές δρομολόγησης έτσι ώστε όλη η κίνηση που αφορά το δίκτυο 147.102.40.0 να διέρχεται μέσω της διεπαφής eth1 του raspberry pi με ip διεύθυνση 147.102.40.60. Για να επιτευχθεί κάτι τέτοιο αρχικά δημιουργήσαμε έναν πίνακα στον πυρήνα kernel με το όνομα **pbr** που θα περιέχει ένα κανόνα. Έτσι λοιπόν όταν εισάγουμε την εντολή **ip rule list** λαμβάνουμε το αποτέλεσμα της παρακάτω εικόνας.

```
pi@pi:~$ sudo -i
root@pi:~# ip rule list
0:      from all lookup local
32765:  from 192.168.1.10 to 147.102.40.13 lookup pbr
32766:  from all lookup main
32767:  from all lookup default
root@pi:~#
```

Εικόνα 5.2.2 ip tables του πυρήνα kernel

Όπως φαίνεται και στην παραπάνω εικόνα πέρα από τον κανόνα που εισάγαμε υπάρχουν και τρεις πίνακες του συστήματος που περιλαμβάνουν

κάποιους κανόνες από προεπιλογή (by default). Αυτοί έχουν ονόματα local, main και default. Επιπλέον παρατηρούμε ότι πριν από κάθε κανόνα υπάρχουν κάποια νούμερα τα οποία δηλώνουν την προτεραιότητα τους. Τέλος το σχόλιο **from all** εννοεί ότι όλοι οι κανόνες εφαρμόζονται σε όλα τα πακέτα.

Γενικά ο πίνακας default είναι κενός οι πίνακες όμως local και main περιέχουν τους κανόνες που φαίνονται στις μετέπειτα εικόνες.

```
root@pi:~# ip route list table local
broadcast 127.0.0.0 dev lo proto kernel scope link src 127.0.0.1
local 127.0.0.0/8 dev lo proto kernel scope host src 127.0.0.1
local 127.0.0.1 dev lo proto kernel scope host src 127.0.0.1
broadcast 127.255.255.255 dev lo proto kernel scope link src 127.0.0.1
broadcast 147.102.7.0 dev eth0 proto kernel scope link src 147.102.7.60
local 147.102.7.0 dev eth0 proto kernel scope host src 147.102.7.60
local 147.102.7.60 dev eth0 proto kernel scope host src 147.102.7.60
broadcast 147.102.7.255 dev eth0 proto kernel scope link src 147.102.7.60
broadcast 147.102.40.0 dev eth1 proto kernel scope link src 147.102.40.60
local 147.102.40.0 dev eth1 proto kernel scope host src 147.102.40.60
local 147.102.40.60 dev eth1 proto kernel scope host src 147.102.40.60
broadcast 147.102.40.255 dev eth1 proto kernel scope link src 147.102.40.60
broadcast 169.254.0.0 dev wlan0 proto kernel scope link src 169.254.245.71
local 169.254.245.71 dev wlan0 proto kernel scope host src 169.254.245.71
broadcast 169.254.255.255 dev wlan0 proto kernel scope link src 169.254.245.71
1
broadcast 192.168.1.0 dev wlan0 proto kernel scope link src 192.168.1.1
local 192.168.1.1 dev wlan0 proto kernel scope host src 192.168.1.1
broadcast 192.168.1.255 dev wlan0 proto kernel scope link src 192.168.1.1
```

Εικόνα 5.2.3 ip table local

```
root@pi:~# ip route list table main
default via 147.102.7.200 dev eth0
default via 147.102.7.60 dev eth0 metric 202
default via 147.102.40.60 dev eth1 metric 203
169.254.0.0/16 dev wlan0 proto kernel scope link src 169.254.245.71 metric 304
192.168.1.0/24 dev wlan0 proto kernel scope link src 192.168.1.1
```

Εικόνα 5.2.4 ip table main

Για να πραγματοποιηθεί η προσθήκη του κανόνα pbr αρχικά εκτελούμε την εντολή :

- **echo 200 pbr >> /etc/iproute2/rt_tables** μέσω της οποίας αποθηκεύουμε τον πίνακα pbr στο αρχείο **/etc/iproute2/rt_tables** το οποίο φαίνεται στην παρακάτω εικόνα.

```
pi@pk:~$ nano /etc/iproute2/rt_tables
GNU nano 2.2.6 File: /etc/iproute2/rt_tables
# reserved values
#
255 local
254 main
253 default
0 unspec
#
# local
#1 inr.ruhep
200 pbr
```

Εικόνα 5.2.5 Αρχείο /etc/iproute2/rt_tables

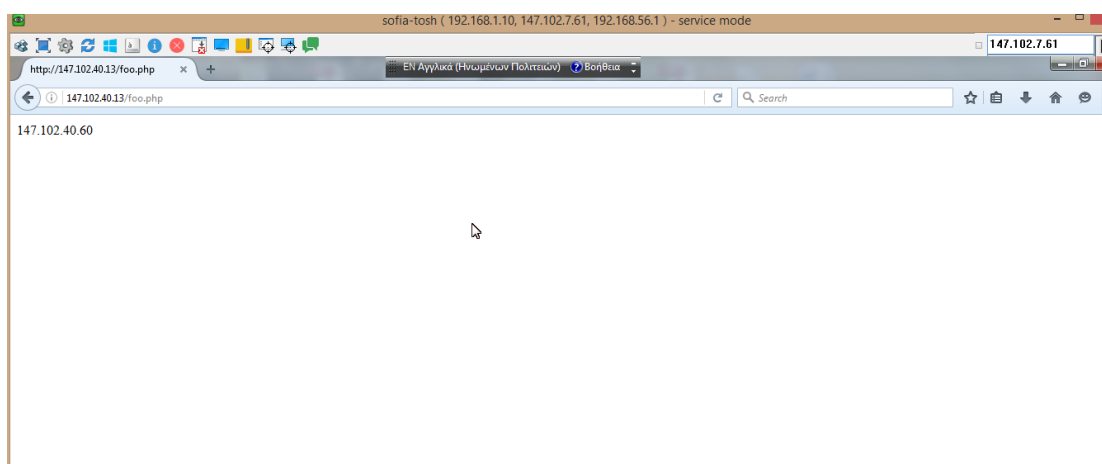
Φυσικά προτού εκτελέσουμε τις παραπάνω εντολές έχουμε εγκαταστήσει πρώτα στο raspberry pi το πακέτο **iproute2** μέσω της εντολής **sudo apt-get install iproute2**. Το iproute2 αποτελεί μια συλλογή για τον έλεγχο της TCP/IP δικτύωσης καθώς και της κυκλοφορίας στα Linux.

- Στην συνέχεια εκτελούμε την εντολή **ip rule add from 192.168.1.10 to 147.102.40.13 table pbr** όπου 192.168.1.10 είναι η ip διεύθυνση του φορητού υπολογιστή και 147.102.40.23 η ip του διακομιστή της ιστοσελίδας που έχουμε κατασκευάσει και έτσι κατασκευάζουμε το κανόνα που επιθυμούμε.
- Έπειτα συνεχίζουμε με την εντολή **ip route add 147.102.40.13 table pbr via 147.102.40.60 proto static** με την οποία ορίζουμε μια διαδρομή στον πίνακα μας που θα έχει ως προορισμό την ip διεύθυνση 147.102.40.13. Επιπλέον όλα τα πακέτα με προορισμό αυτή την διεύθυνση θα μεταβαίνουν εκεί μέσω της διεπαφής eth1 με διεύθυνση 147.102.40.60.

Βέβαια για να επιτευχθεί ο τελικός μας στόχος είναι απαραίτητη η εισαγωγή κάποιων επιπλέον κανόνων NAT που αφορούν την διεπαφή eth1 πέρα αυτών που αναφέρθηκαν στο τρίτο κεφάλαιο. Οι κανόνες αυτές είναι οι εξής :

- **iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE**
- **iptables -A FORWARD -i eth1 -o wlan0 -m state --state RELATED,ESTABLISHED -j ACCEPT**
- **iptables -A FORWARD -i wlan0 -o eth1 -j ACCEPT**

Στη συνέχεια σειρά έχει η προσθήκη μιας διαδρομής στον πίνακα δρομολόγησης του φορητού υπολογιστή. Ο πίνακας δρομολόγησης ορίζει ποιά διαδρομή θα ακολουθήσουν τα πακέτα όταν φύγουν από το σύστημα. Έτσι λοιπόν προσθέτοντας διαδρομές στον πίνακα δρομολόγησης μπορούμε να καταστήσουμε το σύστημα μας πιο ευέλικτο. Στην συγκεκριμένη περίπτωση μέσω της εντολής **route add 147.102.40.0 mask 255.255.255.0 192.168.1.1** στο command line των windows 7 home premium, στο οποίο εισήλθαμε ως διαχειριστές ,πραγματοποιήσαμε την προσθήκη μια εγγραφής με προορισμό το δίκτυο 147.102.40.0 μέσω της πύλης (gateway) που χρησιμοποιεί ο υπολογιστής όταν συνδέεται στο ασύρματο δίκτυο. Ουσιαστικά με αυτή την εγγραφή ορίσαμε όλα τα πακέτα που έχουν προορισμό το δίκτυο 147.102.40.0 να διέρχονται από την προεπιλεγμένη πύλη του ασύρματου δικτύου. Έπειτα από όλα αυτά τα βήματα όπως θα δούμε από την εικόνα που ακολουθεί η κίνηση για το δίκτυο 147.102.40.0 διέρχεται από την διεπαφή eth1 με διεύθυνση 147.102.40.60.



Εικόνα 5.2.6 Σύνδεση μετά την εφαρμογή πολιτικής δρομολόγησης

5.3 Παράλληλη χρήση δύο διεπαφών

Όπως αναφέρθηκε και στο τέταρτο κεφάλαιο το `quagga` αποτελεί ένα λογισμικό δρομολόγησης που παρέχει στο σύγχρονο χρήστη ένα τεράστιο εύρος δυνατοτήτων. Σε αυτό το κεφάλαιο θα αναλυθεί η χρήση του `quagga` ως το μέσο για την επίτευξη της παράλληλης χρήσης και των δύο διεπαφών δηλαδή του `eth0` και του `ppp0`. Μέσω αυτού μπορεί να επιτευχθεί καλύτερη διαχείριση της κίνησης του δικτύου. Κάτι τέτοιο φυσικά είναι υλοποιήσιμο με τις εντολές του `quagga` που αφορούν την στατική δρομολόγηση ,όπως έχει παρουσιαστεί και στα άλλα κεφάλαια στη παρούσα διπλωματική έχει γίνει αποκλειστικά χρήση της στατικής δρομολόγησης .Η στατική δρομολόγηση δίνει την δυνατότητα στον χρήστη να τροποποιεί και να διαχειρίζεται την κίνηση του δικτύου όπως αυτός το επιθυμεί.

Για να επιτευχθεί λοιπόν αυτή η υλοποίηση δημιουργήθηκε ένας κώδικας (shell script) με την ονομασία `parallel.sh` όπως παρουσιάζεται παρακάτω.

parallel.sh

```
#!/bin/bash

Logfile1="ip_route.txt"

vtysh -c "show run" -c "conf t" -c " ip route 0.0.0.0/0
10.64.64.64 "

vtysh -c "show run" -c "conf t" -c " ip route 0.0.0.0/0
147.102.7.200"

vtysh -c "show ip route">> $Logfile1
```

Όπως φαίνεται στον παραπάνω πρόγραμμα αρχικά δημιουργείται ένα αρχείο σε μορφή `txt` που θα περιέχει τα αποτελέσματα των εντολών που εκτελούνται. Στην πρώτη εντολή αρχικά πραγματοποιείται η εισαγωγή στο `configure terminal` του `quagga` και στην συνέχεια μέσω της εντολής `ip route` επιτυγχάνεται η δρομολόγηση των πακέτων προς το δίκτυο `0.0.0.0/0` το οποίο

αποτελεί το προεπιλεγμένο δίκτυο (default network) από την προεπιλεγμένη πύλη (default gateway) της διεπαφής eth0 ή αντίστοιχα την προεπιλεγμένη πύλη της διεπαφής ppp0. Όταν εκτελείται ο κώδικας το αποτέλεσμα που προκύπτει φαίνεται στην εικόνα που ακολουθεί που είναι από το αρχείο ip_route.txt, για την εκτέλεση του κώδικα χρησιμοποιούμε την εντολή **./parallel.sh**.

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, A - Babel,
       > - selected route, * - FIB route

S    0.0.0.0/0 [1/0] via 10.64.64.64, ppp0
      via 147.102.7.200, eth0
K>*  0.0.0.0/0 via 147.102.40.200, eth1
C>*  10.64.64.64/32 is directly connected, ppp0
C>*  127.0.0.0/8 is directly connected, lo
C>*  147.102.7.0/24 is directly connected, eth0
C>*  147.102.40.0/24 is directly connected, eth1
C>*  169.254.0.0/16 is directly connected, wwan0
```

Εικόνα 5.3.1 Αρχείο ip_route.txt

Όπως απεικονίζεται και στην εικόνα που προηγήθηκε έχουν προστεθεί δύο νέες στατικές εγγραφές οι οποίες απεικονίζονται με το σύμβολο S που σημαίνει ότι είναι στατικές. Επιπλέον βλέπουμε ότι στην εγγραφή εμφανίζεται η καταχώρηση [1/0] που σημαίνει ότι η κίνηση και στις δύο διαδρομές είναι ισοβαρής και διαμοιράζεται μεταξύ των δύο διεπαφών eth0 και ppp0.

6 Συμπεράσματα

Σε μια εποχή όπου η τεχνολογία εξελίσσεται συνεχώς και οι απαιτήσεις των χρηστών αυξάνονται καθημερινά το Raspberry Pi έχει δώσει λύση σε πολλά τεχνολογικά προβλήματα της καθημερινότητας. Το χαμηλό του κόστος σε συνδυασμό με τις υψηλές του επιδόσεις το έχει καταστήσει αναπόσπαστο κομμάτι όσον αφορά στη δημιουργία νέων εφαρμογών και στην υποστήριξη των υπαρχουσών.

Στα πλαίσια της παρούσας διπλωματικής αναπτύχθηκε με τη χρήση του raspberry pi ένας οικιακός δρομολογητής με δύο διεπαφές WAN. Η μια περιλαμβάνει σύνδεση μέσω Ethernet και η άλλη μέσω ασύρματου δικτύου 3^{ης} γενιάς όπως περιγράφηκε αναλυτικά στα προηγούμενα κεφάλαια. Με αυτές τις συνδέσεις, αλλά και με την παραλλαγή που δημιουργήσαμε με δύο συνδέσεις Ethernet, καταφέραμε να υλοποιήσουμε έναν οικιακό δρομολογητή με εξελιγμένες δυνατότητες πέραν αυτών που διαθέτει σήμερα ένα τυπικός οικιακός δρομολογητής. Έτσι επιτύχαμε να φτιάξουμε ένα δρομολογητή ο οποίος θα έχει συνεχή σύνδεση με το διαδίκτυο αφού, όποια και από τις δύο διεπαφές σταματήσει να λειτουργεί, η δρομολόγηση θα συνεχίζει να πραγματοποιείται μέσω της άλλης. Επιπλέον έγινε εφικτή η παράλληλη χρήση και των δύο διεπαφών, δηλαδή του Ethernet και του 3G καθώς και ο διαμοιρασμός της κίνησης μεταξύ αυτών. Τέλος σε αυτό το σημείο πρέπει να αναφερθεί ότι κατά την ταυτόχρονη σύνδεση του 3G dongle με το wi-fi adapter αντιμετωπίσαμε διάφορα προβλήματα σχετικά με την υπερβολική κατανάλωση ρεύματος και των δύο. Αυτό είχε ως αποτέλεσμα όταν προσπαθούσαμε να στείλουμε κίνηση στο 3G δίκτυο από τον φορητό υπολογιστή και όντας συνδεδεμένοι στο ασύρματο δίκτυο, να αποσυνδέονται και τα δύο εξαρτήματα λόγω της μέγιστης κατανάλωσης ρεύματος. Για αυτό τον λόγο αντικαταστήσαμε το 3G dongle με μια επιπλέον Ethernet σύνδεση. Έτσι λοιπόν η πολιτική δρομολόγησης για το δίκτυο 147.102.40.0 επιτεύχθηκε μέσω της διεπαφής Ethernet και συγκεκριμένα της eth1. Φυσικά τα βήματα που εκτελέστηκαν μπορούν να υλοποιηθούν και με το 3G dongle αρκεί να μη υπάρχει το τεχνικό πρόβλημα της κατανάλωσης ρεύματος. Κάτι τέτοιο θα είναι

πιο εφικτό στην τελευταία έκδοση του raspberry pi αφού εμπεριέχει ήδη ένα wi-fi adapter.

Γενικά το raspberry pi αποτελεί ένα πολύ χρήσιμο εργαλείο ανάπτυξης εφαρμογών και η συνεχής εξέλιξη του προσφέρει ένα ευρύ πλήθος λύσεων στους τεχνολογικούς προβληματισμούς των καιρών μας. Μια από τις ποικίλες τεχνολογικές λύσεις αποτελεί και η μετατροπή του Raspberry Pi σε οικιακό δρομολογητή με αναβαθμισμένες δυνατότητες. Κλείνοντας οφείλεται να τονιστεί ότι διαμέσου αυτών των εφαρμογών η τεχνολογία προάγεται δημιουργώντας νέους γνωστικούς ορίζοντες και βελτιώνοντας την καθημερινότητα του σύγχρονου ανθρώπου.

ΒΙΒΛΙΟΓΡΑΦΙΑ

- [1] Design Challenges for Home Gateway Devices
<http://www.hometoys.com/content.php?url=/htinews/dec02/articles/satish/homegateway.htm>
- [2] ευριζωνικότητα <http://broadband.cti.gr/el/evrizonikotita/dsl.php>
- [3] ADSL <http://www.windowsnetworking.com/articles-tutorials/netgeneral/adslinfo.html>
- [4] Δικτύωση Υπολογιστών James F.Kurose, Keith W.Ross, 6^η έκδοση, εκδόσεις Μόσχος Γκιούρδας, Αθήνα 2013
- [5] Router (computing)
https://en.wikipedia.org/wiki/Router_%28computing%29#cite_note-22
- [6] RASPBERRY PI 1 MODEL B+ <https://www.raspberrypi.org/products/model-b-plus/>
- [7] 7 Operating Systems You Can Run With Raspberry Pi
<http://www.makeuseof.com/tag/7-operating-systems-you-can-run-with-raspberry-pi/>
- [8] USB to Ethernet Adapter <http://www.tech-faq.com/usb-to-ethernet-adapter.html>
- [9] 3G (third generation of mobile telephony)
<http://searchtelecom.techtarget.com/definition/3G>
- [10] Wi-Fi <https://en.wikipedia.org/wiki/Wi-Fi>
- [11] How-To: Add Wifi to the Raspberry Pi <http://raspberrypiHQ.com/how-to-add-wifi-to-the-raspberry-pi/>
- [12] iptables <https://wiki.archlinux.org/index.php/Iptables>
- [13] Security Guide https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/4/html/Security_Guide/s1-firewall-iptables.html
- [14] Install Quagga As Linux Router
<https://opensourcecentre.wordpress.com/article/install-quagga-as-linux-router/>
- [15] Simple Network Management Protocol
https://el.wikipedia.org/wiki/Simple_Network_Management_Protocol
- [16] How to monitor Linux servers with SNMP and Cacti
<http://xmodulo.com/monitor-linux-servers-snmp-cacti.html>

[17] How to install and configure Cacti on Linux <http://xmodulo.com/install-configure-cacti-linux.html>

[18]Linux Advanced Routing &Traffic Control HOW TO
<http://www.tldp.org/HOWTO/Adv-Routing-HOWTO/index.html>

[19]Policy Routing with Linux –Online Edition by Matthew G.Marsh
<http://www.policyrouting.org/PolicyRoutingBook/ONLINE/TOC.html>