«ΤΟ ΠΡΩΤΟΚΟΛΛΟ IPV6 ΚΑΙ ΤΟ INTERNET ΤΩΝ ΠΡΑΓΜΑΤΩΝ»

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
Τμήμα Ψηφιακών Συστημάτων
Π.Μ.Σ. Τεχνοοικονομική Διοίκηση Ψηφιακών Συστημάτων

Μεταπτυχιακή εργασία
Ζώτος Χρήστος
Αρ. Μητρώου: MTE0939
2013

Επιβλέπων Καθηγητής: Δρ. Κανέλλος Λεωνίδας

Ευχαριστίες

Προτού ξεκινήσω την ανάπτυξη της εργασίας μου, επιθυμώ να αποδώσω ευχαριστίες σε όλους όσους βοήθησαν στην συγγραφή της. Οφείλω ένα μεγάλο ευχαριστώ στον επιβλέποντα καθηγητή μου Δρ. Κανέλλο Λεωνίδα, ο οποίος με στήριξε, με συμβούλευε, με καθοδηγούσε, με διόρθωνε και με διαφώτιζε όποτε αυτό χρειαζόταν σε όλη τη διάρκεια εκπόνησης της εργασίας μου. Δε θα μπορούσα να παραλείψω το υπόλοιπο εκπαιδευτικό προσωπικό της σχολής μου, τους καθηγητές μου, οι οποίοι μου έδωσαν τα απαραίτητα εφόδια ώστε να ολοκληρώσω με επιτυχία τις σπουδές μου. Επίσης, τις απαραίτητες ευχαριστίες αποδίδω στην οικογένειά μου, η οποία με στήριξε ηθικά και υλικά καθ` όλη τη διάρκεια της φοιτητικής μου ζωής. Τέλος , αποδίδω ευχαριστίες στη Μανουσοπούλου Μαρία για τη στήριξη της σε όλη τη διάρκεια εκπόνησης της πτυχιακής αυτής και την αμέριστη βοήθεια της στην τελική διαμόρφωση.

Περιεχόμενα

ΒΙΟΓΡΑΦΙΚΟ ΣΗΜΕΙΩΜΑ 4

Abstract 5

Εισαγωγή 6

1. Το πρωτόκολλο IP 9

1.1 Εισαγωγή 9

1.2. Το πρωτόκολλο IP. 11

1.3. Η φόρμα του δεδομενογράμματος IP. 12

1.4 CIDR Classless Interdomain Routing (Αταξική Δρομολόγηση) 15

1.5 Γιατί χρειαζόμαστε το IPv6; 18

1.6 Οι βελτιώσεις που εισάγει το IPv6. 27

1.7 Το Mobile IPv6 31

1.7.1. Ο Τρόπος Λειτουργίας του Mobile IPv6. 35

1.8 Η εξέλιξη του IPv6 37

2. The Internet Of Things 43

2.1 Εισαγωγή 43

2.2. Ορισμοί 45

2.3 Τι πραγματικά είναι όμως το «Internet των Πραγμάτων»; 47

2.4 Στοιχεία ανατομίας του Internet of things. 49

2.5 Παραδείγματα χρήσεων του internet of things 52

3. Θεσμικό πλαίσιο 65

3.1 Εισαγωγή 65

3.2 Ηθική και IoT 67

3.3 Διαμόρφωση πολιτικής - Ερωτήσεις Τακτικής-Ασφάλεια 70

3.4 Διαφορές ανάμεσα στους πολιτισμούς και τις ηπείρους σχετικά με το απόρρητο προσωπικών πληροφοριών. 71

3.5 Αποδοχή του Internet των πραγμάτων. 72

3.6 Οι Ρυθμιστικές Αρχές και ο ρόλος τους. 74

3.7 Ελληνικό Νομικό Πλαίσιο 77

3.7.1 Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.) 78

3.7.2 Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα. 80

3.7.3 Η Αρχή Διασφάλισης του Απορρήτου των επικοινωνιών. 81

3.8 Προστασία προσωπικών δεδομένων και ασφάλεια απορρήτου των επικοινωνιών στον τηλεπικοινωνιακό τομέα. 82

3.9 Κοινοτικό Πλαίσιο 85

3.10 Προβλήματα αναφορικά με την προστασία προσωπικών δεδομένων και της χρήσης της Rfid τεχνολογίας. 87

3.11 IPv6 και Νομικά Θέματα 88

3.12 Νομικές - ρυθμιστικές προκλήσεις που φέρνει στο προσκήνιο το internet of things. 92

3.13 Προτεινόμενες ρυθμιστικές λύσεις. 94

3.14 Συμπεράσματα 95

Βιβλιογραφία 97

ΒΙΟΓΡΑΦΙΚΟ ΣΗΜΕΙΩΜΑ

Ο Χρήστος Ζώτος γεννήθηκε και μεγάλωσε στην Αθήνα. Αποφοίτησε από το 61ο Λύκειο Αθηνών και εισήχθη στο ΤΕΙ Πειραιά στο τμήμα Βιομηχανικής Πληροφορικής από το οποίο αποφοίτησε το 2005. Ενόσω ήταν φοιτητής, εργάστηκε στους Ολυμπιακούς Αγώνες στο Διεθνές Κέντρο Ραδιοτηλεόρασης σαν Win2k Venue Specialist. Έπειτα από την αποφοίτησή του από το ΤΕΙ, εκπλήρωσε τις στρατιωτικές του υποχρεώσεις υπηρετώντας στην Προεδρική Φρουρά. Το Φεβρουάριο του 2007 ξεκίνησε να εργάζεται στην Fujitsu - Siemens ως information technology products specialist. Τον Απρίλιο του 2008 αποχώρησε από την Fujitsu - Siemens και εργάστηκε στην Μονάδα Οργάνωσης και Διαχείρισης των κοινωνικών πλαισίων στήριξης (ΜΟΔ Α.Ε.) με την ιδιότητα του systems and network administrator. Από τον Ιούλιο του 2011 έως σήμερα, εργάζεται στην Alfabetaroto A.B.E.E. ως ICT manager and administrator.

Abstract

The main goal of this work is to make a detailed presentation of the "new" Internet which in recent years has obtained large dimensions and is now called internet of things. At the same time we will see how and in which way the new technologies contribute to the development and its dissemination and what the prospects for further development are.

Particularly, the first chapter refers to the protocol IP, which is the most common protocol network layer and is synonymous to the Internet. Starting with a brief presentation, we end up with newer versions and capabilities of the protocol. The latest version - IPv6 - seems to offer a benefit to the development of internet of things, which is described in detail in the 2nd chapter.

The "Internet of Things" is a future situation in which everyday objects - such as cell phones, cars, household appliances, clothes, even food - will be connected wirelessly to the internet through smart chips and will be able to collect and exchange data. Each of these objects has a different identity. The recognition of each of these objects is achieved by the use of RFID technology which is described in this chapter. If all objects of daily life were equipped with RFID tags , then they could be identified and inventoried by computer systems.

And while this technology is still being debated on and at the same time developed, the legal framework around it should be determined before the Internet of Things becomes fully functional. The analysis of the institutional and legal framework which primarily relates to the privacy of users and compliance requirements of any telecommunications equipment associated with the internet of things, is thoroughly investigated in the third chapter.

Εισαγωγή

Σκοπός της παρούσας εργασίας, είναι να γίνει μια αναλυτική παρουσίαση του "νέου είδους" διαδικτύου που τα τελευταία χρόνια έχει πάρει μεγάλες διαστάσεις, το αποκαλούμενο internet των πραγμάτων. Ταυτόχρονα θα δούμε πώς και με ποιό τρόπο οι νέες τεχνολογίες συμβάλλουν στην ανάπτυξη και διάδοση του και ποιές είναι οι περαιτέρω προοπτικές ανάπτυξής του.

Συγκεκριμένα στο 1ο κεφάλαιο γίνεται λόγος για το πρωτόκολλο IP, το οποίο είναι το πιο διαδεδομένο πρωτόκολλο του επιπέδου δικτύου και είναι συνώνυμο με το Διαδίκτυο. Ξεκινάμε από μια σύντομη παρουσίασή του και καταλήγουμε στις νεότερες εκδόσεις του και τις δυνατότητες που δίνουν στον χρήστη τους. Η τελευταία έκδοση του - IPv6 - φαίνεται πως έχει ευνοήσει ιδιαίτερα την ανάπτυξη του internet των πραγμάτων, αναλυτικός λόγος για το οποίο γίνεται στο 2ο κεφάλαιο.

Το «Διαδίκτυο των Πραγμάτων» είναι μια μελλοντική κατάσταση, κατά την οποία καθημερινά αντικείμενα - όπως κινητά τηλέφωνα, αυτοκίνητα, οικιακές συσκευές, ρούχα, ακόμη και τρόφιμα - θα συνδέονται ασύρματα στο διαδίκτυο μέσω έξυπνων μικροκυκλωμάτων και θα μπορούν να συλλέγουν και να ανταλλάσσουν δεδομένα. Κάθε ένα από αυτά τα αντικείμενα θα έχει μια διαφορετική ταυτότητα. Η αναγνώριση καθενός από αυτά τα αντικείμενα, γίνεται με την χρήση RFID τεχνολογίας η οποία στο παρόν κεφάλαιο αναπτύσσεται διεξοδικά. Αν όλα τα αντικείμενα της καθημερινής ζωής ήταν εξοπλισμένα με RFID ετικέτες, θα μπορούσαν να εντοπιστούν και να απογραφούν από συστήματα ηλεκτρονικών υπολογιστών.

Και ενώ αυτή η τεχνολογία εξακολουθεί να συζητείται και να αναπτύσσεται, το νομικό πλαίσιο γύρω από αυτή θα πρέπει να καθοριστεί πριν το Ίντερνετ των πραγμάτων καταστεί πλήρως λειτουργικό. Η ανάλυση του θεσμικού και νομικού πλαισίου η οποία σχετίζεται κυρίως με την προστασία προσωπικών δεδομένων των χρηστών και τις απαιτήσεις συμμόρφωσης κάθε τηλεπικοινωνιακού εξοπλισμού σχετικού με το internet των πραγμάτων, αναλύονται λεπτομερώς στο 3ο κεφάλαιο.

Μέρος 1ο

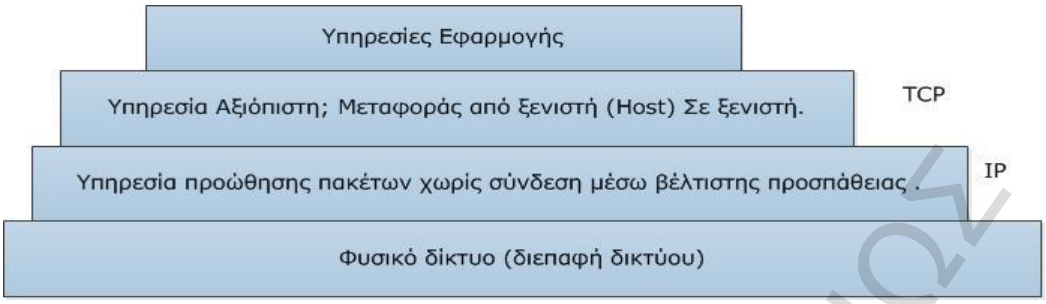
IPv6 **Πρωτόκολλο**

1. **Το πρωτόκολλο** IP

1.1 **Εισαγωγή**

Το IP πρωτόκολλο είναι το πιο διαδεδομένο πρωτόκολλο του επιπέδου δικτύου και είναι συνώνυμο με το Διαδίκτυο. Χαρακτηρίζεται από το μοντέλο επικοινωνίας χωρίς σύνδεση (Connectionless) και το μη εγγυημένο χαρακτήρα προώθησης που υιοθετεί και που έχει γίνει γνωστός σαν «προώθηση βέλτιστης προσπάθειας» ή «προώθηση κατά δύναμιν» (best effort forwarding). Η βασική υπόθεση εκκίνησης είναι ότι το IP εφαρμόζεται πάνω από διάφορα υποδίκτυα με εξ' αντικειμένου μη εγγυημένη αξιοπιστία. Επομένως, δεν έχει νόημα να επιχειρηθεί κάποια αξιόπιστη επικοινωνία σε αυτό το επίπεδο, αφού η συνολική αξιοπιστία θα χαρακτηρίζεται από αυτήν του λιγότερο αξιόπιστου ενδιαμέσου υποδικτύου. Υιοθετήθηκε, λοιπόν, μία λύση άνευ συνδέσεων, βασισμένη σε δεδομενογράμματα (datagrams) μεγέθους έως 64K bits, τα οποία προωθούνται από δρομολογητή σε δρομολογητή χωρίς παρακολούθηση της πορείας τους, αλλά ούτε και της τύχης τους μέσα στο δίκτυο και τα οποία στην πρώτη δυσκολία απορρίπτονται χωρίς πολλές διαδικασίες.

Θα αναρωτηθεί κανείς πώς, αφού το Διαδίκτυο μεταφέρει αρχεία δεδομένων μεγέθους χιλιάδων ή εκατομμυρίων megabytes, χωρίς ούτε ένα λανθασμένο ψηφίο, μπορεί να βασισθεί σε ένα αναξιόπιστο πρωτόκολλο δικτύου. Η απάντηση βρίσκεται στο άλλο πρωτόκολλο με το οποίο αλληλοσυμπληρώνονται, το TCP, το οποίο προβαίνει από τα άκρα της σύνδεσης σε σχολαστική παρακολούθηση της αποστολής, ώστε να μη χαθεί ούτε ένα bit χωρίς να αναμεταδοθεί.



Σχήμα 1.1 Τα στρώματα στο Διαδίκτυο

Το μοντέλο στρωμάτων του Διαδικτύου φαίνεται στο σχήμα 1.1. Δεν ακολουθεί το μεταγενέστερο μοντέλο OSI, αλλά συγχωνεύει τις λειτουργίες σε 4 επίπεδα. Πάνω από το φυσικό, που ενσωματώνει και τις λειτουργίες της ζεύξης, υπάρχουν άλλα τρία στρώματα. Στο χαμηλότερο επίπεδο είναι η υπηρεσία παράδοσης πακέτων χωρίς σύνδεση μέσω του IP. Στο επόμενο επίπεδο είναι η υπηρεσία αξιόπιστης μετάδοσης και στο υψηλότερο οι υπηρεσίες εφαρμογής.

Επειδή χρησιμοποιούνται πολλά ανομοιογενή φυσικά δίκτυα, έχει γίνει προσπάθεια να δημιουργηθεί μία αφαίρεση που να δίνει στο χρήστη την εντύπωση ενός ενιαίου δικτύου, κρύβοντας την ανομοιομορφία πίσω από τη βασική λειτουργία κατά την οποία το δίκτυο παίρνει πακέτα και τα παραδίδει στον προορισμό τους, επιτρέποντας στις εφαρμογές να τρέχουν από μακριά.

Για το χρήστη το διαδίκτυο είναι ένα ενιαίο δίκτυο που διασύνδεει όλους τους ξενιστές υπολογιστές (hosts). Στην πραγματικότητα, όταν στέλνουμε πακέτα από τον υπολογιστή μας, στον οποίο έχουμε φορτώσει τη στοίβα TCP/IP, πιθανότατα ξεκινάμε από ένα τοπικό δίκτυο, για το οποίο τα πακέτα IP είναι πολύ μεγάλα και αφού σπάσουν σε πακέτα LLC, θα διεκδικήσουν το κοινό μέσο υπακούοντας στο πρωτόκολλο MAC του τοπικού δικτύου. Στη συνέχεια θα φθάσουν στην πύλη διόδευσης IP (IP gateway), όπου καταλήγουν όλα τα πακέτα που ανήκουν στο IP επίπεδο και έχουν ως προορισμό τον έξω κόσμο.

Εκεί, θα ξανασυναρμολογηθούν και θα σταλούν μέσω κάποιας ζεύξης, που διαθέτει ο οργανισμός του παραδείγματός μας, προς κάποιον δρομολογητή IP (IP router) κάποιου άλλου οργανισμού, ο οποίος μας παρέχει υπηρεσίες Διαδικτύου. Από εκεί αρχίζει μία σειρά παρόμοιων δρομολογήσεων από πύλη σε πύλη μέχρι τον τελικό προορισμό που πιθανόν να είναι κάποια βάση δεδομένων, κάποιος διακομιστής ή κάποιος άλλος host.

Εν κατακλείδι, η βασική φιλοσοφία του πρωτοκόλλου IP χαρακτηρίζεται από στιβαρότητα, αντοχή και προσαρμοστικότητα, αλλά λίγες εγγυήσεις.

1.2. Το **πρωτόκολλο** IP.

Η θεμελιώδης υπηρεσία του πρωτοκόλλου IP είναι η μεταφορά πακέτων, η οποία χαρακτηρίζεται ως μη αξιόπιστη, ελλείψει των κατάλληλων μηχανισμών που θα εξασφάλιζαν εγγυημένη παράδοση σε αυτό το επίπεδο. Αυτό πρακτικά σημαίνει ότι το πακέτο μπορεί να καθυστερήσει ή να παραδοθεί εκτός της σειράς του, όπως επίσης να απορριφθεί, να διπλασιαστεί, ή να βρεθεί σε λάθος προορισμό. Η υπηρεσία IP ούτε ανιχνεύει τέτοιες καταστάσεις, αλλά ούτε ειδοποιεί τον αποστολέα ή τον λήπτη γι' αυτές. Η πιο συνήθης αστοχία είναι η απόρριψη πακέτου λόγω υπερχείλισης του ταμιευτήρα δρομολογητή.

Η υπηρεσία, επίσης, χαρακτηρίζεται ως «χωρίς σύνδεση» (connectioneless), γιατί το κάθε πακέτο είναι ανεξάρτητο από τα άλλα. Μία ακολουθία από πακέτα που στέλνονται από έναν υπολογιστή σε έναν άλλο, μπορεί να ακολουθήσουν διαφορετικά δρομολόγια και ορισμένα από αυτά να χαθούν. Η υπηρεσία που παρέχει το IP χαρακτηρίζεται ως καλύτερης δυνατής προσπάθειας

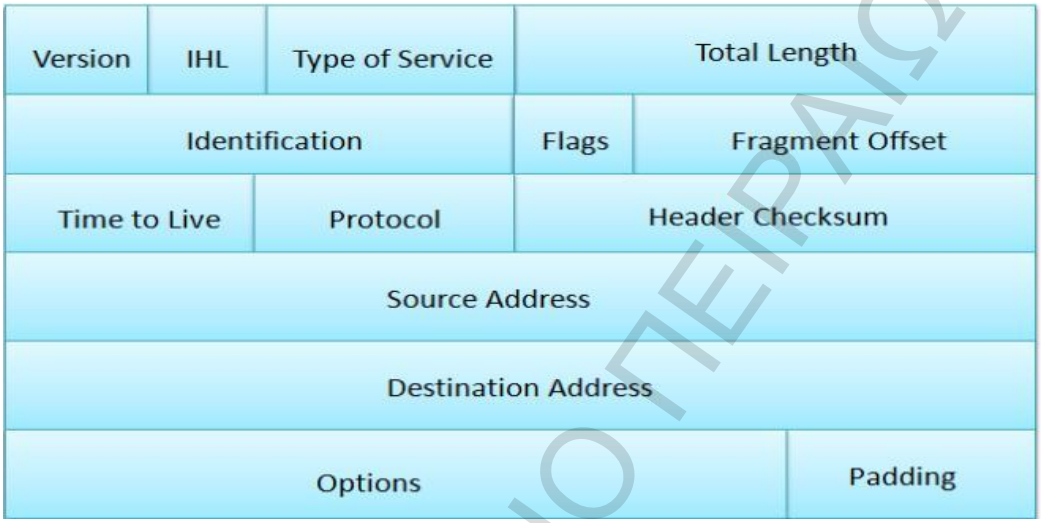
(best-effort delivery), καθώς το λογισμικό του Διαδικτύου καταβάλει προσπάθεια να παραδώσει τα πακέτα στον προορισμό τους, χωρίς όμως να έχει εξασφαλίσει τις προϋποθέσεις εκείνες που θα καθιστούσαν αυτή την προσπάθεια αρκετή για εγγυημένο αποτέλεσμα. (Αυτό δε συμβαίνει με άλλα πρωτόκολλα δικτύου, και κυρίως με αυτά που βασίζονται σε συνδέσεις και μηχανισμούς αποδοχής, ώστε να εγγυώνται την επάρκεια των πόρων δικτύου για το ζητούμενο ποιοτικό αποτέλεσμα υπηρεσίας, όπως π.χ. το X.25). Η έκφραση "καλύτερη" προσπάθεια αναφέρεται στο γεγονός ότι δε γίνεται απώλεια πακέτων από μη αντικειμενικά αίτια, όπως εξάντληση των πόρων του δικτύου (π.χ. υπερχείλιση ταμιευτήρων) ή βλάβη φυσικών υποδικτύων (π.χ. κομμένες ζεύξεις).

Το πρωτόκολλο IP ορίζει τρεις σημαντικές παραμέτρους της επικοινωνίας. Πρώτον, το IP πρωτόκολλο ορίζει τη βασική μονάδα της μετάδοσης δεδομένων (πακέτο) που χρησιμοποιείται για οργάνωση των δεδομένων. Δεύτερον, το λογισμικό IP εκτελεί τη διαδικασία της δρομολόγησης, διαλέγοντας μια πόρτα εξόδου για να στείλει τα δεδομένα και τρίτον, το IP παρέχει ένα σύνολο κανόνων που υλοποιούν την ιδέα της μη αξιόπιστης παράδοσης πακέτων. Οι κανόνες χαρακτηρίζουν τον τρόπο που οι ξενιστές υπολογιστές και οι πύλες διόδευσης θα επεξεργάζονται τα πακέτα, πώς και πότε θα παραχθούν τα μηνύματα λάθους και τις συνθήκες κάτω από τις οποίες κάποια πακέτα θα απορριφθούν.

1.3. **Η φόρμα του δεδομενογράμματος** IP.

Η βασική μονάδα μετάδοσης του διαδικτύου είναι το δεδομενόγραμμα Διαδικτύου (IP datagram). Το δεδομενόγραμμα αποτελείται από την επικεφαλίδα και το πεδίο της πληροφορίας. Η επικεφαλίδα του περιέχει τις διευθύνσεις του προορισμού και της

πηγής και το πεδίο της πληροφορίας περιέχει τα δεδομένα. Δεν πρέπει να λησμονείται ότι το Διαδίκτυο είναι ένα νοητό δίκτυο, που έχει υπερτεθεί σε πολλά και ποικίλα φυσικά δίκτυα (δηλ. πραγματικά όπως τα διάφορα LAN, δορυφορικές ζεύξεις, ζεύξεις PCM. SONET κλπ.).



Σχήμα 1.2 IPv4 δεδομενόγραμμα.

Οι πρώτες 6 γραμμές του σχήματος ανήκουν στην κεφαλίδα. Στην τυπική της μορφή η κεφαλίδα δεν έχει επιλογές (options) και padding και το μέγεθός της είναι 20 bits. Ακολουθούν τα δεδομένα, το μήκος των οποίων προκύπτει από το συνολικό μήκος (total length) με αφαίρεση του μήκους κεφαλίδας.

Επειδή η επεξεργασία των δεδομενογραμμάτων γίνεται από λογισμικό, τα περιεχόμενα και η φόρμα μπορούν να εξελίσσονται και δεν είναι υποχρεωτικά αυστηρά αμετάβλητα. Για να διευκολύνεται η εξέλιξη, το πεδίο των πρώτων 4-bits (VERS) περιέχει την έκδοση του IP πρωτοκόλλου που χρησιμοποιήθηκε για να δημιουργηθεί το δεδομενόγραμμα. Γίνεται επαλήθευση ότι ο αποστολέας, ο λήπτης και κάθε δρομολογητής συμφωνούν μεταξύ τους στη μορφή των δεδομενογραμμάτων. Το λογισμικό ελέγχει το πεδίο έκδοσης πριν από την επεξεργασία του καθενός, για να εξασφαλίσει ότι η μορφή

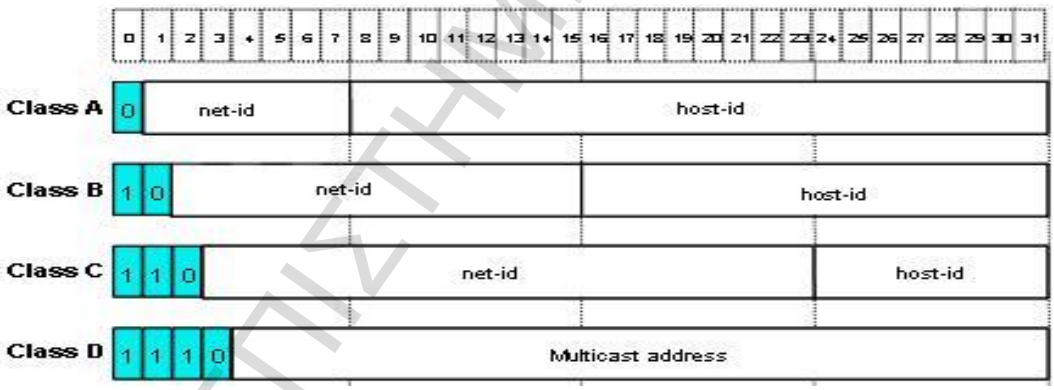
ταιριάζει με την αναμενόμενη μορφή του λογισμικού. Φυσικά, νεώτερες εκδόσεις μπορούν να υποστηριχθούν από ξενιστές και δρομολογητές στους οποίους έχει φορτωθεί το νέο λογισμικό. Είναι αυτονόητο, ότι οι υπολογιστές θα απορρίψουν τα δεδομενογράμματα (datagrams) με εκδόσεις πρωτοκόλλων που δεν υποστηρίζουν, προλαμβάνοντας λανθασμένη μετάφραση των περιεχομένων τους.

Το πεδίο μήκους επικεφαλίδας Header Length (IHL) αποτελείται από 4bits και προσδιορίζει το μήκος της επικεφαλίδας του δεδομενόγραμματος. Για να μπορεί το λογισμικό να βρίσκει και να ερμηνεύει κάθε πεδίο, όλα τα πεδία της κεφαλίδας έχουν σταθερό μήκος που είναι πολλαπλάσιο της λέξης (32 bits). Επειδή το μήκος του πεδίου επιλογών (IP OPTIONS) είναι το μόνο μεταβλητό, υπάρχει και το αντίστοιχο έρμα (PADDING), που ο ρόλος του είναι να συμπληρώσει το πεδίο με τα bits που λείπουν για να συμπληρωθεί η τελευταία λέξη.

Το πεδίο συνολικό μήκος (TOTAL LENGTH), δίνει το μήκος του IP δεδομενογράμματος μετρημένο σε οκτάδες, περιλαμβάνοντας την επικεφαλίδα και το πεδίο πληροφορίας. Τα 16 bits αυτού του πεδίου καθορίζουν και το μέγιστο πιθανό μέγεθος ενός IP δεδομενογράμματος, δηλαδή 216 ή 65535 οκτάδες και αποτελεί καλό συμβιβασμό μεταξύ αφ' ενός της μονοπώλησης των ζεύξεων και της χρήσης μεγάλων ταμιευτήρων, όπως συμβαίνει με τα μεγάλα πακέτα, και αφ' ετέρου της σπατάλης μεγάλου ποσοστού πληροφορίας σε κεφαλίδες, όπως συμβαίνει με τα μικρά πακέτα.

1.4 CIDR Classless Interdomain Routing (**Αταξική Δρομολόγηση**)

Στο ξεκίνημα του Διαδικτύου ορίσθηκαν τέσσερις κλάσεις διευθύνσεων, οι οποίες από την εκρηκτική αύξηση των χρηστών του Διαδικτύου εξαντληθήκαν (ο Icann στις 3 Φεβρουαρίου του 2011 ανακοινώσε την εξάντλησή τους). Στις τέσσερις αυτές κλάσεις, για να αποφεύγεται η σπατάλη διευθύνσεων, δεν ορίσθηκε σταθερό μήκος για τα πεδία Net Id και Host Id, αλλά τρία μεγέθη που αντίστοιχα καθορίζουν τρεις κλάσεις διευθύνσεων (κλάσεις A, B ή C), με φόρμες όπως φαίνεται στο σχήμα (Σχήμα 1.3). Παράλληλα, υπάρχει και μία φόρμα (κλάση D) για πολλαπλή διεύθυνση (multicast) και μία τελευταία για μελλοντικές χρήσεις.



Σχήμα 1.3

Τα πρώτα ψηφία υψηλής τάξεως προσδιορίζουν την κλάση της διεύθυνσης. Η πρώτη κλάση, με μέγεθος πεδίου Net Id ενός byte, καλύπτει λίγα πολύ μεγάλα δίκτυα με πολλά εκατομμύρια υπολογιστές το καθένα, π.χ. στο ARPANET οι διευθύνσεις αρχίζουν με 00001010. Η δεύτερη, δίκτυα που μπορεί να έχουν μέχρι 65536 ξενιστές, ενώ η τρίτη μικρά δίκτυα π.χ. τοπικά. Πρέπει να σημειώσουμε ότι η σύμβαση του Διαδικτύου είναι ότι πάντα

προηγείται το πιο σημαντικό οκτέτο και αυτό ισχύει και για τα πεδία των διευθύνσεων, όπως και για όλα τα πακέτα του Διαδικτύου.

Για να ξεπεραστεί το πρόβλημα της εξάντλησης των διευθύνσεων περνάμε στην 6η έκδοση του πρωτοκόλλου IP όπου το μήκος των διευθύνσεων έγινε 128 bits.

Ωστόσο το IPv6 βρίσκεται ακόμα στα πρώτα βήματά του σε παγκόσμια κλίμακα. Μέχρι να διαδοθεί πλήρως, υιοθετήθηκε η προσωρινή λύση με την παραβίαση των ορίων των κλάσεων. Το πρόβλημα έγινε καταρχάς αισθητό με την εξάντληση των διευθύνσεων κλάσεως Β. Τα σχετικά δίκτυα μπορούν πλέον να πάρουν πολλές διευθύνσεις κλάσεως C και να τις χρησιμοποιούν σαν μία μικτή κλάση. Αυτή η κατάργηση των κλάσεων δημιουργεί ωστόσο ένα νέο σοβαρό πρόβλημα: κάθε υποδίκτυο πρέπει να έχει μια δική του καταχώρηση σε κάθε δρομολογητή του κόσμου. Αυτό μεγενθύνει επικίνδυνα τους πίνακες δρομολόγησης και επιβραδύνει δραματικά τη λειτουργία της δρομολόγησης με μακρές αναζητήσεις. Η απάντηση σε αυτό το πρόβλημα είναι το CIDR, που επιτρέπει τη σύνοψη πολλών διευθύνσεων σε μια καταχώρηση του πίνακα στη βάση των κοινών bit ανώτερης τάξης.

Έτσι, εάν ένα υποδίκτυο πάρει π.χ. 16 διευθύνσεις κλάσεως C σε τρόπο ώστε τα ανώτερης τάξεως bits να είναι τα ίδια, τότε οι διευθύνσεις τους μπορούν να συνοψισθούν σε μια καταχώριση, αρκεί να συνοδεύονται με μια μάσκα που να δείχνει πόσα είναι τα κοινά bits (τα 20 από αριστερά στο παράδειγμα). Αυτό γίνεται με τη μάσκα να έχει 1 στη θέση όλων των κοινών bits ανώτερης τάξεως και 0 στη θέση των μη κοινών κατώτερης τάξεως που-προσδιορίζουν τον ξενιστή, π.χ. 1111 1111 1111 1111 1111 0000 0000 0000. Δηλαδή, η ουσιαστική πληροφορία της μάσκας είναι σε ποιο σημείο σταματούν οι άσοι και αρχίζουν τα μηδενικά. (Αυτή η πληροφορία ήταν σταθερή στην κάθε κλάση και φαινόταν στα πρώτα bits της

κάθε διεύθυνσης, αλλά τώρα αυτές οι 3 τυποποιημένες κλάσεις δεν αρκούν).

Για να υλοποιηθεί η αταξική δρομολόγηση χρειάζονταν δύο ακόμη στοιχεία:

Πρώτον, να εμπλουτισθούν οι δρομολογητές, ώστε να αναζητούν διευθύνσεις στους πίνακες με βάση όχι μόνο τη διεύθυνση των 32 ψηφίων, αλλά και τη μάσκα. Η αναζήτηση μάλιστα βελτιώθηκε, ώστε να μπορεί να γίνεται με βάση το μακρύτερο ταίριασμα ψηφίων από αριστερά της διεύθυνσης (longest address match), ώστε όσο πιο πολλά ψηφία ταιριάζουν με την καταχώριση του πίνακα, τόσο το καλύτερο.

Δεύτερον, να εμπλουτισθούν τα πρωτόκολλα ανταλλαγής πληροφοριών δρομολόγησης μεταξύ των δρομολογητών, ώστε να μεταφέρουν και τις μάσκες εκτός από τις διευθύνσεις. Αυτό έγινε με το OSFP, το RJP-2 και το BGP version 4. Έχοντας εφοδιασθεί με όλα αυτά τα στοιχεία το IPv4 μπορεί ακόμη να χρησιμοποιεί τις διευθύνσεις 32 bits, αλλά καθίσταται πολύπλοκο και βαρύ όσο οι IP διευθύνσεις αυξάνουν.

Ας δούμε ένα παράδειγμα. Έστω ένας πάροχος (ISP) που πήρε 16 διαδοχικές διευθύνσεις class C με το μπλοκ 194.0.16.0 έως 194.0.31.255. Η καταχώριση που αντιστοιχεί στους πίνακες θα είναι μόνο η: 194.0.16.0 με μάσκα 255.255.240.0. Εάν αναζητείται η διεύθυνση του ξενιστή 194.0.22.44, θα αναζητηθεί το ταίριασμα των αριστερών ψηφίων και θα ευρεθεί η καταχώριση: 194.0.16.0 που οδηγεί στη σωστή πόρτα.

Το πρωτόκολλο IPv4 γνώρισε τεράστια εξάπλωση και αυτή ακριβώς είναι η αιτία της αντικατάστασής του. Η εξάντληση του χώρου διευθύνσεων, λόγω της ραγδαίας διάδοσης του IPv4, ήταν αναπόφευκτη. Το IPv6 έρχεται να λύσει το πρόβλημα αυτό και να

μας δώσει νέα χαρακτηριστικά. Το πρωτόκολλο έχει εγκατασταθεί ως αναβάθμιση λογισμικού στις περισσότερες συσκευές και λειτουργικά συστήματα. Σε κάθε νέο σύστημα, hardware ή λειτουργικό σύστημα, το IPv6 υποστηρίζεται συνήθως και χρειάζεται μόνο την ενεργοποίηση ή ρύθμισή του. Επί του παρόντος, διαθέσιμοι μηχανισμοί επιτρέπουν τη μετάβαση βήμα προς βήμα στο IPv6, χωρίς να δημιουργείται πρόβλημα στην τρέχουσα IPv4 υποδομή.

1.5 **Γιατί χρειαζόμαστε το** IPv6;

Εξάντληση διευθύνσεων IPv4.

Για ιστορικούς λόγους, οι οργανισμοί και οι κυβερνητικές υπηρεσίες στις Ηνωμένες Πολιτείες χρησιμοποιούν περίπου το 60% του χώρου διευθύνσεων IPv4. Το υπόλοιπο 40% μοιράζεται με τον υπόλοιπο κόσμο. Από τα 6,4 δισεκατομμύρια ανθρώπους στον κόσμο, περίπου 330 εκατομμύρια ζουν στη Βόρεια Αμερική, 807 εκατομμύρια στην Ευρώπη και 3,6 δισ. Ασία. Αυτό σημαίνει ότι το 5% του πληθυσμού, που ζει στις Ηνωμένες Πολιτείες, χρησιμοποιεί 60% των διατιθέμενων στο χώρο διευθύνσεων. Από τα 3,6 δισεκατομμύρια ανθρώπους που ζουν στην Ασία, περίπου 364 εκατομμύρια έχουν πρόσβαση στο Διαδίκτυο, και ο ρυθμός ανάπτυξης είναι εκθετικός. Αυτό εξηγεί το λόγο για τον οποίο η χρήση του IPv6 στην Ασία είναι μεγαλύτερη από ότι στην Ευρώπη και τις Ηνωμένες Πολιτείες (όλα τα στατιστικά στοιχεία βασίζονται σε αριθμούς μετρήσεις του 2005).

Την ευθύνη για τη διανομή των διευθύνσεων IP σε παγκόσμιο επίπεδο έχει η Internet Assigned Numbers Authority (IANA), καθώς και πέντε περιφερειακά μητρώα του Internet (RIR), που είναι υπεύθυνα στις καθορισμένες περιοχές τους για την εκχώρηση

διευθύνσεων στους τελικούς χρήστες, στις τοπικές κρατικές γραμματείες Internet και στους παρόχους υπηρεσιών Διαδικτύου.

Στις 31 Ιανουαρίου 2011 ο IANA ανακοίνωσε την εξάντληση των διευθύνσεων του, ο RIR APNIC στις 15 Απριλίου 2011 και ο RIPE NCC στις 14 Σεπτεμβρίου 2012 επίσης. Οπότε, σε ορισμένα μέρη του κόσμου έχουν ήδη εξαντληθεί οι IPv4 διευθύνσεις που είναι διαθέσιμες προς κατανομή και οι διευθύνσεις των υπολοίπων περιφερειακών μητρώων RIR αναμένεται να εξαντληθούν πολύ σύντομα.

Το IPv4 παρέχει περίπου 4,29 δισεκατομμύρια διευθύνσεις. Από αυτές, έχουν δοθεί πακέτα των 16,8 εκατομμύριων διευθύνσεων σε κάθε περιφερειακό μητρώο internet (RIR). Η ανησυχία εξάντλησης των IPv4 διευθύνσεων πρωτοεμφανίστηκε τη δεκαετία του 1980, όταν το Διαδίκτυο άρχισε να εξαπλώνεται δραματικά. Η Internet Engineering Task Force (IETF) δημιούργησε το Routing and Addressing Group (ROAD) το Νοέμβριο του 1991 για την αντιμετώπιση του προβλήματος που προκλήθηκε από την επεκτασιμότητα του δικτύου. Η αναμενόμενη έλλειψη έγινε ο κινητήριος μοχλός για τη δημιουργία και την έγκριση πολλών νέων τεχνολογιών, συμπεριλαμβανομένων της αταξικής δρομολόγησης (CIDR) το 1993, της μετάφρασης διευθύνσεων δικτύου (NAT) και του IPv6 το 1998.

Παρά το γεγονός ότι η αρχική πρόβλεψη εξάντλησης των διευθύνσεων τοποθετούνταν το 2008, οι περισσότεροι πάροχοι υπηρεσιών Internet και προμηθευτές λογισμικού άρχιζαν μόλις τότε την εισαγωγή του IPv6 στα συστήματά τους.

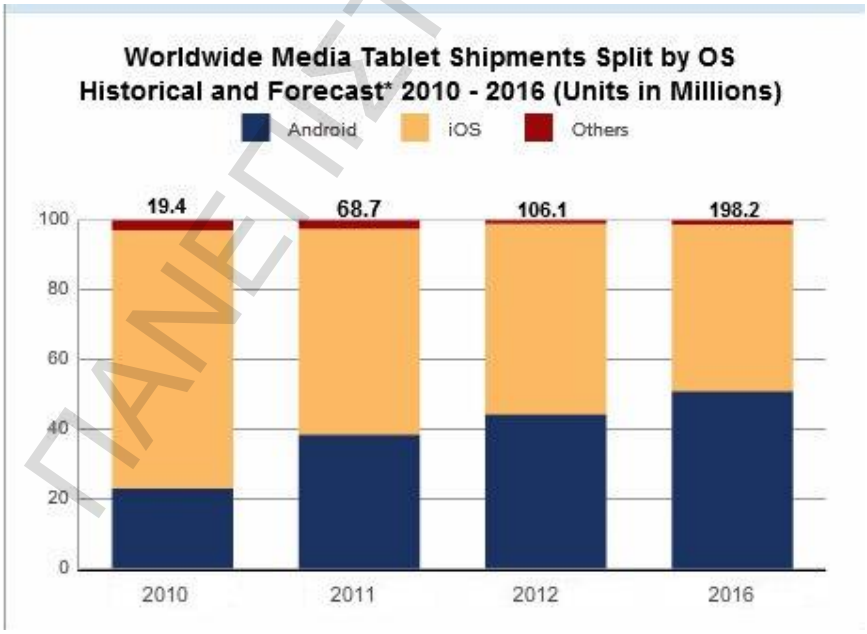
Ο πρωταρχικός λόγος της εξάντλησης των IPv4 διευθύνσεων είναι ο ανεπαρκής σχεδιασμός της αρχικής υποδομής του Διαδικτύου. Ορισμένοι οργανισμοί έχουν λάβει μπλοκ διευθύνσεων πολύ μεγαλύτερο από ότι χρειάζονται και όσες διευθύνσεις τους

περισσεύουν θα μπορούσαν να χρησιμοποιηθούν αλλού. Εάν ήταν δυνατή η ανακατανομή των διευθύνσεων IPv4, θα μπορούσε να υλοποιηθεί μια αποτελεσματική κατανομή. Αυτή δεν είναι εφικτή, αφού μια παγκόσμια ανακατανομή και αναρίθμηση είναι πρακτικά αδύνατη. Παράλληλα, πρέπει να επισημάνουμε το γεγονός ότι σήμερα, που οι διευθύνσεις IPv4 εξαντληθήκαν, μόνο περίπου 14% του παγκόσμιου πληθυσμού έχει πρόσβαση στο Internet.

Ωστόσο, υπάρχουν πολλοί επιπλέον παράγοντες που οδήγησαν στην όξυνση του προβλήματος. Κάθε ένας από αυτούς αύξησε τη ζήτηση για την παροχή διευθύνσεων, συχνά με τρόπους απροσδόκητους από την αρχική σχεδίαση του δικτύου.

Οι Κινητές συσκευές

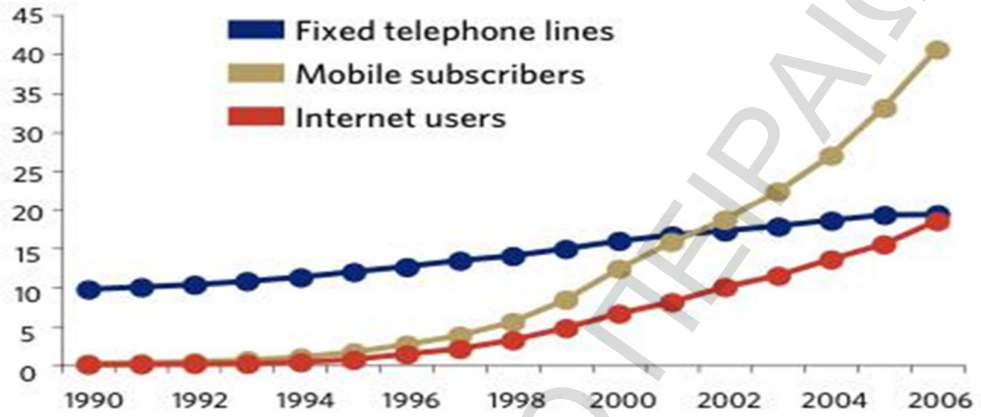
Πλέον τα smartphones – tablets κατέχουν πολύ μεγάλο κομμάτι της αγοράς. Στον παρακάτω πίνακα μπορούμε να δούμε πόσα εκατομμύρια tablets ανά λειτουργικό σύστημα πουλήθηκαν παγκοσμίως το 2010 & το 2011, καθώς και τις προβλέψεις αντίστοιχα για το 2012 και 2016.



Πίνακας 1

Στις προδιαγραφές του αναπτυσσόμενου δικτύου 4G της κινητής τηλεφωνίας απαιτείται IPv6 τεχνολογία καθώς είναι προαπαιτούμενο στις LTE συνδέσεις.

Οι συνδέσεις που είναι πάντα ενεργές (ADSL, VDSL, Fixed Lines)



Από τις αρχές της δεκαετίας του 1990, ο συνηθέστερος τρόπος πρόσβασης στο Διαδίκτυο των καταναλωτών ήταν τα dial-up modem. Η ταχεία ανάπτυξη των dial-up δικτύων οδήγησε σε αυξημένα ποσοστά κατανάλωσης διευθύνσεων, αλλά αφού δεν ήταν πάντα ενεργές μπορούσαμε να μοιράσουμε μια ομάδα IP διευθύνσεων, σε μια μεγαλύτερη βάση πελατών. Από το 2007, ωστόσο, η ευρυζωνική πρόσβαση στο Διαδίκτυο έχει αρχίσει να υπερβαίνει το 50% διείσδυσης σε πολλές αγορές. Οι ευρυζωνικές συνδέσεις είναι πάντα ενεργές, έτσι οι ανάγκες IP διευθύνσεων πολλαπλασιάστηκαν.

Δημογραφικοί λόγοι

Υπάρχουν εκατοντάδες εκατομμύρια νοικοκυριά στον ανεπτυγμένο κόσμο. Το 1990, μόνο ένα μικρό ποσοστό από αυτά είχαν σύνδεση στο Διαδίκτυο. Ακριβώς 15 χρόνια μετά, σχεδόν οι μισοί από αυτούς απέκτησαν συνεχείς συνδέσεις ευρείας ζώνης. Οι πολλοί νέοι χρήστες του Διαδικτύου από σταθερά ή κινητά μέσα σε

ηπείρους όπως η Ασία και σε χώρες όπως η Κίνα και η Ινδία έχουν επίσης οδηγήσει στην εξάντληση των διευθύνσεων. Σύμφωνα με τα Ηνωμένα Έθνη, πάνω από το 40% του πληθυσμού της γης έχει κινητό τηλέφωνο και οι χρήστες του Internet έχουν πολλαπλασιαστεί την τελευταία 15ετία.

Ο αναποτελεσματικός διαμοιρασμός των IP **διευθύνσεων**.

Στη δεκαετία του 1980 διανεμήθηκαν πολύ περισσότερες διευθύνσεις IP σε οργανισμούς από όσες πραγματικά χρειαζόντουσαν, λόγω ανεπάρκειας της μεθόδου κατανομής. Για παράδειγμα, σε μεγάλες εταιρείες ή πανεπιστήμια δόθηκαν μπλοκ διευθύνσεων κατηγορίας Α, με πάνω από 16 εκατομμύρια διευθύνσεις IPv4 η κάθε μία, επειδή η αμέσως μικρότερη μονάδα κατανομής, ένα μπλοκ κατηγορίας Β με 65536 διευθύνσεις, ήταν πάρα πολύ μικρό για τη χρήση που προοριζόταν. Πολλοί οργανισμοί, επίσης, εξακολουθούν να χρησιμοποιούν δημόσιες διευθύνσεις IP (public) για συσκευές οι οποίες δεν είναι προσβάσιμες εκτός του τοπικού δικτύου τους.

Αν θέλουμε να παρέχουμε πρόσβαση στο Internet μόνο στο 20% του παγκόσμιου πληθυσμού, θα χρειαστεί ο χώρος διευθύνσεων που το IPv6 δύναται να δώσει. Ο υπολογισμός αυτός δε λαμβάνει υπόψη το γεγονός ότι στο μέλλον θα χρειαστούμε τις διευθύνσεις IP για δισεκατομμύρια συσκευές. Οι προμηθευτές σε όλες τις βιομηχανίες αναπτύσσουν συστήματα παρακολούθησης, έλεγχου και διαχείρισης που βασίζονται στο IPv6.

Η ομάδα εργασίας του IPv6 έχει να κάνει πολλά περισσότερα από την επέκταση του χώρου διευθύνσεων. Για πολλά πολύπλοκα δίκτυα του σήμερα και του αύριο, και για τον αριθμό των συσκευών IP, η δυνατότητα αυτόματης διαμόρφωσης του IPv6 θα είναι μια αναγκαιότητα. Η διαχείριση των εν λόγω υπηρεσιών δεν μπορεί να επιτευχθεί με τις παραδοσιακές μεθόδους διευθυνσιοδότησης, και η

αυτόματη ρύθμιση αυτής θα συμβάλει στη μείωση του διαχειριστικού κόστους για τους οργανισμούς.

Ο εκτεταμένος χώρος διευθύνσεων και η αποκατάσταση του αρχικού μοντέλου από άκρο σε άκρο του Διαδικτύου, επιτρέπει την εξάλειψη του Network Address Translation (NAT), στο οποίο μία μόνο ή μερικές δημόσιες διεύθυνση (εις) IPv4 χρησιμοποιούνται για τη σύνδεση ενός υψηλού αριθμού χρηστών με ιδιωτικές διευθύνσεις στο Διαδίκτυο με την αντιστοίχηση των πολλών αυτών εσωτερικών διευθύνσεων σε μία ή κάποιες περισσότερες δημόσιες διευθύνσεις. Το NAT εμφανίστηκε ως βραχυπρόθεσμη λύση για την επίλυση του περιορισμού του χώρου διευθύνσεων του IPv4, δεδομένου ότι το IPv6 δεν ήταν έτοιμο ακόμα (αναφέρεται στο RFC 1631 ενώ η αρχική προδιαγραφή του NAT γίνεται στο RFC 3022 το 2001). Το NAT είναι αρκετά κοινό σε δίκτυα IPv4, αλλά έχει σοβαρά μειονεκτήματα όσον αφορά τη διαχείριση και τη λειτουργία, αφού για να κάνουμε την αντιστοίχιση διεύθυνσης, το NAT τροποποιεί την κεφαλίδα της διεύθυνσης IP. Υπάρχει ένας μακρύς κατάλογος των πρωτοκόλλων και εφαρμογών που δημιουργούν προβλήματα όταν χρησιμοποιούνται σε ένα περιβάλλον NAT. Το IPsec και οι peer-to-peer εφαρμογές είναι τα δύο πιο γνωστά παραδείγματα. Η εξάλειψη του προβλήματος του περιορισμένου χώρου διευθύνσεων με το IPv6, που παράλληλα ήταν και ο βασικός λόγος δημιουργίας του NAT, οδήγησε στο να μην υποστηρίζεται το NAT στο σχεδιασμό του IPv6.

Με την εισαγωγή μιας πιο ευέλικτης δομής της κεφαλίδας (extension header), το πρωτόκολλο έχει σχεδιαστεί ώστε να είναι ανοικτό και επεκτάσιμο. Στο μέλλον, νέες επεκτάσεις θα μπορούν εύκολα να προσδιοριστούν και να συμπεριληφθούν σε αυτό το πρωτόκολλο. Η ανάπτυξη του IPv6 βασίστηκε στο γεγονός ότι το IPv4 ήταν σε χρήση για σχεδόν 30 χρόνια, ώστε να δημιουργήσει ένα επεκτάσιμο μοντέλο, το οποίο θα μπορεί να καλύψει τις ανάγκες για μεγάλο χρονικό διάστημα.

Τα ποσοστά ευρυζωνικής διείσδυσης σε χώρες όπως η Νότια Κορέα, Ιαπωνία, Γερμανία, Γαλλία, και οι Ηνωμένες Πολιτείες συνεχίζουν να αυξάνονται και, σε ορισμένες περιπτώσεις, έχουν φτάσει το 65% ή περισσότερο. Αυτό το επίπεδο της πάντα “online” σύνδεσης, με σημαντικό εύρος μεταγωγής δεδομένων, (σε σύγκριση με τις dial-up συνδέσεις) σημαίνει ότι υπάρχει μεγαλύτερη δυνατότητα σύνδεσης για συσκευές. Πολλοί κατασκευαστές καταναλωτικών ηλεκτρονικών έχουν επωφεληθεί από αυτό.

Το online gaming είναι πλέον η μόνη αρμοδιότητα των παιχνιδιών για υπολογιστές. Κονσόλες παιχνιδιών, όπως το PlayStation 3 της Sony, το Nintendo DS και το Xbox της Microsoft, έχουν προσθέσει δυνατότητες για απευθείας σύνδεση στο Internet. Πολλοί φορείς τηλεπικοινωνιών παρέχουν τηλεοπτικές υπηρεσίες (ταινίες, ηχητικό υλικό, κλπ.) πάνω από τα IP δίκτυα τους. Μπορούν να συνδεθούν ακόμα και συσκευές, όπως ψυγεία, φούρνοι, θερμοσίφωνες και μπανιέρες. Αρχικά μπορεί να φαίνεται κάπως ανόητη η σύνδεση μιας μπανιέρας στο δίκτυο, όμως πολλές από αυτές τις συσκευές συνδέονται για τη διευκόλυνση διαδικασιών, όπως η διαχείριση τροφοδοσίας, ο απομακρυσμένος έλεγχος για την αντιμετώπιση προβλημάτων και για σκοπούς τηλεμετρίας/ παρακολούθησης. Το τελικό αποτέλεσμα θα είναι ένας μεγάλος αριθμός συσκευών να συνδέονται με το δίκτυο χάρη στην ευρύτητα των διευθύνσεων IPv6. Αυτό, σε συνδυασμό με χαρακτηριστικά όπως το Neighbor Discovery, η αυτόματη διαμόρφωση και το Mobile IPv6, θα εγκαινιάσουν μια νέα εποχή μηχανοργάνωσης στο σπίτι, αλλά χωρίς το τεράστιο πονοκέφαλο ανάπτυξής της που θα προκαλούσε, αν επιχειρούνταν με το ισχύον πρωτόκολλο το IPv4.

Η ανάπτυξη της ασύρματης βιομηχανίας (τόσο της κινητής τηλεφωνίας όσο και των ασύρματων δικτύων που βασίζονται σε πρωτόκολλα όπως 802.11x, 802,16, 802,20, UMTS, UWB, MIMO, κλπ.) είναι αλματώδης. Σε ορισμένες χώρες, όπως η Ιταλία και η

Μεγάλη Βρετανία, ο αριθμός των κινητών τηλεφώνων, στην πραγματικότητα, υπερβαίνει τον αριθμό των ατόμων. Σε αυτόν τον κόσμο της συνεχούς προσβασιμότητας και της ανάγκης πρόσβασης στην πληροφορία ανά πάσα στιγμή, το «mobility» των υπηρεσιών είναι εξαιρετικά σημαντικό για τους τελικούς χρήστες. Από την πλευρά τους οι πάροχοι, ιδίως εκείνοι που υποστηρίζουν πολλαπλούς τύπους πρόσβασης στα μέσα (π.χ. 3G και WiMax), αξιοποιούν την IP ως μέθοδο μεταφοράς και δρομολόγησης. Τα κινητά τηλέφωνα, τα PDAs και τα smartphones έχουν πρόσβαση ήδη στο Internet, πραγματοποιούν τηλεφωνικές κλήσεις, video-κλήσεις και έχουν ροή περιεχομένου βίντεο. Έτσι, αντί να υποστηριχθούν όλες αυτές οι λειτουργίες με διαφορετικά πρωτόκολλα μεταφοράς και να δημιουργηθούν ενδιάμεσες εφαρμογές ώστε να επιτευχτεί η επικοινωνία μεταξύ τους, είναι πολύ πιο αποδοτικό να αξιοποιηθεί το ήδη υπάρχον δίκτυο υποδομής του Διαδικτύου και των δικτύων των εταιρειών. Το mobile IPv6 σχεδιάστηκε και δημιουργήθηκε για να υποστηρίξει το Mobility με έναν εξαιρετικά αποτελεσματικό τρόπο για το χρήστη, έτσι ώστε όταν μετακινείται μεταξύ δικτύων, να μπορεί ανά πάσα στιγμή να διατηρεί τη σύνδεσή του.

Για πολλούς από τους προαναφερθέντες λόγους, μεγάλο μέρος του κόσμου έχει ήδη υιοθετήσει το IPv6. Υπάρχει σημαντική υιοθέτηση στην Ιαπωνία και την Κορέα, με παραγωγικά δίκτυα και καταναλωτές να πληρώνουν για υπηρεσίες με βάση το IPv6. Η Κίνα δαπανά εκατομμύρια δολάρια (USD) για την ανάπτυξη ενός νέου κορμού δικτύου που πρόκειται να είναι IPv6 . Η Ευρωπαϊκή Ένωση (ΕΕ) έχει ξοδέψει εκατομμύρια για την έρευνα και την ανάπτυξη IPv6 δικτύων κορμού και καινοτόμες υπηρεσίες που αξιοποιούν τις δυνατότητές του. Η Ινδία, με μια αυξανόμενη μεσαία τάξη και μια ισχυρή παρουσία στον κόσμο της πληροφορικής, έχει επιδείξει σημαντικό ενδιαφέρον στην ανάπτυξη και τη χρήση του IPv6. Τον Ιούνιο του 2003 και στη συνέχεια τον Ιούλιο του 2005, η

Αμερικανική κυβέρνηση προχώρησε στην υιοθέτηση του IPv6. Άλλες χώρες όπως η Αυστραλία, η Ταϊβάν, η Σιγκαπούρη, η Αγγλία και η Αίγυπτος έχουν κάνει παρόμοιες ανακοινώσεις.

Εξακολουθούν ακόμα να υπάρχουν κάποια ερωτήματα σχετικά με την επιχειρησιακή αξία του IPv6 και κάθε οργανισμός οφείλει να αξιολογήσει τα οφέλη προσεκτικά για τη δική του εσωτερική χρήση και να καθορίσει τον καλύτερο χρόνο για την μετάβασή του σε αυτό. Σε πολλές περιπτώσεις, οι οργανισμοί μπορούν να βρουν έξυπνους τρόπους για να χρησιμοποιούν το IPv6 για να λύσουν «επίπονα» θέματα, χωρίς να χρειαστεί να αλλάξουν ολόκληρο το δίκτυο τους.

Παράλληλα με όλες αυτές τις σκέψεις και τις εκτιμήσεις, ας μη λησμονούμε και το πιο βασικό πλεονέκτημα του IPv6. Με τη νέα δομή και τις επεκτάσεις του, το IPv6 παρέχει τα θεμέλια για μια νέα γενιά υπηρεσιών. Θα υπάρξουν συσκευές και υπηρεσίες στην αγορά στο εγγύς μέλλον, που δε θα μπορούν να αναπτυχθούν με το IPv4. Αυτό ανοίγει νέες αγορές και επιχειρηματικές ευκαιρίες, τόσο για τους πωλητές, όσο και για τους παρόχους υπηρεσιών. Ο κύκλος ζωής πολλών προϊόντων και υπηρεσιών θα επεκταθεί, ανανεώνοντας την τεχνολογία τους με το IPv6. Από την άλλη πλευρά, αυτό σημαίνει ότι οι οργανισμοί και οι χρήστες θα απαιτήσουν τέτοιου είδους υπηρεσίες στο μεσοδιάστημα. Επομένως, είναι σκόπιμο η ενσωμάτωση του νέου πρωτόκολλου να γίνει προσεκτικά, με ένα βήμα τη φορά για να προετοιμαστεί η υποδομή για τις νέες αυτές υπηρεσίες. Με αυτό τον τρόπο, θα προστατευτούμε από την υποχρέωση της υλοποίησης σημαντικών επιχειρηματικών εφαρμογών βασισμένων στο IPv6, με ελάχιστο χρόνο στη διάθεσή μας για σωστό προγραμματισμό, κάτι που φυσικά, θα αύξανε αδικαιολόγητα το κόστος.

1.6 **Οι βελτιώσεις που εισάγει το** IPv6.

Ας περάσουμε λοιπόν στις πρακτικές βελτιώσεις που συνιστά το IPv6. Η μορφή διεύθυνσης επεκτάθηκε από 32 bits σε 128 bits. Αυτό παρέχει μια διεύθυνση IP για κάθε κόκκο άμμου στον πλανήτη. Επιπλέον, επιτρέπει την ιεράρχηση της δομής του χώρου της διεύθυνσης, προς όφελος της βελτιστοποίησης της παγκόσμιας δρομολόγησης.

Αρχικά, στο IPv4, το ελάχιστο μήκος της κεφαλίδας είναι 20 bytes και το μέγιστο 60 bytes. Στο IPv6 αποκτά σταθερό μήκος 40 bytes, κάτι που θα διευκολύνει την κατασκευή ολοκληρωμένων κυκλωμάτων γρήγορης δρομολόγησης. Τα πρόσθετα πεδία που απαιτούνται για καινούργιες λειτουργίες μπαίνουν σε νέες προαιρετικές επικεφαλίδες (extension headers) που ακολουθούν την βασική επικεφαλίδα.

Επιπλέον, το πεδίο Header Checksum αφαιρέθηκε για να βελτιωθεί η ταχύτητα επεξεργασίας. Οι δρομολογητές δε χρειάζεται να ελέγξουν και να ενημερώσουν τα αθροίσματα και έτσι η επεξεργασία γίνεται πολύ πιο γρήγορα. Την εποχή που αναπτύχθηκε το IPv4, το checksumming σε επίπεδο πληροφορίας δεν ήταν κοινό και το άθροισμα ελέγχου πεδίου στην κεφαλίδα IPv4 είχε νόημα. Σήμερα, ο κίνδυνος για απαρατήρητα λάθη και για λάθος δρομολογημένα πακέτα είναι ελάχιστος. Επίσης, υπάρχει ένα πεδίο ελέγχου στο επίπεδο μεταφοράς (UDP και TCP). Με το IPv4 ο UDP έλεγχος είναι προαιρετικός, ενώ με το IPv6 είναι υποχρεωτικός.

Κατ' επέκταση, εισάγεται ο προσδιορισμός ροών κίνησης (traffic flows), για να μπορούν να προσδιορίζονται ειδικές τεχνικές απόρριψης ανάλογα με τη ροή, ώστε να μπορούν να υποστηριχθούν διαφορετικές υπηρεσίες πραγματικού χρόνου (π.χ. φωνή, βίντεο).

Επιπροσθέτως, εισάγονται εργαλεία αυθεντικοποίησης και κρυπτογράφησης (authentication and encryption) για υποστήριξη ασφάλειας στο επίπεδο δικτύου (σήμερα αυτό γίνεται μόνο στο επίπεδο εφαρμογής). Έτσι, θα μπορούν να δημιουργηθούν νοητά ασφαλή υποδίκτυα μέσα στο Διαδίκτυο.

Εν κατακλείδι, θα πρέπει να αναφερθεί ότι έχει γίνει μεγάλη προσπάθεια απλοποίησης της επεξεργασίας που πρέπει να κάνουν οι δρομολογητές, ώστε να μπορούν πολλές λειτουργίες να γίνονται με ολοκληρωμένα κυκλώματα και όχι με λογισμικό. Οι διευθύνσεις αποδίδονται στις διεπαφές και όχι στους κόμβους. Οι μεγάλες διευθύνσεις του IPv6, σε συνδυασμό με τις διαφορετικές διευθύνσεις σε κάθε διεπαφή του δρομολογητή, επιτρέπουν μικρότερους πίνακες στους δρομολογητές. Αυτή η φαινομενική αντίφαση εξηγείται διότι επιτρέπει την ομαδοποίηση διευθύνσεων σε ιεραρχημένες δομές κατά γεωγραφική ή διοικητική (δηλ. ανά πάροχο υπηρεσίας). Έτσι, ομάδες διευθύνσεων αντιπροσωπεύονται από μία καταχώριση στον πίνακα δρομολόγησης. Ομοίως, η ύπαρξη διαφορετικής διεύθυνσης σε κάθε διεπαφή, επιτρέπει να ομαδοποιηθεί ο κόμβος κάτω από την ομαδική διεύθυνση του κάθε παρόχου υπηρεσιών, αλλιώς θα έπρεπε να καταχωρηθεί χωριστά η διεύθυνσή του.

Autoconfiguration

Ίσως το πιο ενδιαφέρον νέο χαρακτηριστικό του IPv6 που διαφοροποιείται κατά πολύ από το IPv4, είναι ο μηχανισμός αυτόματης διαμόρφωσης του. Όταν μια συσκευή εκκινεί στον IPv6 κόσμο, ζητά το πρόθεμα δικτύου της. Ο IPv6 δρομολογητής που συνδέεται της δίνει ένα ή περισσότερα προθέματα δικτύου. Χρησιμοποιώντας αυτό ή τα προθέματα αυτά, η συσκευή μπορεί αυτόματα να δεσμεύει μία ή περισσότερες έγκυρες παγκόσμιες διευθύνσεις IP, χρησιμοποιώντας για αναγνωριστικό την MAC

διεύθυνσή* της ή έναν τυχαίο δικό της αριθμό για να οικοδομήσουμε μια μοναδική διεύθυνση IP. Στο IPv4 αντιθέτως, η εκχώρηση μοναδικής διεύθυνσης IP σε κάθε συσκευή, γίνεται είτε με χειροκίνητη ρύθμιση είτε με τη χρήση DHCP.

Η αυτόματη ρύθμιση των συσκευών μέσω του πρωτοκόλλου IPv6 θα κάνει τη ζωή των διαχειριστών δικτύου ευκολότερη και θα επιφέρει σημαντική μείωση του κόστους για τη διαχείριση των νέων δικτύων IP. Επιπλέον, αν φανταστούμε τον αριθμό των συσκευών που μπορεί να έχουμε στα σπίτια μας στο μέλλον, ο οποίος θα χρειάζεται μια διεύθυνση IP για να συνδεθεί στο δίκτυο, το χαρακτηριστικό αυτό γίνεται απαραίτητο. Αν αγοράζαμε μια νέα τηλεόραση στο σπίτι θα έπρεπε είτε να της αποδίδαμε διεύθυνση IP με το χέρι είτε να είχαμε έναν DHCP server με το IPv4. Αλλά με το χαρακτηριστικό της αυτόματης διαμόρφωσης του IPv6, πλέον η σύνδεση είναι εύκολη, σαν αυτή των φορητών συσκευών, πχ ενός κινητού τηλεφώνου ή ενός υπολογιστή χειρός, όταν μετακινούνται από δίκτυο σε δίκτυο.

* Διεύθυνση MAC

Μια διεύθυνση Media Access Control (διεύθυνση MAC) είναι ένας δεκαεξαδικός σειριακός αριθμός (ως προς την αναπαράσταση), ο οποίος είναι μοναδικός για κάθε δικτυακή συσκευή. Ο αριθμός έχει τη μορφή xx:xx:xx:xx:xx:xx, για παράδειγμα 0A:12:A1:B2:AE:04 για την 16-δική αναπαράσταση. Η διεύθυνση MAC χρησιμοποιείται για την επικοινωνία μεταξύ των δικτυακών συσκευών εντός ενός τοπικού δικτύου. Σε κάθε επικοινωνία οποιασδήποτε δικτυακής συσκευής με μια άλλη, ο αριθμός αυτός αποκαλύπτεται από τον αποστολέα (source) στον παραλήπτη (destination).

Διαλειτουργικότητα

Το IPv6 και IPv4 θα συνυπάρξουν για πολλά χρόνια, και υπάρχει ένα ευρύ φάσμα τεχνικών που κάνουν τη συνύπαρξη αλλά κυρίως τη μετάβαση στο IPv6 εύκολη και επιτυχημένη. Οι τεχνικές αυτές χωρίζονται σε τρεις βασικές κατηγορίες:

Dual-stack τεχνικές.

Αυτές οποίες επιτρέπουν στα IPv4 και IPv6 να συνυπάρχουν στις ίδιες συσκευές και δίκτυα.

Tunneling τεχνικές

Με αυτές επιτυγχάνεται η μεταφορά της κίνησης δεδομένων IPv6 πάνω από την υπάρχουσα IPv4 υποδομή.

Translation τεχνικές:

Μέσω αυτών επιτυγχάνεται η επικοινωνία μεταξύ IPv6 και IPv4 κόμβων.

Οι τεχνικές αυτές μπορούν να χρησιμοποιηθούν και σε συνδυασμό μεταξύ τους. Η μετάβαση στο IPv6 μπορεί να γίνει βήμα-βήμα, αρχίζοντας με ένα μόνο ξενιστή ή υποδίκτυο. Μπορεί το εταιρικό μας δίκτυο ή τμήματά του να λειτουργούν στο Ipv6 πρωτόκολλο, ενώ ο ISP μας να εξακολουθεί να είναι στο IPv4, ή ο ISP μας να αναβαθμιστεί σε IPv6, ενώ το εταιρικό μας δίκτυο να είναι ακόμα στο IPv4.

1.7 **Το** Mobile IPv6

Το Mobile IPv6 είναι ένα πρωτόκολλο που επιτρέπει σε ένα κινητό host να μετακινείται από το ένα δίκτυο στο άλλο χωρίς να χάνει τις συνδέσεις του, ορίζεται στο RFC 3775 και είναι μια από τις τεράστιες βελτιώσεις που εισάγει το IPv6. Αξίζει συνεπώς να δούμε τον τρόπο λειτουργίας του.

Η περισσότερη κίνηση στο Internet χρησιμοποιεί TCP συνδέσεις. Μια σύνδεση TCP καθορίζεται από το συνδυασμό της διεύθυνσης IP και τον αριθμό θύρας των δύο τελικών σημείων της σύνδεσης. Αν κάποιος από αυτούς τους τέσσερις αριθμούς αλλάξει, η επικοινωνία διακόπτεται και πρέπει να αποκατασταθεί. Εάν ένας κινητός host συνδέεται από διαφορετικό σημείο πρόσβασης στο δίκτυο, χρειάζεται μια νέα διεύθυνση IP κάθε φορά. Το Mobile IP αντιμετωπίζει την πρόκληση της μεταφοράς ενός host σε ένα διαφορετικό σημείο σύνδεσης χωρίς αλλαγή της IP διεύθυνσης του με την ανάθεση στον κινητό κόμβο δύο διαφορετικών διευθύνσεων IP. Η μία είναι η «διεύθυνση του σπιτιού» (home address), η οποία είναι στατική και δεν αλλάζει και συνεπώς, χρησιμοποιείται για να προσδιορίσει τη σύνδεση TCP. Η δεύτερη διεύθυνση IP, η οποία ονομάζεται «care-of» διεύθυνση, αλλάζει ανάλογα με το δίκτυο στο οποίο ο host είναι συνδεμένος. Έτσι, αυτό λειτουργεί εντός ομοιογενών δικτύων (εάν ο host συνδέεται από έναν Ethernet κόμβο σε έναν άλλο Ethernet κόμβο) αλλά και σε ετερογενή δίκτυα (περίπτωση μετακίνησης του host από Ethernet κόμβο σε ασύρματο LAN κόμβο).

Σε ένα ασύρματο δίκτυο, είμαστε εξοικειωμένοι με την εναλλαγή των IP «handover», όταν μια συσκευή μετακινείται από ένα σημείο πρόσβασης σε ένα άλλο. Αυτή είναι μια μετακίνηση στο επίπεδο σύνδεσης. Το Mobile IPv6 λύνει το ζήτημα του “handover” στο

επίπεδο δικτύου και διατηρεί τις συνδέσεις με εφαρμογές και υπηρεσίες, ακόμα και εάν η συσκευή αλλάζει την προσωρινή IP διεύθυνσή της.

Ακολουθούν κάποιοι όροι που θα χρησιμοποιηθούν για να εξηγήσουν τον τρόπο λειτουργίας του Mobile IPv6.

Διεύθυνση «Home Address»

Είναι η παγκόσμια μοναδική διεύθυνση που ανατίθεται σε έναν κινητό host. Είναι η μόνιμη διεύθυνση του host. Οι μηχανισμοί δρομολόγησης παραδίδουν πακέτα σε αυτή τη διεύθυνση.

Αρχικό πρόθεμα υποδικτύου

Το πρόθεμα του IP υποδίκτυου που αντιστοιχεί στη home address ενός κινητού host.

«Home» σύνδεσμος (link)

Ο σύνδεσμος στον οποίο ορίζεται το πρόθεμα υποδικτύου.

Κινητός host

Ένας host που μπορεί να αλλάξει σημείο πρόσβασης, ενώ εξακολουθεί να είναι προσβάσιμος μέσω της διεύθυνσης «home».

Εξωτερικός κόμβος

Είναι ο κόμβος με τον οποίο ο κινητός host επικοινωνεί. Ο κόμβος αυτός μπορεί να είναι είτε σταθερός είτε κινητός.

Ξένο πρόθεμα υποδικτύου

Κάθε IP πρόθεμα διαφορετικό από το πρόθεμα υποδικτύου της διεύθυνσης «home».

Εξωτερική σύνδεση

Κάθε σύνδεση εκτός αυτής με το «home» κόμβο.

«Care off» διεύθυνση

Μια παγκόσμια unicast διεύθυνση του κινητού host, ενώ είναι σε ξένο δίκτυο (μακριά από το Home δίκτυο). Το πρόθεμα υποδικτύου της care-off διεύθυνσης είναι ξένο πρόθεμα υποδικτύου. Ένας κινητός host μπορεί να έχει πολλαπλές care-off διευθύνσεις. Αυτή που έχει καταχωρηθεί με τη «home» διεύθυνση θα είναι η πρωτεύουσα διεύθυνση.

Μέσο παρακολούθησης «home» (home agent)

Είναι ο router που βρίσκεται στη «home» σύνδεση του κινητού Host και καταχωρείται σε αυτόν η τρέχουσα care-off διεύθυνσή του. Ενώ ο host είναι μακριά από τη «home» σύνδεση, παρακολουθεί τα πακέτα που προορίζονται για τη «home» διεύθυνση του host και φροντίζει να φτάσουν στην «care-off» διεύθυνση.

Binding

Η σχέση της διεύθυνσης «home» με την care-off διεύθυνση, μαζί με την υπόλοιπη διάρκεια της εν λόγω ένωσης.

Καταχώριση (Registration)

Η διαδικασία κατά την οποία ένας κινητός host στέλνει αίτημα (binding update message) στον κόμβο που είναι συνδεδεμένος και προκαλεί μια νέα binding εγγραφή. Η εγγραφή με τον αντίστοιχο κόμβο ονομάζεται Καταχώριση Ανταποκριτή «Correspondent Registration».

Άδεια Binding

Η καταχώριση θα πρέπει να εγκριθεί, έτσι ώστε ο παραλήπτης να διασφαλίσει ότι ο αποστολέας έχει το δικαίωμα να καθορίσει μια νέα biding σύνδεση.

Return routability procedure

Η διαδικασία που πιστοποιεί καταχωρίσεις προερχόμενες από έναν «cryptographic token exchange».

Token παραγωγής κλειδιών

Τυχαίοι αριθμοί χρησιμοποιούνται από τον εξωτερικό κόμβο στη δρομολόγηση «return routability procedure» για να ενεργοποιηθεί ο κινητός host και να δημιουργήσει το απαραίτητο κλειδί για την έγκριση ενός Binding Update.

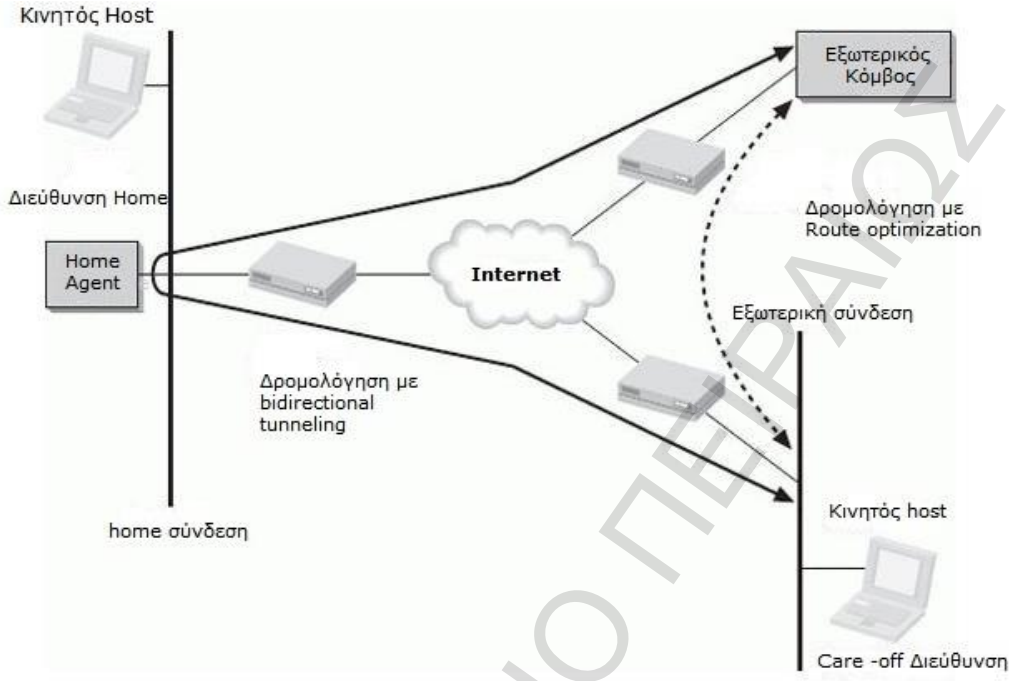
Nonce

Τυχαίοι αριθμοί χρησιμοποιούνται από τον εξωτερικό κόμβο για τη δημιουργία keygen tokens που σχετίζονται με τη δρομολόγηση τύπου «return routability procedure». Οι nonces δεν αφορούν ειδικά ένα μόνο κινητό host και κρατούνται μυστικοί στους εξωτερικούς κόμβους.

Nonce index

Χρησιμοποιείται για να υποδείξει ποιοί nonces αριθμοί έχουν χρησιμοποιηθεί κατά τη δημιουργία keygen τιμών.

1.7.1. **Ο Τρόπος Λειτουργίας του** Mobile IPv6.



Σχήμα 1.5 Ο Τρόπος Λειτουργίας του Mobile IPv6

Η διεύθυνση «home» είναι η διεύθυνση IPv6 μαζί με το πρόθεμα της home σύνδεσης ενός κινητού host. Εφόσον είναι στο σπίτι, λαμβάνει πακέτα μέσω των κανονικών μηχανισμών δρομολόγησης IP και συμπεριφέρεται όπως και κάθε άλλη σταθερή IP σύνδεση. Όταν ο host είναι μακριά από την Home σύνδεση, σε μια εξωτερική σύνδεση, επιπλέον λαμβάνει την care-off διεύθυνση, μέσω κανονικών IPv6 μηχανισμών όπως ο DHCPv6 κατά τη νέα σύνδεση.

Η σχέση της διεύθυνσης home με την care-off διεύθυνση ονομάζεται “binding”. Αν και μακριά από τη home σύνδεση, ο host καταγράφει την care-off διεύθυνσή του σε ένα router στη home σύνδεση, που είναι ο home agent. Για να καταχωρηθεί η care-off διεύθυνσή του, ο host στέλνει ένα αίτημα (binding update message) στο home κόμβο

και αυτός απαντά με αναγνώριση του αιτήματος. Κάθε κόμβος που επικοινωνεί με έναν κινητό κόμβο ονομάζεται εξωτερικός κόμβος.

Υπάρχουν δύο τρόποι για να επικοινωνούν ο εξωτερικός κόμβος με τον κινητό host:

Αμφίδρομη (Bidirectional) Tunneling

Τα πακέτα από τον εξωτερικό κόμβο αποστέλλονται στο home agent, που τα ενθυλακώνει (encapsulation) σε IPv6 πακέτα και τα στέλνει στην care-off address του κινητού host. Τα πακέτα από τον κινητό host αποστέλλονται, μέσω αντίθετης σήραγγας (tunneling), πίσω στο home agent που τα προωθεί στον εξωτερικό κόμβο, μέσω κανονικών μηχανισμών δρομολόγησης. Αυτή η λειτουργία δεν απαιτεί καμία Mobile IPv6 υποστήριξη στον εξωτερικό κόμβο και λειτουργεί χωρίς registration του εξωτερικού κόμβου.

Βελτιστοποίηση διαδρομής (Route optimization).

Με τη μέθοδο αυτή, η επικοινωνία μεταξύ του κινητού κόμβου και κόμβου ανταπόκρισης μπορεί να είναι άμεση, χωρίς να περάσει από το home agent. Αυτό είναι ένα από τα κύρια πλεονεκτήματα του Mobile IPv6 έναντι του IPv4 Mobile, όπου η βελτιστοποίηση διαδρομής δεν είναι δυνατή. Η Βελτιστοποίηση διαδρομής απαιτεί από τον κινητό host να καταχωρεί (registration) την care-off address του κόμβου στον εξωτερικό κόμβο (correspondent registration) και αυτή η σύνδεση να έχει εγκριθεί με τη διαδικασία «Return routability». Ο εξωτερικός κόμβος χρησιμοποιεί μια ειδική κεφαλίδα δρομολόγησης όταν στέλνει πακέτα στο κινητό host άμεσα. Ο κινητός κόμβος χρησιμοποιεί τη home διεύθυνση (που ορίζεται για το Mobile IPv6) κατά την αποστολή πακέτων στον εξωτερικό κόμβο.

Το πλεονέκτημα της βελτιστοποίησης διαδρομής είναι ότι η συντομότερη διαθέσιμη διαδρομή μπορεί να χρησιμοποιηθεί μεταξύ του εξωτερικού κόμβου και του κινητού host και τα πακέτα δεν

πρέπει να περάσουν από το home agent. Αυτό όχι μόνο εξασφαλίζει μικρότερες διαδρομές επικοινωνίας, αλλά ταυτόχρονα μειώνει το φορτίο στο home agent και στη home σύνδεση. Αυτό είναι πολύ σημαντικό όταν μιλάμε για μεγάλο αριθμό κινητών hosts που διαρκώς κινούνται, για παράδειγμα, σε ένα VoIP (Voice over IP) σενάριο.

Το Mobile IPv6 υποστηρίζει, επίσης, τη δυνατότητα να υπάρχουν πολλαπλοί home agents, και ο κινητός host μπορεί να μαθαίνει για την αναδιαμόρφωση της home σύνδεσης ή την αλλαγή της IP διεύθυνση του home agent μέσω του Δυναμικού Πράκτορα Ανακάλυψης Εσωτερικής Διεύθυνσης (Dynamic Home Agent Address Discovery). Αν αλλάξει το πρόθεμα της home σύνδεσης το κινητό, ο host χρησιμοποιεί το μηχανισμό Mobile Prefix Discovery για να μάθει το νέο πρόθεμα.

1.8 **Η εξέλιξη του** IPv6

Πώς φτάσαμε όμως να κάνουμε λόγο για το IPv6; Ξεκινώντας από τα πρωτόκολλα του Διαδικτύου, είναι κοινή παραδοχή ότι είναι τα πιο δημοφιλή ανοικτού συστήματος (μη ιδιόκτητα) πρωτόκολλα στον κόσμο, επειδή μπορούν να χρησιμοποιηθούν για την επικοινωνία μεταξύ οποιουδήποτε συνόλου διασυνδεδεμένων δικτύων και έχουν εξίσου καλά προσαρμοσθεί σε τοπικά (LAN-Local Area Network) και ευρείας (WAN- Wide Area Network) περιοχής δίκτυα. Τα πρωτόκολλα του Διαδικτύου αποτελούνται από μια ακολουθία πρωτόκολλων επικοινωνίας, εκ των οποίων τα δύο πιο γνωστά είναι το πρωτόκολλο ελέγχου μετάδοσης (TCP) και το Internet Protocol (IP) με το οποίο ασχοληθήκαμε ιδιαίτερα στο παρόν κεφάλαιο. Η ακολουθία πρωτοκόλλων του Internet δεν περιλαμβάνει μόνο τα πρωτόκολλα TCP και IP, αλλά καθορίζει επίσης κοινές εφαρμογές

όπως το ηλεκτρονικό ταχυδρομείο, την εξομοίωση τερματικών, και τη μεταφορά αρχείων.

Τα πρωτόκολλα του Διαδικτύου αναπτύχθηκαν για πρώτη φορά στα μέσα της δεκαετίας του 1970, όταν η Defense Advanced Research Projects Agency (DARPA) άρχισε να ενδιαφέρεται για τη δημιουργία ενός δικτύου μεταγωγής πακέτων που θα διευκόλυναν την επικοινωνία μεταξύ ανόμοιων συστημάτων πληροφορικής σε ερευνητικά ιδρύματα. Για το σκοπό αυτό η DARPA χρηματοδότησε μια έρευνα στο Πανεπιστήμιο του Στάνφορντ με σκοπό την ανάπτυξη των πρωτοκόλλων του διαδικτύου, η οποία ολοκληρώθηκε στα τέλη της δεκαετίας του 1970.

Τα πρωτόκολλα διαδικτύου έχουν τρείς εκδόσεις εκ των οποίων δύο είναι οι κύριες και αυτές που βρίσκονται σε χρήση, την IPv4 και την IPv6 για τις οποίες συζητήσαμε παραπάνω, ενώ αυτή που χρησιμοποιήθηκε σε πειραματικό στάδιο ήταν η IPv5. Κάθε μια από τις παραπάνω εκδόσεις δίνει έναν διαφορετικό ορισμό για την διεύθυνση IP. Το 1984, με την 4η έκδοση του πρωτοκόλλου του διαδικτύου (IPv4), εξασφαλίστηκαν παραπάνω από 4 δισεκατομμύρια διευθύνσεις. Όταν πρωτοσχεδιάστηκε το πρωτόκολλο IPv4, ελάχιστοι μπορούσαν να προβλέψουν τη ραγδαία εξέλιξη του Διαδικτύου. Τον Φεβρουάριο του 2011 λοιπόν, εξαιτίας της ολοένα αυξανόμενης ανάγκης για νέες υπηρεσίες διαδικτύου, εκχωρήθηκαν και οι τελευταίες διευθύνσεις του IPv4. Έτσι υπήρξε η ανάγκη μετάβασης σε μια νέα έκδοση πρωτοκόλλου διαδικτύου, το IPv6. Η χρήση του IPv6 κατέστησε διαθέσιμο έναν – πρακτικά απεριόριστο – αριθμό διευθύνσεων στο διαδίκτυο, υποστηρίζοντας έτσι τις ανάγκες του μέλλοντος.

Με την εξέλιξη του διαδικτύου, δισεκατομμύρια αισθητήρες που αποτελούν το λεγόμενο «internet των πραγμάτων» όπως έξυπνα τηλέφωνα, αυτοκίνητα, ακόμα και οικιακές συσκευές αναμένεται ότι

θα συνδεθούν με αυτό. Για καθεμία από αυτές τις συσκευές θα απαιτηθεί μια διεύθυνση IP. Το «internet των πραγμάτων» σημαίνει τη συνεχή ανάπτυξη ενός ανοικτού, παγκόσμιου Internet. Το εργαλείο που θα συντελέσει ώστε να γίνει αυτό δυνατόν είναι το πρωτόκολλο IPv6, και οργανώσεις όπως οι IEEE, ISOC και άλλες έχουν αρχίσει να συντελούν στην προώθηση του. Εφόσον εξασφαλιστεί η διάθεση πολλών δισεκατομμυρίων διευθύνσεων, θα εξασφαλιστεί και η ανάπτυξη του μελλοντικού διαδικτύου, σημαντική συνιστώσα του οποίου αποτελεί το «internet των πραγμάτων», για το οποίο αναλυτικά θα κάνουμε λόγο στο επόμενο κεφάλαιο. Η εκχώρηση ενός απεριόριστου αριθμού διευθύνσεων IP καθιστά δυνατή την δημιουργία ξεχωριστών υποδικτύων στον ίδιο χώρο, το κάθε ένα για διαφορετικό σκοπό.

Η IETF (Internet Engineering Task Force, Τακτική Δύναμη Μηχανικών Internet) αναπτύσσει και προωθεί πρότυπα του Internet. Ο οργανισμός αυτός έχει ήδη έχει αρχίσει να εργάζεται πάνω στην κινητικότητα δικτύων χρησιμοποιώντας το IPv6. Με τον όρο κινητικότητα των δικτύων εννοούμε την μετάβαση από το ένα δίκτυο στο άλλο, χρησιμοποιώντας την ίδια διεύθυνση IP. Έτσι μια κλήση μέσω διαδικτύου (VoIP) που έχει ξεκινήσει στο δίκτυο μιας κατοικίας, θα μπορεί να συνεχιστεί φεύγοντας έξω από αυτό (μέσω ασύρματων υπηρεσιών) και να καταλήξει στον χώρο εργασίας μέσω του εκεί δικτύου.

Η νέα έκδοση IPv6 έχει ήδη αρχίσει να κερδίζει έδαφος σε διάφορες χώρες, ιδίως στην Κίνα και την Ιαπωνία, όπου μέσω της καινούργιας τεχνολογίας οι διάφορες κινητές συσκευές διατηρούν τις διευθύνσεις τους, μετακινούμενες από το ένα δίκτυο στο άλλο. Σημαντική εφαρμογή της νέας αυτής τεχνολογίας έγινε στους Ολυμπιακούς Αγώνες που διοργάνωσε η Κίνα το 2008, καθώς χιλιάδες συσκευές όπως κάμερες ασφαλείας και μαγνητοσκόπησης, αυτοκίνητα και άλλα, με τη χρήση του IPv6, εξασφάλισαν τη ζωντανή μετάδοση των

αγώνων μέσω διαδικτύου, ακόμα και την παρακολούθηση της κίνησης στους δρόμους της χώρας. Η Ιαπωνία επίσης έχει επενδύσει σημαντικά στο μέλλον του IPv6. Περίπου 3000 οχήματα σε όλη τη χώρα όπως ταξί, υπηρεσιακά φορτηγά, και δημόσια λεωφορεία έχουν σύνδεση στο διαδίκτυο. Κάθε ένα από αυτά τα οχήματα έχει τη δική του διεύθυνση IP δίνοντας την ευκαιρία στις αρχές της χώρας να παρακολουθούν τις συνθήκες κυκλοφορίας μέσω της ανίχνευσης της ταχύτητας τους, τις οδικές συνθήκες από την κίνηση των υαλοκαθαριστήρων και πολλά άλλα. Έξω από όλα αυτά φυσικά δεν θα μπορούσαν να είχαν μείνει οι εταιρείες κατασκευής και παραγωγής ηλεκτρονικών ειδών.

Η Toshiba, γνωστή εταιρεία παραγωγής και διάθεσης ηλεκτρονικών και ηλεκτρικών ειδών, έχει προωθήσει την ιδέα σύνδεσης όλων των ηλεκτρικών συσκευών στο δίκτυο. Το 2010 παρουσίασε ένα πρωτότυπο ψυγείο IPv6. Με τη χρησιμοποίηση ενός τέτοιου ψυγείου ο καταναλωτής μπορεί να αποφασίσει τι θα αγοράσει στο σουπερμάρκετ, εξετάζοντας το περιεχόμενο του ψυγείου απομακρυσμένα, χρησιμοποιώντας ένα κινητό τηλέφωνο συνδεδεμένο στο διαδίκτυο. Κάθε άλλη συσκευή, όπως ένας φούρνος μικροκυμάτων ή ένα κλιματιστικό μηχάνημα, έχει ένα ξεχωριστό σύνολο πιθανών εφαρμογών. Όταν ένας πελάτης ζητά συντήρηση ή επισκευή των ηλεκτρικών συσκευών του από την εταιρεία, μηχανικοί εξυπηρέτησης πελατών είναι σε θέση να εντοπίσουν ποιό είναι το πρόβλημα μέσω του διαδικτύου. Εάν η βλάβη είναι μικρή, είναι δυνατόν να αποκατασταθεί μέσω του Διαδικτύου, καταργώντας έτσι την επίσκεψη στο σπίτι.

Η τεχνολογική έκθεση CES που πραγματοποιείται μια φορά το χρόνο, φέτος, το 2013 παρουσίασε προϊόντα τεχνολογίας IPv6, τα οποία έδειξαν καθαρά το μέλλον του «internet των πραγμάτων». Το «Hapifork» ήταν ένα από αυτά. Πρόκειται για ένα ηλεκτρονικό πιρούνι που βοηθά τον χρήστη του να παρακολουθεί τις διατροφικές

του συνήθειες καθώς τον ειδοποιεί όταν για παράδειγμα τρώει πολύ γρήγορα. Αυτή η πληροφορία αποστέλλεται μέσω USB σε ένα ηλεκτρονικό ταμπλό για να παρακολουθεί την πρόοδό του. Ακόμα στην έκθεση αυτή η εταιρεία Pioneer παρουσίασε το πρώτο της ηλεκτρονικό αυτοκίνητο με δυνατότητα αναπαραγωγής ραδιοφωνικών σταθμών μέσω ίντερνετ και πλοήγησης στο δρόμο. Τέλος έγινε η παρουσίαση της εταιρείας- συμμαχίας ZigBee, η οποία αποτελείται από πάνω από 400 εταιρείες (και 600 προϊόντα), με στόχο την παροχή βοήθειας στους καταναλωτές για την καλύτερη σύνδεση στο δίκτυο και τον έλεγχο των συσκευών στο σπίτι τους. Η συμμαχία αυτή έδωσε την ευκαιρία στους καταναλωτές να δημιουργήσουν το δικό τους «internet of the things» με ασύρματα δίκτυα αισθητήρων όπως τηλεοράσεις, κλειδαριές στις πόρτες, συστήματα ασφαλείας, τηλεχειριστήρια και πολλά άλλα. Είναι πολύ σημαντικό να θυμόμαστε ότι όλες οι συνδεδεμένες συσκευές (ηλεκτρονικοί υπολογιστές, φορητές συσκευές, αυτοκίνητα, σπίτια, κλπ.) πρέπει να είναι συμβατές με το IPv6.

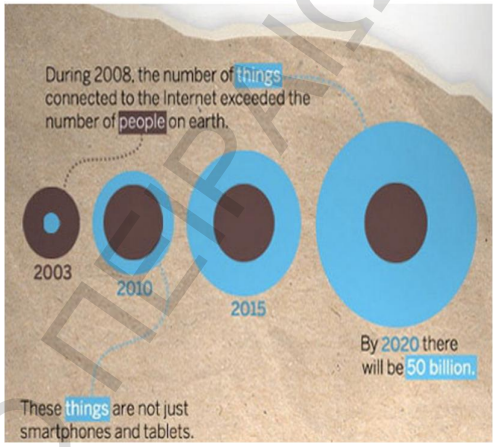
Συνοψίζοντας, μπορούμε να πούμε ότι το 2013 το «ίντερνετ των πραγμάτων» θα επεκταθεί ακόμα περισσότερο, δεδομένου ότι το IPv6 (Internet Protocol version 6) είναι η εφαρμογή που θα οδηγήσει σε τεράστια αύξηση των διευθύνσεων IP, δίνοντας μεγαλύτερη δυνατότητα σε κάθε φυσικό αντικείμενο να συνδέεται στο Internet και να επικοινωνεί με οποιοδήποτε άλλο αντικείμενο. Η υιοθέτηση του IPv6, ωστόσο θα απαιτήσει μαζικές τροποποιήσεις των υποδομών των εταιρειών που θα κατασκευάσουν τέτοιου είδους προϊόντα, καθώς αυτά θα πρέπει να είναι συμβατά με τη νέα τεχνολογία.

Μέρος 2ο

The Internet Of Things

2. The Internet Of Things

2.1 **Εισαγωγή**



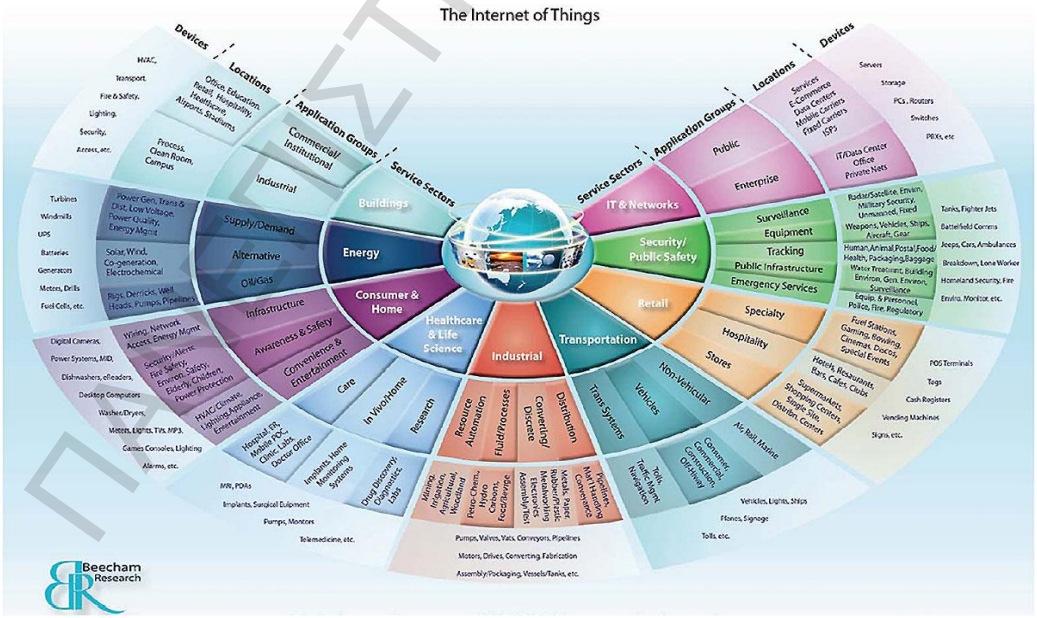
Το 2008 οι συσκευές “πράγματα” που ήταν συνδεδεμένα στο internet, ξεπέρασαν τον αριθμό του πληθυσμού της γης. Σήμερα χρησιμοποιούνται 2 δισεκατομμύρια κινητά τερματικά και πάνω από 1 δισεκατομμύριο είναι οι χρήστες του Internet παγκοσμίως. Έως το 2020 πενήντα δισεκατομμύρια «πράγματα» θα είναι διασυνδεμένα στο internet με αντιστοίχιση περίπου έξι συσκευών ανά άνθρωπο πάνω στη γη, ενώ το ipv6 μας επιτρέπει να διασυνδεθούν πολύ περισσότερα ακόμα. Ασύρματες, κινητές και δικτυακές τεχνολογίες έδωσαν σε πρώτη φάση τη δυνατότητα της διασύνδεσης και επικοινωνίας μεταξύ συστημάτων και εφαρμογών και δημιούργησαν πολύ σημαντικές οικονομικές ευκαιρίες. Αυτό όμως δεν ήταν παρά μόνο η αρχή. Οι τεχνολογίες δικτύωσης εξελίσσονται. Τεχνολογίες όπως η ταυτοποίηση μέσω ραδιοσυχνοτήτων (RFID tags), ενδεχομένως θα μπορούν να αναπτυχθούν σε εκατοντάδες δισεκατομμύρια τερματικών και για μια σχεδόν απεριόριστη γκάμα εφαρμογών.

Αναμένεται οι απλές ετικέτες του σήμερα να εξελιχθούν σε ευφυέστερα δικτυωμένα αντικείμενα με αυξημένη αποθήκευση, επεξεργασία, καθώς και δυνατότητα προσθήκης αισθητήρων. Αυτό με τη σειρά του θα οδηγήσει στη ανάπτυξη νέων δικτυακών εφαρμογών, όπως π.χ. οι M2M "Man-to-Machine, Machine-to-Man,

Machine -to-Mobile and Mobile-to-Machine" και context-aware επικοινωνίες.

Το "Διαδίκτυο των πραγμάτων" θα είναι ένα δίκτυο δισεκατομμυρίων ή τρισεκατομμυρίων μηχανών οι οποίες επικοινωνούν μεταξύ τους. Είναι πολύ σημαντικό και κυρίαρχο θέμα για την εξέλιξη των πληροφοριών και των επικοινωνιών τις επόμενες δεκαετίες, καθώς η απλούστερη μορφή αυτού, είναι ήδη σε χρήση. Υπάρχουν ήδη 1,3 δισεκατομμύρια ταυτοποιήσεις μέσω ραδιοσυχνοτήτων (RFID) και δύο δισεκατομμύρια χρήστες κινητών υπηρεσιών, σε όλο τον κόσμο.

Οι πιθανές εφαρμογές της διαδεδομένης δικτύωσης είναι απεριόριστες και μερικές από αυτές φαίνονται να είναι τουλάχιστον απαραίτητες. Για να θεωρηθεί ότι αυτή η τεχνολογία πραγματικά αξίζει τον κόπο, υπάρχει ανάγκη για αντιμετώπιση του μεγάλου όγκου των εφαρμογών και των δεδομένων προκειμένου να κατανοηθούν καλύτερα οι διάφορες απαιτήσεις (π.χ. πραγματικός χρόνος, η ποιότητα των υπηρεσιών), που θα οδηγήσουν τελικά στην απαραίτητη "γενική" τεχνολογική εξέλιξη.



2.2. **Ορισμοί**

Περνώντας στο θέμα των ορισμών που έχουν δοθεί στο Internet των Πραγμάτων, εντοπίζουμε κάποια ποικιλία, ενώ όσο η τεχνολογία και η εφαρμογή των ιδεών προχωρούν, τόσο ο όρος θα εξελίσσεται. Παρατίθενται δε κάποιοι από τους ορισμούς αυτούς με στόχο μια πρώτη ματιά στο πώς η κοινωνία αντιλαμβάνεται το φαινόμενο αυτό.

1.Για τον οργανισμό CORDIS (Community Research and Development Information Service) το Internet των Πραγμάτων είναι ένα σχέδιο δράσης της Ευρωπαϊκής Ένωσης για την εισαγωγή της διακυβέρνησης που θα βασίζεται στο Διαδίκτυο των πραγμάτων.

2.Για το χρηματοδοτούμενο από την Ευρωπαϊκή Ένωση έργο CASAGRAS ('Coordination and support action for global RFID-related activities and standardisation') ορίζεται ως μια παγκόσμια υποδομή του δικτύου, που συνδέει φυσικά και εικονικά αντικείμενα, αξιοποιώντας τη συλλογή δεδομένων και τις δυνατότητες επικοινωνίας αυτών. Η υποδομή αυτή περιλαμβάνει υφιστάμενες και νέες τεχνολογίες και δυνατότητες του Διαδικτύου. Θα προσφέρει επιπλέον συγκεκριμένες δυνατότητες RFID με τους αισθητήρες και τη συνδεσιμότητά τους να αποτελούν τη βάση για την ανάπτυξη ανεξάρτητων υπηρεσιών και εφαρμογών. Αυτές οι υπηρεσίες και εφαρμογές θα πρέπει να χαρακτηρίζονται από υψηλό βαθμό αυτόνομης συλλογής δεδομένων, από τη μεταφορά γεγονότων, από τη σύνδεση με το δίκτυο και τη διαλειτουργικότητα.

3. Για τη SAP το Internet των Πραγμάτων είναι ένας κόσμος όπου τα φυσικά αντικείμενα ενσωματώνονται στο δίκτυο πληροφοριών και μπορούν να συμμετέχουν ενεργά στις επιχειρηματικές διαδικασίες. Οι υπηρεσίες αλληλεπιδρούν με αυτά τα «έξυπνα αντικείμενα» μέσω του Διαδικτύου, διερευνούν και αλλάζουν την κατάστασή τους και

κάθε πληροφορία που σχετίζεται με αυτές, λαμβάνοντας υπόψη την ασφάλεια και τα θέματα προστασίας της ιδιωτικότητας (privacy).

4. Για τον ευρωπαϊκό οργανισμό IERP (European research Cluster on the Internet of Things) το Internet των Πραγμάτων (IoT) αποτελεί αναπόσπαστο μέρος του μελλοντικού Internet και θα μπορούσε να οριστεί ως μια παγκόσμια υποδομή δικτύου με δυναμικές δυνατότητες ιδίας ρύθμισης (self configured), βασισμένες σε πρότυπα και διαλειτουργικά πρωτόκολλα επικοινωνίας, όπου τα φυσικά και τα εικονικά «πράγματα» έχουν ταυτότητες, φυσικές ιδιότητες, εικονικές προσωπικότητες, χρησιμοποιούν έξυπνες διεπαφές και συνεργάζονται άψογα μέσα στο δίκτυο πληροφοριών. Στο «Internet των Πραγμάτων», τα «πράγματα» θα συμμετέχουν ενεργά στις επιχειρηματικές, πληροφοριακές και κοινωνικές διεργασίες, όπου θα αλληλεπιδρούν μεταξύ τους και με το περιβάλλον, ανταλλάσσοντας πληροφορίες και δεδομένα. Οι διεργασίες (applications) που τρέχουν θα επηρεάζονται και θα ενεργοποιούν τις κατάλληλες υπηρεσίες, είτε με την ανθρώπινη παρέμβαση είτε χωρίς αυτή. Διεπαφές με τη μορφή υπηρεσίας θα διευκολύνουν την αλληλεπίδραση με τα «έξυπνα πράγματα» μέσω του Διαδικτύου και θα αλλάζουν την κατάστασή τους ανάλογα με κάθε πληροφορία που σχετίζεται με αυτά, λαμβάνοντας υπόψη την ασφάλεια και τα θέματα προστασίας της ιδιωτικής ζωής.

Γίνεται αντιληπτό ότι μια κεντρική ιδέα λοιπόν, μπορεί να έχει πολλές προεκτάσεις και επίπεδα αντίληψής της , ενώ η κάθε είδους τροποποίηση έχει σαν απαρχή το ποιός και με ποιό στόχο διατυπώνει κάθε φορά έναν ορισμό. Πέρα όμως από τα στενά πλαίσια που χωρίς αμφισβήτηση θέτει ένας απλός ορισμός λίγων γραμμών, κρίνεται απαραίτητο να υπάρξει μια ευρύτερη ματιά στο ζήτημα, η οποία θα διαμορφώνει μια γενικότερη και σίγουρα πιο ουσιαστική αντίληψη περί του θέματος.

2.3 **Τι πραγματικά είναι όμως το** «Internet **των Πραγμάτων**»;

Ο όρος «Internet των Πραγμάτων» χρησιμοποιήθηκε για πρώτη φορά από τον Kevin Ashton το 1999. Η έρευνα για το πώς θα μπορεί να αναπτυχθεί στην πράξη ο όρος αυτός, έχει ξεκινήσει από το 1940. Από τότε μέσα στη διάρκεια ετών, έχουν γίνει τεράστια βήματα προς μια εξελικτική πορεία. Τις δύο τελευταίες δεκαετίες όμως, τόσο η ευρύτητα όσο και η πρακτική εφαρμογή του ερευνώνται τόσο διεξοδικά, με αποτέλεσμα να είναι γεγονός ότι ήδη έχει τεθεί σε εφαρμογή και ήδη ζούμε το αρχικό-σύμφωνα πάντα με τις δυναμικές του- στάδιο του Internet of things.

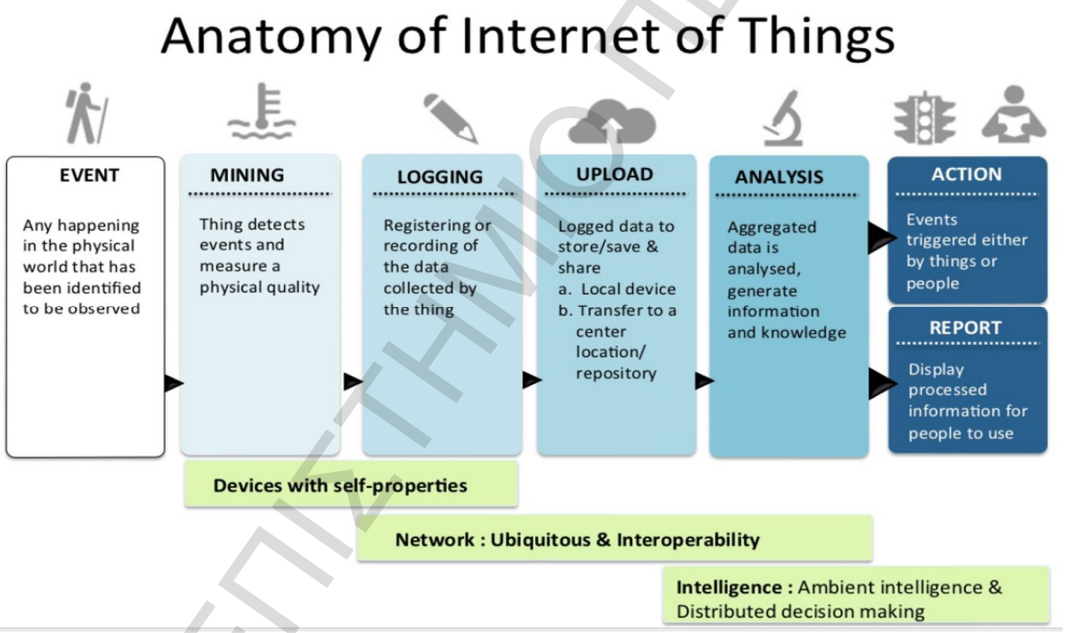
Σήμερα έχουμε καταφέρει να ζούμε σε έναν κόσμο όπου όλοι οι άνθρωποι έχουν τη δυνατότητα να επικοινωνούν μεταξύ τους, έχοντας καταρρίψει τα στενά όρια της γλώσσας και των αποστάσεων. Διευρύνοντας τη σκέψη αυτή, ας προχωρήσουμε σε ένα περιβάλλον όπου τα αντικείμενα θα μπορούν να επικοινωνούν με το ίντερνετ αλλά και με άλλα αντικείμενα, ώστε να παρέχεται η επιθυμητή πληροφόρηση στον άνθρωπο, ο οποίος με τη σειρά του θα μπορεί να δημιουργεί μέσω του συστήματος αυτού μία επιθυμητή για τον ίδιο πραγματικότητα κατά την οποία ο ίδιος θα λειτουργεί ως διαχειριστής ενός οργανωμένου συστήματος συστημάτων, όπου όλα θα επικοινωνούν και θα αλληλεπιδρούν μεταξύ τους με τελικό όμως αποδέκτη τον ίδιο. Το ίδιο το περιβάλλον θα μιλάει στον άνθρωπο και αυτός θα μπορεί να παρέμβει ώστε να δώσει την τροπή που θα επιλέξει, έτσι ώστε να αυτοεξυπηρετηθεί, αλλά και να διευκολύνει σε ευρύτερο επίπεδο πολλούς και διάφορους τομείς της ίδιας της κοινωνίας. Επεκτείνοντας το μοτίβο αυτό στα μηνύματα που ο πλανήτης μας πάντα μας απέστελλε αλλά εμείς μέχρι τώρα δεν

είχαμε τη δυνατότητα να αντιληφθούμε, τότε σίγουρα κάνουμε λόγο για μια τεράστια αναβάθμιση της θέσης του ανθρώπου μέσα στο σύμπαν, ενός ανθρώπου που μπορεί πλέον να οργανώσει και να δρομολογήσει απλά καθημερινά πράγματα και καταστάσεις, αλλά και να έχει πια λόγο στην ίδια την πορεία πραγμάτων που μέχρι τώρα τον ξεπερνούσαν.

Απώτερος στόχος του Internet of things είναι να ιδρυθεί αλλά και να εδραιωθεί ένας «έξυπνος κόσμος». Ας φανταστούμε έναν κόσμο όπου τα πάντα μπορεί να είναι τόσο αναλογικά όσο και ψηφιακά. Πρόκειται για μια πραγματική αναδιατύπωση της σχέση του ανθρώπου με τα αντικείμενα - τα πράγματα, καθώς και για διαφοροποίηση αντίληψης των ίδιων των αντικειμένων. Κάθε αντικείμενο που φέρει ετικέτα RFID σχετίζεται όχι μόνο με ένα άτομο ή πράγμα, αλλά αναφέρεται και σε άλλα αντικείμενα, στις σχέσεις ή στις τιμές σε μια βάση δεδομένων. Δεν είναι υπερβολή να ειπωθεί ότι μέσω του φιλόδοξου αυτού σχεδίου, ο πλανήτης ολόκληρος θα αναπτύξει νευρώνες μέσω των οποίων θα μπορεί να συντονίζεται και να ανταλλάζει πληροφορίες με αυτόν που τον κατοικεί. Ο άνθρωπος θα έχει πια επιρροή σε ένα ευρύτατο φάσμα πραγμάτων αλλά και καταστάσεων και θα του δοθεί η δυνατότητα να εξελιχθεί, να δημιουργήσει αλλά και να προστατευτεί από αυτά που μέχρι τώρα δε μπορούσε να αντιμετωπίσει. Ένας ψηφιακός πλανήτης είναι ένας πλανήτης όπου τον πρώτο λόγο τον έχει η ίδια η ανθρώπινη ύπαρξη, ως εφευρέτης του τρόπου διαχείρισης της οποιασδήποτε πληροφορίας. Και ένας πλανήτης με ηγέτη τον ανθρώπινο νου- εφόσον η κύρια επιδίωξη καταστεί το κοινό καλό-σίγουρα είναι καλύτερος.

2.4 **Στοιχεία ανατομίας του** Internet of things.

Για να κατανοήσει όμως κανείς κάτι σε βάθος, πρέπει να βρίσκει τα κομμάτια που το απαρτίζουν αλλά και τη λογική αλληλουχία με την οποία αυτά συνδέονται. Έτσι και στην περίπτωση αυτή είναι πρέπον να προσπαθήσουμε να ρίξουμε φως στο πώς διαρθρώνεται όλο αυτό το σύστημα που επιχειρεί να εντοπίσει, να καταγράψει, να μεταφέρει και να χρησιμοποιήσει ανάλογα με τον αρχικό στόχο - μέσω ενός αντικειμένου («πράγματος»)- μια οποιαδήποτε πληροφορία.



Η όλη διαδικασία ξεκινάει από το λεγόμενο «γεγονός». Γεγονός νοείται οτιδήποτε συμβαίνει στο φυσικό κόσμο και στο οποίο έχει δοθεί μια συγκεκριμένη ταυτότητα με σκοπό να παρατηρείται και να παρακολουθείται.

Σε δεύτερη φάση έρχεται το αντικείμενο(πράγμα) που χρησιμοποιείται ως μέσο εντοπισμού και αξιολόγησης του «γεγονότος» αυτού.

Το τρίτο στάδιο δεν είναι τίποτε άλλο παρά η καταγραφή όλων των πληροφοριών-δεδομένων που πηγάζουν από το εν λόγω «γεγονός», τα οποία το αντικείμενο κατάφερε να συλλέξει.

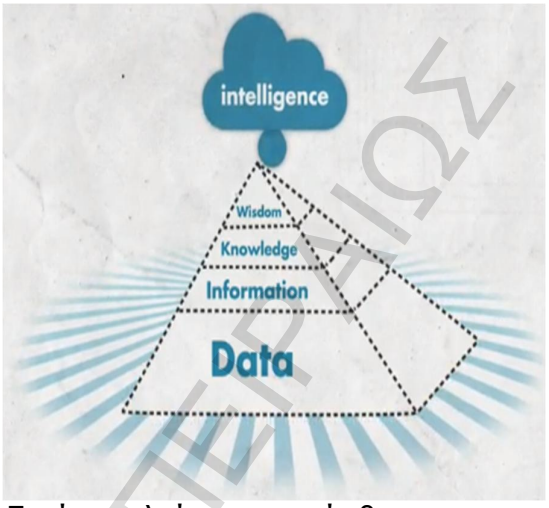
Στη συνέχεια τα καταγεγραμμένα δεδομένα αρχικά αποθηκεύονται και έπειτα προωθούνται είτε σε μια τοπική συσκευή που μπορεί να είναι και το ίδιο το αντικείμενο, είτε σε μια κεντρική τοποθεσία.

Ακολουθεί το σημαντικότατο στάδιο της ανάλυσης και επεξεργασίας των πληροφοριών-δεδομένων, γεγονός το οποίο έχει ως απόρροια την επίτευξη της ενημέρωσης και της πραγματικής γνώσης (data mining).

Σε τελική φάση, ο τρόπος χρήσης της ενημέρωσης που έχει επιτευχθεί είναι διττός. Το αντικείμενο ή και ο ίδιος ο άνθρωπος έχει τη δυνατότητα να λάβει δράση και να υλοποιήσει μια ενέργεια ώστε να πετύχει ένα επιθυμητό κατά περίπτωση αποτέλεσμα. Από την άλλη μπορούμε να κάνουμε λόγο για την απλή παράθεση πληροφορίας την οποία ο καθένας μπορεί να έχει στη διάθεσή του για να τη χρησιμοποιήσει όταν και όπως εκείνος επιλέξει.

Συμπεραίνει κανείς από τα παραπάνω ότι μιλάμε πρώτον για μια ουσιαστική αλλαγή στον τρόπο της αρχικής σύλληψης των όσων συμβαίνουν στον κόσμο- αφού φέρουν πλέον μια συγκεκριμένη ταυτότητα- και δεύτερον στον εντοπισμό και την καταγραφή των παρεχομένων πληροφοριών που πια γίνεται μέσω ενός «πράγματος». Σε συνδυασμό με την προώθηση και την ανάλυση των δεδομένων που προκύπτουν , οδηγούμαστε τελικά όχι μόνο στην απόκτηση γνώσης αλλά και στην ύπαρξη επιλογής όσον αφορά στον τρόπο χρήσης της πληροφορίας αυτής, ο οποίος επιλέγεται σύμφωνα με τον αρχικό στόχο, τις συνθήκες και τα διάφορα περιβάλλοντα όπου θα λάβει χώρα όλη η παραπάνω αλληλουχία γεγονότων.

Internet of things **και ανθρώπινος παράγοντας**



Τα δεδομένα που μπορούμε να αντλήσουμε από τις διασυνδεδεμένες συσκευές και κατ΄ επέκταση όλο αυτό το σύστημα είναι ανεξάντλητα, αλλά όχι και όλα χρήσιμα οπότε κατά συνέπεια, σε εκείνο ακριβώς το σημείο η ανθρώπινη παρέμβαση είναι και απολύτως καθοριστική. Εκεί καλείται ο άνθρωπος να χρησιμοποιήσει την οξύτητα του νου του για να μπορέσει να επεξεργαστεί τα δεδομένα αυτά και να τα μετατρέψει σε κατάλληλη πληροφορία, την πληροφορία αυτή σε γνώση και εν τέλει τη γνώση σε σοφία. Ο άνθρωπος είναι αυτός που πάντα τελικά παίρνει την τελευταία απόφαση και ορίζει τα πράγματα, αποδεικνύοντας ότι οι μηχανές κρατούν μόνο το ρόλο του διαχειριστικού μέσου.

Ήδη το IoT έχει αρχίσει να εμφανίζεται δυναμικά σε διάφορες πτυχές της ζωής μας και κάποιες εφαρμογές του ήδη χρησιμοποιούνται στην αυτοκινητοβιομηχανία ,στις μεταφορές και σε συστήματα επιτήρησης. Για παράδειγμα, αρκετά αυτοκίνητα έχουν αισθητήρες παρακολούθησης των εσωτερικών τους λειτουργιών και ειδοποιούν τους ιδιοκτήτες για τυχόν βλάβες και επισκευές που χρειάζονται. Σε σπίτια στην Washigton D.C. και σε μέρη του Maryland, αποκαταστάθηκε η ηλεκτροδότηση σε 2 μόνο μέρες μετά το πέρασμα του τυφώνα Sandy, χάρη σε σήματα που έστειλαν αισθητήρες στο κέντρο παρακολούθησης του δικτύου.

Αυτές όμως οι εφαρμογές δεν είναι παρά μονό ένα ελάχιστο από το τι είναι δυνατό να γίνει μέσω της χρήσης του IoT. Το Iot θα

επιφέρει ριζικές αλλαγές στην ζωή του ανθρώπου, στη λειτουργία των επιχειρήσεων και των κρατικών οργανισμών. Χρησιμοποιώντας το «έξυπνα» προς όφελος της βελτίωσης της ποιότητας ζωής, της οικολογίας, της οικονομίας και της αύξησης της παραγωγικότητας σε όλους τους τομείς της παραγωγής, το αποτέλεσμα θα μπορούσε να μας καταπλήξει. Οι εφαρμογές που θα αναπτυχθούν θα δώσουν ευκαιρίες στις εταιρείες ανάπτυξης λογισμικού και υλικού να αναπτύξουν νέα προϊόντα και να εισβάλλουν στις αγορές, ενώ ο καταναλωτής θα μπορεί να αξιολογήσει ποιές από αυτές θα διευκολύνουν την καθημερινότητά του και σε επόμενη φάση να επενδύσει σε αυτές. Σε ποιούς τομείς όμως και σε τι έκταση μπορεί να έχει επίδραση η όλη αυτή η διαδικασία ανταλλαγής δεδομένων την οποία καθιστά δυνατή το Ipv6 με την καινοτόμα τεχνολογία του, χωρίς την οποία η υλοποίηση του Iot θα ήταν αδύνατη ή τουλάχιστον κατά πολύ περιορισμένη;

2.5 **Παραδείγματα χρήσεων του** internet of things

1. **Έξυπνο σπίτι και έξυπνη πόλη**

Ολοένα και περισσότερο έχουμε υπερσυγκεντρωτισμό των ανθρώπων στις πόλεις. Τα έξυπνα σπίτια και η έξυπνη πόλη αφορούν πλέον στο μεγαλύτερο ποσοστό των ανθρώπων στον πλανήτη. Ένα έξυπνο σπίτι θα μπορεί να κάνει τη διαβίωση των ανθρώπων ευκολότερη. Ας φανταστούμε ένα σπίτι που θα μπορεί να ρυθμίζει την εσωτερική θερμοκρασία του χωρίς αλλεπάλληλη ανθρώπινη παρέμβαση, ένα σπίτι που θα μπορεί να παρακολουθεί

και να ρυθμίζει την ενέργεια και το νερό που καταναλώνεται, ώστε να επιτυγχάνεται η οικονομία στους πόρους άλλα και στα χρήματα που δαπανώνται γι' αυτούς. Ένα σπίτι που θα μας ειδοποιούσε για τυχόν παραβίαση σε πόρτα ή παράθυρο ή αμέλεια μας στο κλείδωμα αυτών. Το ψυγείο θα μας ειδοποιεί ότι το γάλα τελείωσε και πρέπει να ψωνίσουμε και ο φούρνος θα ανάβει για να ψήσει το φαγητό μας την ώρα που θα ειδοποιούμε μέσω του έξυπνου κινητού μας ότι φεύγουμε από τη δουλειά. Αισθητήρες στο μπαλκόνι θα ανιχνεύουν την υγρασία στα φυτά μας και θα τα ποτίζουν όποτε χρειάζεται.

Τέτοιου είδους διευκολύνσεις θα συνεχίζονται από τη στιγμή που ζει κανείς σε μια «έξυπνη» πόλη. Ένα σύστημα ειδοποίησης θα έχει φροντίσει να ειδοποιήσει το σπίτι μας και εκείνο με τη σειρά του το ξυπνητήρι μας ότι κάποιος αστάθμητος παράγοντας έχει προκαλέσει κίνηση και θα χρειαστεί να ξυπνήσουμε 10 λεπτά νωρίτερα ώστε να είμαστε εγκαίρως στη δουλειά μας . Στο δρόμο για τη δουλειά μας ,

έξυπνοι δρόμοι θα μας ειδοποιούν και θα μας δίνουν οδηγίες με μηνύματα λαμβάνοντας υπόψη την κίνηση και τις κλιματικές συνθήκες που επικρατούν σε αυτούς. Φτάνοντας στην δουλειά μας, θα μαθαίνουμε πού υπάρχει ελεύθερη θέση πάρκινγκ και θα σταθμεύουμε σε αυτή χωρίς περαιτέρω καθυστερήσεις. Οι φωτεινοί σηματοδότες (φανάρια) θα μπορούν να προσαρμόζονται στην κίνηση των αυτοκινήτων και να ρυθμίζουν την κυκλοφορία για μια πιο ομαλή ροή, ενώ στους δρόμους τα φώτα θα μπορούν να ανάβουν και να σβήνουν ανάλογα με τις συνθήκες που επικρατούν σε αυτές, ώστε να είναι πάντα ασφαλείς αλλά και να γίνεται ταυτόχρονα οικονομία στην ενέργεια. Επιπλέον, θα καθίσταται δυνατό να ελέγχονται οι στάσεις των μέσων μαζικής μεταφοράς και ανάλογα να αναπροσαρμόζονται τα δρομολόγια τους .

Σε άλλους τομείς εκτός των οδικών δικτύων, θα μπορεί να γίνεται παρακολούθηση στους κάδους απορριμμάτων ώστε τα απορριμματοφόρα να αδειάζουν όσους χρειάζεται και μόνο. Θα μπορεί να γίνεται παρακολούθηση της κατάστασης των υλικών κτίριων, γεφυρών και Ιστορικών μνημείων ώστε να προβλεφθεί έγκαιρα κάποια βλάβη ή καταστροφή. Επίσης θα μπορεί να παρακολουθείται σε αληθινό χρόνο (real time) η ένταση του ήχου σε περιοχές με μαγαζιά διασκέδασης για τυχόν υπερβάσεις των ορίων με στόχο μια πιο «καθαρή» πόλη από θορύβους.

2. **Καθημερινές δραστηριότητες και έξυπνο πορτοφόλι**

Οι διευκολύνσεις κατ' επέκταση θα αφορούν και σε όλες τις καθημερινές δραστηριότητες του ατόμου. Θα μπορεί κανείς να

αντεπεξέρχεται στα πρακτικά θέματα και ζητούμενα που επιτάσσουν οι γρήγοροι ρυθμοί

ζωής ταχύτερα και ευκολότερα. Για παράδειγμα, έχοντας κανείς μεταφέρει στο κινητό του τα προϊόντα που το έξυπνο ψυγείο ενημέρωσε ότι λείπουν από το σπίτι, πηγαίνοντας στο super market θα μπορεί κανείς να καθοδηγείται με ακρίβεια στα ράφια όπου είναι τοποθετημένα τα προϊόντα αυτά. Φτάνοντας στο ταμείο μέσω του κινητού του θα είναι δυνατόν να ολοκληρωθεί η χρηματική συναλλαγή άμεσα και άκοπα.

3. **Το έξυπνο αυτοκίνητο**

Το έξυπνο αυτοκίνητο θα είναι άλλη μια ευρέως χρησιμοποιούμενη εφαρμογή του IoT στον καθημερινό ρυθμό ζωής. Τα οχήματα θα μπορούν να επικοινωνούν μεταξύ τους αλλά και με τον έξυπνο δρόμο και θα μπορεί να γίνει μια ακριβέστατη εκτίμηση της κίνησης με στόχο ο οδηγός να ειδοποιείται έγκαιρα και έγκυρα. Ακόμα, οι

αισθητήρες των ελαστικών θα ειδοποιούν για τυχόν φθορές στα ελαστικά ώστε να προλαμβάνονται τα ατυχήματα. Επίσης θα μπορούν να παρέχονται ειδοποιήσεις στον οδηγό σχετικά με τις αποστάσεις και να αντιδρά το ίδιο το όχημα σε περίπτωση που χρειαστεί να φρενάρει. Αυτή είναι μια εφαρμογή που θα μπορούσε να συνδυαστεί με e-health συστήματα που να ακινητοποιούν το αυτοκίνητο σε περιπτώσεις που το ίδιο αντιλαμβάνεται κάποια αδιαθεσία του οδηγού, ώστε να προλαμβάνονται διάφορα ατυχήματα.

Η Toyota Motor Corp. (TMC) και η Microsoft Corp. ανακοίνωσαν ότι έχουν συνάψει στρατηγικό συνεταιρισμό, σχεδιάζοντας να χτίσουν μια παγκόσμια πλατφόρμα για υπηρεσίες τηλεματικής, η οποία θα χρησιμοποιείται από την Toyota, βασισμένη στην πλατφόρμα Windows Azure(cloud). Η τηλεματική είναι η συνένωση των τεχνολογιών της πληροφορίας και των τηλεπικοινωνιών στα οχήματα, συμπεριλαμβανομένων συστημάτων GPS, συστημάτων διαχείρισης ενέργειας καθώς και άλλων τεχνολογιών πολυμέσων. Οι δύο εταιρίες έχουν ως σκοπό να προωθήσουν τις τηλεματικές εφαρμογές που είναι βασισμένες στην πλατφόρμα Azure, ξεκινώντας από τα ηλεκτρικά και plug-in υβριδικά οχήματα της TMC από το 2012.

Η Toyota στοχεύοντας στη δημιουργία μιας κοινωνίας με χαμηλά επίπεδα κατανάλωσης άνθρακα, μέσω της αποδοτικής χρήσης της ενέργειας, ξεκίνησε το πιλοτικό πρόγραμμα Toyota Smart Center, το οποίο έχει σκοπό να ενώνει ανθρώπους, αυτοκίνητα και σπίτια, για ενσωματωμένο έλεγχο της κατανάλωσης ενέργειας. Κατά την TMC, η αυξανόμενη δημοτικότητα των ηλεκτρικών και plug-in υβριδικών οχημάτων, ολοένα και περισσότερο θα οδηγεί στα τηλεματικά συστήματα για επίτευξη αποδοτικής διαχείρισης ενέργειας.

Η Microsoft, από την άλλη, έχει μια μακριά ιστορία παροχής πλατφόρμων και υπηρεσιών στην αυτοκινητοβιομηχανία, συμπεριλαμβανομένων συστημάτων ενημέρωσης/ψυχαγωγίας βασισμένα στην πλατφόρμα Windows Embedded Automotive, συστημάτων χαρτογράφησης με την Bing, τη φωνητική εφαρμογή Microsoft Tellme, καθώς και πολλές άλλες λύσεις για τους καταναλωτές.

Οι δύο εταιρίες σχεδιάζουν να επενδύσουν 1 δισεκατομμύριο γιεν (περίπου 9 εκατομμύρια ευρώ) στο έργο, ώστε μέχρι το 2015 να υπάρχει μια ολοκληρωμένη παγκόσμια πλατφόρμα, που να παρέχει

εξελιγμένες υπηρεσίες τηλεματικής σε προσιτές τιμές, στους πελάτες της Toyota σε όλο τον κόσμο.

4. **Τομέας υγείας**

Ένα πολύ σημαντικός τομέας ζωής του ανθρώπου που θα επηρεαστεί θετικά μέσω τέτοιου είδους εφαρμογών, είναι ο τομέας της υγείας. Οι γιατροί θα μπορούν πλέον πολύ εύκολα να παρακολουθούν τους ασθενείς στο σπίτι αλλά και σε οποιοδήποτε σημείο εκείνοι μπορεί να βρίσκονται. Ο ασθενής θα μπορεί να φέρει συστήματα παρακολούθησης σακχάρου, σφυγμού, θερμοκρασίας και πίεσης του αίματος και να στέλνει άμεσα και ανά πάσα στιγμή τα δεδομένα στον ιατρό του ή σε κάποιο συγγενικό πρόσωπο ώστε να προλαμβάνονται διάφορες επιπλοκές στην υγεία του. Με την ψηφιακή κάρτα υγείας, η πρόσβαση στο φάκελο του ασθενούς θα γίνεται άμεσα και εύκολα από τη στιγμή που ακόμα και ένα δευτερόλεπτο μπορεί να είναι καταλυτικό για τη ζωή του ασθενούς.

5. **Εκπαίδευση**

Όλοι αναγνωρίζουν το σημαντικότατο ρόλο της εκπαίδευσης για την κοινωνία. Τα σχολικά συστήματα χρειάζονται αδιαμφισβήτητα αναβάθμιση στα συστήματα που χρησιμοποιούν για να μεταλαμπαδεύσουν την γνώση στους μαθητές. Τα άτομα νεαρής ηλικίας γοητεύονται και δείχνουν ενδιαφέρον πιο πολύ για την εικόνα και για οτιδήποτε μπορεί να ζωντανέψει κάτι που τυχόν ακούνε μπροστά στα μάτια τους, κάτι το οποίο μπορεί να επιτευχθεί κάλλιστα μέσω των λεγομένων διαδραστικών πινάκων οι οποίοι θα δίνουν απεριόριστες δυνατότητες στα παιδιά. Η δυνατότητα να

επικοινωνούν άμεσα οι μαθητές με ανθρώπους που ανήκουν σε διαφορετικές εθνικότητες, η χρήση μιας νέας τεχνολογικής προσέγγισης που θα μπορεί να καταργήσει τις αποστάσεις και να μεταφράζει άμεσα τα όσα πρόκειται να παρασχεθούν ως γνώση, αναμφίβολα είναι καίριας σημασίας. Έτσι μπορεί να γίνει λόγος για ένα εκπαιδευτικό σύστημα στο οποίο θα έχουν προσαρμοστεί σύμφωνα με τις ανάγκες όλα αυτά τα νέα δεδομένα που εισάγει το IoT.

6. **Αθλητισμός**

Σημαντικές αλλαγές θα υπάρξουν σίγουρα και στο χώρο του αθλητισμού. Εν ώρα άθλησης θα είναι δυνατόν να παρακολουθούνται οι σφυγμοί, η αντοχή, η επίδοση και γενικά η φυσική κατάσταση των αθλητών ώστε να προλαμβάνονται τα καρδιακά ή άλλου είδους επεισόδια στα γήπεδα , φαινόμενο το οποίο απαντάται συχνά στην εποχή μας.Η Nike έχει ήδη πλασάρει το Nike + ένα τσιπάκι που ενσωματώνεται σε παπούτσια τρεξίματος και συνδέεται ασύρματα με ειδικό ρολόι ή με το έξυπνο κινητό μας. Έτσι στην οθόνη του κινητού μας ή του ρολογιού μπορούμε να δούμε στοιχεία όπως την απόσταση που διανύσαμε, τις θερμίδες που κάψαμε και τον ρυθμό μας ανά χιλιόμετρο. Κατόπιν με ένα κλικ μπορούμε να ανεβάσουμε τις επιδόσεις μας στα κοινωνικά δίκτυα.

7. **Περιβάλλον**

Ο άνθρωπος είναι σε άμεση αλληλεπίδραση με το περιβάλλον στο οποίο ζει και προσπαθούσε πάντα να το αναγνώσει, να το καταλάβει αλλά και να αναπτύξει πάνω του κάποια ισχύ, ώστε να προστατεύει τον εαυτό του από αυτά που η φύση κατά καιρούς επιτάσσει. Μέσω του Iot, θα μπορούν πλέον να τοποθετηθούν συστήματα παρακολούθησης της στάθμης των νερών λιμνών και ποταμών , συστήματα παρακολούθησης τσουνάμι και βροχοπτώσεων, ώστε να αποφεύγονται οι πλημμύρες ή έστω να υπάρχει το περιθώριο για έγκαιρη εκκένωση περιοχών. Αισθητήρες θα ελέγχουν το ύψος του χιονιού σε δρόμους , χιονοδρομικά κέντρα και περιοχές ευρύτερου κίνδυνου, ώστε να αποφεύγονται ατυχήματα και αποκλεισμοί ανθρώπων. Επίσης θα μπορούν να τοποθετηθούν συστήματα παρακολούθησης των ρύπων στο νερό, συστήματα εποπτείας των δασών για τον εντοπισμό πυρκαγιών με στόχο την έγκαιρη ειδοποίηση των κατάλληλων φορέων για την κατάσβεση αυτών. Σε εργοστασιακές μονάδες θα μπορούν να εγκατασταθούν συστήματα εποπτείας και ελέγχου των ρύπων CO2 ώστε να μην μολύνεται η ατμόσφαιρα από αυξημένη εκπομπή ρύπων CO2. Επίσης θα μπορούμε να παρακολουθούμε πληθυσμούς ζώων, πτηνών και ψαριών ώστε να καταλάβουμε τους κινδύνους που διατρέχουν και να αναλαμβάνουμε δράση ώστε να τα διαφυλάττουμε.

8. **Έξυπνα συστήματα μέτρησης ενέργειας και πόρων**

Τα έξυπνα συστήματα μέτρησης θα παίξουν καταλυτικό ρόλο στο χώρο της ενέργειας. Έξυπνα συστήματα μέτρησης είναι αυτά που θα παρακολουθούν και θα διαχειρίζονται την ενεργειακή κατανάλωση. Θα παρακολουθούν τα επίπεδα του νερού, πετρελαίου και φυσικού αερίου στις δεξαμενές αποθήκευσης. Θα παρακολουθούν και βελτιστοποιούν την απόδοση σε φωτοβολταϊκών συστημάτων, θα μετρούν την πίεση του νερού στα συστήματα

μεταφοράς νερού όπως επίσης θα μετρούν τις ελλείψεις αγαθών στα σιλό και το βάρος των προϊόντων.

9. **Τομέας μεταφορών**

Στις μεταφορές η επίδραση του Iot μπορεί να είναι καθοριστικής σημασίας. Οι εταιρίες θα μπορούν να παρακολουθούν τα container τους ή τα εμπορευματοκιβώτιά τους μέσω δικτύου αισθητήρων και

να ξέρουν ανά πάσα στιγμή το πού βρίσκονται και σε τι κατάσταση είναι. Θα μπορεί επιπλέον να αξιολογηθεί η ποιότητα της μεταφοράς, παρακολουθώντας τυχόν χτυπήματα και αναταράξεις, ή ακόμα και για παράδειγμα πόσες φόρες ένα container ψυγείο άνοιξε κατά τη διάρκεια της μεταφοράς του, ώστε να διασφαλιστεί η ποιότητα των προϊόντων αλλά και για λόγους ακόμα ασφαλιστικής κάλυψης. Με την παράδοση ενός δέματος στον τελικό παραλήπτη, θα μπορεί κανείς σαρώνοντας με το κινητό του την ετικέτα του δέματος να κάνει αυτομάτως και την απαραίτητη πληρωμή.

9. **Βιομηχανία**

Στον τομέα της βιομηχανίας, χρησιμοποιώντας κατάλληλα αισθητήρια, ξεκινώντας από τις πρώτες ύλες μέχρι το τελικό προϊόν, θα μπορούμε πολύ εύκολα να παρακολουθηθούμε την παραγωγή. Σε βιομηχανίες που έχουν μεγάλη τοξικότητα λόγω των υλικών που χρησιμοποιούν, θα μπορεί να παρακολουθείται η τοξικότητα του αέρα και τα ποσοστά οξυγόνου με σκοπό να διασφαλιστεί η ασφάλεια των εργατών και των προϊόντων. Machine to Machine τεχνολογίες θα διασφαλίζουν την ποιότητα της παραγωγής, καθώς όταν μια

μηχανή δεν θα μπορεί να παράγει σωστά, θα μπορεί να ειδοποιεί τις υπόλοιπες μηχανές να σταματήσουν ή να ειδοποιεί μια μηχανή η οποία και θα μπορεί να επισκευάσει τη βλάβη.

10. **Γεωργία**

Ραγδαίες εξελίξεις θα παρατηρηθούν ακόμα και στον τομέα της γεωργίας. Λόγου χάριν, στοχεύοντας στη βελτίωση της ποιότητας του παραγόμενου κρασιού, συστήματα θα παρακολουθούν την υγρασία του εδάφους και τη διάμετρο του κορμού του αμπελιού, ώστε να μπορεί να ελέγχεται η ποσότητα ζάχαρης στα σταφύλια. Στα θερμοκήπια θα ελέγχονται οι μικροκλιματικές συνθήκες μέσα σε αυτά ώστε να επιτευχθεί η μεγιστοποίηση της παραγωγής και η βελτίωση της ποιότητας των παραγόμενων φρούτων και λαχανικών. Ένα μεγάλο μέρος της γεωργικής παραγωγής σήμερα είναι τα βιολογικά προϊόντα. Έτσι το βιολογικό λίπασμα (compost) είναι πολύ σημαντικό να παράγεται σωστά. Θα ελέγχεται η υγρασία και τα επίπεδα θερμοκρασίας στα συστατικά του compost (τριφύλλι, σανό, άχυρο) για την αποφυγή μυκητιάσεων και άλλων μικροβιακών προσμείξεων. Οι μετεωρολογικές συνθήκες θα παρακολουθούνται για την πρόβλεψη σχηματισμού πάγου, βροχής , χιονιού, ξηρασία ή αλλαγής του αέρα. Στις αγροτικές εκτάσεις ή σε μεγάλες εκτάσεις πρασίνου όπως πάρκα ή γήπεδα του γκολφ, θα μπορεί να γίνει επιλεκτική άρδευση στις ξηρές ζώνες για τη μείωση των υδάτινων πόρων που απαιτούνται για το πότισμα. Επίσης ένα σημαντικό πρόβλημα που υφίσταται στη γεωργία και είναι αυτό του καθορισμού των χερσαίων συνόρων του χωραφιού, θα μπορούσε να επιλυθεί, εφόσον ο καθορισμός και η σήμανσή των χερσαίων συνόρων γινόταν με ηλεκτρονικές ετικέτες.

11. **Κτηνοτροφία**

Στην κτηνοτροφία παράλληλα, θα μπορούμε πλέον μέσω ετικετών να γίνεται ο εντοπισμός των ζώων ανά πάσα στιγμή, να ελέγχουμε τις συνθήκες στις οποίες μεγαλώνουν αυτά ώστε να διασφαλίσουμε την επιβίωση και την υγεία τους . Επιπροσθέτως, θα διευκολύνεται ο έλεγχος του αερισμού στα αγροκτήματα και θα υπάρχει εντοπισμός των τοξικών αέριων που παράγονται από τα περιττώματα των ζώων.

12. **Πολεμική βιομηχανία**

Η επέκταση του Iot στις πολεμικές επιχειρήσεις θα είναι και εκεί μεγάλη. Οι επικοινωνίες θα είναι πλέον κρυπτογραφημένες πλήρως, άρα και σχεδόν τελείως ασφαλείς αλλά θα είναι ακόμα δυνατή και η Ad-Hoc επικοινωνία μεταξύ των στρατιωτών μέσα στα ίδια πλαίσια ασφάλειας. Θα μπορεί να υπάρχει σήμανση των οχημάτων και των στρατιωτών με ετικέτες, ώστε οι επικεφαλής να ξέρουν ανά πάσα στιγμή πού βρίσκονται αλλά και θα καθίσταται δυνατή η ακριβής οριοθέτηση περιοχών με ετικέτες όπου θα διεξαχθεί κάποια πολεμική επιχείρηση, όπως για παράδειγμα ένας βομβαρδισμός , με μοναδικό στόχο το χτύπημα να είναι πιο ακριβές και να αποφεύγονται παράπλευρες απώλειες.

Όλα τα παραπάνω εκτενώς παρουσιάζουν μια ζωή ασφαλώς ευεργετημένη από τη διείσδυση του ίντερνετ των πραγμάτων σε όλους σχεδόν τους τομείς αυτής. Ιδανικά θα λειτουργούσε μια κοινωνία, εφόσον ο μοναδικός σκοπός των μελών αυτής θα ήταν το κοινό καλό , πράγμα το οποίο μέχρι τώρα δυστυχώς έχει καταστεί ακατόρθωτο και μη εφαρμόσιμο. Έτσι και στην περίπτωση αυτή, η συγκεκριμένη καινοτομία εγκυμονεί κινδύνους για ανθρώπους,

χώρες ακόμα και ηπείρους, που είναι στο χέρι των ρυθμιστικών αρχών αν όχι να τους εξαλείψουν, τουλάχιστον να τους μετριάσουν κατά πολύ. Στο σημείο αυτό λοιπόν κρίνεται σκόπιμο να εντοπίσει κανείς τις ενδεχόμενες απειλές, τα ερωτήματα που αναπόφευκτα γεννιούνται και να διερευνήσει στη συνέχεια ποιός είναι τελικά ο ρόλος των ρυθμιστικών αρχών, πώς έχουν δράσει μέχρι τώρα σε ειδικό αλλά και γενικό επίπεδο, αλλά και τι είδους προκλήσεις καλούνται επιπλέον να αντιμετωπίσουν όσο υπάρχει η εξελικτική αυτή πορεία των πραγμάτων.

Μέρος 3ο

Θεσμικό Πλαίσιο

3. **Θεσμικό πλαίσιο**

3.1 **Εισαγωγή**

Το Ίντερνετ των πραγμάτων ως αναδυόμενη παγκόσμια Internet-based αρχιτεκτονική μετάδοσης πληροφορίας που διευκολύνει την ανταλλαγή αγαθών και υπηρεσιών αναπτύσσεται προοδευτικά. Και ενώ αυτή η τεχνολογία εξακολουθεί να συζητείται και να αναπτύσσεται, το νομικό πλαίσιο γύρω από αυτή θα πρέπει να καθοριστεί πριν το Ίντερνετ των πραγμάτων καταστεί πλήρως λειτουργικό. Το ρυθμιστικό πλαίσιο πρέπει να προβλέπει διατάξεις που θα διασφαλίζουν την ασφάλεια της κατασκευής, καθώς και την προστασία της ιδιωτικής ζωής των χρηστών του. Επιπλέον, τα νομικά εμπόδια που ενδέχεται να μεσολαβήσουν στη λειτουργία του Ίντερνετ των πραγμάτων πρέπει να οριστούν. Το Ίντερνετ των πραγμάτων έχει θετικά αποτελέσματα σε διάφορους τομείς, όπως η ένταξη των αναπτυσσόμενων χωρών στο παγκόσμιο εμπόριο και η χρήση των μηχανών αναζήτησης προς όφελος της κοινωνίας των πολιτών. Στην πρώτη παράγραφο του παρόντος κεφαλαίου γίνεται λόγος για το νομοθετικό πλαίσιο στο οποίο υπόκειται η νέα τεχνολογία στην Ελλάδα.

Ενώ η προστασία και ο σεβασμός της ιδιωτικής ζωής συχνά αναγνωρίζεται ως ανθρώπινο δικαίωμα, δεν υπάρχει συναίνεση σχετικά με το τι συνεπάγεται η προστασία της ιδιωτικής ζωής ή με το πώς μπορούν να αντιμετωπιστούν οι αξίες αυτές επαρκώς στην πολιτική και το δίκαιο. Σε εθνικό ή περιφερειακό επίπεδο, το Ίντερνετ των πραγμάτων έχει γίνει αναπόσπαστο μέρος της τεχνολογίας των πληροφοριών και των επικοινωνιών (ΤΠΕ), και

ανησυχίες σχετικά με την προστασία της ιδιωτικής ζωής και των προσωπικών δεδομένων αντιμετωπίζονται με διάφορους τρόπους ανά χώρα. Στις Ηνωμένες Πολιτείες για παράδειγμα, δεν υπάρχει συνολική νομοθεσία για την προστασία της ιδιωτικής ζωής. Σε ομοσπονδιακό επίπεδο, διάφοροι οργανισμοί όπως η Δράση για την ιδιωτικότητα των ηλεκτρονικών επικοινωνιών (Electronic Communications Privacy Act, 1986), δεν αντιμετωπίζουν επαρκώς τις σύγχρονες τεχνολογίες πληροφορίας, τα δεδομένα που συγκεντρώνονται και ανταλλάσσονται στο διαδίκτυο και τις νέες πρακτικές και τεχνολογίες που αναπτύσσονται.

Σκοπός είναι να εντοπιστούν και να κατανοηθούν οι συγκεκριμένες αλλαγές που θα επιφέρει το Διαδίκτυο των πραγμάτων οι οποίες είναι πιθανό να εκληφθούν ως παραβιάσεις της ιδιωτικής ζωής των πολιτών. Στην Ευρώπη τουλάχιστον έχουν εκδοθεί αρκετά ψηφίσματα από το Ευρωπαϊκό Κοινοβούλιο σχετικά με νομικά θέματα που αφορούν στο ιντερνέτ των πραγμάτων. Σε ένα από αυτά, το οποίο εγκρίθηκε τον Ιούνιο του 2010, το Κοινοβούλιο θεωρεί ότι η ανάπτυξη νέων εφαρμογών διαδικτύου είναι άρρηκτα συνδεδεμένη με την εμπιστοσύνη των καταναλωτών. Θεωρεί ότι εμπιστοσύνη υπάρχει όταν δεν υπάρχουν αμφιβολίες σχετικά με ενδεχόμενες απειλές που η νέα τεχνολογία θα φέρει. Ένας πολύ σημαντικός παράγοντας που ενδέχεται να λάβει τεράστιες διαστάσεις σχετικά με το internet των πραγμάτων είναι η προστασία της ιδιωτικής ζωής και γενικότερα η προστασία των προσωπικών δεδομένων. Το Ευρωπαϊκό Συμβούλιο τονίζει ότι η εμπιστοσύνη αυτή πρέπει να βασίζεται σε ένα σαφές νομικό πλαίσιο, συμπεριλαμβανομένων των κανόνων που διέπουν τον έλεγχο, τη συλλογή, την επεξεργασία και τη χρήση των δεδομένων που συλλέγονται και διαβιβάζονται από το Ίντερνετ των πραγμάτων, καθώς και τους τύπους της συμμόρφωσης που απαιτείται από τους καταναλωτές. Μόνο εφόσον εξασφαλιστούν όλα

τα παραπάνω, το Ίντερνετ των πραγμάτων θα μπορέσει να αποκτήσει ευρύτερη κοινωνική αποδοχή.

Ο σεβασμός της ιδιωτικής ζωής και η προστασία προσωπικών δεδομένων έχει πολλές συνιστώσες. Σύμφωνα με τη γνώμη του Ευρωπαίου Επόπτη Προστασίας Δεδομένων (ΕΕΠΔ),η σημασία της ιδιωτικής ζωής θα πρέπει να λαμβάνεται υπόψη από τα πρώτα στάδια κατασκευής της νέας τεχνολογίας. Πολύ σημαντικό ρόλο εδώ διαδραματίζουν οι φορείς εποπτείας της νέας τεχνολογίας, ένας εκ των οποίων είναι η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων, η οποία ρυθμίζει και εποπτεύει τον τομέα των τηλεπικοινωνιακών και των ταχυδρομικών υπηρεσιών.

3.2 **Ηθική και** IoT

Ξεκινώντας τη διερεύνηση των νομικών παραμέτρων, πρέπει να γίνει απαραίτητα λόγος για την ουσιαστική σημασία της ηθικής που αφορά στο ίντερνετ των πραγμάτων και η οποία συνοψίζεται στο ακόλουθο ρητό: «Η δύναμη και η ευθύνη πρέπει να βρίσκονται σε ισορροπία». Όποιος συνεργάτης έχει περισσότερη δύναμη σε μια συναλλαγή, έχει επίσης και την ευθύνη να εξασφαλίσει ένα περιβάλλον εμπιστοσύνης και αξιοπιστίας.

Για να διατηρηθεί η ισορροπία ευθύνης και δύναμης, θα πρέπει να προάγεται η εμπιστοσύνη και η εξέλιξη της Πληροφορικής. Η ηθική προσέγγιση της χρήσης του IoT μπορεί να συνοψιστεί στις παρακάτω εντολές:

1. **Σεβασμός της Εμπιστευτικότητας**

Σε περίπτωση που οι συλλέκτες ή και προμηθευτές δεδομένων επιθυμούν να διαβιβάσουν ή να μοιραστούν με άλλους οργανισμούς

(κυβερνητικούς ή μη) τα δεδομένα, πρέπει να σιγουρευτούν ότι είναι επιτρεπτό. Εάν αυτό είναι δύσκολο, πρέπει να αφαιρέσουν όλες τις προσωπικές πληροφορίες που έχουν συλλέξει για τον καταναλωτή κατά την αγορά του προϊόντος.

2. **Επεξεργασία των δεδομένων**

Τα συγκεντρωμένα στοιχεία δεν πρέπει να εκδοθούν χωρίς να έχουν επεξεργαστεί, ειδάλλως μπορούν να προκαλέσουν μεγάλη ζημιά στον καταναλωτή για τον οποίο αρχικά συλλέχθηκαν. Το δεδομένα που παραδίδονται ηλεκτρονικά είναι εύκολο να μεταφερθούν, να επαναχρησιμοποιηθούν και να τροποποιηθούν με ανυπολόγιστες συνέπειες.

3. **Όχι στην ανωνυμία**

Οι συλλέκτες δεδομένων και οι κάτοχοι βάσεων δεδομένων πρέπει να δηλώνουν πότε, πού, πώς και για ποιο σκοπό συλλέχθηκαν τα στοιχεία, κατά τη διάδοση τους σε τρίτους.

4. **Να μην επιτρέπεται η πρόσβαση σε στοιχεία τρίτων**

Η πρόσβαση σε στοιχεία άλλου ατόμου δεν είναι δικαιολογημένη, εκτός αν ενεργείται με την άδειά του. Η εξέταση στοιχείων και πληροφοριών κάποιου, χωρίς πραγματικούς και ισχυρούς λόγους, είναι παράνομη.

5. **Τήρηση των κυβερνητικών γενικών οδηγιών**

Οι κάτοχοι βάσεων προσωπικών δεδομένων πρέπει να ελέγξουν για να δουν εάν ο φορέας παροχής υπηρεσιών, ακολουθεί την υφιστάμενη νομοθεσία και πολιτική.

6. **Κατάλληλη παρουσίαση του μηνύματος**

Οι κάτοχοι βάσεων δεδομένων πρέπει να αξιολογήσουν το περιεχόμενο των στοιχείων που διαδίδονται. Πρέπει να γνωρίζουν τις

πολιτιστικές διαφορές ή άλλα ζητήματα που μπορούν να έχουν επιπτώσεις στον παραλήπτη. Έστω και ένας ιδιοκτήτης βάσης δεδομένων να μην ακολουθεί την πολιτική αυτή, θα πρέπει τελικά να την εφαρμόσει, καθώς επίσης και να καθιερώσει μία πρακτική η οποία να λαμβάνει υπόψη όλες τις ανησυχίες των καταναλωτών περί παραβίασης του ιδιωτικού απορρήτου. Οι φορείς χάραξης πολιτικής, όταν βρίσκονται αντιμέτωποι με ένα ζήτημα προστασίας ιδιωτικού απορρήτου, θα πρέπει πρώτα να καθορίσουν εάν ο υφιστάμενος νόμος αντιμετωπίζει το ζήτημα.

«Μεγάλος αδελφός»

Φέροντας πλέον κανείς ένα μοναδικό αναγνωριστικό παντού μαζί του, ο κίνδυνος του μεγάλου αδερφού είναι πιο υπαρκτός από ποτέ. Hackers είναι πιθανόν να αποκτήσουν πρόσβαση στο μοναδικό αναγνωριστικό του είτε στην βάση δεδομένων όπου αποθηκεύονται οι ενέργειες αυτού και να μπορούν πλέον να παρακολουθούν κάθε του κίνηση.

Οι καταναλωτικές συνήθειες καθώς και λεπτομερή προσωπικά δεδομένα, μπορούν να περιέλθουν στην δικαιοδοσία μη εξουσιοδοτημένων πρόσωπων, από ασφαλιστικούς φορείς, έως και κυβερνητικές αντιπροσωπείες, εάν αποφασισθεί ότι η πώληση των προσωπικών πληροφοριών θα αποφέρει κέρδος. Επίσης υπάρχουν πιθανότητες τα στοιχεία που συλλέγονται από τα εξουσιοδοτημένα συμβαλλόμενα μέρη να πέσουν στα χέρια απατεώνων, εάν το σύστημα ασφάλειας και πρόσβασης δεν είναι σύμφωνο με ορισμένα πρότυπα.

3.3 **Διαμόρφωση πολιτικής - Ερωτήσεις Τακτικής-Ασφάλεια**

Αναφορικά και σε άμεση σχέση με το θέμα της ασφάλειας εύλογα κανείς θα αναρωτηθεί για τα παρακάτω:

1. "Ποιός έχει την ευθύνη στην καθιέρωση μιας υπεύθυνης πολιτικής σχετικά με την πρόσβαση και την κοινοποίηση των δεδομένων μιας βάσης δεδομένων; Πώς η πολιτική έχει επιπτώσεις στους καταναλωτές, στους λιανοπωλητές, στους κατασκευαστές, σε τρίτους φορείς, στις αρχές επιβολής του νόμου και στους φορείς παροχής υπηρεσιών αποθήκευσης δεδομένων;"

2. "Ποιά βασικά νόμιμα δικαιώματα και υποχρεώσεις περιορίζουν οποιαδήποτε πολιτική;"

3. "Ποιά λειτουργικά χαρακτηριστικά γνωρίσματα του RFID και της συλλογής δεδομένων, της αποθήκευσης και των συστημάτων διάδοσης πρέπει να έχουν επιπτώσεις σε οποιαδήποτε πολιτική για την πρόσβαση, τη χρήση και την κοινοποίηση;"

4."Ποιά κριτήρια πρέπει να χρησιμοποιηθούν για την αξιολόγηση των προτεινόμενων πολιτικών;"

5. "Η πολιτική έχει γνωστοποιηθεί εκ των προτέρων σε όλους τους ενδιαφερομένους;"

6. "Ποιοί πρέπει να συμμετέχουν στην ανάπτυξη της πολιτικής, από τις επιχειρήσεις, τους υποστηρικτές του ιδιωτικού απορρήτου και τις κυβερνητικές αντιπροσωπείες;"

7. "Ποιοί εταιρικοί πόροι, από άποψη κόστους, χρόνου και προσωπικού, πρέπει να χρησιμοποιηθούν για τη διατύπωση των γενικών πολιτικών ιδιωτικού απορρήτου;"

8. "Ποιές πληροφορίες πρέπει να συλλεχθούν εκ των προτέρων ή και κατά τη διάρκεια της διατύπωσης της πολιτικής;"

9. "Ποιό είδος ερευνητικών μεθόδων θα χρησιμοποιηθεί από τους φορείς χάραξης πολιτικής για να καταγραφεί και να αναλυθεί η κοινή γνώμη και μέχρι ποιό επίπεδο; "

3.4 **Διαφορές ανάμεσα στους πολιτισμούς και τις ηπείρους σχετικά με το απόρρητο προσωπικών πληροφοριών**.

Σε σχέση με τα προαναφερθέντα, θα πρέπει να δοθεί απαραίτητα βάση στις διαφοροποιήσεις που παρουσιάζονται πάνω στα ζητήματα αυτά και που πηγάζουν από τη διαφορετικότητα των λαών και των ευρύτερων αντιλήψεων. Οι Ηνωμένες Πολιτείες και η Ευρώπη κυρίως υιοθετούν πολύ διαφορετικές προσεγγίσεις σχετικά με το απόρρητο των προσωπικών πληροφοριών τόσο από ρυθμιστική όσο και από διοικητική σκοπιά. Στηριζόμενες στις διαφορετικές πολιτιστικές αξίες και τις υποθέσεις σχετικά με τη σημασία του ιδιωτικού απορρήτου, οδηγήθηκαν σε ρυθμιστικές και διοικητικές συγκρούσεις. Γενικότερα, οι Ηνωμένες Πολιτείες δεν εξυπηρετούνται από τη δημιουργία μιας ομοσπονδιακής ρυθμιστικής δομής όπως συνηθίζεται στην Ευρώπη.

Κατά συνέπεια βλέπουμε ότι εάν οι ΗΠΑ δεν δημιουργήσουν μία περιεκτική πολιτική PIA, τότε πιθανότατα να προκύψουν τα ακόλουθα προβλήματα:

1. Δεδομένου ότι οι ΗΠΑ στερούνται σημαντικών μέτρων PIA σε πολλούς τομείς, κάποιες αμερικανικές επιχειρήσεις μπορεί να μην είναι σε θέση να συναλλαγούν με επιχειρήσεις στην Ευρώπη και οι υπεύθυνοι προστασίας του ιδιωτικού απορρήτου στην Ευρωπαϊκή Ένωση να περιορίσουν τη ροή των προσωπικών στοιχείων προς τις ΗΠΑ λόγω της ανεπαρκούς προστασίας των καταναλωτών.

2. Επιπλέον υπάρχει κίνδυνος αύξησης της δυσπιστίας των καταναλωτών ως προς τους οργανισμούς (δημόσιους και ιδιωτικούς).

Οι ηθικές επιπτώσεις της PIA για την εφαρμογή του RFID δεν έχουν ερευνηθεί αρκετά, αλλά μπορούν να χαρτογραφηθούν στις υπάρχουσες πολιτικές και τις διαδικασίες που ακολουθούνται από τους εμπόρους και την επιχειρηματική κοινότητα.

Οι κυβερνήσεις σε όλο τον κόσμο, πλαισιώνοντας τη δημόσια πολιτική, πρέπει παράλληλα να λάβουν μέτρα για τις πολιτικές PIA έτσι ώστε να εξασφαλίζεται ο τρόπος με τον οποίο συγκεντρώνονται τα στοιχεία των καταναλωτών, από οργανισμούς που χρησιμοποιούν το RFID, καθώς και ο τρόπος με τον οποίο χρησιμοποιούνται τα συγκεντρωθέντα στοιχεία.

3.5 **Αποδοχή του** Internet **των πραγμάτων**.

Ένα από τα μεγαλύτερα προβλήματα στις νέες τεχνολογίες είναι η αποδοχή τους από το κοινό και τους λόγους για τους οποίους γίνονται αποδεκτές ή μη. Το Internet των Πραγμάτων θα συμβάλει στην αντιμετώπιση πολλών προβλημάτων όπως προαναφέρθηκε.

Με τη σειρά του, θα εισαγάγει προβλήματα, ορισμένα από τα οποία θα επηρεάσουν άμεσα τους πολίτες. Για παράδειγμα, ορισμένες εφαρμογές μπορεί να είναι στενά συνδεδεμένες με υποδομές ζωτικής

σημασίας, όπως η παροχή ενέργειας, ενώ άλλες θα χειρίζονται πληροφορίες σχετικές με το ιατρικό ιστορικό του ατόμου. Σε αυτή την περίπτωση, η ιδιωτικότητα των προσωπικών δεδομένων και της ιδιωτικής ζωής πώς θα διασφαλίζονται;

Τίθενται σαφώς ερωτήματα για το ποιός θα έχει πρόσβαση σε αυτά τα δεδομένα και πώς μπορεί να επιτραπεί πρόσβαση σε τρίτους. Για παράδειγμα, σε μια υπηρεσία ιατρικής παρακολούθησης, πώς θα διασφαλίζεται ότι άτομα από την εταιρεία υλοποίησης της υπηρεσίας δε θα έχουν πρόσβαση ή σε περίπτωση που χρειαστεί να υπάρξει πρόσβαση, ποιός τελικά θα έχει;

Για την επίλυση τέτοιου είδους προβλημάτων θα χρειαστεί η συνεργασία των επιχειρήσεων (ιδιωτικός φορέας) με τις κρατικές αρχές. Αν δεν δοθεί απάντηση σε όλους τους αναφερθέντες προβληματισμούς, θα μπορούσαν να υπάρξουν σοβαρές αρνητικές συνέπειες, όπως:

- η αποκάλυψη προσωπικών δεδομένων ενός ατόμου ή η έκθεση σε κίνδυνο του απορρήτου των επιχειρηματικών δεδομένων
- να οδηγηθούμε σε έλλειψη καινοτομίας αν αποδοθούν λάθος δικαιώματα και υποχρεώσεις στις επιχειρήσεις (ιδιωτικός φορέας)
- να τεθεί σε κίνδυνο η ίδια η λειτουργία του Internet των Πραγμάτων από την έλλειψη λογοδοσίας και καταλογισμού ευθυνών

Το ηθικό και νομικό πλαίσιο το οποίο οφείλει να ισχύει για τα διάφορα ενδιαφερόμενα μέρη με σκοπό την προάσπισή τους και την αποφυγή περεταίρω κίνδυνου, είναι καθήκον των υπευθύνων οργανισμών να το ορίσουν και να το διασφαλίσουν.

3.6 **Οι Ρυθμιστικές Αρχές και ο ρόλος τους**.

Το IoT αναμένεται να προκαλέσει σαρωτικές αλλαγές κοινωνικά και τεχνολογικά καθώς νέες εφαρμογές και συστήματα θα αναπτυχθούν, ενώ παράλληλα θα δημιουργήσει επιχειρηματικές ευκαιρίες. Η μετάβαση όμως στην κοινωνία του IoT δεν θα πρέπει να γίνει άναρχα, αλλά συγκροτημένα, βασισμένη σε κανόνες κατανοητούς και εφαρμόσιμους για όλους. Οι ρυθμιστικές Αρχές είναι αυτές που είναι αρμόδιες να οριοθετήσουν ένα νομικό περιβάλλον το οποίο θα εξασφαλίζει τόσο την ομαλή μετάβαση, όσο και τη διασφάλιση από τους κινδύνους όλων των μερών που εμπλέκονται σε αυτό. Τα συγκρουόμενα συμφέροντα είναι τεράστια γι' αυτό και θα πρέπει να υπάρχει σαφής κατανομή αρμοδιοτήτων , περιοριστικοί κανόνες και δικλείδες διασφάλισης της ιδιωτικότητας και των προσωπικών δεδομένων, ώστε να μπορέσει να επιτευχθεί η υγιής υλοποίηση όλου αυτού του σχεδίου. Οφείλει να δοθεί βάση στην ανάληψη δράσεων με στόχο να προαχθεί η επιχειρηματικότητα , ταυτόχρονα να ληφθούν κατάλληλα μέτρα ώστε να ικανοποιηθούν οι πολιτικές των εθνικών Κυβερνήσεων, αλλά κυρίως να ανταποκριθεί το όλο σύστημα στις προσδοκίες που αναμφισβήτητα θα έχουν οι ίδιοι οι καταναλωτές .

Όσο το IoT διευρύνεται, τόσο θα προκύπτουν νέοι προβληματισμοί και ζητήματα που θα απαιτούν την άμεση επέμβαση των ρυθμιστικών αρχών. Θα πρέπει να βρεθεί τρόπος να καταπολεμηθεί η μη εξουσιοδοτημένη παρακολούθηση της πληροφορίας που διακινείται και σε ευρύτερο πλαίσιο θα πρέπει να προστατευτεί η ασφάλεια, το απόρρητο των προσωπικών δεδομένων, τα πνευματικά δικαιώματα και γενικότερα η προστασία του χρήστη από κινδύνους τους οποίους διατρέχει κρατώντας τον ρόλο αυτό.

Στην εποχή του IoT, μια από τις σημαντικότερες παραμέτρους που πρέπει να εξετάσουμε είναι η ανοικτή πρόσβαση σε όλους τους πάροχους, με τους ίδιους αντικειμενικούς και ισότιμους όρους , ώστε να προστατευτεί η επιχειρηματικότητα και ο υγιής ανταγωνισμός σε επίπεδο υπηρεσιών.

Η ουδετερότητα του δικτύου (Net Neutrality) είναι μια ακόμα φλέγουσα παράμετρος που πρέπει να ρυθμιστεί. Η απρόσκοπτη και χωρίς περιορισμούς κυκλοφορία δεδομένων έσω δικτύων, θα πρέπει να συνοδεύεται από διασυνδεσιμότητα των δικτύων αυτών και διαλειτουργικότητα των συσκευών , ώστε αυτές να μπορούν να συνδέονται σε όλα δίκτυα, παρέχοντας έτσι ενοποιημένες υπηρεσίες.

Το φάσμα των συχνοτήτων και η διαχείριση ενός τόσο σπάνιου πόρου είναι επίσης μια παράμετρος προς ρύθμιση. Τα πράγματα στο IoT είναι πάντα συνδεδεμένα και το φάσμα είναι ένας σημαντικότατος πόρος. Ήδη ανακοινώθηκε από την samsung το 5G δίκτυο και στην Νέα Υόρκη έχουν γίνει οι πρώτες δοκιμές . Στον Ελληνικό χώρο το 4G κάνει τα πρώτα του βήματα. Η ψηφιακή τηλεόραση είναι γεγονός και η αξιοποίηση του $2^{ου}$ ψηφιακού μερίσματος θα καταστεί επιτυχής μέσα από κατάλληλη ρύθμιση.

Ταυτόχρονα ρυθμιστικές αρχές που είναι υπεύθυνες για το θέμα της ιδιωτικότητας και της ασφάλειας, θα πρέπει να συνεργαστούν αρμονικά με αρχές που έχουν να κάνουν με τις ηλεκτρονικές επικοινωνίες καθώς και με αυτές που ορίζουν τα ευρύτερα πλαίσια του ανταγωνισμού. Θα πρέπει από κοινού να εργαστούν ώστε να καλύψουν ένα πολύ ευρύ φάσμα με τρόπο που να μην υποδαυλίζει η μια την άλλη, αλλά ούτε και να ξεπερνά τα προκαθορισμένα όρια.

Η προστασία της ιδιωτικότητας των χρηστών και των δεδομένων τους θα πρέπει να προαχθεί από την ανάπτυξη του IoT, ώστε να δομηθούν με στέρεες βάσεις και αρχές τα συστήματα και τα συστατικά του. Τα δίκτυα υψηλών ταχυτήτων θα πρέπει να

προσφέρουν αδιάλειπτη ασφάλεια των δεδομένων στον πελάτη π.χ κρυπτογραφία στα αποθηκευμένα δεδομένα στο cloud αλλά και προστασία των χρηστών από ακατάλληλο ή επιβλαβές περιεχόμενο.

Όταν το IoT θα έχει φτάσει στην πλήρη έκταση του, τότε πολλά και πολύ απαραίτητα συστήματα για τον άνθρωπο θα έχουν ενσωματωθεί σε αυτό π.χ. η υγεία, οι μεταφορές, κ εκπαίδευση και η ενέργεια. Αμέσως καταλαβαίνουμε πόσο απαραίτητη είναι η ασφάλεια καθώς το κυβερνοέγκλημα πλέον ανάγεται σε No1 κίνδυνο. Η τρομοκρατία πλέον θα δρα σε επίπεδό ηλεκτρονικών υπολογιστών. Πρόσφατο είναι το παράδειγμα του «σκουληκιού» Stuxnet που έθεσε έκτος λειτουργίας τις πυρηνικές εγκαταστάσεις του Ιράν. Άλλα τέτοιου είδους παραδείγματα είναι το hacking βηματοδοτών και συσκευών ενέσιμης ινσουλίνης που μπορούν να οδηγήσουν σε τραγικά αποτελέσματα. Το FBI αναφέρει την αύξηση στις προσπάθειες “hacking” συσκευών έξυπνης μέτρησης . Αναφέρονται ήδη έξυπνες συσκευές μέτρησης ηλεκτρικού ρεύματος στην Αμερική παραβιασμένες, έτσι ώστε να μειώνεται ο λογαριασμός του ρεύματος 50% έως 60%, κάτι το οποίο μπορεί να οδηγήσει σε μια ζημία 400 εκατομμύριων δολαρίων τις εταιρείες ηλεκτροδότησης.

Το IoT θα γεννήσει και ανάγκές νέων μορφών αδειοδότησης και πώλησης προϊόντων ή υπηρεσιών, οπότε θα πρέπει νέες μορφές προστασίας των πνευματικών δικαιωμάτων να υλοποιηθούν για να προστατευτούν εταιρίες και δημιουργοί. Εάν υποθέσουμε ότι τελικός σκοπός είναι ένα ευρυζωνικό δίκτυο να παραδοθεί στα χέρια κάθε καταναλωτή προς χρήση και εξυπηρέτηση του, ως καθολική υπηρεσία, τότε αυτό που μένει είναι να βρεθούν οι κατάλληλες πηγές που θα μπορέσουν να χρηματοδοτήσουν τον απώτερο αυτό στόχο . Φυσικά κάτι τέτοιο θα μπορούσε ακόμα να επιτευχθεί μέσω της ίδια της αγοράς αλλά και μέσω της ενίσχυσης που θα προσφέρει το ίδιο το κράτος. Εάν μπορέσει ο ρυθμιστής του νομικού πλαισίου να

κατανοήσει, να ιεραρχήσει , να υιοθετήσει και να πορευτεί μαζί με όλη αυτή τη διαδικασία, τότε θα κάνουμε λόγο για την ποθητή σύγκλιση του ρυθμιστή και των διαφόρων τεχνολογικών προσεγγίσεων.

3.7 **Ελληνικό Νομικό Πλαίσιο**

Ας δούμε λοιπόν τι ορίζεται στον ελληνικό χώρο για το θέμα που συζητούμε. σύμφωνα με τις αρμόδιες αρχές, η αποθήκευση, διατήρηση και επεξεργασία δεδομένων προσωπικού χαρακτήρα, η χρήση ραδιοσυχνοτήτων και η λειτουργία των συσκευών ραδιοσυχνικής αναγνώρισης (RFID) ,υπόκεινται κυρίως στο παρακάτω νομοθετικό πλαίσιο:

- Π.Δ. υπ' αρίθμ 44 «Ραδιοεξοπλισμός και τηλεπικοινωνιακός τερματικός εξοπλισμός και αμοιβαία αναγνώριση της συμμόρφωσης των εξοπλισμών αυτών - Προσαρμογή της ελληνικής νομοθεσίας στην οδηγία 99/5/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 9 Μαρτίου 1999» (ΠΔ 44/2002, ΦΕΚ 44/Α/7-3-2002). [5]

- Νόμος υπ' αρίθμ 3431 «Περί Ηλεκτρονικών Επικοινωνιών και άλλες διατάξεις» (Ν. 3431/2006, ΦΕΚ 13/Α/03-02-2006). [4]

- Ν. 2472/1997 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα και ο ειδικότερος και συμπληρωματικός Ν. 2774/1999

- Απόφαση αριθμ. οικ. 17225/655 των υπουργών Εθνικής Άμυνας και Μεταφορών και Επικοινωνιών, «Έγκριση Εθνικού Κανονισμού Κατανομής Ζωνών Συχνοτήτων (ΕΚΚΖΣ)» (Αριθμ. Οικ. 17225/655, ΦΕΚ 399/Β/3-4-2006). [1]

• Απόφαση αριθμ. οικ. 390/1 της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ), «Κανονισμός Χρήσης και Χορήγησης Δικαιωμάτων Χρήσης Ραδιοσυχνοτήτων υπό καθεστώς Γενικής Άδειας για τη Παροχή Δικτύων ή / και Υπηρεσιών Ηλεκτρονικών Επικοινωνιών» (Αριθμ. Οικ. 390/1, ΦΕΚ 750/Β/21-6-2006). [2]

• Απόφαση αριθμ. οικ. 399/34 της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ), «Κανονισμός Όρων Χρήσης Μεμονωμένων Ραδιοσυχνοτήτων ή Ζωνών Ραδιοσυχνοτήτων» (Αριθμ. Οικ. 399/34, ΦΕΚ 1456/Β/3-10-2006). [3]

• Νόμος υπ' αρίθμ 4070 «Ρυθμίσεις Ηλεκτρονικών Επικοινωνιών, Μεταφορών, Δημοσίων Έργων, και άλλες διατάξεις» (Ν.4070/2012,ΦΕΚ 82/10-04-2012)

Διαπιστώνουμε λοιπόν ένα μεγάλο ενδιαφέρον του ελληνικού κράτους για να μπορέσει να ρυθμίσει τις διάφορες παραμέτρους του Iot, αναγνωρίζοντας την εξαιρετική σημασία του.

3.7.1 **Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ**.)

Σημαντικό ρόλο αναμφισβήτητα διαδραματίζει η Εθνική Ρυθμιστική Αρχή (NRA), η λεγόμενη Ε.Ε.Τ.Τ, η οποία συστάθηκε με το Νόμο 2246/1994 και διαχειρίζεται θέματα παροχής δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών, συναφών ευκολιών και συναφών υπηρεσιών. Σύμφωνα με το Νόμο 3431/2006, σε αυτή υπόκεινται ο έλεγχος, η ρύθμιση και η εποπτεία της αγοράς των ηλεκτρονικών επικοινωνιών. Οι αποφάσεις της Ε.Ε.Τ.Τ. γνωστοποιούνται με μέριμνά της στον Υπουργό Μεταφορών και Επικοινωνιών.

Ίσως η σημαντικότερη αρμοδιότητα της Ε.Ε.Τ.Τ. να είναι ο έλεγχος της ποιότητας της καθολικής υπηρεσίας. Η διασφάλιση της καθολικής υπηρεσίας και η ενσωμάτωση της ευρυζωνικότητας σε αυτή, είναι το μεγαλύτερο βήμα προς το IoT. Αυτό είναι ένα μεγάλο στοίχημα της ΕΕΤΤ προς ρύθμιση.

Η ΕΕΤΤ επίσης διαχειρίζεται το φάσμα συχνοτήτων και σίγουρα η επιτυχής ρύθμισή του είναι άλλο ένα μεγάλο βήμα προς την ψηφιακή εποχή του IoT. Δίκτυα 4G, 5G αλλά και το φάσμα της ψηφιακής τηλεόρασης με τη σύγκλιση τεχνολογιών και πλατφόρμων π.χ θέαση τηλεόρασης στο κινητό μας, θα δημιουργήσει πολλούς καινούργιους προβληματισμούς για τη ρύθμιση και διαμοίραση του φάσματος.

Επιπροσθέτως, στις αρμοδιότητες της ΕΕΤΤ περιλαμβάνεται και η διατήρηση του ανταγωνισμού σε υγιές επίπεδο, καθώς νέα επαγγέλματα, νέες επιχειρηματικές ευκαιρίες και επιχειρηματικά μοντέλα θα αναδειχθούν. Με τις σωστές ρυθμίσεις θα αποφευχθούν μονοπωλιακές καταστάσεις που μόνο πίσω μπορούν να πάνε την ανάπτυξη του IoT σε βάρος του τελικού χρήστη. Η ρύθμιση θα πρέπει να κατευθύνεται προς τη διαθεσιμότητα των αναβαθμισμένων δικτύων προς όλους, σε προσιτές τιμές, ευρυζωνική πρόσβαση σε υπηρεσίες παντού, πάντα ανεξάρτητα από τεχνολογία, πάροχο και γεωγραφική περιοχή.

Η ΕΕΤΤ εν κατακλείδι, εκχωρεί δικαιώματα πρόσβασης σε σύνδεση ή σε δίκτυο παροχής υπηρεσιών τηλεφωνίας . Είναι πολύ σημαντικό να ελεγχθεί ποιοί παίρνουν αυτή την πρόσβαση ώστε να μην δημιουργούνται κενά ασφαλείας στο IoT και ανεπιθύμητη πρόσβαση στα προσωπικά δεδομένα.

3.7.2 **Η Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα**.

Απαραίτητο όμως είναι να γίνει αναφορά και στην Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, η οποία ως ανεξάρτητη αρχή διασφαλίζει, εποπτεύει και έχει τη συνολική ευθύνη για την εφαρμογή της νομοθεσίας περί προστασίας των δεδομένων περιλαμβανομένων και των τηλεπικοινωνιακών με την έκδοση αποφάσεων και γνωμοδοτήσεων. Κάποιες αρμοδιότητες σχετικά με την επεξεργασία των προσωπικών δεδομένων και την προστασία της ιδιωτικότητας στον τηλεπικοινωνιακό τομέα ασκούνται σε συνεργασία με την Ε.Ε.Τ.Τ.

Οι αρμοδιότητες της αρχής σύμφωνα με τον Ν.2472/1997 διακρίνονται σε δύο μεγάλες κατηγορίες:

α) τις ρυθμιστικές

Η Αρχή εκδίδει οδηγίες με σκοπό την ενιαία εφαρμογή των ρυθμίσεων που αφορούν στην προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα, κανονιστικές πράξεις για τη ρύθμιση ειδικών, τεχνικών και λεπτομερειακών θεμάτων, αλλά και μιλά με επαγγελματικά σωματεία και λοιπές ενώσεις φυσικών ή νομικών προσώπων που διατηρούν αρχεία δεδομένων προσωπικού χαρακτήρα με σκοπό την κατάρτισή τους όσον αφορά κώδικες δεοντολογίας. Εξετάζει επιπλέον αιτήσεις του υπευθύνου επεξεργασίας, απευθύνει συστάσεις και υποδείξεις στους υπεύθυνους επεξεργασίας και συνεργάζεται με τις αρχές άλλων κρατών μελών για την έκδοση οδηγιών. Τέλος, γνωμοδοτεί για κάθε νομοθετική ή κανονιστική ρύθμιση που αφορά στην επεξεργασία και προστασία δεδομένων προσωπικού χαρακτήρα.

β) Ελεγκτικές

Εδώ η Αρχή εξετάζει καταγγελίες, προσφυγές, αντιρρήσεις και παράπονα σχετικά με την εφαρμογή του νόμου. Διενεργεί αυτεπάγγελτα ή κατόπιν καταγγελίας, ελέγχους στην τεχνολογική υποδομή και στα μέσα που υποστηρίζουν την επεξεργασία δεδομένων, εξετάζει τις γνωστοποιήσεις που υποβάλλονται και χορηγεί άδειες ίδρυσης και λειτουργίας αρχείου ευαίσθητων δεδομένων, διαβίβασης δεδομένων σε χώρες εκτός Ε.Ε. και διασύνδεσης αρχείων στην περίπτωση που αφορούν ευαίσθητα δεδομένα. Εξετάζει τέλος τις αιτήσεις για πρόσβαση σε δημόσια και ιδιωτικά έγγραφα που περιέχουν προσωπικά δεδομένα τρίτων.

Στο IoT θα συνδέεται μια ανεξάντλητη βάση πραγμάτων που θα δημιουργούν μια πολύ πλούσια και συνεχή ροή δεδομένων. Η διαφύλαξη της ιδωτικότητας αυτών των δεδομένων, το πού θα φυλάσσονται και το ποιός και πότε θα έχει πρόσβαση σε αυτά, είναι το πολύ σημαντικό έργο της παραπάνω ρυθμιστικής αρχής.

3.7.3 **Η Αρχή Διασφάλισης του Απορρήτου των επικοινωνιών**.

Τέλος, η Αρχή Διασφάλισης του Απορρήτου των επικοινωνιών (ΑΔΑΕ) λειτουργεί από το 2003 ως ανεξάρτητη αρχή σύμφωνα με τις διατάξεις του Ν3115/2003. Ο σκοπός της ΑΔΑΕ είναι η προστασία του απορρήτου των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο. Στην έννοια της προστασίας του απορρήτου των επικοινωνιών περιλαμβάνεται και ο έλεγχος της τήρησης των όρων και της διαδικασίας άρσης του απορρήτου.

Το IoT θα είναι ένας κόσμος συνεχόμενης επικοινωνίας με αμέτρητες πληροφορίες να βρίσκονται σε αυτό. Τα datacenters όπου θα

φιλοξενούνται δεδομένα και υπηρεσίες του IoT, θα είναι πάρα πολλά και στις αρμοδιότητες της αρχής αυτής είναι η διενέργεια τακτικών και έκτακτων ελέγχων σε τέτοιες εγκαταστάσεις, είτε δημόσιες είτε ιδιωτικές, για τη διασφάλιση του απορρήτου και τις ιδιωτικότητας. Ελέγχει επίσης από πλευρά νομιμότητας σε ό,τι αφορά τους όρους και τις διαδικασίες που ακολουθούνται κατά την εφαρμογή των διατάξεων για την άρση του απορρήτου, σύμφωνα με τα προβλεπόμενα από την υπάρχουσα νομοθεσία. Μπορεί και διενεργεί ακόμα ακροάσεις των παρόχων υπηρεσιών ηλεκτρονικών επικοινωνιών για πιθανές παραβάσεις της κείμενης νομοθεσίας σχετικά με τις πολιτικές ασφάλειας για τη διασφάλιση του απορρήτου των επικοινωνιών.

Η Αρχή επιπροσθέτως εξετάζει καταγγελίες για παραβίαση του απορρήτου τηλεφωνικών και διαδικτυακών επικοινωνιών και επιβάλλει τις προβλεπόμενες διοικητικές κυρώσεις με βάση το άρθρο 11 του Ν. 3115/2003, σε συνδυασμό με το άρθρο 11 του Ν. 3674/2008, σε περιπτώσεις που διαπιστώνεται παραβίαση της κατάθεσης περί απορρήτου των επικοινωνιών ή περί άρσης του απορρήτου. Επίσης προχωράει σε κανονιστικές και άλλες αναγκαίες πράξεις αναφορικά με τα εφαρμοστέα μέτρα για τη διασφάλιση του απορρήτου των επικοινωνιών.

3.8 **Προστασία προσωπικών δεδομένων και ασφάλεια απορρήτου των επικοινωνιών στον τηλεπικοινωνιακό τομέα**.

Η προστασία του ατόμου από τη συλλογή, επεξεργασία και χρήση προσωπικών δεδομένων στον τηλεπικοινωνιακό τομέα θεσμοθετείται από το άρθρο 9Α, και συνιστά παράλληλα, μία από τις βασικές αρχές

για την οργάνωση και λειτουργία του τομέα των τηλεπικοινωνιών.

Οι διατάξεις των Ν. 2472/1997 για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα και ο ειδικότερος και συμπληρωματικός Ν. 2774/1999 περί προστασίας δεδομένων προσωπικού χαρακτήρα στον τηλεπικοινωνιακό τομέα, έχουν σχεδόν εφαρμόσει αυτολεξεί τις αντίστοιχες κοινοτικές οδηγίες 95/46/24/10/1995 και 97/66/15/12/1997.

Ειδικότερα, αναφορικά με την προστασία προσωπικών δεδομένων και του απορρήτου των τηλεπικοινωνιών, η κείμενη νομοθεσία προβλέπει τα ακόλουθα:

(1) Σύμφωνα με το άρθρο 9Α του Συντάγματος καθένας έχει δικαίωμα προστασίας από τη συλλογή, επεξεργασία και χρήση, ιδίως με ηλεκτρονικά μέσα, των προσωπικών του δεδομένων, όπως ο νόμος ορίζει.

(2) Σύμφωνα με το άρθρο 19 παρ. 1 του Συντάγματος το απόρρητο των επιστολών και της ελεύθερης ανταπόκρισης ή επικοινωνίας με οποιονδήποτε άλλο τρόπο, είναι απόλυτα απαραβίαστο. Ο νόμος ορίζει τις εγγυήσεις υπό τις οποίες η δικαστική αρχή δε δεσμεύεται από το απόρρητο για λόγους εθνικής ασφαλείας ή για διακρίβωση ιδιαίτερα σοβαρών εγκλημάτων.

(3) Σύμφωνα με το άρθρο 9 παρ. 2, στ. (ε) του Ν. 2867/2000 κάθε χρήστης έχει το δικαίωμα να διατηρεί εμπιστευτικό και απόρρητο το χαρακτήρα των επικοινωνιών του.

(4) Σύμφωνα με το άρθρο 4 παρ. 1 του Ν. 2774/1999 οποιαδήποτε χρήση των τηλεπικοινωνιακών υπηρεσιών, όπως ορίζονται στον παρόντα νόμο, προστατεύεται από τις ρυθμίσεις για το απόρρητο των επικοινωνιών. Η άρση του απορρήτου σε δημόσιες αρχές είναι

επιτρεπτή μόνο για τους λόγους και υπό τους όρους και διαδικασίες που ορίζει ο Ν. 2225/1994.

(5) Σύμφωνα με το άρθρο 4 παρ. 2 του Ν. 2774/1999 η επεξεργασία δεδομένων προσωπικού χαρακτήρα μόνο αν έχει προηγηθεί η συγκατάθεση του χρήστη και η επεξεργασία, είναι αναγκαία για την εκτέλεση σύμβασης ή κατά το προσυμβατικό στάδιο.

(6) Σύμφωνα με το άρθρο 5 παρ. 1 του Ν. 2472/1997 η επεξεργασία δεδομένων προσωπικού χαρακτήρα επιτρέπεται μόνο όταν το υποκείμενο των δεδομένων έχει δώσει τη συγκατάθεσή του ή κατ' εξαίρεση χωρίς τη συγκατάθεσή του στις περιοριστικά απαριθμούμενες περιπτώσεις του νόμου.

(7) Σύμφωνα με το άρθρο 1 παρ. 2 του Ν. 2225/1994 αποστολή της Εθνικής Επιτροπής Προστασίας Απορρήτου των Επικοινωνιών είναι α) η προστασία του απορρήτου των επιστολών και της τηλεφωνικής και κάθε άλλης μορφής τηλεπικοινωνιακής ανταπόκρισης ή επικοινωνίας κατά το άρθρο 19 του Συντάγματος και β) ο έλεγχος της τήρησης των όρων άρσης του απορρήτου που έθεσε η δικαστική αρχή.

(8) Σύμφωνα με το άρθρο 370Α του Ποινικού Κώδικα κολάζεται ποινικά όποιος αθέμιτα παγιδεύει ή με οποιονδήποτε άλλο τρόπο παρεμβαίνει σε τηλεφωνική σύνδεση ή συσκευή με σκοπό να πληροφορηθεί ή να μαγνητοφωνήσει το περιεχόμενο τηλεφωνικής συνδιάλεξης μεταξύ τρίτων.

(9) Σύμφωνα με το άρθρο 370 του Ποινικού Κώδικα τιμωρείται ποινικά όποιος αθέμιτα και με σκοπό να λάβει γνώση του περιεχομένου τους ανοίγει κλειστή επιστολή ή άλλο κλειστό έγγραφο ή παραβιάζει κλειστό χώρο στον οποίο είναι φυλαγμένα αυτά, ή με οποιονδήποτε τρόπο εισχωρεί σε ξένα απόρρητα διαβάζοντας ,

αντιγράφοντας ή αποτυπώνοντας με άλλον τρόπο επιστολή ή άλλο έγγραφο.

Συνεπώς μια ομάδα νόμων αποπειράται να διασφαλίσει το ιδιωτικό απόρρητο και να προασπίσει το δικαίωμα του καθενός στην προστασία των προσωπικών του δεδομένων.

3.9 **Κοινοτικό Πλαίσιο**

Το ευρύτερο κοινοτικό πλαίσιο ορίζεται καθ ‘ υπόδειξη του Σώματος Ευρωπαίων Ρυθμιστών Ηλεκτρονικών Επικοινωνιών (BEREC). Βασικός στόχος του είναι να αναπτύξει ένα σύγχρονο δίκτυο και κατ’ επέκταση μια ανταγωνιστική αγορά ηλεκτρονικών επικοινωνιών σε συνδυασμό με τη σωστή αξιολόγηση της θέσης των καταναλωτών καθώς και την προστασία των δικαιωμάτων που αυτοί έχουν. Διαθέτοντας τη σύγχρονη τεχνογνωσία ο BEREC αποσκοπεί στη διαμόρφωση συγκεκριμένων ευρωπαϊκών πολιτικών με απώτερο σκοπό τη δημιουργία μιας δυνατής αλλά και υγιούς ψηφιακής αγοράς.

Ας δούμε λοιπόν κάποιους από τους κανόνες που αποτελούν το ευρωπαϊκό νομοθετικό πλαίσιο σχετικά με τη διασφάλιση της ιδιωτικότητας, την αποθήκευση, τη διατήρηση και διάθεση των δεδομένων του χρήστη, αλλά και τη λειτουργία των συσκευών ραδιοσυχνικής αναγνώρισης (RFID) και τις συχνότητες λειτουργίας, θεμελιώδη συστατικά του IoT:

• Η Σύσταση "ERC RECOMMENDATION 70-03 / Relating to the use of short range devices (SRD)", έκδοση της 09-02 2007. [6]

• Η οδηγία 2002/58/ΕΚ, για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών , της 12-07-2002

• Η οδηγία 2006/24/ΕΚ, για τη διατήρηση δεδομένων που παράγονται ή υποβάλλονται σε επεξεργασία σε συνάρτηση με την παροχή διαθεσίμων στο κοινό υπηρεσιών ηλεκτρονικών επικοινωνιών ή δημοσίων δικτύων επικοινωνιών και για την τροποποίηση της οδηγίας 2002/58/ΕΚ, της 15-03-2006

• Η Απόφαση 2006/804/ΕΚ της επιτροπή, «Σχετικά με την εναρμόνιση του ραδιοφάσματος για συσκευές ταυτοποίησης ραδιοσυχνοτήτων (RFID) που λειτουργούν στη ζώνη υπερυψηλών συχνοτήτων (UHF)», [κοινοποιηθείσα υπό τον αριθμό Ε(2006) 5599], της 23ης Νοεμβρίου 2006. [17]

• Η οδηγία 2009/140/ΕΚ για την τροποποίηση των οδηγιών 2002/21/ΕΚ σχετικά με κοινό κανονιστικό πλαίσιο για δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, 2002/19/ΕΚ σχετικά με την πρόσβαση σε δίκτυα ηλεκτρονικών επικοινωνιών και συναφείς ευκολίες καθώς και με τη διασύνδεση τους, και ο 2002/20/ΕΚ για την αδειοδότηση δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών, της 25-10-2009.

• Η οδηγία 2009/136/ΕΚ, για τροποποίηση της οδηγίας 2002/22/ΕΚ για την καθολική υπηρεσία και τα δικαιώματα των χρηστών όσον αφορά δίκτυα και υπηρεσίες ηλεκτρονικών επικοινωνιών, της οδηγίας 2002/58/ΕΚ σχετικά με την επεξεργασία των δεδομένων προσωπικού χαρακτήρα και την προστασία της ιδιωτικής ζωής στον τομέα των ηλεκτρονικών επικοινωνιών και του κανονισμού (ΕΚ) αριθ. 2006/2004 για τη συνεργασία μεταξύ των εθνικών αρχών που είναι αρμόδιες για την επιβολή της νομοθεσίας για την προστασία των καταναλωτών.

3.10 **Προβλήματα αναφορικά με την προστασία προσωπικών δεδομένων και της χρήσης της** Rfid **τεχνολογίας**.

Η κύρια χρησιμοποιούμενη τεχνολογία στο internet των πραγμάτων, η RFID τεχνολογία, βρίσκεται ακόμα στο στάδιο της τεχνολογικής ωρίμανσης, οπότε ακόμα σε πολλούς τομείς χρήζει βελτίωσης. Η ανάπτυξη μια στρατηγικής για την ιδιωτικότητα, σε σχέση με την το internet των πραγμάτων και την rfid τεχνολογία είναι απαραίτητη.

Νομοθετικά θα πρέπει να προσεγγιστεί πολύ αυστηρά. Η αυστηρή εφαρμογή ενός κώδικα δεοντολογίας και τα υψηλά πρόστιμα για την παράβαση της νομοθεσίας καθίστανται απαραίτητα. Επίσης θα πρέπει να γίνει υποχρεωτική η διενέργεια ανάλυσης μέσω «Privacy enhancing technologies» τεχνικών και εργαλείων, ώστε να εντοπιστούν πιθανές απειλές εναντίον των ευαίσθητων προσωπικών δεδομένων.

Η συλλογή δεδομένων εγκυμονεί μεγάλους κινδύνους, καθώς τα δεδομένα μπορεί να είναι προσβάσιμα σε μη εξουσιοδοτημένους χρήστες (είτε με φυσικό τρόπο είτε μέσω hacking μιας βάσης δεδομένων), οπότε οι οργανισμοί που συλλέγουν τα δεδομένα θα πρέπει να σταθούν υπεύθυνα στην ασφαλή φύλαξή τους . Επίσης, για τις πληροφορίες που αποθηκεύονται σε μια ετικέτα rfid ποιός θα πρέπει να θεωρηθεί υπεύθυνος αν διαρρεύσουν; Όταν μια ετικέτα rfid συνδεθεί με έναν άνθρωπο , τότε αυτόματα αυτή γίνεται προσωπικό δεδομένο. Όταν σε μια εταιρεία οι υπάλληλοι είναι εφοδιασμένοι με rfid ετικέτα, τότε η ανίχνευση των υπαλλήλων εγείρει ανησυχίες όσον άφορα στην ιδωτικότητα.

Από τεχνικής άποψης είναι γνωστό ότι τα πρότυπα (νομικά και όσον αφορά στις αξίες) διαφέρουν παγκοσμίως, οπότε θα πρέπει να ολοκληρωθεί η παγκοσμία προτυποποίηση. Η τεχνολογία RFID αυξάνει τον κίνδυνο να κατασκοπευτούν δεδομένα και η κρυπτογράφηση στη διαμεταγωγή των δεδομένων λογίζεται απαραίτητη.

Θα πρέπει η ιδιωτικότητα να ενισχυθεί μέσω αλλαγών στους οργανισμούς και θα πρέπει να λαμβάνεται σοβαρά υπόψη κατά τον τεχνολογικό και επιχειρησιακό σχεδιασμό ενός έργου. Οφείλει επιπλέον να υπάρξει διάκριση μεταξύ ανοικτών και κλειστών δικτυακών συστημάτων και να υφίσταται περιορισμός στην έκταση και στο χρόνο της συλλογής και αποθήκευσης δεδομένων από ένα σύστημα.

3.11 IPv6 **και Νομικά Θέματα**

Η εκπληκτική ανάπτυξη των νέων τεχνολογιών και, συγκεκριμένα, η μελλοντική εφαρμογή του πρωτοκόλλου IP στην έκδοση 6 (IPv6), ανοίγει μια τεράστια ποικιλία δυνατοτήτων, δραστηριοτήτων, νέους τρόπους επικοινωνίας και εργασίας και ως εκ τούτου συνδέεται με τις περισσότερες από τις δραστηριότητες της καθημερινής ζωής μας.

Για το λόγο αυτό το IPv6 λαμβάνει ιδιαίτερη σημασία σε σχέση με την έκδοση 4 του πρωτοκόλλου IP (IPv4), η οποία εσώκλειε κάποιους περιορισμούς που εμπόδιζαν την ανάπτυξη νέων εξελίξεων. Τέτοιοι περιορισμοί είχαν να κάνουν κυρίως με τεχνικές προδιαγραφές που δεν επέτρεπαν εύκολα την επέκταση του, με τον περιορισμένο αριθμό των διαθέσιμων διευθύνσεων IP, κλπ.

Για το λόγο αυτό, αν και ο κύριος στόχος αυτών των νέων τεχνολογικών εξελίξεων που βασίζεται στο IPv6 είναι η βελτίωση της

ποιότητας ζωής των χρηστών του, μπορεί επίσης να υφίσταται ως στόχος η πραγματοποίηση σημαντικών έργων για την ανάπτυξη και την τεχνολογική έρευνα που απαιτεί η χρήση τους διεθνώς. Επιπροσθέτως, είναι απαραίτητο να εξεταστεί το ενδεχόμενο νομικών συνεπειών που η εισχώρηση του IPv6 συνεπάγεται, προκειμένου να διασφαλιστεί ότι η χρήση του γίνεται σύμφωνα με την ισχύουσα νομοθεσία και ότι η υλοποίησή του δεν βλάπτει αυτή την νομοθεσία, ούτε τα δικαιώματα των χρηστών του.

Η ανησυχία σχετικά με τις νομικές επιπτώσεις που θα μπορούσε να έχει το IPv6, παρουσιάστηκε για πρώτη φορά στη γνωμοδότηση 2/2002 της Ευρωπαϊκής Ένωσης σχετικά με τη χρήση μοναδικών αναγνωριστικών. Γενικότερα υπάρχει μια ανησυχία που στηρίζεται στην ύπαρξη των «μοναδικών αναγνωριστικών» σε ορισμένους τύπους διευθύνσεων IPv6. Αυτά τα αναγνωριστικά είναι σε θέση να αφήσουν «σημάδια», για παράδειγμα της πρόσβασης ενός ατόμου σε μια ιστοσελίδα, ενώ επιπλέον είναι δυνατό να γίνει μια λεπτομερής μελέτη του προφίλ του, των προτιμήσεων του, και γενικώς να παρακολουθούνται όλες οι δραστηριότητές του μέσω του Διαδικτύου.

Έτσι λοιπόν η κύρια μέριμνα είναι επικεντρωμένη στο γεγονός ότι το IPv6 θα μπορούσε να αποτελεί παράβαση στο δικαίωμα της ιδιωτικής ζωής των χρηστών του. Επίσης, βάσει των παραπάνω, προκύπτουν αμφιβολίες σχετικά με τις νομικές συνέπειες της θεώρησης μια διεύθυνσης IP ως δεδομένο προσωπικού χαρακτήρα.

Ο σκοπός της γνωμοδότησης 2/2002 της Ευρωπαϊκής Ένωσης ήταν να εκθέσει τις απόψεις της Επιτροπής των Ευρωπαίων σε θέματα που αφορούν την ανάπτυξη του IPv6 στην Ευρώπη και ένα από τα ζητήματα που ρυθμίζονται ρητά είναι η προστασία της ιδιωτικής ζωής. Οι σκέψεις της Ευρωπαϊκής Επιτροπής τονίζονται στην επόμενη παράγραφο ως εξής:

«Ωστόσο, οι νέες υπηρεσίες Internet είναι καίριας σημασίας για τη δομή, την ενοποίηση και ολοκλήρωση των ευρωπαϊκών προσπαθειών για το IPv6. Η ανάπτυξη του ειδικευμένου ανθρώπινου δυναμικού, η πλήρης εναρμόνιση, όπου είναι αναγκαίο, οι πολιτικές προσεγγίσεις, πρέπει να διατηρήσουν την ερευνητική προσπάθεια, και να προωθήσουν τα πρότυπα και τις προδιαγραφές ώστε να εξασφαλιστεί ότι όλοι οι τομείς της νέας οικονομίας που ενδέχεται να επηρεαστούν από το IPv6, έχουν πλήρως συνειδητοποιήσει το δυνητικό όφελος που προκύπτει από τη χρήση του».

Επίσης, η Επιτροπή προτείνει μια σειρά δράσεων για να εξασφαλιστεί ότι η Ευρωπαϊκή Ένωση διατηρεί την πρωτοβουλία και την ηγεσία σε αυτές τις παγκόσμιες εξελίξεις. Οι δράσεις αυτές απαιτούν μια συντονισμένη δράση με σκοπό τη διάρθρωση, την ενοποίηση και ολοκλήρωση των ευρωπαϊκών προσπαθειών για το IPv6, ιδίως μέσω:

Α. Της αύξησης της υποστήριξης του IPv6 στα δημόσια δίκτυα και υπηρεσίες.

Β. Της ίδρυσης και έναρξης των εκπαιδευτικών προγραμμάτων για το IPv6.

Γ. Της υιοθέτηση του IPv6 μέσω εκστρατειών ευαισθητοποίησης.

Δ. Της συνεχούς διέγερσης του Διαδικτύου αφομοίωσης σε ολόκληρη την Ευρωπαϊκή Ένωση.

Ε. Της ενίσχυσης της υποστήριξης προς το IPv6 των εθνικών και ευρωπαϊκών Δικτύων Έρευνας.

Στ. Μιας ενεργούς συμβολής στην προώθηση του IPv6 σε πρότυπα εργασίας.

Ζ. Της ενσωμάτωσης του IPv6 σε όλα τα στρατηγικά σχέδια που αφορούν στη χρήση των νέων υπηρεσιών του διαδικτύου.

Η ανακοίνωση ασχολείται ειδικά με θέματα προστασίας προσωπικών δεδομένων για το IPv6.

«Λόγω του γεγονότος ότι το Διαδίκτυο έχει, από την αρχή, θεωρηθεί ως ένα ανοικτό δίκτυο, υπάρχουν πολλά χαρακτηριστικά των πρωτοκόλλων επικοινωνίας του, τα οποία, μπορεί να οδηγήσουν σε παραβίαση της ιδιωτικής ζωής των χρηστών του. Οι ανησυχίες εκφράζονται σε τακτική βάση σχετικά με την ανάγκη να βρεθεί μια ισορροπία μεταξύ του «ανοικτού χαρακτήρα» του Διαδικτύου και τις αντικρουόμενες ανάγκες για την αποτελεσματική διατήρηση της προστασίας των προσωπικών δεδομένων των χρηστών του. Το θεμελιώδες δικαίωμα στην προστασία της ιδιωτικής ζωής και την προστασία των δεδομένων κατοχυρώνεται στο Χάρτη της ΕΕ για τα θεμελιώδη δικαιώματα και έχουν αναπτυχθεί λεπτομερώς στις οδηγίες 95/46/ΕΚ και 97/66/ΕΚ που ισχύουν για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα στο Διαδίκτυο.»

Σε ανακοίνωσή της σχετικά με την οργάνωση και διαχείριση του Συστήματος Ονομάτων Τομέα του Διαδικτύου, τον Απρίλιο του 2000, η Επιτροπή δήλωσε ήδη ότι μια διεύθυνση IP μπορεί να είναι από μόνη της δεδομένο προσωπικού χαρακτήρα κατά την έννοια του νομικού πλαισίου. Επίσης, το άρθρο 29 για την προστασία των δεδομένων ομάδας εργασίας, το ανεξάρτητο Συμβουλευτικό όργανο της ΕΕ για την προστασία των δεδομένων και της ιδιωτικής ζωής συστάθηκε με την οδηγία 95/46/ΕΚ, και εφιστά την προσοχή σε πολλές περιπτώσεις σε θέματα ιδιωτικής ζωής που θέτει η χρήση του Διαδικτύου. Το άρθρο αυτό για την προστασία των δεδομένων ομάδας εργασίας, καθώς και η Διεθνής Ομάδα Εργασίας για την Προστασία Δεδομένων στις Τηλεπικοινωνίες (η «ομάδα του Βερολίνου») λειτουργεί ειδικά για το IPv6. Συνεπώς, είναι απαραίτητο η Ευρωπαϊκή Επιτροπή και η Ευρωπαϊκή Ένωση στο σύνολό της να εξετάσει τα ζητήματα της ιδιωτικής ζωής στην περαιτέρω ανάπτυξη του Διαδικτύου. Ενώ τα θέματα της ιδιωτικής

ζωής λαμβάνονται υπόψη κατά την ανάπτυξη του IPv6, είναι σημαντικό ότι η εμπιστοσύνη των χρηστών του Διαδικτύου σε ολόκληρο το σύστημα, συμπεριλαμβανομένου του σεβασμού των θεμελιωδών δικαιωμάτων, εξασφαλίζεται.

Στα συμπεράσματά της, η Ευρωπαϊκή Επιτροπή ζήτησε από τα μέρη να μελετηθούν οι επιπτώσεις της περαιτέρω εξέλιξης του Διαδικτύου, συμπεριλαμβανομένων των νέων IPv6 γενεών πρωτοκόλλων, σχετικά με το θεμελιώδες δικαίωμα της προστασίας της ιδιωτικής ζωής και των δεδομένων, έτσι ώστε να διασφαλιστεί ότι τα απαιτούμενα πρότυπα και οι προδιαγραφές λαμβάνουν αυτές τις πτυχές πλήρως υπόψη. Έτσι κάλεσε μια γενική μελέτη σχετικά με τα ζητήματα της ιδιωτικής ζωής, λίγους μήνες αργότερα, το Μάιο του 2002, και η Ομάδα του άρθρου 29 δημοσίευσε ένα έγγραφο με τίτλο «Γνώμη 2/2002 σχετικά με τη χρήση μοναδικών αναγνωριστικών στον τηλεπικοινωνιακό τερματικό εξοπλισμό: Το παράδειγμα της IPv6». Η εργασία αυτή αναδεικνύει τον κίνδυνο της ιδιωτικής ζωής όσον αφορά «τη δυνατότητα ενσωμάτωσής του ως ένα μοναδικό αναγνωριστικό αριθμό της διεύθυνσης IP, όπως έχει σχεδιαστεί σύμφωνα με το νέο πρωτόκολλο». Η ουσία αυτής της εργασίας είναι ότι οι διευθύνσεις IP που αποδίδονται στους χρήστες του Διαδικτύου είναι προσωπικά δεδομένα και ως εκ τούτου υπόκεινται στις κατευθυντήριες γραμμές που προβλέπονται στις οδηγίες της Ευρωπαϊκής Ένωσης.

3.12 **Νομικές - ρυθμιστικές προκλήσεις που φέρνει στο προσκήνιο το** internet of things.

Όπως ήδη έχει προαναφερθεί, η τεράστια ανάπτυξη των δικτύων και των υπηρεσιών εκτός από τις αδιαμφισβήτητες διευκολύνσεις που θα επιφέρει, σίγουρα θα αυξήσει τους επικείμενους κινδύνους και

απειλές, ενώ ταυτόχρονα θα γεννήσει και πολλά ερωτήματα. Ο έλεγχος των τιμών, η διασύνδεση, η αδειοδότηση, η πολιτική διαχείρισης και ελέγχου του ραδιοφάσματος, η εποπτεία της εκπομπής ραδιοτηλεοπτικού περιεχομένου και η κυβερνοασφάλεια, είναι κάποιες από τις ήδη υπάρχουσες αρμοδιότητες των ρυθμιστών. Με την ανάπτυξη του IoT, νέοι κίνδυνοι θα εμφανιστούν, όπως η αθέμιτη παρακολούθηση από μη εξουσιοδοτημένους χρήστες της πληροφορίας που διακινείται σε ιστοσελίδες ή κοινωνικά δίκτυα, της αποθηκευμένης πληροφορίας στο cloud αλλά και η δυνατότητα εντοπισμού της θέσης και των κινήσεων του συνδρομητή από τους διαχειριστές κινητών δικτύων. Επίσης, τίθεται θέμα όσον αφορά στην ασφάλεια των επικοινωνιών και των ηλεκτρονικών συναλλαγών, στην προστασία του απορρήτου και των προσωπικών δεδομένων, στην προστασία του χρήστη από απάτες και από μη ζητηθείσες μορφές διαφήμισης και εμπορικής επικοινωνίας , στην αθέμιτη αναπαραγωγή πνευματικών έργων και στην γενικότερη ύπαρξη κυβερνοεγκλήματος . Τεράστιο ζήτημα φυσικά αποτελεί και η «παγκοσμιοποίηση» του ίντερνετ των πραγμάτων, αφού τίθεται άμεσα το θέμα ποιάς χώρας, ή ηπείρου το νομικό πλαίσιο θα είναι και αυτό που θα επιλύσει και τα διάφορα προβλήματα που προκύπτουν. Τέλος, οι ρυθμίσεις που θα αφορούν στις αγορές, στον ανταγωνισμό που θα προκύψει με τα νέα προϊόντα, στις διάφορες υπηρεσίες και στα επαγγέλματα που θα εμφανιστούν μέσω όλης της διαδικασίας αυτής, θα πρέπει να γίνουν ιδιαίτερα προσεκτικά, καθώς κρίνονται ζωτικής σημασίας για την ψηφιακή οικονομία. Αυτές λοιπόν είναι κάποιες από τις προκλήσεις που θα κληθούν να αντιμετωπίσουν οι ρυθμιστές και μάλιστα οφείλουν να το κάνουν με τέτοιο τρόπο, ώστε το IoT να μπορέσει να αναπτυχθεί και να δομηθεί σωστά, με τελικό και βασικό στόχο να καταφέρει να εξαπλωθεί και να γίνει κοινωνικά αποδεκτό.

3.13 **Προτεινόμενες ρυθμιστικές λύσεις**.

Δεν απομένει παρά να κάνει κανείς κάποιες προτάσεις σχετικά με τα θέματα που τυχόν προκύπτουν. Το ρυθμιστικό πλαίσιο αρχικά θα πρέπει να προστατεύει την ιδιωτικότητα και να ασφαλίζει τις επικοινωνίες του χρήστη και να τον προστατεύει από κυεβερνοαπάτες, ενώ οφείλει να καθιστά τα αναβαθμισμένα δίκτυα διαθέσιμα σε όλους και σε προσιτές τιμές, με καλή ποιότητα ευρυζωνικής σύνδεσης ανεξαρτήτως τεχνολογίας και παρόχου.

Αδιαμφισβήτητα, θα πρέπει οι αρμόδιοι να φροντίσουν ώστε οι όροι χρήσης των υπηρεσιών να είναι διαφανείς, χωρίς αθέμιτες χρεώσεις ή αθέμιτες πρακτικές marketing από τους παρόχους των δικτύων και των υπηρεσιών.

Τέλος, ένας καταναλωτής που αγοράζει μια υπηρεσία στην Ευρώπη και το hosting της γίνεται στην Αμερική θα πρέπει να ξέρει εξ' αρχής το νομικό πλαίσιο στο οποίο υπόκειται σε περίπτωση διχογνωμίας με τον πωλητή. Αυτό το μικρό παράδειγμα μας οδηγεί όμως σε μεγαλύτερα προβλήματα όπως το κοινό νομικό πλαίσιο στις περιπτώσεις πρόσβασης τρίτου σε πληροφορίες χρηστών που από χώρα σε χώρα και από ήπειρο σε ήπειρο αλλάζουν, όπως επίσης αλλάζει και το νομικό πλαίσιο περί πνευματικών έργων ενώ ίσως η εφαρμογή των νόμων που οριοθετούν όλα αυτά είναι πολύ χαλαρή.

Εν κατακλείδι, κύριο μέλημα συνεπώς των αρχών θα πρέπει να είναι ένα παγκόσμιο ρυθμιστικό πλαίσιο, με εφαρμογή σε όλα τα μήκη και πλάτη του πλανήτη μας. Η οριστικοποίηση του νομικού πλαισίου σε επίπεδο ηπείρου φαντάζει μικρή, πόσο μάλλον μικρή κρίνεται σε εθνικό επίπεδο. Ένα κοινό για όλους ρυθμιστικό πλαίσιο που θα

επιλύει άμεσα όλα τα προβλήματα και θα νοείται υποστηρικτικό και βοηθητικό για τους χρήστες αλλά και για την αγορά, ορίζοντας και την πιο μικρή λεπτομέρεια κατά τρόπο αρμοστό και ακριβοδίκαιο, θα ήταν ένα ιδανικό σενάριο που μόνο θα προωθούσε τον ίντερνετ των πραγμάτων σε μηδενικό χρόνο και θα το έκανε άμεσα αποδεκτό στο εύρος των κοινωνιών .

3.14 **Συμπεράσματα**

Από όσα έχον αναφερθεί σε όλο το σώμα της μελέτης αυτής, μπορούμε λοιπόν ποια να κατανοήσουμε με ευκολία την λογική αλληλουχία πρακτικών θεμάτων αλλά και ουσιωδών προβληματισμών που εμπεριέχονται στο ευρύτερο πλαίσιο του IoT. Η αρχική μετάβαση στην εξάπλωση του IoT απαιτούσε την επίλυση του θέματος της εξάντλησης των Ipv4 διευθύνσεων, κάτι το οποίο επιτεύχθηκε με την δυναμική είσοδο του Ipv6 στα τεχνολογικά πράγματα. Μέσω του πρωτοκόλλου αυτού, ολοένα και περισσότερα αντικείμενα δύνανται να συνδέονται στο δίκτυο και να αλληλεπιδρούν μεταξύ τους αλλά και με τους χρήστες, εισάγοντας νέα δεδομένα από καθημερινούς τομείς της ανθρώπινης ζωής αλλά και επηρεάζοντας το κοινωνικό-οικονομικό γίγνεσθαι ολοκλήρου του πλανήτη. Η ισχύς του ανθρώπου καθόλου δεν μειώνεται παρά ενισχύεται αφού ο ίδιος αναλαμβάνει πια το ρόλο της συνεχούς ροής των πραγμάτων κατά τρόπο που ο ίδιος επιθυμεί αλλά και εξυπηρετείται. Εύλογα ερωτήματα σε σχέση με όλη αυτή τη διαδικασία η οποία ουσιαστικά έχει ως απαρχή τη διακίνηση της πληροφορίας προκύπτουν και μόνο οι αρμόδιες αρχές σε Εθνικό, Ευρωπαϊκό αλλά και παγκόσμιο κατ' επέκταση επίπεδο είναι ικανές να αντιμετωπίσουν μέσω της κατάλληλης νομολογίας τους κινδύνους που προκύπτουν. Οι προσπάθειες που έχουν γίνει μέχρι τώρα

αξιολογούνται ως ικανές , αλλά σίγουρα υπάρχει μεγάλος δρόμος ακόμα μέχρι να επιτευχθεί η πλήρης εναρμόνιση του IoT με τα δεδομένα της ζωής σε όλους του τομείς και η ταυτόχρονη προστασία όμως του ίδιου το ατόμου μέσα σε όλο αυτό το σύστημα. Όπως ταιριάζει σε όλα τα πράγματα, ο τρόπος χειρισμού θα αποδειχθεί καταλυτικός και είναι αυτός που θα ορίσει το αν τελικά το Iot θα γίνει αποδεκτό από το ευρύ κοινό ως ένας νέος τρόπος ζωής με πάμπολλες διευκολύνσεις.

Βιβλιογραφία

[1] http://www.icann.org/en/news/releases/release-03feb11-en.pdf

[2]http://www.ripe.net/internet-coordination/news/announcements/ripe-ncc-begins-to-allocate-ipv4-address-space-from-the-last-8

[3] http://tools.ietf.org/html/rfc4632

[4] http://en.wikipedia.org/wiki/IPv4_address_exhaustion

[5]http://meetings.ripe.net/ripe-57/presentations/Colitti-Global_IPv6_statistics_-_Measuring_the_current_state_of_IPv6_for_ordinary_users_.7gzD.pdf

[6] http://www.idc.com/getdoc.jsp?containerId=prUS23371312

[7] http://www.personal.psu.edu/dvm105/blogs/ipv6/2009/06/verizon-mandates-ipv6-support.html

[8]www.news.com/Broadband-adoption-passes-halfway-mark-in-U.S./2110-1034_3-6160422.html

[9] http://www.census.gov/prod/1/pop/p25-1129.pdf

[10]http://www.un.org/millenniumgoals/pdf/The%20Millennium%20Development%20Goals%20Report%202008.pdf

[11] IPv6 Essentials, Silvia Hagen, May 2006.

[12] Θεωρία Διαδικτυακών Πρωτοκόλλων, Ι.Δ. Αγγελόπουλος

Shah Zubin, Simulation and Analysis of RFID Localization Algorithms

[13]Απόφαση αριθμ. οικ. 399/34 της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ), «Κανονισμός Όρων Χρήσης Μεμονωμένων Ραδιοσυχνοτήτων ή Ζωνών Ραδιοσυχνοτήτων» (Αριθμ. Οικ. 399/34, ΦΕΚ 1456/Β/3-10-2006).

[14]European Commission, Information Society and Media Directorate-General: From RFID to the Internet of Things, Pervasive networked systems, www.iot-visitthefuture.eu,2006

[15]Communication from the commission to the European parliament, the council ,the European economic and social committee and the committee of the regions, early Early Challenges regarding the "Internet of Things",{COM(2008) aaa},{SEC(2008) bbb}

[16]Maarten Botterman for the European Commission,Information Society and Media DirectorateGeneral:Internet of Things: an early reality of the Future Internet, Prague, http://ec.europa.eu/information_society/tl/policy/, 2009

[17] ΑΝΑΚΟΙΝΩΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ ΣΤΟ ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΟΒΟΥΛΙΟ, ΤΟ ΣΥΜΒΟΥΛΙΟ, ΤΗΝ ΕΥΡΩΠΑΪΚΗ ΟΙΚΟΝΟΜΙΚΗ ΚΑΙ ΚΟΙΝΩΝΙΚΗ ΕΠΙΤΡΟΠΗ ΚΑΙ ΤΗΝ ΕΠΙΤΡΟΠΗ ΤΩΝ ΠΕΡΙΦΕΡΕΙΩΝ, «Το Ίντερνετ των πραγμάτων — Ένα σχέδιο δράσης για την Ευρώπη», Βρυξέλλες, 18.6.2009, COM(2009) 278

[18]Gerald Santucci. From Internet of Data to Internet of Things, Presented at International Conference on Future Trends of the Internet,2009

[19] Soghoian Christopher, “RFID and Privacy”, Spar Lab Seminar, September 2003

[20] “RFID Systems, Security & Privacy Implications”, a white paper published by AUTO-ID CENTER, November 2002

[21] Violino Bob, “Get Ready for Reality Online”, RFID Journal, www.rfidjournal.com

[22]http://www.eett.gr/export/sites/default/sites/EETT/ElectronicCommunications/Radio Com munications/Rigths Of Use/AP399 034.pdf

[23]http://msdn.microsoft.com/en-us/library/aa479355.aspx

[24]http://www.iot-visitthefuture.eu/

[25]http://www.future-internet.eu/home.html

[26]http://en.wikipedia.org/wiki/RFID

[27]http://www.ieee.com

[28]http://www.itu.com

[29] http://www.eett.gr/conference2013/pdf/EETTPresidentSpeech-17May.pdf

[30] http://www.youtube.com/watch?v=t5X2PxtvMsU

[31] http://www.youtube.com/watch?v=Cpbbrpgwu2I

[32] http://www.youtube.com/watch?v=sfEbMV295Kk

[33] http://www.youtube.com/watch?v=QaTIt1C5R-M

[34] http://thenextweb.com/insider/2013/05/19/the-internet-of-things-in-action/