**Δ Ι Ε Θ Ν Ε Σ  Π Α Ν Ε Π Ι Σ Τ Η Μ Ι Ο  Τ Η Σ  Ε Λ Λ Α Δ Ο Σ**
**Σ Χ Ο Λ Η  Μ Η Χ Α Ν Ι Κ Ω Ν**
**Τ Μ Η Μ Α  Μ Η Χ Α Ν Ι Κ Ω Ν  Π Λ Η Ρ Ο Φ Ο Ρ Ι Κ Η Σ ,**
**Υ Π Ο Λ Ο Γ Ι Σ Τ Ω Ν  Κ Α Ι  Τ Η Λ Ε Π Ι Κ Ο Ι Ν Ω Ν Ι Ω Ν**

# ΤΟ STATE-OF-THE-ART ΤΟΥ ΔΙΑΔΙΚΤΥΟΥ ΤΩΝ ΠΡΑΓΜΑΤΩΝ (INTERNET OF THINGS) ΚΑΙ Η ΑΞΙΟΠΟΙΗΣΗ ΤΟΥ ΔΗΜΙΟΥΡΓΙΑ ΈΞΥΠΝΩΝ ΣΠΙΤΙΩΝ

**Πτυχιακή Εργασία του**

Δημήτριος Κ. Φούντας (3790)

Επιβλέπων: Λουκάς Πρωτόπαππας, Ειδικό Εκπαιδευτικό Προσωπικό

**ΣΕΡΡΕΣ, ΦΕΒΡΟΥΑΡΙΟΣ 2022**

***Υπεύθυνη Δήλωση :*** *Βεβαιώνω ότι είμαι συγγραφέας αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία. Επίσης έχω αναφέρει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης, βεβαιώνω ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του Τμήματος Μηχανικών Πληροφορικής, Υπολογιστών και Τηλεπικοινωνιών του Διεθνούς Πανεπιστημίου της Ελλάδας.*

## Περιληψη

Αντικείμενο της πτυχιακής αυτής είναι η παρουσίαση του State-Of-The-Art του Διαδικτύου των Πραγμάτων (Internet Of Things) και η αξιοποίηση του στη δημιουργία Έξυπνων Σπιτιών (Smart Homes). Παρότρυνση για την ανάπτυξη της πτυχιάκης αυτής και πιο συγκεκριμένα των Smart Homes είναι η αναγκαιότητα που "προσφερει" ο σύγχρονος τρόπος ζωής για έλεγχο της οποιαδήποτε πτυχής της ζωής μας απομακρυσμένα καθώς έτσι εξοικονομείται και χρόνος αλλά και χρήμα δυο "αγαθά" πολύτιμα στον 21ο αιώνα. Θα αναλυθούν τα διαθέσιμα πρωτόκολλα και τα μοντέλα επικοινωνίας του σε οικιακά περιβάλλοντα. Θα γίνουν αναφορές στους αισθητήρες που χρησιμοποιεί ένα σύγχρονο σύστημα IoT και πιο συγκεκριμένα θα γίνει συγκριτική ανάλυση των ασύρματων δικτύων αισθητήρων Zigbee,6LOWPAN και Thread τα οποία δεν παρέχουν μόνο εκπομπές ραδιοσυχνοτήτων μικρής εμβέλειας, χαμηλής ισχύος και χαμηλό ρυθμό δεδομένων αλλά είναι κατάλληλα και για συσκευές ασύρματης επικοινωνίας ,όπως ενεργοποιητές και αισθητήρες. Τέλος σε πρακτικό επίπεδο ,μέσω εφαρμογής προσομοίωσης δικτύων (Cisco Packet Tracer) θα σχεδιαστούν και θα υλοποιηθούν σενάρια που βασίζονται σε συσκευές IoT σε οικιακό περιβάλλον.



**ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ**: Έξυπνο σπίτι , IoT , έξυπνες συσκευές, ασφάλεια , αισθητήρες

## Abstract

The object of this thesis is the presentation of the State-Of-The-Art of the Internet of Things and its use in the creation of Smart Homes. Encouraging the development of this thesis and more specifically of Smart Homes is the necessity that "offers" the modern way of life for control of any aspect of our life remotely , as this saves both time and money two "goods" valuable in the 21st century. The available protocols and communication models in home environments will be analyzed. References will be made to the sensors used by a modern IoT system .More specifically a comparative analysis of the wireless networks of Zigbee, 6LOWPAN and Thread sensors will be made, which not only provide short-range, low-power and low data rate radio frequency emissions, but are also suitable for wireless communication devices such as actuators and sensors.Finally, on a practical level, through a network simulation application (Cisco Packet Tracer), scenarios based on IoT devices in a home environment will be designed and implemented.

**KEYWORDS**: Smart Home , IoT , smart devices , security , sensors

## Περιεχόμενα

# Κεφάλαιο 1

## 1.1 Εισαγωγή

Το Internet-of-Things (IoT) είναι ένα επαναστατικό παράδειγμα επικοινωνίας που στοχεύει να δημιουργήσει ένα αόρατο και καινοτόμο πλαίσιο για τη σύνδεση μιας πληθώρας ψηφιακών συσκευών με το Διαδίκτυο. Η αναδυόμενη αγορά IoT αποκτά συνεχώς δυναμική καθώς αρχίζουν οι χειριστές, οι πωλητές, οι κατασκευαστές και οι επιχειρήσεις να αναγνωρίζουν τις ευκαιρίες που προσφέρει.

Το IoT θεωρείται ως το επόμενο βήμα στην παγκόσμια βιομηχανία της πληρόφοριας μετα το Διαδίκτυο.Το IoT είναι ενα έξυπνο δίκτυο το οποίο σύνδεει όλα τα φυσικά στοιχεία μέσω Ίντερνετ με σκοπό την ανταλλαγή πληροφοριών προς επίτευξη κάποιας απομακρυσμένης εργασίας. Τα στοιχεία αυτά έχουν ένα μοναδικό αναγνωριστικό, ένα ενσωματωμένο σύστημα και τη δυνατότητα μεταφοράς δεδομένων μέσω ενός δικτύου διαμέσου συγκεκριμένων και συμφωνημένων προτοκόλλων κάνοντας ετσι τον υπολογισμό πανταχού παρόν.

Το IoT σκοπεύει να καταστίσει το Διαδίκτυο πιο συναρπαστικό και διεισδυτικό στην καθημερινή ζωή.Επιτρέποντας εύκολη πρόσβαση και αλληλεπίδραση με μια τεράστια γκάμα συσκευών όπως οικιακές συσκευές ,αισθητήρες , κάμερες ενεργοποιητές , οθόνες κ.τ.λ. , το IoT προωθεί την ανάπτυξη πολυάριθμων εφαρμογών για την παροχή νέων υπηρεσιών στους χρήστες.Το IoT βρίσκει εφαρμογή σε πολλούς διαφορετικούς τομείς , όπως , ο αυτοματισμός του σπιτιού, ο βιομηχανικός αυτοματισμός , η βοήθεια για ηλικιωμένους , η αυτοκινητοβιομηχανία τα ιατρικά βοηθήματα ,η κινητή υγειονομική περίθαλψη και πολλά άλλα. (Sinha, 2001).


**Εικόνα 1. Παράδειγμα Smart Home**

## 1.2 Σκοπός

Σκοπός της αυτοματοποίησης ενός σπιτιού είναι :

**1)**Ο έλεγχος όλων των συσκευών άπο ένα σήμειο (ηλεκτρονικός πολογιστής , τάμπλετ ,κινητό τηλέφωνο κλπ.

**2)**Η ελαστικότητα στην πρόσθηκη οποιάσδηποτε έξυπνης συσκευής με απλά και εύκολα βήματα.

**3)**Η μέγιστη ασφάλεια αφού πλέον είναι εφικτή η επιτήρηση του σπιτιού 24/7

**4)**Ο απομακρύσμενος έλεγχος ηλεκτρικών η ψηφιακών συσκευών.

**5)** Η αυξημενη ενεργειακή απόδοση.Πιο ακρίβης χειρισμός συσκεύων που σε άλλη περίπτωση θα καταναλώναν περισσότερη ενέργεια (πχ άνοιγμα και κλείσιμο καλοριφέρ σε συγκεκριμένους βαθμούς με βάση τις προτιμήσεις του κάθε ατόμου.

**6)**Κάλυτερος έλεγχος απασχόλησης κάθε συσκευής που μπορει να αποφέρει μεγαλύτερη διαρκεια ζωής.

**7)** Καλύτερη ανάλυση βάση καταγεγραμένων δεδόμενων των συνηθειών και της ρουτίνας του κάθε ατόμου προς επίτευξη καλύτερης απόδοσης στην καθημερινοτητα του.

## 1.3 Στόχοι

Το Έξυπνο Σπίτι είναι ένα σύνολο εξαρτημάτων υπολογιστών,πρωτοκόλλων επικοινωνίας και ηλεκτρικών συσκεύων τα οποία δουλεύουν ως μία οντότητα και επικοινωνούν μεταξύ τους μέσω του διαδικτύου.Κάθε συσκευή έχει αισθήτηρες η είναι προγραμμάτισμενη με συγκεκριμένο τρόπο για να εκτελεί κάποια εργάσια ,είναι συνδεδεμένη μέσω WiFi η μέσω φυσικού καλώδιου(καλωδιο χαλκού,UTP) έτσι ώστε να είναι εφίκτη η διαχείρηση της άπο κάποιο κινητο smartphone,ταμπλετ η απομακρύσμενα από αποιαδήποτε συσκευή (τύπου smartphone η ηλεκτρονικός υπολογιστής ) βρίσκεται συνδεδεμένη στο ίντερνετ.

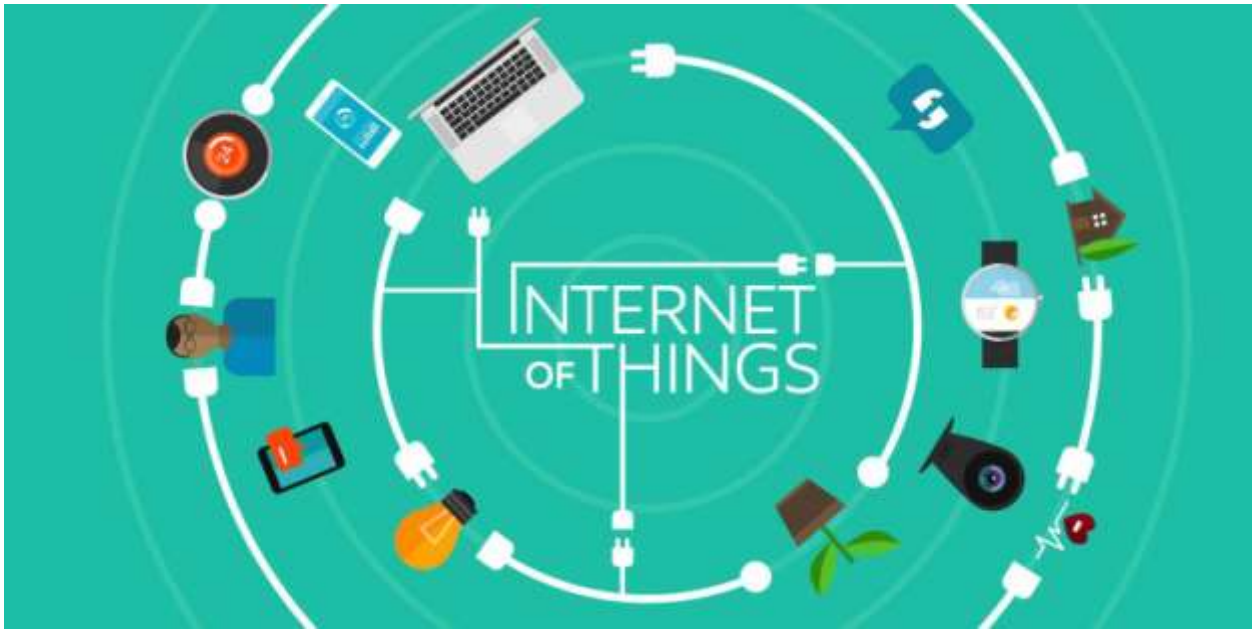
Στόχος ειναι η βελτίωση της ποιότητας ζωής και η άνεση του να ζείς σε ένα σπίτι απόλυτα ελεγχόμενο και στα μέτρα του κάθε ατόμου παράλληλα με την αυξημένη ασφάλεια που προσφέρει. (Alshammari, 2019)

# Κεφάλαιο 2 Internet Of Things

## 2.1 Εισαγωγή στο IOT

Με την ανάπτυξη του διαδικτύου και την ζήτηση οποιάσδηποτε εφαρμογής η νέας τεχνολογίας σχετίζεται εστω και λίγο με το ίντερνετ η "ανακάλυψη" του IOT κατέληξε να γίνεται πολυ σημαντίκη τεχνολογία και μπορεί να έχει πολλές εφαρμογές σε διαφορους κλάδους. Το Διαδίκτυο των Πραγμάτων είναι μια έννοια η οποία σημαίνει το να πάρουμε οποιόδηποτε φυσικό υλικό και να το συνδέσουμε με το διαδίκτυο.Κάθε "πράγμα" που είναι συνδεδεμενο στο διαδίκτυο μπορεί να λάβει και να στείλει πληροφορίες-δεδόμενα σε οποιόδηποτε άλλο "πράγμα" απο , και σε οποιόδηποτε σήμειο της γης.Η ικανότητα αυτή είναι που κάνει ενα φυσικό υλίκο π.χ καλοριφέρ , τηλεόραση , φώτα κλπ "έξυπνο" και καταλήγουμε στην έννοια το 'Διαδίκτυο των Πραγμάτων' (Internet Of Things).

Ουσιαστικά το IoT είναι ενα δίκτυο στο οποίο όλα τα φυσικά υλικά είναι συνδεδεμένα στο ίντερνετ μέσω δρομολογητών (router) και αντάλλασουν πληροφορίες.Το IoT δίνει την δυνατότητα σε αυτές τις συσκευές να λειτούργησουν αυτόνομα χώρις εντολές απο ανθρώπινο παράγοντα αλλά μέσω προγραμματισμένων λειτουργιών , απομακρύσμενα μέσω υποδομών δικτύου ή με μικρή αλληλεπίδραση του ανθρώπου μειώνοντας έτσι την σπατάλη πολυτιμου χρόνου του ανθρώπου στην σύγχρονη εποχη και αυξάνοντας την αποδοτικότητα. (Qusay f. Hassan, 2018)




**Εικόνα 2. Internet of Things – IoT (Διαδίκτυο των πραγμάτων)**

## 2.2 Θεμελιώδη χαρακτηριστικά IoT

Υπηρεσίες που σχετίζονται με τα πράγματα: Το IoT είναι ικανό να παρέχει υπηρεσίες, που σχετίζονται με τα πράγματα, χωρίς όμως να αγνοεί τη σημασιολογική συνοχή, που υπάρχει μεταξύ των φυσικών και των εικονικών πραγμάτων, γεγονός που θα οδηγήσει στην αλλαγή, τόσο των τεχνολογιών του φυσικού κόσμου όσο, και του κόσμου της πληροφορίας.

**Διασυνδεσιμότητα**: Οποιαδήποτε συσκευή (πράγμα) μπορεί να διασυνδεθεί με την παγκόσμια υποδομή πληροφόρησης και επικοινωνίας.

**Ετερογένεια**: Οι συσκευές στο Διαδίκτυο είναι ετερογενείς, καθώς βασίζονται σε διαφορετικές πλατφόρμες και δίκτυα. Μπορούν, όμως, να αλληλεπιδρούν με άλλες συσκευές ή πλατφόρμες υπηρεσιών, μέσω διαφορετικών δικτύων.

**Δυναμικές αλλαγές**: Η κατάσταση των συσκευών αλλάζει δυναμικά π.χ. είναι ενεργές ή απενεργοποιημένες, συνδέονται ή αποσυνδέονται, αλλάζει η θέση και η ταχύτητά τους. Επιπλέον, ο αριθμός των διασυνδεδεμένων συσκευών μπορεί να αλλάξει δυναμικά.

**Τεράστια κλίμακα χρηστών**: Ο αριθμός συσκευών, που οι χρήστες διαχειρίζονται και επικοινωνούν μεταξύ τους, μέσω IoT, θα είναι μεγαλύτερος από το πλήθος των συσκευών που είναι συνδεδεμένες στο τρέχον Διαδίκτυο. Ακόμη πιο κρίσιμη θα είναι η αποτελεσματική διαχείριση και η ερμηνεία των παραγόμενων δεδομένων.

**Ασφάλεια**: Επιβάλλεται ασφαλής σχεδιασμός, τόσο για τους δημιουργούς, όσο και για τους παραλήπτες του IoT και ασφάλεια προσωπικών δεδομένων και ιδιωτικής ζωής. Η ασφάλεια πρέπει να κλιμακωθεί ανάμεσα στις συσκευές, τα δίκτυα και τα δεδομένα που διακινούνται.

**Συνδεσιμότητα**: Η συνδεσιμότητα αφορά, τόσο την προσβασιμότητα, όσο και τη συμβατότητα του δικτύου. Η προσβασιμότητα επιτρέπει τη σύνδεση σε ένα δίκτυο, ενώ η συμβατότητα παρέχει την κοινή δυνατότητα δημιουργίας και χρήσης δεδομένων του δικτύου. (Chandrashekhar, 2016)

## 2.3 Βασικοί Όροι

**Gateway** : Οποιοδήποτε σήμειο πέρναει ηλεκτρονική πληροφορία σε ένα σύστημα IoT (πχ Router).

**Zigbee** : Πρωτόκολλο επικοινώνιας για συσκεύες χαμηλής κατανάλωσης

**Z-Wave**: Πρωτόκολλο επικοινώνιας για συσκεύες χαμηλής κατανάλωσης

**6lOwPAN** : Το πρωτοκολλο 6lOwPAN βοηθάει συσκεύες χαμηλής κατανάλωσης ενέργειας να συνδεθούν με το WPAN (gateway)

**LoRaWAN (Long Range Wireless Area Network**) : Βοηθάει στην αποστολή δεδομένων μεταξύ συσκευών χαμηλής κατανάλωσης.

**QoS** : Πρωτόκολλο το οποίο ελέγχει την ποιότητα του δικτύου και του backbone , real-time.Διαχειριζεται καθυστερήσεις,bandwidth,απώλειες φορτίων κλπ για την καλύτερη ποιότητα υπηρεσιών

**Big Data** : Μεγάλος όγκος δεδομένων που αναλύεται με ανάλυση δεδόμενων και γραφημάτων

**Bluetooth Low Energy (BLE)** : Είναι ένα πρωτόκολλο ασύρματης επίκοινωνίας το οποίο δουλεύει με συσκευές χαμηλής καταναλώσης

**Bluetooth** : Ένα απο τα πιο διαδεδομένα πρωτόκολλα επικοινωνίας για IoT συσκευές.

**RFID** :Μηχανισμός ταυτοποίησης ειδικών tags χρησιμοποιώντας ηλεκτρομαγνητικά κύματα.

**Smart Meter :** Ηλεκτρονική συσκευήπου καταγράφει πληροφορίες όπως κατανάλωση ηλεκτρικής ενέργειας , τάση , ισχύ και απόδοση ενέργειας.

**Cloud Computing :** Επεξεργασία δεδομένων σε απομακρυσμένη κεντρική μόναδα και αποθήκευση (cloud).Πιο γρήγορη επεξεργάσια απο ένα συμβατικό υπολογιστή και πολύ μεγαλύτερη χωρητικότητα.

**Advanced Encryption Standard (AES)** : Το AES είναι ένα 128μπιτό στάνταρ κρυπτογράφησης

**Application Programming Interface (API)** : Το API είναι βοήθημα για την επικοινώνια IoT σύσκευών μεταξύ τους.

**Home Automation** : Η αυτοματοποίηση ενός οικιακού περιβάλοντος.Η Σύνδεση οποιασδήποτε συσκευής στο ίντερνετ.

**Machine-to-Machine (M2M**): Οποιαδήποτε επικοινωνια μεταξύ έξυπνων συσκευών

**Near Field Communication (NFC**):Τρόπος επικοινωνίας μεταξύ φορητών συκευών που βρίσκονται πολυ κοντά η μία στην άλλη.

**Thread:** Πρωτόκολλο της Google που χρησιμοποιεί το 6LoWPAN με IP διευθυνσιοδότηση.

## 2.4 Ιστορική Αναδρομή

Το ίδιο το Ίντερνετ είναι σημαντικό μέρος του IoT,το οποίο δημιουργήθηκε απο την DARPA.Με την δυνατότητα πλέον να συνδεόμαστε στο Ίντερνετ μέσω υπολογιστών γεννήθηκε και η ιδέα της διασύνδεσης διαφόρων συσκεύων με αυτό και αλληλεπίδρασης μεταξύ τους αλλα

και με το ίδιο το περιβάλλον γύρω τους,έτσι εμφανίζεται ο όρος IOT για επιτρέψει την επικοινωνία των συσκευών.

- Η αρχή του IoT ξεκινά όταν ο Normn Joeph Woodland εφευρίσκει το barcode σχεδιάζοντας στην άμμο 4 γραμμές άμμο και λατοχυρώνει την πατέντα του barcode το 1952.

- Οι μηχανικοί της IBM είχαν την ανάγκη να ορίσουν ταυτότητες σε κάθε αντικείμενο και μηχάνημα που χρησιμοποιούσαν στην επιχείρηση. Η πρώτη και αξιοσημείωτη συσκευή του Edward O. Throrp το 1955 ο οποίος κατασκεύασε ένα ρολόι (wearable) το οποίο πρόβλεπε τους κύκλους που έκαναν οι ρουλέτες στα καζίνα.

- Το 1967 από τον Hubet Upton δημιουργήθηκε η πρώτη συσκευή , ενας αναλογικός wearable υπολογιστής ο οποίος βοηθούσε τα άτομα με ειδικές ανάγκες να διαβάζουν τα χείλια των ανθρώπων .

- Το 1969 , το Υπουργείο Εθνικής Αμύνης των Ηνώμενων Πολιτειών στέλνει το πρώτο μήνυμα μεσα απο το δίκτυο ARPANET ΄προκάτοχο του Ίντερνετ το οποίο σημοτοδότησε μία νέα εποχή , την εποχή του διαδικτύου.

- Το 1982 ήταν η γενιά του Internet και του πρωτόκολλου TCP/IP, το οποίο έγινε πρότυπο. Με το πρωτόκολλο TCP/IP ξεκινά μια νέα εποχή, ενός παγκόσμιου ιστού με δίκτυα που ενώνονται μεταξύ τους, για να δημιουργηθεί το διαδίκτυο όπως το ξέρουμε σήμερα.

- Η τεχνολογία του RFID , είναι η τεχνολογία που μας επιτρέψει την ασύρματη αλλά παθητική ανάγνωση και εγγραφή δεδομένων σε συσκευές. Η τεχνολογία αυτήν δημιουργήθηκε το 1973 από τον Mario Cardullo.12 μήνες μετά την ανάπτυξη του RFID ξεκίνα η παραγωγή του για την διεκπεραίωση αγόρων σε σουπερμάρκετ (Wringley’s Chewing Gum).

- Το 1980 , ο αυτόματος πωλήτης της Coca-Cola στο Carnegie Mellon University γίνεται η πρώτη συσκεύη συνδεδεμένη με το Διαδίκτυο η οποία έχει την δυνατότητα να καταγράφει

δεδομένα απο τον χώρο αποθήκευσης του και να ενημερώνει εάν τα αναψυκτικά που εχει αποθηκευμένα είναι αρκετά η χρειάζεται γέμισμα ή εάν είναι αρκετά κρύα.

- Το 1995 , η Siemens αναπτύσει την πρώτη Machine to Machine επικοινωνία μέσα απο μια ασύρματη σύνδεση η οποία χρησιμοποιήθηκε για απομακρυσμένο έλεγχο και tracking.

- Τον ίδιο χρόνο ο Nickolas Negreponte και ο Neil Gershenfeld απο το MIT δημοσιεύουν ένα αρθρο στο Wired ονόματι " Wearable Computer" (Φορετός Υπολογιστης).

- Το 2000 ο υπάλληλος της IBM Andy Stanforf και ο υπάλληλος Arlen Nipper της εταιρίας Eurotech δημιούργησαν το πρώτο πρωτόκολλο επικοινωνίας Machine to Machine, για συσκευές οι οποίες είναι διασυνδεδεμένες με τον ιστό. Το πρωτόκολλο ονομάστηκε από τους ίδιους MQ Telemetry Transport (MQTT), και ήταν ένα σημαντικό βήμα προς την ενίσχυση της ιδέας για το IoT.

- Το 2005 μέλη από το πρόγραμμα Interaction Design Institute Ivrea κατασκευάσανε την πλατφόρμα του Arduino, για μια φτηνή και φιλίκη προς τον χειρηστη λύση μικροελεγκτή.

- Λιγα χρόνια ακόμα και έχει δημιουργηθεί μια τεράστια γκάμα απο πρωτοκολλα,εφαρμογές και IOT πλατφορμών.

- Το 2010, η κινεζική κυβέρνηση ανακοίνωσε ότι θα κάνει το IoT να αποτελεί στρατηγική προτεραιότητα στο πενταετές σχέδιο τους.

- Το επόμενο έτος, ανακοινώνεται το IPV6 πρωτόκολλο το οποίο επιτρέπει σε 2^128 καινουργιές συσκευές να συνδεθούν στο διαδίκτυο οι οποίζες είναι γρηγορότερες και αποδοτικότερες σε θέματα διασύνδεσης. (D.Foote, 2018)

# Κεφάλαιο 3 Το Έξυπνο Σπίτι

## 3.1 Εισαγωγή

Η έννοια του σπιτιού είναι γνώριμη και οικεία στους περισσότερους ανθρώπους.Είναι ο φυσικός χώρος ο οποίος ικανοποιέι τις περισσότερες ανάγκες ενός ατόμου,'οπως στέγαση, πρόφυλαξη, ζεστασία.Με το πέρασμα των χρόνων όμως και την ανάπτυξη της τεχνολογίας και του καθήμερινου τρόπου ζωής το σπίτι έχει υιοθετήσει κι'άλλες ανάγκες.Εκτός απο την ασφάλεια ο άνθρωπος πλέον αναζητεί και την αίσθηση της άνεσης σε όλες τις πτυχές της ζωής του,πόσο μάλλον στον ίδιο τον χώρο στον οποίο ζει..

Ο πρωταρχικός ρόλος του σπιτιού είναι να παρέχει ασφάλεια και στέγαση,ταυτόχρονα όμως ικανοποιεί τις ανάγκες του ανθρώπου για άνεση και έλευθερια.Την άνεση αυτήν μεσα σε ένα σπίτι την παρέχουν όλες οι συσκευές που βρίσκονται μέσα σε αυτό.Οι συσκευές αυτές όπως το πλυντήριο , ο φούρνος , το κλιματιστικό , το σίδερο κ.α. βοηθούν τον άνθρωπο στην γρηγορότερη και ασφάλεστερη κάλυψη των αναγκών του με την λιγότερη δυνατή καταβολή προσπάθειας και κόπου.Είναι φανερό ότι ένα νοικοκυριό δεν μπορεί να λειτουργήσει χώρις αυτές τις πλέον αναγκαίες συσκευές.

Οι ρυθμοί όμως στους οποίους πρέπει να συμβαδίσει ο άνθρωπος μέσα στην κοινωνία του, καθημερινά και αυξάνονται , το ίδιο γρήγορα που αναπτύσσεται και η τεχνολογία γύρω του.Αυτό ως αποτέλεσμα τον ωθεί να αυτοματοποιήσει όσες περισσότερες ανάγκες του μπορεί και να τις ελέγξει απομακρύσμενα και άμεσα.Ένα ζωντανό παραδειγμα είναι η ζεστασία που θέλει να έχει το κάθε άτομο οταν γυρίσει στο σπίτι του απο την δουλεία του η απο μια βόλτα . Οι ανάγκες αυτές οδήγησαν στην δημιουργία του «Έξυπνου Σπιτιού». (Harper, 2006)

## 3.2 Τι είναι το Εξυπνο Σπίτι

Έξυπνο σπίτι χαρακτηρίζεται ως το σύνολο των ηλέκτρικων συσκευών που έχουν την δυνατότητα να επικοίνωνησουν η μία με την άλλη,να αλληλεπιδράσουν με τον χρήστη και να

ανταλλάξουν πληροφορίες και δεδομένα.Οι έξυπνες αυτές συσκευές συνδέονται μεταξύ τους ενσύρματα η ασύρματα και μέσω ειδικών αισθητήρων και διακοπτών εκτέλουν διαφόρων ειδών εργάσιες .Η διαχείρηση γίνεται μεσα από κάποιο κεντρικό υπόλογιστη ,τάμπλετ η κινητό τα οποία είναι συνδεδεμένα στις υπηρεσίες cloud , σε κάποιο τοπικό δίκτυο lan ή Server και λείτουργούν αρμόνικα και απομακρυσμένα.

Τα Έξυπνα Σπίτια, επίσης γνωστά ως αυτοματοποιημένα σπίτια, έξυπνα κτίρια, ολοκληρωμένα οικιακά συστήματα ή domotics, είναι μια νέα τεχνολογία.Τα Έξυπνα Σπίτια ενσωματώνουν κοινές συσκευές που ελέγχουν τις λειτουργίες του σπιτιού. Αρχικά, η έξυπνη οικιακή τεχνολογία χρησιμοποιήθηκε για τον έλεγχο περιβαλλοντικών συστημάτων όπως φωτισμός και θέρμανση, αλλά πρόσφατα η χρήση της έξυπνης τεχνολογίας έχει αναπτυχθεί , έτσι ώστε σχεδόν οποιοδήποτε ηλεκτρικό στοιχείο εντός του σπιτιού να περιλαμβάνεται στο σύστημα. Επιπλέον, έξυπνη οικιακή τεχνολογία δεν ενεργοποιεί και απενεργοποιεί απλώς τις συσκευές, αλλά μπορεί να παρακολουθεί το εσωτερικό περιβάλλον και τις δραστηριότητες που υλοποιούνται ενώ το σπίτι είναι κατειλημμένο. Το αποτέλεσμα αυτών των τροποποιήσεων στην παρούσα τεχνολογία είναι ότι το έξυπνο σπίτι μπορεί τώρα να παρακολουθήσει τις δραστηριότητες του ενοίκου , να εκτελέσει ενέργειες με βάση προκαθορισμένα μοτίβα ή ενέργειες που έχει ορίσει ο χρήστης.

Με τη σημαντική ανάπτυξη του Διαδικτύου και την πρόσβαση υψηλής ταχύτητας (ADSL, δορυφόρος, οπτικές ίνες,…), το δυναμικό οικιακής εργασίας και τηλεργασίας γίνεται δυνατόν. Έτσι, αρκετά χρόνια τώρα , πολλά έργα που αφορούν τα έξυπνα σπίτια αναδύονται. Τα έξυπνα σπίτια είναι πλέον αφιερωμένα στην απλοποίηση της ζωής των κατοίκων της, για εξοικονόμηση ενέργειας, για την παροχή λύσεων άνεσης και ασφάλειας (Harper, 2006).


**Εικόνα 3. Έλεγχος συσκευών με smartphone**

## 3.3 Χαρακτηριστικά – Λειτουργίες

Σε ένα έξυπνο σπίτι όλα τα εξαρτήματα-συσκευές διαχειρίζονται απο ένα home gateway (οικιακό μόντεμ IoT στο οποίο σύνδεονται όλες οι έξυπνες συσκευές).Το home gateway είναι επιίσης υπεύθυνο για τα πρώτοκολλα τα οποία χρησιμοποιούνται για την διαχείρηση των συσκευών και την αρμονική τους επικοινωνία. Μέσα απο το home gateway δίνεται η δυνατότητα στον κάθε χρήστη να ελέγξει η και να ρυθμίσει οποιαδήποτε συσκευή είναι συνδεδεμένη σ'αυτο.

Πιο συγκεκριμένα το Έξυπνο σπίτι είναι ένα ολοκληρωμένο σύστημα ελέγψου που συνδέει και διαζειρίζεται ολα τα υποσυστήματα που είναι συνδεδεμένα σε αυτό (πχ ψυγειο, κλιματιστικό, καφετιέρα, θερμοσίφωνο.φώτα,καλοριφέρ) κάτω απο μια ενιαία διαχειριση.Το σύστημα αυτό διαχειρίζεται τις λειτουργίες που πρέπει να εκτελεστούν έξυπνα, σύμφωνα με τις απαιτήσεις του κάθε χρήστη αλλά και της ίδιας της εγκατάστασης λαμβάνοντας υπόψη εσωτερικές αλλά και εξωτερικές συνθήκες με την χρήση κατάλληλων αισθητήρων.

Για την εγκατάσταση του έξυπνου σπιτιού είναι απαραίτητη η εγκατάσταση περαιτέρω ηλεκτρολογικού και μη εξοπλίσμου.Κάλωδια για ανταλλαγή δεδομένων αυτοματισμού και τροφοδοσίας ανάμεσα στις συσκευές αλλά και της κεντρικής μονάδας ελέγχου για την επίτευξη της επικοινωνίας.Προσαρμογή διακοπτών για τον έλεγχο φώτων και διαφόρων ηλεκτρικών συσκεύων όπως καφετιέρα , θερμοστάτης ,πόρτες κ.α. και τέλος ένας πίνακας ελέγχου ο οποίος μπορεί να εγκατασταθεί σε οποιοδήποτε δωμάτιο και σε παραπάνω απο ένα για μεγαλύτερο έλεγχο του σπιτιού.

Το Εξυπνο σπίτι παρέχει ,ασφάλεια , ενεργειακή απόδοση .χαμηλό κόστος διαχείρησης και ευκολία .Ολόκληρο αυτό το σύστημα είναι προσαρμόσιμο και ευκανόνιστο έτοιμο να ανταποκριθεί στις συνεχιζόμενες μεταβαλλόμενες ανάγκες του κάθε οικιακού χρήστη.

Το Έξυπνο σπίτι έχει λάβει μεγάλη αναγνωρισιμότητα και έχει αρχίσει να διεισδύει με πολύ γρήγορο ρυθμό στην καθημερινότητα.Με κύρια πλεονεκτήματα του την τεράστια εξοικονόμηση ενέργειας και την προσαρμοστικότητα σε κάθε ανάγκη που προσφέρει , είναι πλέον μέρος του μοντέρνου κόσμου και αναπόσπαστο κομμάτι του.

## 3.4 Υπηρεσίες

**Μέτρηση καταστάσεων σπιτιού ( εντός και εκτός ) :**

Μια τυπική εγκατάσταση έξυπνου σπιτιού είναι εξοπλισμένη με ένα σετ διαφόρων αισθητήρων ο οποίος ρόλος τους είναι να μετράνε σε συνέχη χρόνο τις καταστάσεις του σπιτιού , για παράδειγμα : την θερμοκράσια ,την υγρασία , τ ο φως , το διοξείδιο του άνθρακα κ.α.Κάθε αίσθητήρας είναι προγραμματισμένος να μετράει και να καταγράφει μία η και περισσότερες καταστάσεις καθε φορά.

Παραδείγματος χάρην η θερμοκρασία και η υγρασία ή το οξύγονο στο χώρο μπορεί να μετριούνται απο έναν αισθητήρα και το φως σε ενα συγκεκρίμενο χώρο που έχει ορίσει ο ίδιος ο χρήστης από κάποιον άλλον.Όλοι οι αισθήτηρες επιτρέπουν την αποθήκευση και την κατάγραφή των δεδομένων , την οπτική παρουσίαση αυτών στον χρήστη οποιαδήποτε στιγμή και ώρα και

παράλληλα απο οπουδήποτε αλλού.Για να γίνει ομως αυτό είναι απαραίτητη η ύπαρξη επεξεργαστών σήματος , ένας διαυλος επικοινωνίας και κάποια υποδομή cloud.

**Διαχείρηση Οικιακών Συσκεύων :**

Η υπηρεσία διαχείρησης επιτρέπει στον χρήστη να ελέγχει την έξοδο του ενεργοποιητή (τι ακριβώς θα κάνει ο ενεργοποιητής) που είναι συνδεδεμένος με την οποιαδήποτε συσκευή , όπως πχ με το διακόπτη της λάμπας ή τον θερμοστάτη.Οι έξυπνοι ενεργοποιητές είναι σύσκευές , 'οπως διακόπτες η ειδικές δικλίδες , οι οποίοι εκτελούν ενέργειες οπως το να κλείσουν η να ανοίξουν κάποια συσκευή , να τροποποιήσουν κάποιο άλλο σύστημα όπως το να θέσουν το καλοριφέρ σε υψηλότερη η χαμηλότερη θερμοκρασία , η και να τερματίσει το σύστημα λόγω βλάβης η επείγουσας ανάγκης.

**Έλεγχος πρόσβασης :**

Η υπηρεσία ελέγχου πρόσβασης χρησιμοποιείται για την μέγιστη ασφάλεια του χώρου του χρήστη . Το σύστημα ελέγχου πρόσβασης χρησιμοποιέι μια βάση δεδομένων με τα χαρακτηριστηκά αναγνώρισης του εξουσιοδοτημένου προσωπικού και των υπόλοιπων εξουσιοδοτήμενων μελών.

Όταν ένα άτομο πλησιάσει το σύστημα έλεγχου εισόδου , συλλέγονται τα ψηφιακά χαρακτηριστηκά του και στέλνονται στο cloud η server.Εκεί καταγράφονται και αναλύονται .Αν το αναγνωριστικό του υπάρχει στο σύστημα τοτε ταυτοποιείται και επιτρέπεται η είσοδος του.Αν όχι , η είσοδος του τερματίζεται και ζητήτε εκ νέου ταυτοποιήση.Το σύστημα αυτο χρησιμοποιείται και σε πολυπλοκότερα συστήματα όπως πχ μια μεγάλη εταιρία η κάποιο ινστιτούτο το οποίο απασχολεί πολύ μεγαλύτερο αριθμό ατόμων σε σύγκριση με ενα σπίτι τετραμελούς οικογένειας.

- Η εγκριση γίνεται με διάφορους τρόπους.Κάποιοι απο αυτούς είναι :
- Ταυτοποίηση προσώπου
- Κάρτες εγγύτητας ταυτότητας (με barcode η μαγνητικές κάρτες)
- Δαχτυλικό αποτύπωμα
- Κάρτες RFID (Domb, 2019)

## 3.5 Κυρίως εξαρτήματα

**IoT firmware :**

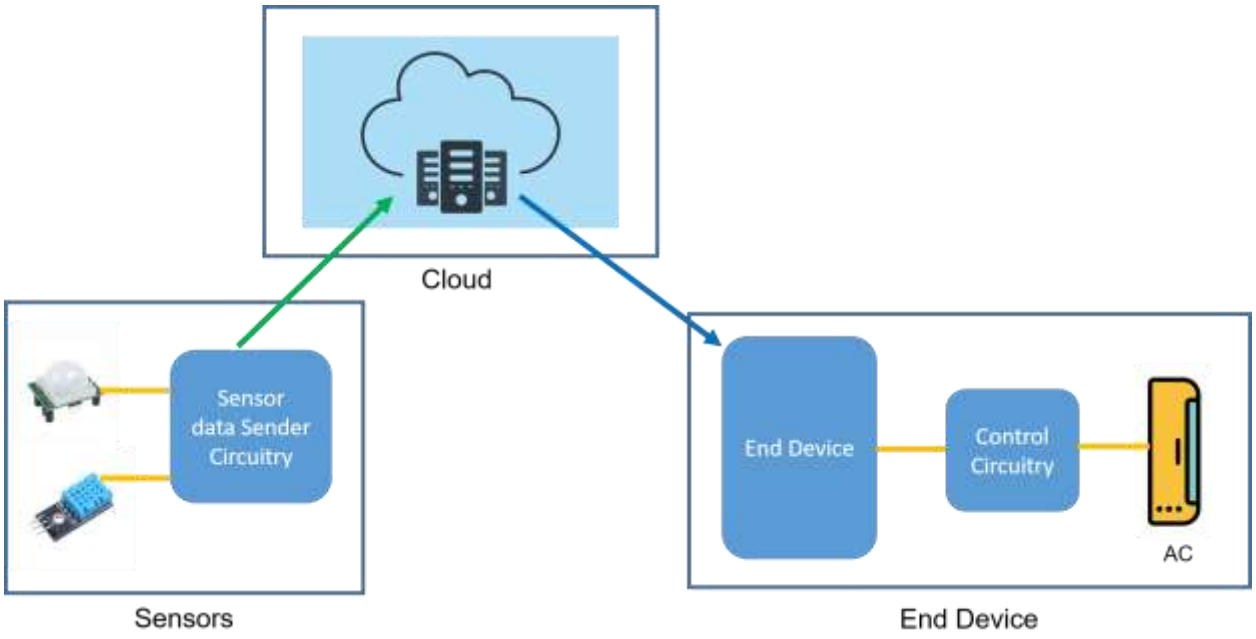
Firmware είναι ενα πρόγραμμα λογισμικού το οποίο είναι προγραμματισμένο σε κάποια συσκευή ( hardware ). Παρέχει τις απαραίτητες οδηγίες στο πως η συσκευή αυτή θα επικοινωνήσει με άλλες συσκευές .

Οι συσκευές σε ένα έξυπνο σπίτι συλλέγουν και ανταλλάσουν πληροφορίες καθ'όλη την διάρκεια της λειτουργίας τους . Η κατανόηση του ερωτήματος «Γιατί χρειάζεται να ασφαλίσω τις συσκευές μου» είναι ζωτικής σημασίας. Υπάρχουν διάφορα εξαρτήματα που απαιτούν ασφάλεια και παρατίθενται παρακάτω.Κάποια απο αυτά θα αναλυθούν και στη συνέχεια :

- Διεπαφή Cloud/Net
- Εφαρμογές mobile
- IoT πρωτόκολλα επικοινωνίας
- IoT διεπαφές hardware

**IoT αισθητήρες**

Οι αισθητήρες χρησιμοποιούνται για να συλλέγουν πληροφορίες και δεδοδένα τόσο για το χώρο του χρήστη αλλά και για τον κήπο , το πάρκινγκ και ότι άλλο βρίσκεται εξωτερικά και ενδιαφέρει τον χρήστη.Είναι συνδεδεμένοι με το ίδιο το σπίτι και τις έξυπνες συσκευές. Δεν είναι απαραίτητα συνδεδεμένα με το διαδίκτυο.Τα δεδομένα απο τους αισθητήρες συλλέγονται και αποθηκεύονται συνέχως στο τοπικό δίκτυο ( server ) για μελλόντική χρήση αλλά και βελτίωση της εμπειρίας του χρήστη.




**Εικόνα 4. Διάγραμμα επικοινωνίας αισθητήρα με τελική συσκευή**

**IoT πύλες (μόντεμ-ρούτερ) :**

Οι πύλες παρέχουν την γέφυρα επικοινώνιας μεταξύ όλων των στοιχείων και των διαφόρων τεχνολογιών στο έξυπνο σπίτι.Είναι ο μεσάζοντας για την επικοινωνία που θέλει να κάνει ο σέρβερ με κάποιον αισθητήρα ή μια έξυπνη συσκευή ή γενικότερα με οποιοδήποτε άλλο στοιχείο μέσα στο σπίτι.

Με τις πύλες επιτυγχάνεται η επικοινωνία device-to-device ή device-to-cloud.Η πύλη σύνηθως είναι hardware μπόρει όμως να είναι και προγραμμα-λογισμικό.Εκτός απο την επίτευξη επικοινωνίας μια πύλη εκτελεί κιάλλες εργασίες 'οπως μεταφράσεις πρωτοκόλλων,συλλόγή όλων των δεδομένων,τοπική επεξεργασία,φιλτράρισμα , διοχέτευση στο cloud και τέλος αυτόνομη διαχείρηση συσκεύων με βάση το ιστορικό και τις προτιμήσεις του χρήστη για μεγαλύτερη ασφάλεια και λειτουργία.

**IoT πρωτόκολλα επικοινωνίας :**

Ένα πολύ σημαντικό κομμάτι για την δημιουργία ενός έξυπνου σπιτιού είναι επιλογή κατάλληλων πρωτοκόλλων επικοινώνιας.Τα πρωτόκολλα είναι ένα σύνολο κανόνων και οδήγιών για την ομάλη επικοινωνία δύο η περισσότερων συσκευών.Είναι απαραίτητο αγάθο για την ομάλη επικοινωνία των συσκευών με τα home gateway τους server και τους αισθητήρες.Πρέπει να ληφθούν υπόψην όλες οι λειτουργίες του σπιτιού καθώς και η τοπολογία για να αποφασιστεί η σώστη επιλογή πρωτοκόλλων καθώς αυτα διαφέρουν σε ποιότητα , ρυθμούς μετάδοσης , ασφάλεια , επηρεάζονται απο τον συνοστισμό ραδιοκυμάτων και καλύπτουν μικρότερες η μεγαλύτερες ασύρματες αποστάσεις.

**Ενεργοποιητές (actuators) :**

Οι ενεργοποιητές είναι εξαρτήματα τα οποία είναι υπεύθυνα για την κίνηση και τον χείρισμο ενός μηχανισμού όπως για παράδειγμα το άνοιγμα του διακόπτη που ελέγχει το φως η την βάνα του νερού.Οι ενεργοποιητές είναι συνδεδεμένοι με κάποιον αισθητήρα και αποκρίνονται με βάση αυτόν.Όταν λάβει ένα σημα είτε τάση , πίεση αέρα η νέρου κ.α. ο ενεργοποιητής ανταποκρίνεται και εκτέλει την ενέργεια που είναι προγραμματισμένος να κάνει μετατρέποντας την ενέργεια της πηγής σε μηχανική κίνηση.

**Βάση δεδομένων :**

Η βάση δεδομένων σε ένα σύστημα smart home είναι απαραίτητη.Όλα τα επεξεργασμένα δεδομένα που έχουν συλλεγεί απο του αισθητήρες και το cloud αποθηκεύονται σε αυτήν για μετέπειτα χρήση.Χρησιμοποιούνται επίσης για ανάλυση απο την βάση και οπτική παρουσίαση (Malche, Internet of Things (IoT) for building Smart Home System, 2017) .

## 3.6 Εφαρμογές

### 3.6.1 Ποιές είναι οι εφαρμογές-αυτοματισμοί ενός έξυπνου σπιτού;

**Φώτα :**

Ο έξυπνος φωτισμός δίνει την δυνατότητα χειρίσμου όλων των φωτών απο το smartphone η το τάμπλετ απο την άνεση του καναπέ.

Δίνεται η δυνατότητα :

- Προγραμμάτισμού των ωρών που θα είναι αναμμένα τα φώτα .Για παράδειγμα ένα άτομο που χρησιμοποιεί συγκεκριμένη ρουτίνα καθημερίνα μπορεί να ¨μάθει¨ το έξυπνο σπίτι πότε να ενεργοποιεί και να απενεργοποιέι τον φωτισμό με βάση το αν βρίσκεται η όχι στο σπίτι όπως και να ανάβει σε συγκεκριμένη ένταση αναλόγως τις ώρες που βρίσκεται στο σπίτι.
- Έλεγχος της έντασης αναλόγως το φυσικό φως που μπαίνει στο σπίτι οποιαδήποτε ώρα.
- Προσομοίωση της ανθρώπινης παρουσίας όταν οι ιδιοκτήτες λείπουν απο τον χώρο προς αποφυγή παραβίασης (με συνδυασμό αισθητήρων κίνησης.
- Αυτόματη ενεργοποίηση διακρίνοντας κίνηση και απενεργοποιήση των φώτων καθώς ο χρήστης κινείται απο δωμάτιο σε δωμάτιο.

**Θερμοκρασία , κλιματισμός και εξαερισμός:**

HVAC είναι ο όρος που χρησιμοποιείται για την θέρμανση , τον κλιματισμό και τον εξαερισμό.Ένα σύστημα HVAC μπορεί να αποκριθεί σε διάφορες εφαρμογές όπως :

- Να ανοίξει τον κλιματισμό και σε συνάρτηση με τις προτιμήσεις μας να εφαρμόσει την θερμοκρασία που προτιμάμε αλλά και χειροκίνητα απο το πάτημα ενός κουμπιου στο κινητό η τάμπλετ μας
- Να κατεβάσει τα ρόλα , να κλείσει τις κουρτίνες ή τα παράθυρα εάν η θερμοκράσια συνεχίσει να ανεβαίνει πάνω απο ένα ορισμένο επίπεδο που έχουμε ορίσει.Το σύστημα φροντίζει έξυπνα γνωρίζοντας τις εξωτερίκες συνθήκες , μέσω αισθητήρων , να προκλιματίσει τον χώρο ή να τον ζέστανει αναλόγως το κρύο η την ζέστη την βροχή ή τον αέρα εξοικονομώντας ενέργεια αφού θέτει ενεργό τον κλιματισμό και την θέρμανση λιγότερη ώρα.

- Τον απαραίτητο αερισμό του σπιτιού ανα τακτά χρονικά διαστήματα ανοιγοκλείνοντας τα ρολά των παραθύρων και λαμβάνοντας υπόψην την προτινώμενη θερμοκράσια που έχει οριστεί.
- Δίνεται η δυνατότητα να ελέγχεται η θερμοκράσια σε κάθε δωμάτιο ανεξάρτητα , ανάλογα την ώρα της μέρας και την εποχή.Για κάθε δωμάτιο μπορεί να ρυθμιστεί διαφορετική θερμοκρασία και όρια θερμοκρασιών ανάλογως πάλι τις προτιμήσεις του κάθε ένοικου.Δίνεται επίσης η δυνατότητα να να παρέχεται θέρμανση η κλιματισμός μόνο στα δωμάτια κατα τις βραδινές ώρες και το υπόλοιπο σπίτι να διατηρείται σταθερά στην προβλεπόμενη θερμοκρασία.
- Αν ο ένοικος ξεχάσει να κλείσει τον κλιματισμό το έξυπνο σπίτι έχει την δυνατότητα να κλείσει η να χαμηλώσει σε θερμοκρασία διατήρησης τον χώρο αν παρατηρήσει ότι δεν υπάρχει για πολύ ώρα κάποιος στον συγκεκριμένο χώρο.
- Στο παραπάνω σύστημα μπορούν να συνδεθούν και άλλες έξυπνες συσκευές όπως θερμοστάτες αφυγραντήρες και αλλα όπως είναι προτιμότερο στην εγκατάσταση του χρήστη.Όλα τα παραπάνω λειτουργούν μεταξύ τους για την καλύτερη απόδοση ενέργειας αλλά και ευκολίας στο χώρο.

**Ασφάλεια :**

Υπάρχουν διάφοροι τρόποι για να εγκατασταθεί και να λειτουργήσει το σύστημα ασφαλειάς αναλόγως παλι τις προτιμήσεις του εκάστοτε χρήστη.Στο σύστημα ασφαλείας μπορούν να εγκατασταθούν διάφορες συσκευές οι οποίες θα παρακολουθούν και θα ελέγχουν το σπίτι , όταν ο χρήστης δεν βρίσκεται στον χώρο αλλά και όταν βρίσκεται μέσα σε αυτό.Μερικές συσκευές είναι οι κάμερες ασφάλειας , βιντεοκάμερες ,τηλέφωνα , αισθητήρες φωτός και κίνησης και υπολογιστές.Το σύστημα ασφαλείας προσφέρει πολύ περισσότερες εφαρμόγες απο το συμβατικό σύτημα ασφαλείας καθώς οποιαδήποτε συσκεύη είναι σε θέση να ενημερώσει για παραβίαση του χώρου είτε με γραπτό και φωνητικό μήνυμα , μέιλ ,κλήση στο κινητό ,live μετάδοση φωνής και βίντεο , να σφραγίσει τις πόρτες και τα παράθυρα του χώρου καθώς και να ενημερώσει την άμεση δράση

**Άρδευση κήπου-χωράφιου :**

Με τις έξυπνες σύσκευες είναι εφικτός ο εκσυγχρονισμός του κήπου θέτοντας μια σείρα γεγονότων για την περιποίηση του , εγκαθιστώντας έξυπνα αρδευτικά και αισθήτηρες θερμοκρασίας και επιπέδου νέρου-υγρασίας μειώνοντας την ανάγκη του ανθρώπινου παράγοντα..Αίσθητήρες ελέγχουν την ξηρασία η την ποσότητα νέρου στο χώμα και ενεργοποιούν η απενεργοποιούν τα αυτόματα ποτιστήρια ενόσω και άλλες συσκευές που έχουν τοποθετηθεί.Μπόρουν να κρατούν δεδόμενα για το πότε ποτίστηκε ο κήπος , πόσο νέρο χρειάστηκε και τα επίπεδα υγρασίας στην ατμόσφαιρα και το έδαφος.Αναλόγως την σπορά και τα δεδομένα τα οποία έχουμε τροφοδοτήσει το σύστημα για το κάθε φυτό ή φρούτο και λαχανικό επεκτείνεται η ζώη του . Όλα αυτά λειτουργούν και χώρις την παρουσία του ιδιοκτήτη εξοικονομώντας γιαυτόν χρόνο και χρήμα.

**Σύστημα πυρανίχνευσης και πλυμμήρας**

Ανιχνευτές καπνού , σειρήνες και το σύστημα ενημέρωσης πυρκαγιάς είναι τα κύρια στοιχεία ενός συστήματος πυρανίχνευσης . Το σύστημα μπορεί όπως είναι προφανές να συνδυαστεί και με άλλες λειτουργίες όπως διακοπη παροχής ρεύματος για αποφυγή ηλεκτροπληξίας , ασφαλές κλείσιμο και διακοπή συσκευών κ.α.

**Το σύστημα πυρανίχνευσης και πλημμύρας :**

- Παρέχει προστασία απο πλημμύρα διακόπτωντας την παροχή νερού σε συσκευές όπως πλυντήρια και θερμοσίφωνα . Σ'αυτήν την περίπτωση το σύστημα διακόπτει
  και την παρόχη ρεύματος για την πρόληψη μεγαλύτερης ζημίας σε περίπτωση που η κατάσταση πρόλαβε να ξεφύγει.
- Προλαμβάνει τυχόν ηλεκτροπληξία διακόπτωντας την παρόχη ρεύματος σε όλο το σπίτι (πρίζες) η σε μεμονωμένα σημεία για την προστασία των ενοίκων.

**Έξυπνοι διακόπτες :**

Σημαντικό κομμάτι ενός έξυπνου σπιτιού είναι οι μηχανικοί διακόπτες οι οποίοι είναι φυσική παρουσία μέσα σε ένα έξυπνο σπίτι.Οι μηχανισμοί αυτοί εγκαταστούνται σχεδόν σε όλο το σπίτι όπως σε πόρτες , παράθυρα , ρολά μπαλκονιού ,καγκελόπορτες και αποτελούν την κινητήρι δύναμη μέσα σε αυτό.

**Σύστημα διανομής ήχου και εικόνας :**

Το σύστημα αυτό αναφέρεται στην διανομή ήχου και εικόνας σε οποιαδήποτε συσκεύη στο σπίτι έχει σύστημα αναπαραγωγής ήχου ή εικόνας.

Ο χρήστης μπορεί με το σύστημα αυτό :

- Να απολαύσει την αγαπημένη του ταινία η μουσική σε οποιονδήποτε χώρο μέσα στο σπίτι έχοντας τον απόλυτο έλεγχο της διασκέδασης του.Μπορεί ενώ βρίσκεται στο σαλόνι με το τάμπλετ του η απο την κεντρική εντοιχισμένη πηγή να μεταφέρει τον ήχο και την εικόνα στο δωμάτιο στο όποιο προτιμάει.
- Να στείλει διαφορετικο οπτικοακουστικό υλικό σε διαφορετικά δωμάτιά.Για παράδειγμα μπορέι να στείλει την εικόνα απο τις κάμερες που επιβλέπουν το παιδί του στο σαλόνι και παράλληλα να στείλει τον ήχο απο το ίδιο δωμάτιο σε κάποιο άλλο .
- Αν κάποιος βρίσκεται στην εξώπορτα της πολυκατοικίας ο χρήστης μπορει να μεταφέρει την εικόνα της κάμερας σε οποιαδήποτε συσκευλη αναπαραγωγής βίντεο και τον ήχο σε κάποιο τηλέφωνο ή κάποια άλλη συσκευη τηλεποικινωνίας .Έτσι εκ του ασφαλούς ο χρήστης μπορεί να ελέγξει ποιός βρίσκεται στην πόρτα του ακόμα και απο την άνεση του κρεβατιού του πριν προβεί σε ενέργειες.

**Φωνητικά ελεγχόμενες εντολές και προγραμματισμός :**

Οι φωνητικά ελεγχόμενες συσκευές κάνουν την επικοινωνία ανθρώπου με συσκευές εφικτή χρησιμοποιώντας τεχνολογίες αναγνώρισης φώνης . Σε ένα έξυπνο σπίτι τον ρόλο αυτής της

λειτουργίας αναλαμβάνουν τα home gateways (πχ Alexa ,Google nest κλπ ) ,Οι συσκευές αυτές έχουν εγκατεστημένες ιδιότητες , παρόλα αυτά είναι δυνατή και η επέκταση των ιδιοτήτων αυτών αναλόγως τις ανάγκες . Είναι ικάνες για αναγνώριση φωνής και αλληλεπίδραση με το άτομο που ομιλεί , αναπαραγωγή μουσικής , αναφορα δελτίο καιρού , streaming , τοποθέτηση ξυπνητηριών και πολλά ακόμα . Τα gateways αυτά είναι και προγραμματιζόμενα και μπορούν να επαναλάβουν λειτουργίες επι καθημερίνη βάση σύμφωνα με την ρούτινα του χρήστη (Malche, Internet of Things (IoT) for building Smart Home System, 2017).

## 3.7 Πρωτόκολλα IOT

Το X10 είναι ένα πρωτόκολλο επικοινωνίας ηλεκτρικών συσκευών για έξυπνο σπίτι και χρησιμοποιεί την υπάρχουσα ηλεκτρική εγκατάσταση για να στείλει και να λάβει εντολές χωρίς να είναι αναγκαία η εγκατάσταση καινούργιας καλωδίωσης.

Το πρωτόκολλο αναπτύχθηκε το 1975 απο την εταιρία Pico Electronics και χρησιμοποιείται μέχρι και σήμερα , αν και δεν έχει εξελιχθεί για να ακολουθεί τα σημερινά πρότυπα και την καινούργια τεχνολογία. Το X10 επικοινωνεί μέσω του σπιτιού χρησιμοποιώντας το υπάρχον ηλεκτρικό σύστημα καλωδίωσης . Η συσκευή εγκαθίσταται σε μια ηλεκτρική έξοδο η ενώνεται με το σύστημα καλωδίωσης του σπιτιού όπως τους διακόπτες φωτισμού.Ένας πομπός X10 συνδέεται επίσης με μια ηλεκτρική έξοδο. Αυτός ο πομπός σημάτων χρησιμοποιείται για να στείλει τις πληροφορίες ελέγχου στη συσκευή X10.Ένας ελεγκτής X10 μπορεί επίσης να συνδεθεί μέσω USB σε υπολογιστή και επιτρέπει σε αυτόν να διαχειριστεί τις X10 συσκευές .

Σε κάθε X10 δέκτη υπάρχει ένα ζευγάρι μετρητών. Ένας μετρητής επιλέγει γράμματα από το A - P (αποκαλούμενο κώδικα σπιτιού), οι άλλοι αριθμοί από 1-16 (αποκαλούμενος κώδικας μονάδας). Συνολικά μπορείτε να έχετε 256 (16 x 16) διαφορετικές X10 συσκευές.Έτσι πραγματοποιείται έλεγχος των συσκεύων.Για παράδειγμα εάν δεν υπήρχαν τα ζευγάρια μετρητών η εντολή του υπολογιστή που θα ΄΄έλεγε΄΄ να ανοίξει κάποια συσκευή θα κατέληξε σε λειτουργία όλων των συσκευών .

Πλεονεκτήματα :

Το X10 εγκαθίσταται εύκολα σε ένα σπίτι χώρις την ανάγκη για εγκατάσταση περαιτέρου καλωδίωσης για μεταφορά δεδομένων.Επιπρόσθετα είναι πιο αξιόπιστη απο την ασύρματη επικοινωνία και μπορεί να εγκατασταθεί και να επικοινωνήσει σε οποιοδήποτε χώρο που έχει οποιαδήποτε ηλεκτρική έξοδο.Είναι σχετικά φθηνή και εύκολη στην εγκατάσταση.Παράλληλα για το X10 έχουν αναπτυχθεί ραδιοπομποί έτσι ώστε ο χρήστης να έχει ασύρματο έλεγχο μέσα απο το σπίτι.

Περιορισμοί :

Το X10 δεν έχει συμβαδίσει με την εξέλιξη της τεχνολογίας οπότε υπάρχουν κάποια μειονεκτήματα.

**Θόρυβος** - Σύχνα βιώνει παρεμβολές απο τον θόρυβο στην καλωδίωση και χρειάζεται περαιτέρω εξοπλισμό για να αποφευχθεί το πρόβλημα αυτό.Συγκεκριμένα εένα φίλτρο σε κάθε ηλεκτρική έξοδο που έχει εγκατασταθεί το X10.Ο θόρυβος αυτός προέρχεται απο τις ήδη υπάρχουσες ηλεκτρικές συσκευές του σπιτιού όπως το ψυγείο , η ηλεκτρική σκούπα ,ο φούρνος , ο ηλεκτρονικός υπολογιστής , φορτιστές κ.α.

Το άλλο ζήτημα έχει να κάνει περισσότερο με το πώς είχε καλωδιωθεί το σπίτι σας. Εάν δηλαδή το σπίτι έχει καλωδιωθεί σε 2 φάσεις του ηλεκτρικού συστήματος του σπιτιού σας 110V. Εάν ο πομπός X10 είναι σε μια πλευρά και ο δέκτης είναι σε μια άλλη πλευρά, το X10 σήμα δεν μπορεί να ληφθεί. Συχνά, το σήμα γεφυρώνεται μέσω μιας συσκευής 220V λειτουργεί ως γέφυρα μεταηύ των δυο φάσεων του σπιτιού . Μια τέτοια συσκευή είναι αναγκαίο να εγκατασταθεί .

**Γείτονες** - Ένα άλλο ζήτητμα είναι εάν οι γείτονες σας έχουν και αυτοί εξοπλισμό X10 . Υπάρχει κίνδυνος να διαχειρίζονται τις συσκευές σας παράλληλα με τις δικές τους και αντίστροφα . Η λύση για το πρόβλημα αυτό είναι η εγκατάσταση ενός φράγματος θορύβου πριν απο τον διακόπτη του κυκλώματος.

**Χαμένες εντολές -** Τα σήματα X10 μπορούν να μεταδωθούν με μία εντολή την φόρα . Πρώτα απευθύνεται στην συσκευή προς έλεγχο , και έπειτα στέλνει την εντολή για να να εκτελέσει μια λειτουργία.Εάν δύο σήματα X10 μεταδωθούν την ίδια στιγμή μπορεί να συγκρουστούν , οδηγώντας σε μηδενική δραστηριότητα η σε λανθασμένες λειτουργίες .

Το πρωτόκολλο Insteon είναι το πιο ιδιαίτερο πρωτόκολλο στην λίστα γιατί συνδυάζει ασύρματη τεχνολογία αλλά και τεχνολογία διάδοσης δεδομένων διαμέσου γραμμής ρεύματος (powerline).Αυτό δίνει την ευελιξία στον χρήστη να εγκαταστήσει εξοπλισμό οπουδήποτε στον χώρο αρκεί να υπάρχει παροχή ρεύματος (πρίζα) η κάποια ασύρματη ζεύξη.

Τεχνολογία :

Το Insteon επικοινωνεί με τις συσκευές διαμέσου ασύρματου ραδιοσήματος 915 MHz se σε δίκτυο peer-to-peer.Ο ρυθμός μετάδοσης δεδομένων σε ένα δίκτυο Insteon είναι περίπου 180bits/s αλλά υπάρχει και η δυνατότητα υπέρβασης αυτής της τιμής. Αυτό σημαίνει ότι το δίκτυο δεν είναι ικανό για streaming υπηρεσίες.Περιορίζεται στην μετάδοση εντολών και μηνυμάτων .Το μέγιστο όριο μετάδοσης είναι τα 45 μέτρα χωρίς φυσικά εμπόδια και η πρακτική τιμή σε οικιακή χρήση τα 10.Χρησιμοποιώντας το δίκτυο πλέγματος η απόσταση μπορεί να αυξηθεί στα 30 μέτρα.Η ασύρματη εμβέλεια δεν είναι πρόβλημα για το Insteon καθώς χρησιμοποιεί και τις γραμμές ρεύματος για επικοινωνία.

Πλεονεκτήματα :

Το μεγαλύτερο πλεονέκτημα του συστήματος είναι το πλεόνασμα που πα΄ρεχει.Εάν στο δίκτυο υπάρχει κάποια βλάβη σε κάποια ασύρματη ζεύξη τότε το σύστημα συνεχίζει να παραμένει ενεργό και να ανταλλάσει δεδομένα μέσω των γραμμών ρεύματος ( powerline ) αντίστροφα.

Ένα δεύτερο πλεονέκτημα είναι οτι δεν είναι απαραίτητη η εγκατάσταση καινούργιας καλωδίωσης καθώς το Insteon χρησιμοποιεί τη νυπάρχουσα εγκατάσταση ρεύματος για ανταλλαγή δεδομένων και μηνυμάτων.

Περιορισμοί :

Αν και το Insteon έχει διάφορα εξαρτήματα και συσκευές για την χρήση σε οικιακό δίκτυο , το μεγάλο πρόβλημα είναι η έλλειψη third-party επιλογών .Οι επιλογές περιορίζονται στο οικοσύστημα της Insteon .Αν για παράδειγμα η εταιρία κλείσει δεν υπάρχει η επιλογή αναβάθμισης σε καινουργιο η συμβατό εξοπλισμό.

**Wi-Fi**

Το Wi-Fi είναι ένα σύνολο πρωτοκόλλων ασύρματης δικτύωσης βασισμένο στην οικογένεια προτύπων IEEE 802.11 , η οποία χρησιμόποιείται ευρέως για την δικτύωση τοπικής περιοχής συσκευών και πρόσβαση στο διαδίκτυο.Είναι ευρέως χρησιμοποιούμενο στα σπίτια και είναι λογικό να εκμεταλευτεί και απο τις συσκευές οικιακού αυτοματισμού.
Τεχνολογία:

Το wifi χρησιμοποιεί ραδιοκύματα στο φάσμα των 2.4 Ghz και 5Ghz.Οι συμβατές συσκευές χρησιμοποιούν μια κεραία με ένα πομπό και ένα δέκτη.Η πρακτική κάλυψη σε ένα σπίτι είναι περίπου 20 μέτρα και είναι εφικτό να συνδεθούν μεχρι και 256 διαφορετικές συσκευές.

Πλεονεκτήματα: Τα μεγαλύτερα πλεονεκτήματα του Wi-Fi είναι οι υψηλές ταχύτητες μετάδοσης , η κάλυψη και γενικότερα η πρακτικότητα της τεχνολογίας αυτής καθώς η εγκατάσταση ενός ρούτερ είναι φθηνή και εύκολη σε σχέση με την εγκατάσταση καλωδίων και κεντρικών σημείων ελέγχου φορτίου και δεδομένων (racks , servers ,swiches ) όπως θα δούμε στην συνέχεια .

<u>Περιορισμοί:</u>

Αν το δούμε απο την μάτια ενός αυτοματοποιημένου σπιτιού υπάρχουν μερικά σενάρια που δεν είναι τοσο θετικά και περιορίζουν την σταθερότητα .

Το Wi-Fi είναι επιρρεπής σε παρεμβολές λόγω bandwidth.Καθώς οι συσκευές όπως κινητά , τάμπλετ ,φώτα , θερμοστάτες προσπαθούν να επικοινωνήσουν με τον σέρβερ η μεταξύ τους

δημιουργείται συνωστισμός καταναλώνοντας bandwidth και είναι πιθανή η μη πραγματοποιήση εντολών ή εντολές να πάνε χαμένες .

Ένα ακόμα πρόβλημα είναι η κατανάλωση ενέργειας απο τις συσκευές.Η ανάγκη για μεγάλη κάλυψη και υψηλές ταχύτητες απαιτούν πού ενέργεια για να λειτουργήσουν.Σε πολλές συσκευές αυτή η κατανάλωση μπορεί να μην είναι εμφανής . Το πρόβλημα φαίνεται σε συσκευές όπως αισθητήρες κίνησης , ποσοστών οξυγόνου και διοξειδίου του άνθρακα που λειτουργούν με μπαταρίες.

Ενώ η κάλυψη είναι θετικό χαρακτηριστικό , είναι και περιορισμένων δυνατοτήτων.Το Wi-Fi μπορεί να περιοριστεί σε ένα μεγάλο σπίτι καθώς οι τοίχοι ,τα μπετό ,οι πόρτες και γενικότερα η τοπολογία του σπιτού δυσκολεύουν την μετάδοση των δεδομένων.

Η Wi-Fi alliance έχει βγάλει πρότυπα για την ασφάλεια του Wi-Fi για να προστατεύσουν απο τυχόν εισβολές παρολαυτά είναι στο χέρι του χρήστη η συνεχής ασφάλεια και θα πρέπει να κάνει ελέγχους ρουτίνας και έγκαιρες ενημερώσεις για την ορθή λειτουργία.

**Ethernet**

Το καλώδιο Ethernet είναι τύπος καλωδίου χρησιμοποιούμενο σε δίκτυο υπολογιστών ενσύρματης τοπικής δικτύωσης υπολογιστών και είναι ικανό να μεταφέρει μεγάλες ποσότητες δεδομένων πολύ γρήγορα.Είναι η κύρια μέθοδος μεταφοράς δικτυακής κίνησης.
Τεχνολογία:

Αποτελείται απο κοινό χαλκό με αθωράκιστα η θωρακισμένα συνεστραμμένα ζεύγη ή οπτικές ίνες .Η μέγιστη απόσταση ενός καλωδίου Ethernet περιορίζεται στα 100 μέτρα ( χωρίς απώλειες ) και η μεταφορά δεδομένων στο 1Gbps.

Χαμηλή τάση συνεχόμενου ρεύματος μπορεί να διοχετευτεί μέσα απο ένα τέτοιο καλώδιο το οποίο βοηθάει στις συσκευές οικιακού αυτοματισμού όπως κάμερες και θυροτηλέφωνα.

Οι ταχύτητες του κυμαίνονται απο 10 mbps εώς 10 Gbps αναλόγως τον τύπο του καλωδίου.

- Ethernet ( 10mbps )
- Fast Ethernet ( 100mbps )
- Gigabit Ethernet ( 1000mbps ή 1Gbps ) με τύπο καλωδίου CAT5e ή CAT6
- Gigabit Ethernet ( 10000 mbps ή 10Gbps ) με οπτική ίνα

Πλεονεκτήματα:

Τα πλεονεκτήματα των καλωδίων Ethernet είναι εύκολο να καθοριστούν.Δύο κυρίως πλεονεκτήματα είναι:

- Υψηλές ταχύτητες μεταφόρας δεδομένων
- Περισσότερη ασφάλεια απο την ασύρματη σύνδεση καθώς τα καλώδια τείνουν να είναι πιο ασφαλή και είναι εγκατεστημένα μέσα απο τους τοίχους και γενικότερα σε σήμεια που δεν είναι εύκολη η πρόσβαση.

Περιορισμοι:

Τα καλώδια Ethernet δεν είναι τέλεια και ενώ προσφέρουν μεγάλες δυνατότητες έχουν και κάποια μειονεκτήματα.

Η εγκατάσταση τους μπορεί να είναι ακριβή εάν δεν είναι ήδη εγκατεστημένα στον υπάρχων χώρο.Για την εγκατάσταση τους είναι αναγκαίος ο χειρισμός απο διάφορους τεχνίτες όπως ηλεκτρολόγους και ηλεκτρονικούς για να ανοίξουν τρύπες και διόδους στον τοίχο και να εγκαταστήσουν σώστα και με σείρα την καλωδίωση.Σε συγκεκριμένες περιπτώσεις μπορεί να είναι και δυνατή η εύρεση μονοπατιού για να περάσουν τα καλώδια στους χώρους που πρέπει.
Το Ethernet απαιτεί κάποιο κεντρικό ντουλάπι δεδομένων , έναν χώρο δηλαδή στον οποίο θα καταλήγουν τα καλώδια η κομμάτια καλωδίων για να συνδεθούν στα switches και hubs για να τροφοδοτηθούν στο υπόλοιπο σπιτι και να είναι εφικτός ο έλεγχος της κίνησης του δικτύου.

**Z-WAVE**

Το Z-WAVE είναι ένα πρωτόκολλο έπικοινωνίας ασύρματης σύνδεσηςπου αναπύχθηκε συγκεκριμένα για την αγόρα του οικιακού αυτοματισμού.Το Z-WAVE είναι ένα απο τα δημοφιλέστερα πρωτόκολλα ασύρματης σύνδεσης χαμηλής ισχύος για την διασύνδεση των οικιακών συσκευών αυτοματισμού.
Τεχνολογία:

Οι συχνότητες της ασύρματης λειτουργίας είναι τα 868.40,868.42 και 869,85 Hz για την Ευρώπη (διαφοροποιούνται ανάλογως την χώρα).Κάθε συσκευή μπορεί να στείλει και να λάβει εντολές η να μεταβιβάσει τις εντολές αυτές σε άλλες συσκευές.Αυτό δημιουργεί ad-hoc δίκτυο ή δίκτυο πλέγματος (mesh network).Η λειτουργία αυτή αυξάνει δραματικά την κάλυψη του δικτύου καθώς εάν μια συσκευή είναι εκτός ορίων μία άλλη που βρίσκεται κοντά της μπορεί να μεταβιβάσει το μήνυμα μέχρι να φτάσει επιτυχώς στον προορισμό του. Οι ταχύτητες μετάδοσης ποικίλουν απο 40 μέχρι 100 Kbps , οι οποίες είναι χαμηλότερες απο τις ταχύτητες Ethernet , Wi-Fi , Zigbee και Thread.Παρόλαυτα οι χαμηλές αυτές ταχύτητες δεν επηρεάζουν την αποτελεσματικότητα του δικτύου καθώς το πρωτόκολλο Z-Wave διαδίδει εντόλες και όχι πολύ μεγάλο όγκο δεδόμένων όπως streaming υπηρεσίες.

Οι κάλυψη σε εξωτερικούς χώρους ορίζεται στα 100 μέτρα ενώ σε κλειστούς χώρους γύρω στα 25 και συνιστάται η απόσταση των συσκευών να μην ξεπερνάνε τα 10 μέτρα η μία απο την άλλη για μεγαλύτερη αξιοπιστία και απόδοση .Επίσης σε ένα δίκτυο Z-Wave μπορούν να συνδεθούν εως 232 συσκευές.

Πλεονεκτήματα:

Ένα πλεονέκτημα που καθιστά το Z-Wave τόσο δημοφιλές είναι το δίκτυο πλέγματος.Παρέχει ένα πιο αξιόπιστο δίκτυο στις μεγαλύτερες αποστάσεις.

Επιπρόσθετο το πρωτόκολλο αυτό χρησιμοποιεί μπάντες συχνοτήτων που δεν έχουν μεγάλο συνωστισμό οπότε υπάρχουν και λιγότερες παρεμβολές.

Τέλος χρησιμοποιεί πολύ χαμηλή ισχύ οπότε αυξάνεται ο χρόνος ζωής στις οικιακές συσκευές και εξουδετερώνεται η ανάγκη για χρήση ενσύρματης σύνδεσης.

Περιορισμοί:

Ο μεγαλύτερος περιορισμός είναι η χαμηλές ταχύτητες που προσφέρει που περιορίζουν το Z-Wave σε λειτουργίες αποστολής και λήψης εντολών.Δεν ελίναι η κατάλληλη τεχνολογία για υπηρεσίες streaming υψηλής ποιότητας ήχου και εικόνας.

**Zigbee**

Το πρωτόκολλο Zigbee χρησιμοποιεί και αυτό ένα ασύρματο δίκτυο mesh χαμηλής ισχύος , εύρους ζώνης και μικρής απόστασης επικοινωνίας.

Τεχνολογία :

Το Zigbee ενεργεί στην μπάντα των 2.4Ghz.Κάθε συσκευή μπορεί να στείλει και να λάβει εντολές , όπως επίσης και να μεταβιβάσει αυτές σε άλλες συμβατές συσκευές του δικτύου.Η ικανότητα αυτή δημιουργεί ένα ad-hoc δίκτυο που συνεπάγεται με μεγαλύτερη κάλυψη στο δίκτυο και ως αποτέλεσμα ολόκληρη την κάλυψη ενός σπιτιού.

Οι ταχύτητες διάδοσης των δεδόμενων δεν είναι πολύ μεγάλες (250kbps στα 2.4Ghz ) και ούτε κατάλληλες για streaming υπηρεσίες αλλά είναι αρκετή για την αποστολή και λήψη εντολών .

Η κάλυψη σε ανοιχτό χώρο αρκείται στα 100 μέτρα , παρόλαυτα η πρακτική κάλυψη είναι περίπου 15 μέτρα μέσα σε ένα σπίτι , η δυνατότητα όμως του δικτύου να μεταπηδά πληροφορίες και εντολές αυξάνει κατα ένα ποσοστό αυτήν την απόσταση .

Τέλος το θεωρητικό μέγεθος που μπορεί να χειριστεί το Zigbee είναι περίπου 65.000 συσκευές.Απίθανο μάλλον ένα σπιτι να χρησιμοποιεί τόσες πολλές συσκευές αλλά βλέπουμε την «δύναμη» αυτού του πρωτοκόλλου.

Πλεονεκτήματα:

Τα δύο μεγαλύτερα πλεονεκτήματα του πρωτοκόλλου Zigbee είναι το δίκτυο πλέγματος και η χαμήλης ισχύς μετάδοσης.Η αποδοτική χρήση ισχύος του επιτρέπει τις συσκευές να λειτουργήσουν με μπαταρίες.

Περιορισμοί :

Το μεγαλύτερο μειονέκτημα του Zigbee είναι ο περιοσμένος αριθμός εξαρτημάτων στην αγόρα.Επειδή δεν είναι τόσο διαδεδομένο ακόμα οι κατασκευάστες δεν έχουν αρχίσει πόλυ μεγάλη παραγωγή .Αναμένετε τα επόμενα χρόνια να διαδώθει πολύ περισσότερο κύριως γιατί η Amazon συμπεριέλαβε τις ραδιοσυχνότητες του Zigbee στα gateway της , Echo Plus και Echo Show.

**Thread**

Το Thread είναι ένα καινούργιο πρωτόκολλο επικοινωνίας IoT συσκευών το οποίο χειρίζεται η Thread Group.Σε αυτήν συμμετέχουν πολλοί κατασκευαστές ηλεκτρονικών και ηλεκτρικών συσκευών όπως η Samsung , Google/Nest , Apple ,Qualcomm , Tyco και άλλοι.Το χαμηλής ισχύς βασιζόμενο σε IP μετάδοση ασύρματο δίκτυο πλέγματος επιτρέπει στις έξυπνες συσκευές να λειτουργήσουν με μπαταρίες και να επικοινωνούν μεταξύ τους αλλά και με το Cloud.

Τεχνολογία :

Το Thread λειτουργεί χρησιμοποιώντας το πρότυπο IEEE 802.15.4 για ασύρματη μετάδοση δεδομένων χαμηλού ρυθμού PAN ( Personal area network-Δίκτυο Προσωπικού Χώρου ) δικτύου που είναι ειδικά σχεδιασμένο για την σύνδεση συσκευών μεταξύ τους σε ένα χαμηλής ισχύς ,χαμηλού εύρους ζώνης δίκτυο πλέγματος.

Το πρωτόκολλο λειτουργεί στην συχνότητα των 2.4Ghz . Όλες οι συσκευές χρησιμοποιούνε IP μετάδοση , που σημαίνει ότι οι συσκευές IoT συνδέονται μεταξύ τους αλλά μπορούν και να συνδεθούν στον διαδίκτυο.Είναι παρόμοιο με το Wi-Fi αλλά με σχεδιασμό χαμηλής ισχύος και εύρους ζώνης , απευθείας για χρήση οικιακού αυτοματισμού.

Η πρακτική κάλυψη στα 2.4 Ghz είναι περίπου 15-20 μέτρα αλλά με την χρήση του δικτύου πλέγματος και μεταβίβασης εντολών σε συσκευές που δεν είναι στα όρια δικτύου αυτή η απόσταση αυξάνεται.

Το Thread προορίζεται για IoT συσκευές και εξαρτήματα για να μεταφέρουν εντολές απο και προς αυτές και το υψηλό εύρος ζώνης δεν απαιτείται.Η ταχύτητα διάδοσης των δεδομένων είναι τα 250 Mbps που είναι παραπάνω απο αρκετή για για smart home συσκευές .

Πλεονεκτήματα :

Εκτός απο την χαμηλή ισχύ ραδιοσυχνοτήτων και το δίκτυο πλέγματος που είδαμε και σε άλλα πρωτόκολλα το Thread ξεχωρίζει για την χρήση IP πρωτοκόλλου που χρησιμοποιεί.

Περιορισμοί :

Το κυριότερο πρόβλημα με το Thread είναι ότι είναι ακόμα είναι καινούργια τεχνολογία και στην αγορά δεν κυκλοφορούν πολλές συμβατές συσκευές και εξαρτήματα για αγορά.

**Bluetooth Low Energy (Bluetooth Χαμηλής Ενέργειας )**

Πολλές έξυπνες οικιακές συσκευές εμπεριέχουν την τεχνολογία Bluetooth για την επικοινωνία σε μικρές αποστάσεις . Το Bluetooth μεταφέρει δεδομένα σε αρκετά ικανοποιητικές ταχύτητες

αλλά σε μικρές μόνο αποστάσεις.Τα περισσότερα smartphone χρησιμοποιούν την τεχνολογία αυτή η οποία είναι ένας πολύ καλός τρόπος διασύνδεσης οικιακών συσκευών και διαχείρηση αυτών μέσω smartphone ή τάμπλετ.Η κυριότερη χρήση του αφορά την υπηρεσία streaming ήχου σε ασύρματα ακουστικά ή μεγάφωνα.

Τεχνολογία :

Το Bluetooth Low Energy είναι ένα ασύρματο δίκτυο προσωπικού χώρου.Το BLE παρέχει σημαντικές μειώσεις κατανάλωσης ενέργειας και κόστους διατηρώντας την επικοινωνιακή κάλυψη στα 100 μέτρα.Ο ρυθμός μετάδοσης των δεδομένων είναι στα 2Mbit/s.

Πλεονεκτήματα :

Η απάντηση είναι ένας συνδυασμός γνωρισμάτων.

Το κυρίως πλεονέκτημα είναι η συμβατότητα.Το BLEόπως και η προηγούμενη εκδοχή το Bluetooth είναι το διασημότερο PAN δίκτυο και υποστηρίζεται από τις μεγαλύτερες και σημαντικότερες εταιρίες καταναλωτικών συσκευών.

Ένα ακόμα πλεονέκτημα είναι η χαμηλή ισχύς.Ο σχεδιασμός του είναι τέτοιος ώστε να βρίσκεται κατά το μεγαλύτερο ποσοστό του ανενεργό τραβώντας αμελητέο ρεύμα πράγμα που το εύκολο να λειτουργήσει με μια μικρής ισχύος μπαταρία. Τέλος το BLE βασίζεται στην κλασική τεχνολογία Bluetooth και η απλή τεχνολογία του το κάνει εύκολα διαχειρίσιμο από μια μικρή στοίβα πρωτοκόλλου.

Περιορισμοί :

Δεν έχει σταθερή σύνδεση και μπορεί να χάσει την επαφή ανα πάσα στιγμή
Έχει χαμηλό εύρος φάσματος συγκριτικά με το WiFi

Επιτρέπει μόνο την επικοινωνία συσκευών σε μικρή απόσταση μεταξύ τους

Η ασφάλεια είναι μία πολύ βασική πτυχή.Δεν έχει αξιόπιστη ασφάλεια και μπορεί να παραβιαστεί (Jayapal, 2019).

**6LoWPAN**

Είναι ακρωνύμιο μεταφράζεται ως πρωτόκολλο IPv6 που λειτουργεί πάνω σε προσωπικού χώρου δίκτυο χαμηλής ισχύος.Το πρωτόκολλο αυτό στέλνει δεδομένα ως πακέτα χρησιμοποιώντας αντίστοιχα το πρωτόκολλο IPv6.Παρέχει κάλυψη απο άκρη σε άκρη επικοινωνίας IPv6 και γιαυτό είναι ικανό να παρέχει σύνδεση σε διαφόρων ειδών δίκτυα καθως και απευθείας συνδεσιμότητα των συσκευών στο διαδίκτυο.

Τεχνολογία :

Το 6LoWPAN χρησιμοποιεί το πρωτόκολλο IPv6 για να επικοινωνήσει με τις υπόλοιπες συσκευές του δικτύου στέλνοντας δεδομένα ως πακέτα με IP διευθυνσιοδότηση.Λόγω ότι όλες οι συσκευές λειτουργούν με IP διευθυνσιοδότηση κάθε κόμβος του δικτύου μπορεί να επικοινωνήσει απευθείας με τις υπόλοιπες συσκευές με IPv6 αλλά και με τον διαδίκτυο με IPv4 ή IPv6 διαμέσου του ISP ρούτερ.Αυτό σημαίνει ότι το 6LoWPAN είναι ένα δίκτυο πλέγματος.

Πλεονεκτήματα :

- Το δίκτυο πλέγματος εξασφαλίζει ευελιξία και κλιμακούμενο μέγεθος στο εγκατεστημένο δίκτυο με εύκολη προσαρμογη στο μέγεθος που θέλει ο ιδιοκτήτης.
- Προσφέρει μεγάλη κάλυψη δικτύου.
- Δεν απαιτεί πύλη IOT.Οποιοδήποτε ρούτερ μπορεί να εγκατασταθεί στο δίκτυο και να λειτουργήσει αποτελεσματικά.

- Καταναλώνει λίγη ενέργεια καθώς χρησιμοποιεί μειωμένο χρόνο μετάδοσης.Εξοικονομεί έτσι ενέργεια και εξασφαλίζει μεγαλύτερη χρόνο διάρκειας μπαταρίας στις συσκευές.
- Προσφέρει χαμηλό κόστος και ασφάλεια στην επικοινωνία IOT.
- Παρέχει δρομολόγηση απο μια συσκευή σε πολλές και το αντίστροφο.

Χρησιμοποιεί το πρωτόκολλο IPv6 και ως εκ τούτου μπορεί να δρομολογηθεί απευθείας στο νέφος.

Μειονεκτήματα :

- Έχει μειωμένη ανοσία σε παρεμβολές σε σχέση με το wifi και το Bluetooth.
- Χωρίς το δίκτυο πλέγματος υποστηρίζει μικρής εμβέλειας μετάδοση.

**LoRa και LoRaWAN**

Τεχνολογία:

Το LoRa είναι ένα σήμα φορέα ραδιοσυχνότητας βασισμένο στο φυσικό επίπεδο αναφοράς OSI.Χρησιμοποιώντας ένα LoRa μόντεμ μπορείτε να μετατρέψετε τα δεδομένα σε σήμα.

Το LoRaWAN ουσιαστικά είναι ο συνδετικός κρίκος που ενώνει το σήμα με την εφαρμογή χειρίζοντας και το πρωτόκολλο και την αρχιτεκτονική.

Οι συσκευές LoRa αποτελούνται απο δύο εξαρτήματα.

- Μια μονάδα ραδιοκεραίας
- Έναν μικροεπεξεργαστή για την επεξεργασία των δεδομένων των αισθητήρων

Ένα μόντεμ LoRa αποτελείται απο δυο εξαρτήματα επίσης :

- Μια ραδιοκεραια
- Έναν μικροεπεξεργαστή για την επεξεργασίια των δεδομένων

Το πρωτόκολλο LoRaWAN δεν υποστηρίζει απευθείας επικοινωνία με με τους κόμβους.Απαιτείται συσγκεκριμένος εξοπλισμός ρούτερ για την δρομολόγηση των πακέτων και τον χειρισμό τους .Για την Ευρώπη οι χρησιμοποιούμενες συχνότητες είναι τα 902-908Mhz και οι ταχύτητες κυμαίνονται απο 0.3 kbps – 5.5kbps.

Πλεονεκτήματα:

- Προσφέρει μεγαλύτερη διάρκεια μπαταρίας στις συσκευές
- Ποιότητα υπηρεσίας
- Ασφάλεια στην μετάδοση και λήψη των δεδομένων
- Ευελιξία στην χωρητικότητα δικτύου
- Μεγάλη ποικιλία στις εφαρμογές που χρησιμοποιούνται
- Χαμηλή ισχύ
- Χαμηλό κόστος

Μειονεκτήματα :

- Μπορεί να χρησιμοποιηθεί σε εφαρμογές που χρησιμοποιούν χαμηλό ρυθμό δεδομένων της τάξεως των 27kbps.
- Δεν είναι ιδανικό για χρήση σε πραγματικού χρόνου εφαρμογές που απαιτούν χαμηλό χρόνο απόκρισης (Sarawi, 2017)

## 3.8 Έξυπνο Σπίτι = Πράσινο σπίτι

Ένα έξυπνο σπίτι πρέπει να συνδυαζει την τεχνολογία με την οικονομία και την οικολογία . Για την σωστή λειτουργία του θα πρέπει να γίνει εγκατάσταση οικολογικού εξοπλισμού όπως :

**Οικολογικά υλικά :**

Ο οικολογικός σχεδιασμός προϊόντων αναφέρεται στην ένταξη του οικολογικού παράγοντα, σε όλα τα στάδια του Κύκλου Ζωής αυτών, με σκοπό την ελαχιστοποίηση της επιβάρυνσης του περιβάλλοντος

**Θερμοπροσόψη :**

Η θερμοπρόσοψη σε κτίριο γίνεται με την τοποθέτηση θερμομονωτικών πλακών στο εξωτερικό μέρος των κατακόρυφων τοίχων του. Το κάθε κτίριο έχει διαφορετικές παραμέτρους που πρέπει να ληφθούν υπόψη για την εφαρμογή μιας επιτυχημένης θερμοπρόσοψης, όπως είναι η υπάρχουσα θερμομονωτική του επάρκεια τα δομικά στοιχεία που αποτελείται και το τοπικό κλίμα της περιοχής .

**Ενεργειακά τζάκια :**

Ο άνθρακας του ξύλου ενώνεται με το οξυγόνο ενός χώρου και παράγονται μονοξείδιο και διοξείδιο του άνθρακα αλλά και θερμική ενέργεια. Είναι γεγονός, όμως, ότι όσο μεγαλύτερη είναι η θερμοκρασία σε ένα χώρο, τόσο μεγαλύτερη ποσότητα μονοξειδίου απελευθερώνεται και συνεπώς έχουμε υψηλότερη απόδοση.Η καύση που γίνεται στα ενεργειακά τζάκια με κλειστή εστία έχουν μεγαλύτερη απόδοση (έως 70-80%) από τα παραδοσιακά λόγω της αποθήκευσης υψηλότερης θερμοκρασίας. Ταυτόχρονα μειώνεται σημαντικά και η ρύπανση του ατμοσφαιρικού αέρα λόγω της καύσης των ξύλων.

**Ενεργειακά τζάμια :**

Σε ένα μέσο σπίτι το 35% της θερμικής απώλειας ,το μεγαλύτερο δηλαδή ποσοστό συγκριτικά με τις αντίστοιχες απώλειες απο το δάπεδο , την σκεπή κλπ οφείλεται στα παράθυρα . Τα ενεργειακά τζάμια λόγω της επίστρωσης μικροσκοπικών οξειδίων στη μία πλευρά τυος δεν επιτρέπουν τη μεταφόρα θερμότητας απο τον εσωτερικό χώρο του σπιτιού η και αντίστροφα. Είναι σαφές λοιπόν οτι η ελαχιστοποίησει των απωλειών θα πρέπει να αποτελεί προτεραιότητα.

**Οικιακές συσκευές ενεργειακής κλάσης Α :**

Η ενεργειακή σήμανση των οικιακών συσκευών παρέχει πληροφορίες για την κατανάλωση ενέργειας, τις επιδόσεις και άλλα ουσιώδη χαρακτηριστικά (όπως για παράδειγμα η χωρητικότητα, η κατανάλωση νερού κ.α.), των προϊόντων οικιακής χρήσης. Μεγαλυτερος ο δείκτης ενεργειακής σήμανσης , χαμηλότερη και η κατανάλωση.Το χαμηλό ετήσιο κόστος λειτουργίας της αποτελεί έναν από τους βασικότερους παράγοντες επιλογής της.

**Συστήματα αυτοματισμού :**

Είναι η τυποποίηση μίας διαδικασίας μέσω της εύρεσης καλώς ορισμένων βημάτων τα οποία πρέπει να ακολουθηθούν για να παραχθεί κάποιο επιθυμητό αποτέλεσμα. Εξοικονομείται ενέργεια με την αποφυγή ανούσιας σπατάλη πόρων.

**Φωτοβολταικά συστήματα :**

Φωτοβολταϊκά ονομάζεται η βιομηχανική διάταξη πολλών φωτοβολταϊκών κυττάρων σε μία σειρά . Τα φωτοβολταϊκά ανήκουν στη κατηγορία των Ανανεώσιμων Πηγών Ενέργειας (ΑΠΕ). Στην κατηγορία των ανανεώσιμων ηλιακών πηγών ενέργειας, τα ηλιοθερμικά συστήματα είναι πιο αποδοτικά από τα φωτοβολταϊκά.

Το μεγαλύτερο ποσοστό ενέργειας που μπορεί να απορροφήσει ένα Φ/Β στοιχείο είναι το 25% της ενέργειας που δέχεται, όμως συνήθως το ποσοστό είναι λιγότερο από 15%.Ο βαθμός απόδοσης εκφράζει το ποσοστό της ηλιακής ακτινοβολίας που μετατρέπεται σε ηλεκτρική ενέργεια στο φωτοβολταϊκό στοιχείο.

**Γεωθερμικά συστήματα κλιματισμού :**

Γεωθερμία (γεωθερμικό δυναμικό) ονομάζεται η αποθηκευμένη ενέργεια υδρολογικών και γεωλογικών σχηματισμών του φλοιού της γης σε μορφή θερμότητας, όταν η θερμοκρασία του

σχηματισμού υπερβαίνει τους 25 °C.Λόγω της χαμηλής κατανάλωσης και της σχεδόν ανύπαρκτης συντήρησης του εξοπλισμού, τα γεωθερμικά συστήματα κλιματισμού μπορούν να εξοικονομήσουν από 55% μέχρι και 70% από την ετήσια δαπάνη σε σύγκριση με ένα συμβατικό σύστημα θέρμανσης και δροσισμού. Το μόνο λειτουργικό κόστος της εγκατάστασης είναι η κατανάλωση ηλεκτρικού ρεύματος από τον συμπιεστή και τις αντλίες, το οποίο είναι οικονομικότερο σε σχέση με τη χρήση λέβητα πετρελαίου κατά 20-25 (Ragheb, 2015).

# Κεφάλαιο 4 Μοντέλα επικοινωνίας

Το "έξυπνο σπίτι" έχει ως βάση την σύνδεση διαφόρων συσκευών με ενσωματωμένους αισθητήρες και εξοπλισμό διασύνδεσης με καλώδιο η ασύρματα τόσο για την επικοινωνία μεταξύ τους όσο και με τον χρήστη , λαμβάνοντας και αποθηκεύοντας δεδομένα με στόχο την προσφορά υπηρεσιών.

## 4.1 Συσκευή-προς-συσκευή (Device-To-Device)

Αύτο το μοντέλο επικοινωνίας απαρτίζεται απο δύο η περισσότερες συσκευές που συνδέονται μεταξύ τους μέσω του ασύρματου δικτύου χώρις κάποια ενδιάμεση πύλη η σέρβερ.Το D2D χρησιμοποιεί φάσμα συχνοτήτων για την μετάδοση δεδομένων το οποίο έχει διάφορα θετικά στοιχεία όπως μεγαλύτερη διακίνηση δεδομένων σε λιγότερο χρόνο και ενεργειακή απόδοση.Μεγάλο χαρακτηριστικό είναι επίσης ότι το μοντέλο αυτό μπόρει να αποδώσει ακόμα και όταν το δίκτυο (home lan) στο οποίο ενεργεί έχει πέσει.Χρησιμοποιούν πρωτόκολλα όπως το Bluetooth,Z-Wave ή Zigbee.  (Gandotra, 2016)

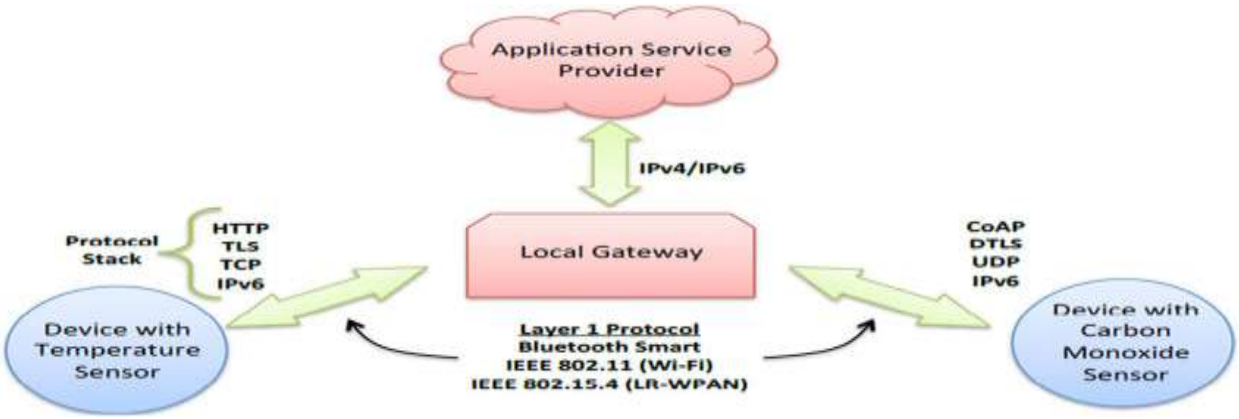
## 4.2 Συσκευή-προς-cloud (Device-To-Cloud)

Σε ένα μοντέλο επικοινωνίας συσκευής προς cloud οι συσκευές iot συνδέονται απευθείας στο cloud για να ανταλλάξουν δεδομένα η να διαχειριστούν αυτά.Επειδή ο όγκος επεξεργασίας δεδομένων σε ένα σπίτι μπορεί να γίνει πολύ μεγάλος και να μην αποφέρει την αναμενόμενη απόδοση και ταχύτητα , οι υπολογιστική ισχύ 'μεταφέρεται' στο cloud προς συλλογή , ανάλυση, αποθήκευση και αποστολής πληροφοριών στον πέλατη.Έτσι επιτυγχάνεται η παροχή υπηρεσιών στον χρήστη  την στιγμή που επιθυμεί πρόσβαση σε εφαρμόγες σε οποιοδήποτε χρόνο και μέρος.Η επικοινωνίας αυτή επιτυγχάνεται πάνω στο υπάρχον ασύρματο και ενσύρματο δίκτυο "έξυπνου σπιτιού". (Stergiou, 2016)


**Εικόνα 5. Μοντέλο επικοινωνίας Device to Cloud**

## 4.3 Συσκευή-προς-δίαυλο επικοινωνίας (Device-To-Gateway)

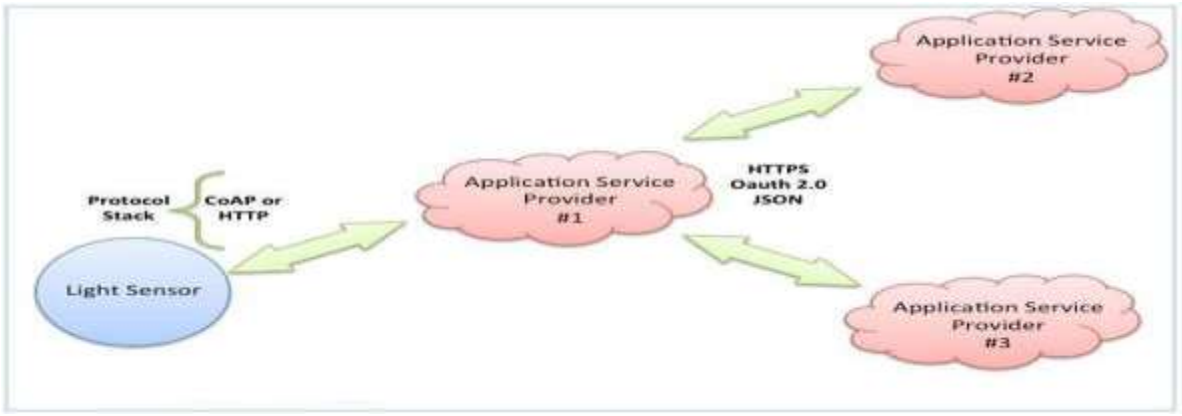
Σε αυτήν την σύνδεση ο χρήστης και οι συσκευές έρχονται σε επικοινωνία μέσω ενός διαύλου επικοινωνίας (gateway - πύλη).Ρόλος του διαύλου επικοινωνίας είναι να παρέχει ασφάλεια στην ανταλλαγή δεδομένων , να μεταφράζει διάφορα πρωτόκολλα για να επιτυγχάνεται η επικοινωνία μεταξύ όλων και γενικότερα να έλεγχει τα πάκετα τα οποία μεταφέρονται στο δίκτυο.Χρησιμοποιούνται πρωτόκολλα όπως το Bluetooth,Wi-fi,LoRaWan κ.α.Για την επικοινωνία με το cloud προτιμάται η συνδεσιμότητα με τα πρωτοκολλα IPv4/IPv6.Κάτα κύριο λογο χρησιμοποιείται το πρωτόκολλο IP/V6 καθώς διαθέτει καλύτερη δυνατότητα αυτορύθμισσης συσκευών ,καλύτερη ποιότητα υπηρεσιών (QoS) και μεγαλύτερη ασφάλεια απο το IPv4.  (Stergiou, 2016)




**Εικόνα 6. Μοντέλο επικοινωνίας Device to Gateway**

## 4.4 Μοντέλο ανταλλαγής δεδομένων (Back-End-Data-Sharing)

Το μοντέλο ανταλλαγής δεδομένων αναφέρεται σε μια αρχιτεκτονική επικοινωνίας η οποία επιτρέπει τους χρήστες να εξάγουν και να αναλύσουν δεδομένα έξυπνων συσκευών απο μια υπηρεσία cloud σε συνδυασμό με δεδομένα απο άλλες πηγές.Με αυτόν τον τρόπο ο χρήστης παραχωρεί με δική του επιθυμία πρόσβαση στα ‘’ανεβασμένα’’ δεδομένα σε τρίτους.Η αρχιτεκτονική αυτή είναι μια επέκταση της αρχιτεκτονικής device-to-cloud και επιτρέπει την συλλογή και ανάλυση όλων των δεδομένων απο ξεχωριστές έξυπνες συσκευές (Stergiou, 2016).




**Εικόνα 7. Μοντέλο επικοινωνίας Back end data sharing**

# 5. Cloud Computing

## 5.1 Χαρακτηριστικά

Το cloud computing γίνεται όλο και πιο αναγνωρίσιμο μέρα με την μέρα.Αυτό οφείλεται στην βαθμιαία επέκταση των επιχειρήσεων οι οποίες χαρακτηρίζονται απο μεγάλη ανάγκη για την αποθήκευση των δεδομένων τους .Έτσι οι επιχειρήσεις Cloud υπηρεσιών μάχονται για την καλύτερη προσφορά υπηρεσιών όσον αφορά την μεγάλη υπολογιστική δύναμη και την αποθήκευση τεράστιων όγκων δεδομένων. Η υπηρεσίες αυτές έχουν αναδειχθεί πολύτιμες όμως τόσο για τις επιχειρήσεις όσο και για τα έξυπνα σπίτια καθώς είναι πανταχού παρών , προσφέρουν ευκολία και κατ'απαίτηση πρόσβαση στο δίκτυο.

Τα χαρακτηριστικά του Cloud Computing είναι :

I. Συγκέντρωση πόρων ( **Resource pooling )** :

   Το χαρακτηριστικό αυτό έχει να κάνει με τον διαμοιρασμό πόρων με τον σέρβερ

II. Διαθεσιμότητα ( Availability ) :

   Σημαίνει ότι το υπολογιστικό σύννεφο είναι διαθέσιμο για εκμετάλευση 24/7

   χωρίς διακοπές.

III. Κατ'απαίτηση πρόσβαση **( On-demand self-services )** :

   Είναι ένα απο τα πολύτιμα χαρακτηριστικά του Cloud Computing καθώς ο χρήστης ή χρήστες μπορούν να έχουν άμεσα πρόσβαση σε υπολογιστικούς πόρους με μηδαμινή η καθόλου βοήθεια απο IT υποστήριξη.Μπορούν πολύ απλά να εγγραφούν σε μια cloud υπηρεσία και να ξεκινήσουν άμεσα να χρησιμοποιούν τις υπηρέσιες ,με το ανάλογο κόστος της.

IV. Ευρεία πρόσβαση στο δίκτυο ( **Broad network access )** :

Αυτό σημαίνει οτι η πρόσβαση στις cloud υπηρεσίες μπόρει να γίνει απο οποιαδήποτε συσκευή είναι συνδεδεμένη στο διαδίκτυο και χρησιμοποιεί τα κατάλληλα πρωτόκολλα όπως πχ smartphones , τάμπλετ , υπολογιστές κ.α.

V. Ελαστικότητα ( **Rapid elasticity )** :

Με τον όρο ελαστικότητα εννοούμε την ευκολία που προσφέρουν οι cloud υπηρεσίες στην αύξηση η μείωση των πόρων που εκμεταλεύεται ο κάτοχος κάθως οι ανάγκες του μεταβάλλονται.

VI. Μετρημένη υπηρεσία ( **Measured service )** :

Οι πόροι όπου κάθε κάτοχος χρησιμοποιεί παρακολουθούνται και καταγράφονται για τον καθένα ξεχωριστά στην cloud υπηρεσία . Στο τέλος του μήνα ο κάτοχος ενημερώνεται επακριβώς για τις υπηρεσίες που χρησιμοποίεισαι και καλείται να καλύψει το ανάλογο μηνιαίο κόστος , ακριβώς όπως γίνεται και με την υπηρεσία νερου η ρεύματος όπου κάθε χρήστης καλείται να πληρώσει για την εκμετάλευση των πόρων αυτών. (Michael Armbrust, 2010)


**Εικόνα 8. Διασυνδεσιμότητα Cloud**

## 5.2 Cloud και Ασφάλεια

Η ασφάλεια είναι ένα εξάρτημα οποιασδήποτε IT εγκατάστασης και για τις υπηρεσίες cloud έχουν προβλεφθεί όλες οι δικλείδες ασφαλείας , όπως ασφαλή πρόσβαση ,ασφάλεια

λογαριασμού , σωστή χρήση δικαιωμάτων χρήστη και άλλα.Προσδιορίζοντας πιθανές απειλές στο περιβάλλον cloud του κάθε χρήστη και καθιερώνοντας διαδικασίες για την αντιμετώπιση των απειλών αυτών πρέπει να είναι προτεραιότητα για οποιαδήποτε εγκατάσταση.Παίρνοντας σώστες αποφάσεις για την cloud υπηρεσία αποτελεί το πιο κρίσιμο σημείο για την επιτυχία του .Για τους προμηθευτές υπηρεσιών cloud υπάρχουν πιστοποιήσεις για να διασφαλιστεί η ανώτερη δυνατή ασφάλεια στον χρήστη.Οι υπηρεσίες cloud χρησιμοποιούν αλγόριθμους κρυπτογράφησης αλλά διαφέρουν στο επίπεδο ασφάλειας και στον τρόπο που λειτουργούν αναλόγως τον πάροχο της υπηρεσίας αυτής.

Ασφάλεια όμως δεν σημαίνει και ιδιωτικότητα. Οι υπηρεσίες cloud χρησιμοποιούν τρίτους servers για την αποθήκευση και διαχείρηση των δεδομένων απο τον χρήστη κάτι το οποίο μπορεί να θεωρήθει επικίνδυνο καθώς τα ευαίσθητα αυτά δεδομένα μπορεί να κλαπούν ή να φθαρούν.

Το cloud είναι ταυτόχρονα και υπηρεσία αλλά και λογισμικό.Οι πάροχοι είναι υποχρεωμένοι να παρέχουν updates για την σωστή λειτουργία του λογισμικού , νέα releases για το λογισμικό , backup ανά τακτά χρονικά διαστήματα ,συντήρηση των servers , εξασφάλιση της υγείας και τον έλεγχο όλων των επιμέρους συστημάτων για τυχόν βλάβες , λύσεις ανάκτησης έτσι ώστε να διασφαλιστεί η ακεραιότητα της υπηρεσίας.

Τα μέτρα ασφάλειας που έχουν προβλεφθεί μπορεί να εξασφαλίζουν κατά ένα μεγάλο ποσοστό την λειτουργικότητα στο cloud παρόλαυτα οι απειλές ασφαλείας βελτιώνονται καθημερινά και βρίσκουν καινούργιους τρόπους επίτευξης του σκοπού τους. Και το cloud όμως συμβαδίζει με τις εξελίξεις αυτές για να προσφέρει την άρτια ασφάλεια καθημερινά. (Tim Mather, 2009)

## 5.3 Cloud Hosts

Παρακάτω παρατίθενται μία λίστα παρόχων cloud υπηρεσιών:

| | |
|---|---|
| Comodo | Network Solutions |
| DropBox | Netfirms |
| iCloud | iPage |
| Mediafire | PowWeb |
| OneDrive | Green Geeks |
| Bluehost | Globat |
| Hostgatow | FatCow |
| WP Engine | CrocWeb |
| Flywheel | HostMetro |
| SiteGround | LightinngBase |
| LiquidWeb | HawkHost |
| Rackspace | Stable Host |
| Cloudways | WebHostingHub |
| A Small Orange | Webline Services |
| GoDaddy | SteadFast,net |
| Dreamhost | Linode |
| Amazon S3 | Web.com |
| InMotion Hosting | BigRock |
| 1&1 | Site5 |
| Arvixe | iPower |
| HostMonster | HostDime |
| HostPapa | DotEasy |
| IX Web Hosting | WestHost |
| JustHost | LaughingSquid |
| LunarPages | Vultr |
| MidPhase | DigitalOcean |
| NameCheap | Atlantiv.net |

| | |
|---|---|
| LeaseWeb | IdealHost |
| 50Megs | Mega |
| JaguarPC | Domain.com |
| APlus.com | Valice |
| Microsoft Azure | T1Hosting |
| Google Drive | WiredTree |
| Synthesis | |

**Πίνακας 1. Λίστα Παρόχων cloud υπηρεσιών**

## 5.4 Περιορισμοί , Πλεονεκτήματα και Μειονεκτήματα

Περιορισμοί

1) **Τεχνικά προβλήματα** –Μπορεί να υπάρξουν στιγμές συντήρησης η παροδικές διακοπές του συστήματος.
2) **Ασφάλεια στο σύννεφο** – Ο χρήστης πρέπει να βεβαιώνεται ότι ο πάροχος που έχει επιλέξει αρμόζει στις δραστηριοτητές του και υπάρχει αξιοπιστία για την ασφάλεια των δεδομένων του.
3) **Επιρρέπεια σε επιθέσεις** – Η αποθήκευση δεδομένων στο σύστημα ενδέχεται να κάνει τα δεδομένα των χρηστών ευάλωτα σε κυβερνοεπιθέσεις και διαδικτυακές απειλές.
4) **Πιθανός χρόνος διακοπής** –Η αξιοπιστία της σύνδεσης στο διαδίκτυο εκμηδενίζει και τον πιθανό χρόνο διακοπής.
5) **Έλλειψη υποστήριξης** – Δεν είναι ακόμα ικανοποιητικό για όλους τους ιστοτόπους το επίπεδο εξυπηρέτησης για εφαρμογές ιστού.

Πλεονεκτήματα

1) **Κόστος απόδοσης** - Το Cloud computing είναι πιθανότατα η πιο αποδοτική μέθοδος για τη διατήρηση δεδομένων , πληροφοριών και αναβάθμιση κατά την χρήση.Η εγκατάσταση καινούργιων desktop υπολογιστών και διαφόρων άλλων εξοπλισμών σε συνάρτηση με την πρόσθηκη λογισμικού σε κάθε ένα από αυτά κοστίζει αρκετά για μια

επιχείρηση.η Ένα παραδοσιακό desktop λογισμικό κοστίζει πολύ, με όρους χρηματοδότησης.Το σύννεφο απο την άλλη μεριά είναι αρκετά φθηνότερο και μπορεί να μειώσει σημαντικά τα έξοδα αυτά της εκάστοτε επιχείρησης.Στο σύννεφο υπάρχουν πολλές επιλογές πληρωμής που συνάδει για οποιονδήποτε το μεταχειρίζεται.

2) **Σχεδόν απεριόριστη αποθήκευση** - Η αποθήκευση πληροφοριών στο υπολογιστικό νέφος δίνει σχεδόν απεριόριστη αποθήκευση / χωρητικότητα.
3) **Δημιουργία αντιγράφων ασφαλείας και αποκατάσταση** –Όλα τα δεδομένα και πληροφορίες που αποθηκεύονται στο υπολογιστικό νέφος είναι διαθέσιμα 24ώρες το 24ώρο Οι πάροχοι υπηρεσιών cloud είναι ικανοί να χειριστούν την ανάκτηση πληροφορών. Ως αποτέλεσμα , αυτό καθιστά το σύνολο της διαδικασία backup και αποκατάστασης πολύ απλούστερη από άλλες μεθόδους φυσικής αποθήκευσης.

4) **Αυτόματη ενσωμάτωση λογισμικού** –Οποιοδήποτε καινούργιο λογισμικό παρέχεται στο σύννεφο γίνεται αυτόματα.Οι χρήστες του υπολογιστικού νέφους δεν χρειάζεται να καταβάλλουν προσπάθειες για την ενσωμάτωση των καινούργιων εφαρμογών και λογισμικού καθώς το σύννεφο φροντίζει για την λειτουργία .
5) **Εύκολη πρόσβαση στις πληροφορίες** – Με την εγγραφή στο υπολογιστικό νέφος οι πληροφορίες είναι διαθέσιμες από οπουδήποτε στον χρήστη με την μόνη προύπόθεση η σύνδεση στο διαδίκτυο.
6) **Γρήγορη ανάπτυξη** – Οι υπηρεσίες cloud είναι άμεσα διαθέσιμες μετά την εγγραφή και πλήρως λειτουργικές σε μερικά λεπτά.
7) **Παροχή νέων υπηρεσιών** – Παρόχη νέων υπηρεσιών στον χρήστη που έχουν διαδραστικό χαρακτήρα για μεγαλύτερη κατανόηση και ευκολία.

### 5.4.1 Μειονεκτήματα

1) **Ασφάλεια και Μυστικότητα:** Οι μεγαλύτερες ανησυχίες για την χρήση του υπολογιστικού συννέφου είναι η ασφάλεια και η μυστικότητα. Δεν είναι εύκολο για όλους τους χρήστες να δώσουν ευαίσθητες πληροφορίες σε τρίτους.

2) **Προσβασιμότητα:** Εάν δεν υπάρχει σύνδεση στο διαδίκτυο δεν υπάρχει και πρόσβαση στις Cloud υπηρεσίες . Επίσης εάν δεν είναι στάθερη η γραμμή του διαδικτύου από τον πάροχο δεν υπάρχει και σταθερή σύνδεση στο υπολογιστικό νέφος κάτι που μπορεί να είναι άμεσο πρόβλημα για τον χρήστη.

3) **Κόστος:** Ενώ μακροπόθεσμα η χρήση του νέφους μπορεί να θεωρήθει οικονομικότερη λύση από την εγκάτασταση καινούργιου εξοπλισμού επειδή η τεχνολογία αυτή είναι ακόμα καινούργια και πρέπει ακόμα να ερευνηθεί και να αναλυθεί την καθιστά ακριβότερη.

4) **Όριο στα αρχεία:** Μεγαλύτερος όγκος δεδομένων σημαίνει και μεγαλύτερο κόστος στο Cloud.Ανάλογα το πακέτο υπηρεσιών θα έχετε και συγκεκριμένο όγκο δεδομένων στην διαθεσή σας.Αν θέλετε να ξεπεράσετε το στάνταρ αυτό είναι απαραίτητη η πληρώμη μεγαλύτερου ποσού (Tim Mather, 2009)

## 5.5 Χρήση Ιδιώτη

Τα οφέλη για τους τελικούς χρήστες από την χρήση της διαδικτυακής δομής Cloud Computing περιλαμβάνουν την σημαντικότατη μείωση του κόστους χρήσης λογισμικού, καθώς η χρέωση πραγματοποιείται τμηματικά ανάλογα με την χρήση και όχι κατά την χρήση/εγκατάσταση όπως με το συμβατικό λογισμικό. Επίσης, την αύξηση ταχύτητας χρήσης, ευελιξίας και συμβατότητας των δεδομένων, καθώς και την χρήση και εφαρμογή της τεχνολογίας χωρίς να απαιτείται η αγορά οποιουδήποτε επιπλέον software ή hardware για την ταχύτατη εκμάθηση εφαρμογών από τους τελικούς χρήστες.Την απεριόριστη χωρητικότητα (on-line) αποθήκευσης δεδομένων χωρίς την ανάγκη προμήθειας συμβατικών μέσων αποθήκευσης όπως οι εξωτερικοί σκληροί δίσκοι καθώς και την ταχύτατη πρόσβαση σε πληροφορίες (on-line) από οποιοδήποτε μέρος του κόσμου με υψηλή ασφάλεια δεδομένων και το ταχύτατο real-time back-up δεδομένων που πραγματοποιείται αυτόματα εξοικονομώντας χρόνο για τους τελικούς χρήστες. Είναι ευνόητο λοιπόν ότι ένας μεγάλος πάροχος υπηρεσιών cloud computing μπορεί να προσφέρει καλύτερες, πιο εξελιγμένες και πιο φθηνές υπηρεσίες ασφάλειας στους χρήστες σε σύγκριση με την αυτόνομη δημιουργία cloud λύσεων από τον ίδιο.

Μπορεί επίσης να προσφέρει μηχανισμούς κωδικοποίησης με σκοπό να αυξήσει την αποδοτικότητα των μέτρων που λαμβάνει, ώστε να αποφεύγει απειλές, ενώ αντίθετα με το αυτόνομο cloud δίκτυο του χρήστη, αυτό είναι δύσκολο να επιτευχθεί. Σχετικά με τα πλεονεκτήματα προς την πράσινη οικονομία εκτιμάται ότι αν σήμερα η εν λόγω τεχνολογία χρησιμοποιούνταν πλήρως από όλους τους χρήστες πληροφορικής οι ατμοσφαιρικοί ρύποι στον πλανήτη θα μπορούσαν να μειωθούν έως και 5% συνολικά ή αλλιώς 2,5 δισεκατομμύρια τόνους διοξείδιο του άνθρακα (CO2). Σημειώνεται ότι η επιβάρυνση του περιβάλλοντος από την χρήση συστημάτων πληροφορικής ενδέχεται να διπλασιαστεί την επόμενη 10ετία, άρα η μείωση των ατμοσφαιρικών ρύπων παγκόσμια θα μπορούσε να μειωθεί σε βάθος χρόνου έως και 5 δισεκατομμύρια τόνους διοξείδιο του άνθρακα (CO2) ετησίως χάρη στην χρήση της τεχνολογίας Cloud Computing. (Clarke, 2010)

# 6 Αρχικτεκτονική και Ασφάλεια IoT

## 6.1 Αρχιτεκτονική προσανατολισμένη στην εξυπηρέτηση (SOA)

Μια κρίσιμη απαίτηση ενός IoT συστήματος είναι ότι τα πράγματα στο δίκτυο πρέπει να είναι διασυνδεδεμένα. Η αρχιτεκτονική συστήματος IoT πρέπει να εγγυάται τη λειτουργία του IoT, το οποίο γεφυρώνει το χάσμα μεταξύ του φυσικού και του εικονικού κόσμου. Σχεδιασμός του IoT Η αρχιτεκτονική περιλαμβάνει πολλούς παράγοντες, όπως η δικτύωση, η επικοινωνία, τα επιχειρηματικά μοντέλα και διαδικασίες και η ασφάλεια. Λόγω του γεγονότος ότι τα πράγματα μπορεί να κινούνται και να πρέπει να αλληλεπιδρούν μεταξύ τους σε λειτουργία σε πραγματικό χρόνο, η αρχιτεκτονική IoT θα πρέπει να προσαρμόζεται για να κάνει τις συσκευές να αλληλεπιδρούν με άλλα πράγματα δυναμικά και υποστηρίζουν την σαφή επικοινωνία των γεγονότων.

Το SoA αντιμετωπίζει ένα πολύπλοκο σύστημα ως ένα σύνολο καθορισμένων αντικειμένων ή υποσυστημάτων. Τα στοιχεία λογισμικού και υλικού σε ένα IoT μπορεί να επαναχρησιμοποίηθούν αποτελεσματικά. Λόγω αυτών των πλεονεκτημάτων, το SoA έχει εφαρμοστεί ευρέως ως κύρια αρχιτε κτονική.

- Το επίπεδο ανίχνευσης είναι ενσωματωμένο με όλα τα διαθέσιμα αντικείμενα (πράγματα) για την αίσθηση της κατάστασής τους.
- Το επίπεδο δικτύου είναι η υποδομή για την υποστήριξη των ασύρματων ή ενσύρματων συνδέσεων μεταξύ των πραγμάτων.
- Το επίπεδο υπηρεσιών είναι η δημιουργία και διαχείριση υπηρεσιών που απαιτούνται από χρήστες ή εφαρμογές.
- Το επίπεδο διεπαφής αποτελείται από τις μεθόδους αλληλεπίδρασης με χρήστες ή εφαρμογές.

### 6.1.1 Στρώμα Αίσθησης (Sensing layer )

Στο επίπεδο ανίχνευσης, τα έξυπνα συστήματα σε ετικέτες ή αισθητήρες μπορούν να αντιλαμβάνονται το περιβάλλον και ανταλλάσσουν δεδομένα μεταξύ συσκευών. Τα πράγματα

μπορούν να αναγνωριστούν και το γύρω περιβάλλον να παρακολουθηθεί για διάφορους σκοπούς και εφαρμογές. Κάθε αντικείμενο στο IoT έχει μια ψηφιακή ταυτότητα και μπορεί εύκολα να εντοπιστεί στον ψηφιακό τομέα. Η τεχνική της εκχώρησης μοναδικής ταυτότητας σε ένα αντικείμενο ονομάζεται καθολικό μοναδικό αναγνωριστικό (UUID). Τα αναγνωριστικά ενδέχεται να περιέχουν ονόματα και διευθύνσεις. Ένα UUID είναι ένας αριθμός 128-bit που χρησιμοποιείται για να προσδιορίζουν μοναδικά κάποιο αντικείμενο ή οντότητα στο διαδίκτυο.

Κατά τον προσδιορισμό του στρώματος ανίχνευσης ενός IoT, θα πρέπει να ληφθούν υπόψη οι ακόλουθες πτυχές:

- Κόστος, μέγεθος, πόρος και κατανάλωση ενέργειας: Τα πράγματα ενδέχεται να είναι εξοπλισμένα με συσκευές ανίχνευσης όπως π.χ ετικέτες RFID, αισθητήρα κόμβου
- Ανάπτυξη: Τα αντικείμενα ανίχνευσης (ετικέτες RFID, αισθητήρες κ.λπ.) μπορούν να αναπτυχθούν μία φορά, ή σταδιακά, ή ανάλογα με τις απαιτήσεις.
- Επικοινωνία. Οι αισθητήρες πρέπει να είναι εν ενεργεία και σε λειτουργία για να κάνουν τα πράγματα προσβάσιμα και ανακτήσιμα.
- Δίκτυο. Τα πράγματα είναι οργανωμένα ως δίκτυα multi-hop, mesh ή ad hoc.

### 6.1.2 Στρώμα Δικτύου (Network layer)

Το επίπεδο δικτύου στο IoT, συνδέει όλα τα πράγματα μεταξύ τους και τους επιτρέπει να γνωρίζουν το περιβάλλον γύρω τους. Μέσω του επιπέδου δικτύου, τα πράγματα μπορούν να μοιράζονται δεδομένα με τα συνδεδεμένα πράγματα, κάτι που είναι ζωτικής σημασίας για την διαχείριση και επεξεργασία συμβάντων στο IoT δίκτυο. Το δίκτυο θα πρέπει επίσης να ανακαλύπτει και να χαρτογραφεί αυτόματα όλα τα πράγματα και διαχειρίζεται αυτόματα την επικοινωνία και την λειτουργία.Αυτό επιτρέπει στις συσκευές να εκτελούν εργασίες συλλογικά.
Στο επίπεδο δικτύωσης, τα παρακάτω προβλήματα θα πρέπει να θετηθούν:

- Τεχνολογίες διαχείρισης δικτύου, συμπεριλαμβανομένης της διαχείρισης σταθερών, ασύρματων και κινητών δικτύων

- Απαιτήσεις QoS
- Τεχνολογίες αναζήτησης δεδομένων, επεξεργασίας δεδομένων
- Ασφάλεια και ιδιωτικότητα

### 6.1.3 Στρώμα υπηρεσίας (Service layer)

Το επίπεδο υπηρεσίας θέτει σε λειτουργία τις υπηρεσίες και τις εφαρμογές στο IoT. Είναι μια οικονομικά αποδοτική πλατφόρμα όπου το λογισμικό και το υλικό μπορούν να επαναχρησιμοποιηθούν. Οι υπηρεσίες στο επίπεδο υπηρεσιών εκτελούνται απευθείας στο δίκτυο για να εντοπίσουν αποτελεσματικά νέες υπηρεσίες για μία εφαρμογή και δυναμική ανάκτηση δεδομένων σχετικά με τις υπηρεσίες.. Ένα καθολικά αποδεκτό επίπεδο υπηρεσιών είναι σημαντικό για την λειτουργία του IoT. Μια πρακτική υπηρεσία στρώματος αποτελείται από ένα σύνολο εφαρμογών , διεπαφές προγραμματισμού εφαρμογών (API) και πρωτόκολλα που υποστηρίζουν απαραίτητες εφαρμογές και υπηρεσίες.

Όλες οι δραστηριότητες στις υπηρεσίες, όπως η ανταλλαγή και η αποθήκευση πληροφοριών, η διαχείριση δεδομένων, οι μηχανές αναζήτησης και η επικοινωνία, πραγματοποιούνται στο επίπεδο υπηρεσιών.

Οι εργασίες που εκτελούνται από το επίπεδο υπηρεσιών είναι:

- Ανακάλυψη υπηρεσίας: Εύρεση αντικειμένων που μπορούν να παρέχουν την απαιτούμενη υπηρεσία και πληροφορίες.
- Σύνθεση υπηρεσίας: Επιτρέπει την αλληλεπίδραση μεταξύ συνδεδεμένων πραγμάτων και περιγράφει τις σχέσεις μεταξύ των πραγμάτων για την ενεργοποίηση της επιθυμητής υπηρεσίας.
- Service API: Παρέχουν τη διεπαφή μεταξύ των υπηρεσιών που απαιτούνται από τους χρήστες.

### 6.1.4 Στρώμα διεπαφής (Interface layer)

Στο IoT, ένας μεγάλος αριθμός συσκευών είναι συνδεδεμένος. Αυτές οι συσκευές μπορεί να ανήκουν σε διαφορετικούς ανθρώπους και να μην περιέχουν τα ίδια πρότυπα. Το ζήτημα της συμβατότητας μεταξύ των πραγμάτων πρέπει να λυθεί για την αλληλεπίδραση μεταξύ τους. Η συμβατότητα περιλαμβάνει την ανταλλαγή πληροφοριών, την επικοινωνία και την επεξεργασία γεγονότωνΕίναι αναγκαία η εύρεση ενός αποτελεσματικό μηχανισμού διεπαφής για την απλοποίηση της διαχείρισης και της διασύνδεσης των πραγμάτων (S. Krčo, 2014)[23] (Naveen, 2016).

### 6.1.5 ARP πρωτόκολλο

Το πρωτόκολλο ARP παίζει βασικό ρόλο μεταξύ των πρωτοκόλλων επιπέδου διαδικτύου που σχετίζονται με το TCP/IP, αφού ενεργοποιεί τη φυσική διεύθυνση μιας κάρτας διασύνδεσης δικτύου που αντιστοιχεί σε μια IP διεύθυνση που είναι γνωστή. Αυτός είναι ο λόγος για τον οποίο ονομάζεται Πρωτόκολλο Επίλυσης Διεύθυνσης. Κάθε μηχάνημα που είναι συνδεδεμένο στο δίκτυο έχει αριθμό αναγνώρισης 48 bit. Αυτό είναι ένα μοναδικός αριθμός που καθορίζεται στο εργοστάσιο όταν κατασκευάζεται η κάρτα.

Ο τρόπος που λειτουργεί το πρωτόκολλο ARP είναι εξαιρετικά απλός. Κάθε φορά που πρέπει να γίνει γνωστή η διεύθυνση MAC που αντιστοιχεί σε κάποια συγκεκριμένη διεύθυνση IP , λαμβάνει χώρα εκπομπή σε όλους τους υπολογιστές (broadcasting) ενός πακέτου δεδομένων που περιέχει τη διεύθυνση IP που θέλουμε να μεταφράσουμε . Ο κάθε ένας από τους υπολογιστές του δικτύου , παραλαμβάνει αυτό το πακέτο , συγκρίνει τη διεύθυνση IP που περιέχει , με τη δική του διεύθυνση IP και εάν οι δύο διευθύνσεις είναι οι ίδιες , αποστέλλει μια απάντηση στον υπολογιστή που υπέβαλλε το ερώτημα . Η απάντηση αυτή περιέχει τη MAC διεύθυνση του υπολογιστή αποστολέα η οποία ταυτοποιείται , απομονώνεται και αποθηκεύεται σε μια ειδική μνήμη ARP cache , έτσι ώστε να μπορεί να χρησιμοποιηθεί στο μέλλον . Η μνήμη αυτή ανανεώνεται σε τακτά χρονικά διαστήματα , διότι τα περιεχόμενα της μπορούν σε κάποια χρονική στιγμή να μεταβληθούν , όπως συμβαίνει για παράδειγμα σε περιπτώσεις κατά τις οποίες αντικαθιστούμε την κάρτα δικτύου του υπολογιστή με κάποια άλλη η οποία έχει τη δική της MAC address . Η εντολή arp καλείται στις πιο συνηθισμένες

περιπτώσεις με την παράμετρο –a η οποία εμφανίζει τα περιεχόμενα του πίνακα arp (arp table) ο οποίος περιέχει την παραπάνω αντιστοιχία διευθύνσεων. (Al Sukkar, 2016)

### 6.1.6 RIP Πρωτόκολλο

Το RIP σημαίνει Routing Information Protocol. Το πρωτόκολλο RIP είναι ένα πρωτόκολλο δρομολόγησης διανυσμάτων απόστασης που χρησιμοποιείται για να χρησιμοποιήσει το πλήθος hop ως μετρική δρομολόγησης. Εφαρμόζοντας ένα όριο στον αριθμό των βημάτων που επιτρέπονται στη διαδρομή από την πηγή στον προορισμό, αποτρέπει τους βρόχους δρομολόγησης. Ένας βρόχος δρομολόγησης είναι ένα σοβαρό πρόβλημα δικτύου που συμβαίνει όταν ένα πακέτο δεδομένων δρομολογείται συνεχώς μέσω των ίδιων δρομολογητών ξανά και ξανά. Ο μεγαλύτερος αριθμός αναπηδήσεων που επιτρέπεται για το RIP είναι 15 που περιορίζει το μέγεθος του δικτύου που μπορεί να υποστηρίξει το RIP. Χρησιμοποιεί το UDP (User Datagram Protocol) ως πρωτόκολλο μεταφοράς και του εκχωρείται ο αριθμός αντίστροφης θύρας 520. Για την αποφυγή εσφαλμένων πληροφοριών δρομολόγησης, εφαρμόζει μηχανισμό δηλητηρίασης split-horizon, hold down και δρομολόγησης (Husein, 2018)

### 6.1.7 OSPF Πρωτόκολλο

Το OSPF είναι ένα πρωτόκολλο δρομολόγησης. Δύο δρομολογητές που μιλούν με OSPF μεταξύ τους ανταλλάσσουν πληροφορίες σχετικά με τις διαδρομές που γνωρίζουν και το κόστος για να φτάσουν εκεί.Όταν πολλοί δρομολογητές OSPF αποτελούν μέρος του ίδιου δικτύου, οι πληροφορίες για όλες τις διαδρομές σε ένα δίκτυο μαθαίνονται από όλους τους δρομολογητές OSPF εντός αυτού του δικτύου — που τεχνικά ονομάζεται περιοχή. Οι δρομολογητές συνδέονται μεταξύ τους με τη βοήθεια συνδέσμων, αυτοί οι δρομολογητές ονομάζονται κόμβοι. Κάθε κόμβος συνδέεται με άλλους κόμβους σαν μια ιεραρχία. Δεν υπάρχει όριο στις συνδέσεις κόμβων.Η δουλειά κάθε κόμβου είναι να στέλνει πληροφορίες τοπολογίας στον άλλο κόμβο αυτή η διαδικασία συνεχίζεται αντίστροφα σημαίνει ότι εάν ο ένας στείλει τις πληροφορίες πλήρως τότε ο άλλος θα στείλει πληροφορίες.Κάθε δρομολογητής OSPF μεταβιβάζει πληροφορίες σχετικά με τις διαδρομές και το κόστος για το οποίο έχουν ακούσει σε όλους τους

παρακείμενους δρομολογητές OSPF, που ονομάζονται γείτονες.Οι δρομολογητές OSPF βασίζονται στο κόστος για τον υπολογισμό της συντομότερης διαδρομής μέσω του δικτύου μεταξύ τους και ενός απομακρυσμένου δρομολογητή ή προορισμού δικτύου. Ο υπολογισμός της συντομότερης διαδρομής γίνεται χρησιμοποιώντας τον αλγόριθμο του Djikstra. Αυτός ο αλγόριθμος δεν είναι μοναδικός για το OSPF.(Tadimety, 2015)

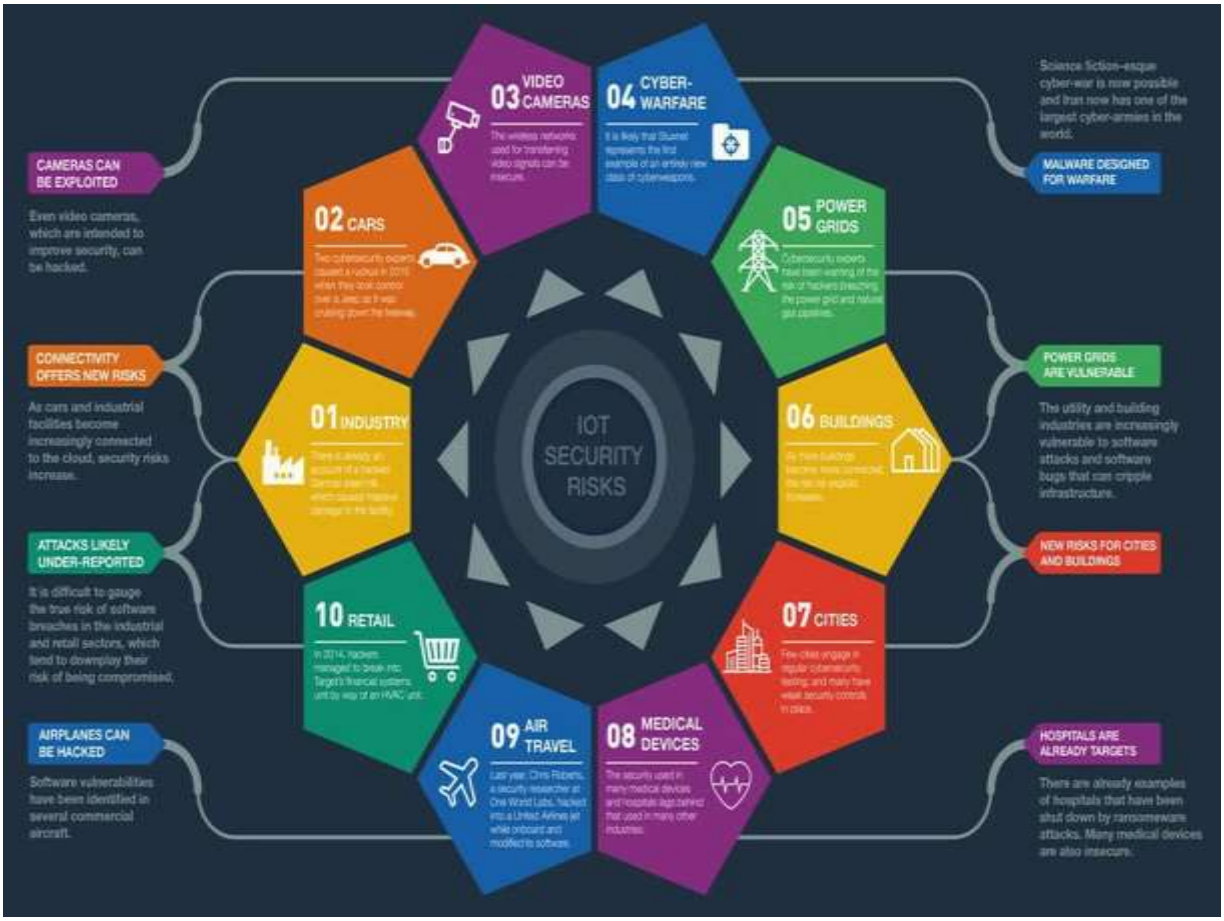
Τι είναι η ασφάλεια IoT

Το Διαδίκτυο των Πραγμάτων μπορεί να οδηγήσει τις επιχειρήσεις και τους ιδιώτες σε μεγάλες οικονομικές δυνατότητες και καινοτομιές που εκτείνονται σε όλα τα πεδία εφαρμογής απο την παιδική φροντίδα και την φροντίδα ηλικιωμένων μέχρι την εκπαίδευση και τις μεταφορές .Οι διαφορετικές λύσεις του IoT –η απομακρυσμένη παρακολούθηση , η προγνωστική συντήρηση και η διασυνδεσιμότητα των συσκευών- μπορούν να επιτύχουν μείωση των λειτουργικών εξόδων , μείωση των εξόδων γενικότερα και να αυξήσουν την ταχύτητα απο την παραγωγή στην κατανάλωση.

Με τους ειδικούς και τους αναλυτές της τεχνολογίας IoT να προβλέπουν ακόμα πιο εκτεταμένη χρήση IoT συσκευών και εφαρμογών στο μέλλον αλλά και άλλων εφαρμογών που αγγίζουν το φάσμα του IoT , οι επιχειρήσεις και οι ιδιώτες  είναι πρόθυμοι να εκμεταλλευτούν όλα τα πλεονέκτήματα του.

Καθώς η παραδοσιακή κυβερνοασφάλεια περιστρέφεται γύρω απο το software και πώς αυτό εφαρμόζεται , η IoT κυβερνοασφάλεια προσθέτει ένα ακόμα στρώμα πολυπλοκότητας καθώς ο κυβερνοχώρος και ο φυσικός κόσμος συγκλίνουν.Ένα μεγάλο εύρος λειτουργικών σεναρίων και σεναρίων συντήρησης στο φάσμα του IoT βασίζεται στην από άκρη-σε-άκρη (end-to-end) συνδεσιμότητα των συσκευών για να δώσει την δυνατότητα στους χρήστες και στις υπηρεσίες να αλληλεπιδράσουν,να συνδεθούν,να αντιμετωπίσουν προβλήματα ,.να αποστείλουν και να παραλάβουν δεδομένα απο τις συσκευές.Είναι αντιληπτό οτι το να ληφθούν προφυλάξεις ασφαλείας είναι αναγκαία  ,καθώς η λειτουργική τεχνολογία είναι πολύ σημαντική και πολύτιμη

για να τεθεί σε ρίσκο από συμβάντα ρήξης ,καταστροφής και άλλων απειλών. (R. Mahmoud, 2015)




**Εικόνα 9. Απειλές στην ασφάλεια του IoT**

## 6.2 Βασικά στοιχεία της ασφάλειας IoT

Η ασφάλεια και ιδιωτικότητα η στο IoT είναι βασικό χαρακτηριστικό για την ομάλη λειτουργία των συστημάτων που την αποτελούν.

- ✓ Διασύνδεση κυβερνοχώρου με το φυσικό κόσμο (Cyber-Physical Systems (CPS))
- ✓ Συστήματα μεταφοράς και κυβενοχώρου ( Cyber Transportation Systems (CTS))
- ✓ Επικοινωνία μηχανής-με-μηχανή (Machine-to-Machine(M2M) Interaction))

Στο IoT υπάρχουν 4 επίπεδα ασφαλείας.Κάθε επίπεδο είναι σε θέση να παρέχει διαφορετικά μέτρα ασφαλείας όταν αυτό κρίνεται αναγκαίο όπως έλεγχος πρόσβασης .έλεγχος ταυτότητας συσκευών , εμπιστευτικότητα στην μετάδοση , διαθεσιμότητα ,ακεραιότητα δεδομένων και αντιμετώπιση προβλημάτων απο κακόβουλο λογισμικό και επιθέσεις.

**1. Επίπεδο ανίχνευσης**

Είναι το IoT επίπεδο το οποίο βρίσκεται στην χαμηλότερη βαθμίδα της ιεράρχισης παρόμοιο με το φυσικό επίπεδο του μοντέλου OSI.Κύρια λειτουργία του είναι είναι να αναγνωρίζει τις φυσικές ιδιότητες των συσκευών IoT.Βασικά συγκεντρώνει πληροφορίες απο το περιβάλλον γύρω του διαμέσο αισθητήρων και τις επεξεργάζεται.Οι πληροφορίες αυτές συμπεραλαμβάνουν τις ιδιότητες του αντικειμένου ,της συσκευής , την κατάσταση του περιβάλλοντος κ.α.'Επειτα μεταφέρονται στο επόμενο επίπεδο.

**2. Επίπεδο δικτύου**

Αυτό το επίπεδο του IoT είναι υπεύθυνο για την συνδεσιμότητα και στην ανταλλαγή μηνυμάτων μεταξυ των πραγμάτων και των υπηρεσιών νέφους.Η επικοινωνία στο διαδίκτυο είναι συνδυασμός ιδιωτικών και δημόσιων δικτύων επομένως η διασφάλιση της σωστής επικοινωνίας είναι προφανώς σημαντική.Αυτό το επίπεδο είναι επίσης υπεύθυνο για την παροχή των αξιόπιστων δεδομένων του προηγούμενου επιπέδου .Ακριβέστερα τα δεδομένα που λήφθηκαν απο το προηγούμενο επίπεδο , επεξεργάζονται.

**3. Επίπεδο υποστήριξης**

Το επίπεδο αυτό λειτουργεί ως μεσάζοντας του άνω και κάτω επιπέδου. Το επίπεδο υποστήριξης του πλαισίου αντιπροσωπεύει το σύστημα διαχείρισης του διαδικτύου και είναι υπεύθυνο για την διαχείριση συσκευών και χρηστών, την εφαρμογή πολιτικών και κανόνων και συντονισμό της αυτοματοποίησης σε όλες τις συσκευές. Ο έλεγχος πρόσβασης για τη διαχείριση της ταυτότητας των χρηστών και των συσκευών και οι ενέργειες στις οποίες έχουν εξουσιοδοτηθεί να λαμβάνουν είναι κρίσιμες σε αυτό το επίπεδο. Είναι επίσης σημαντικό να διατηρηθεί ένα ίχνος ελέγχου των αλλαγών που γίνονται από κάθε χρήστη και συσκευή, έτσι ώστε να είναι αδύνατο να αντικρούονται οι ενέργειες που λαμβάνονται στο σύστημα.

**4. Επίπεδο εφαρμογής**

Σε αυτό το επίπεδο πραγματοποιείται η εξατομικευμένη παροχή της εφαρμογής, οποιαδήποτε και αν είναι αυτή , και οποιαδήποτε εφαρμογή επιθυμεί ο χρήστης . Αυτό το επίπεδο εφαρμόζεται μέσω μιας ειδικής εφαρμογής στο τέλος της συσκευής. Όπως για έναν υπολογιστή, το επίπεδο εφαρμογής εφαρμόζεται από το πρόγραμμα περιήγησης. Είναι το πρόγραμμα περιήγησης που εφαρμόζει πρωτόκολλα επιπέδου εφαρμογής όπως HTTP, HTTPS, SMTP και FTP. Με τον ίδιο τρόπο, υπάρχουν πρωτόκολλα επιπέδου εφαρμογής που καθορίζονται και στο πλαίσιο του IOT όπως MQTP , SMQTT,HTTP/2 και άλλα.

## 6.3 Θέματα ασφαλείας IoT

Το σημαντικότερο πρόβλημα ασφαλείας στο διαδίκτυο των πραγμάτων, είναι ότι παρέχει το κατάλληλο έδαφος για κακόβουλες επιθέσεις. Το διαδίκτυο των πραγμάτων είναι ένα οικοσύστημα που αποτελείται από πολλές συσκευές που επικοινωνούν μεταξύ τους αδιάκοπα ,ενημερώνουν η μία την άλλη για την κατάσταση λειτουργίας τους και ανταλλάσουν πληροφορίες .Το μειονέκτημα είναι πως δεν ελέγχονται συνεχώς για την ασφάλεια τους καθώς σε ένα δίκτυο χιλιάδων έξυπνων συσκευών αυτό είναι αδύνατο απο τον ανθρώπινο παράγοντα.Ετσι δημιουργούνται κενά ασφαλειάς στο σύστημα , με αποτέλεσμα οι κίνδυνοι απο κακόβουλα λογισμικά και χάκερ να είναι πολλοί και επικινδυνοι για ασφάλεια των πληροφοριώνους να ελέγχονται.

Τα πιο κοινά και εύκολα διευθυνσιοδοτούμενα θέματα ασφαλείας περιέχουν :

- **Προβλήματα ιδιωτικότητας** : 8 στις 10 συσκευές που ελέγχονται , μαζί με τις εφαρμογές τους και τις υπηρεσίες νέφους τους πρόβαλλουν ανησυχίες για την προστασία της ιδιωτικής ζωής όσον αφορά την συλλογή δεδομένων καταναλωτή όπως ονόμα , διεύθυνση email , διεύθυνση κατοικίας ,ημερομηνίια γέννησης , διαπιστευτήρια τραπεζικής κάρτας και πληροφορίες υγείονομικής κατάστασης.Επιπρόσθετα το 90% των ελεγμένων έξυπνων συσκευών συγκέντρωνεε τουλάχιστον ένα ποσοστό προσωπικών πληροφοριών μέσω των της ίδιας της συσκευής , των εφαρμογών του και το νέφος.

- **<u>Ελλειπής εξουσιοδότηση</u>** : 80% των ελεγμένων συσκευών ,συμπεριλαμβανομένου το νέφος των συσκευών και τις ίδιες τις εφαρμογές τους απέτυχε να απαιτήσει κωδικούς επαρκής πολυπλοκότητας για μεγαλύτερη ασφάλεια , με τις συσκευές να επιτρέπουν απλούς κωδικούς όπως ΄΄1234΄΄.
- **<u>Ελλειπής κρυπτογράφηση κατά την μεταφόρα δεδομένων</u>** : 70% των συσκευών που αναλύθηκαν δεν είχαν επαρκή κρυπτογράφηση κατα την ανταλλάγη δεδομένων στο διαδίκτυο αλλά και στο τοπικό δίκτυο , καθώς επίσης και οι μισές απο αυτές εκτελούσαν μη κρυπτογραφημένη επικοινωνία με το νέφος , το διαδίκτυο και το τοπικό δίκτυο.Η κρυπτογραφημένη μεταφορά πληροφορίας είναι ζωτικής σημασίας απο την στιγμή που μεταφέρονται και συλλεγονται ευαίσθητα δεδομένα .
- **<u>Μη ασφαλή διεπαφή ιστού</u>** : 6 στις 10 συσκευές που εκτιμήθηκαν έφεραν στην επιφάνεια ανησυχίες ασφάλειας με τις διεπαφές των χρηστών στο διαδίκτυο όπως επίμονες επιθέσης XSS , κακή διαχείρηση συνεδρίας , αδύναμοι κωδικοί και κωδικοί που αποστέλλονται σε απλό κείμενο , μη κρυπτογραφημένο . 70% των συσκευών ΄΄επιτρέπει΄΄ έναν πιθανό εισβολέα να ανακαλύψει δεδομένα χρηστών καθώς και να εισβάλλει σε λογαριασμούς με την δυνατότητα επαναφοράς κωδικού.
- **<u>Ανεπαρκής προστασία λογισμικού</u>** : 60% των συσκευών που ελέγχθηκαν δεν χρησιμοποίησαν κρυπτογράφηση για την λήψη της αναβάθμισης λογισμικού .Κατά την αναβάθμιση είναι εύκολη η παρεμπόδιση της λήψης καθώς και η απόσπαση πληροφοριών και δεδομένων κατά την εγκατάσταση της. (R. Mahmoud, Internet of things (IoT) security: Current status, challenges and prospective measures, 2015)

*<u>Υπάρχουν βέβαια πολλά ακόμα προβλήματα στην ασφάλεια IoT .Κάποια άλλα απο αυτά είναι :</u>*

**<u>Απρόβλεπτη συμπεριφορά</u>** :

Ο τεράστιος όγκος των συσκευών που έχουν αναπτυχθεί και η μεγάλη λίστα των τεχνολογιών ενεργοποίησης σημαίνει ότι η συμπεριφορά τους στο πεδίο μπορεί να είναι απρόβλεπτη. Ένα συγκεκριμένο σύστημα μπορεί να είναι καλά σχεδιασμένο και εντός του ελέγχου της διοίκησης, αλλά δεν υπάρχουν εγγυήσεις για το πώς θα αλληλεπιδρά με άλλους.

**<u>Ομοιότητα συσκευών</u> :**

Οι συσκευές IoT είναι αρκετά ομοιόμορφες. Χρησιμοποιούν την ίδια τεχνολογία και τα ίδια στοιχεία σύνδεσης. Εάν ένα σύστημα ή συσκευή πάσχει από ευπάθεια, πολλά άλλα έχουν το ίδιο πρόβλημα.

**Μεγάλη διάρκεια ζωής και υποστήριξη που έχει λήξει** :

Ένα από τα πλεονεκτήματα των συσκευών IoT είναι η μακροζωία, ωστόσο, ότι η μεγάλη διάρκεια ζωής σημαίνει επίσης ότι μπορεί να επιβιώσει από την υποστήριξη των συσκευών τους. Συγκρίνετε αυτό με τα παραδοσιακά συστήματα που έχουν συνήθως υποστήριξη και αναβαθμίσεις πολύ καιρό αφού πολλοί έχουν σταματήσει να τα χρησιμοποιούν. Οι συσκευές που δεν παράγονται πλέον και το εγκαταλελειμμένο λογισμικό δεν διαθέτουν την ίδια ασφάλεια με άλλα συστηματα λόγω της εξέλιξης της τεχνολογίας με την πάροδο του χρόνου.

**Αδύναμη ή καθόλου διαφάνεια** :

Πολλές συσκευές IoT δεν παρέχουν διαφάνεια ως προς τη λειτουργικότητά τους.Οι χρήστες δεν έχουν κανέναν έλεγχο επί ανεπιθύμητων λειτουργιών ή συλλογής δεδομένων. Επιπλέον, όταν ένας κατασκευαστής ενημερώνει τη συσκευή, μπορεί να φέρει περισσότερες ανεπιθύμητες λειτουργίες.

**Χωρίς ειδοποιήσεις** :

Ένας άλλος στόχος του IoT είναι να παρέχει την λειτουργικότητά του χωρίς να είναι ενοχλητικός.Εδώ είναι σημαντική η ευαισθητοποίηση των χρηστών Αυτό εισάγει το πρόβλημα της ευαισθητοποίησης των χρηστών. Οι χρήστες δεν παρακολουθούν τις συσκευές ή δεν γνωρίζουν πότε κάτι πάει στραβά. Οι παραβιάσεις ασφαλείας μπορούν να συνεχιστούν για μεγάλα χρονικά διαστήματα χωρίς να ανακαληφθούν.

Προκειμένου να προστατευθούν οι χρήστες από τους κινδύνους ασφαλείας που έρχονται μαζί με την άνοδο του IoT, είναι επιτακτική ανάγκη για τους οργανισμούς να εφαρμόσουν μια προσέγγιση από άκρο σε άκρο για τον εντοπισμό τρωτών σημείων λογισμικού πριν από την εκμετάλλευσή τους. Υπάρχουν διάφορες λύσεις που επιτρέπουν στους οργανισμούς να ελέγχουν την ασφάλεια του λογισμικού γρήγορα, με ακρίβεια, οικονομικά προσιτά και χωρίς κανένα

λογισμικό για εγκατάσταση ή διαχείριση - εξαλείφοντας προληπτικά τον άμεσο κίνδυνο σε εφαρμογές παλαιού τύπου και τον συστημικό κίνδυνο κατά την ανάπτυξη εφαρμογών. (N. Neshenko, 2019).

## 6 .4 Ασφάλεια Συσκευών

1. Παρόλο που οι έξυπνες συσκευές φέρνουν επιπρόσθετες ανησυχίες στο δίκτυο , η ασφάλεια των έξυπνων συσκευών πρέπει να παρέχεται σε όλη της διάρκεια ζωής της συσκευής.Είναι δυνατή η ανάπτυξη του IoT στο περιβάλλον του σπιτιού με ασφάλεια για να ελαχιστοποιηθεί η πιθανότητα επιθέσεων που σχετίζονται με το IoT.Παρακάτω παρουσιάζονται οι πρακτικές για την εισαγωγή των συσκευών IoT στο δίκτυο με μεγαλύτερη ασφάλεια. Εξέταση εάν απαιτείται η χρήση της οποιαδήποτες συσκευής σε συγκεκριμένη εξκατάσταση και πού είναι δικαιολογημένη η χρήση της και περαιτέρω εάν είναι δυνατό να διαχωριστεί από άλλες σημαντικές συσκευές του δικτύου.
2. Αλλαγή του προεπιλεγμένου κωδικού πρόσβασης και του ονόματος χρήστη και αξιοποιήση διαφορετικών κωδίκων για διάφορους τύπους συσκευών.Μετά την αλλαγή σημαντικό είναι να βεβαιωθεί ο χρήστης ότι ο κωδικός έχει αλλάξει και πως ο προεπιλεγμένος κωδικός του κατασκευαστεί δεν λειτουργεί πλέον.Εάν από κατασκευαστικής άποψης οι κωδικοί και τα ονόματα δεν αλλάζουν καλό θα ταν να επιλεχθεί ένα άλλο προιόν.
3. Απενεργοποίηση των περιττών υπηρεσιών και θυρών σε συσκευές IoT. Ορισμένες συσκευές IoT επιτρέπουν απομακρυσμένη διαχείριση τόσο μέσω διεπαφής ιστού όσο και μέσω εργαλείων γραμμής εντολών όπως το Telnet ή το SSH. Εάν είναι δυνατό αυτές οι υπηρεσίες να απενεργοποιηθούν. Παράλληλα εάν μια συσκευή χρειάζεται μόνο εσωτερική πρόσβαση μέσα στο κτίριο, να αποκλειστεί πλήρως απο το τείχος προστασίας.
4. Τμηματοποίηση των συσκευών IoT απο το υπόλοιπο δίκτυο.Στο σπίτι αυτό μπορεί να έχει τη μορφή ενός συνόλου δεσμευμένων διευθύνσεων IP ή NAT που μπορεί να περιοριστεί και να παρακολουθηθεί απο την κονσόλα διαχείρησης του ευρυζωνικού δρομολογήτη.

5. Τακτικός έλεγχος της λίστας εγγραφών IoT όταν γίνεται ενημέρωση των συσκευών και αφαίρεση προηγούμενων συσκευών που δεν χρειάζονται πλέον.
6. Ενεργοποίηση ισχυρής κρυπτογράφησης (AES-128 ή AES-256 εάν υπάρχει). Εάν μια συσκευή δεν υποστηρίζει κρυπτογράφηση, εξετάστε το ενδεχόμενο αγοράς διαφορετικής συσκευής ή διαχωρισμού τη συσκευή από το υπόλοιπο δίκτυό σας. Για άλλη μια φορά, η αξία της συσκευής δεν είναι το ερώτημα, είναι η αξία όλων των άλλων στοιχείων στο ίδιο δίκτυο για την αποφυγή παραβίασης συσκευής.
7. Τακτική ενημέρωση των συσκευών.Τουλάχιστον μια φορά τον χρόνο.Έλεγχος του ιστιότοπου του κατασκευαστή για την όσο πιο γρήγορη δυνατή ενημέρωση των συσκευών και έλεγχος της διαθεσιμότητας και παροχής ενημερώσεν για τα συγκεκριμένα στοιχεία που έχουν εγκατασταθεί στο δίκτυο.
8. Απενεργοποίηση των συσκευών όταν δεν χρησιμοποιούνται.Αναζήτηση σχετικά με το ποιές συσκευές είναι αναγκαίες κατα τις πρωινές ώρες καθώς και βραδυνές και απενεργοποίση με βάση τις ανάγκες του χρήστη πχ δρομολογητές Wi-Fi ,DVR ,κονσόλες και άλλες συσκευές.
9. Εκπαίδευση χρηστών.Η τακτική εκπαίδευση ασφαλείας θα πρέπει να περιλαμβάνει την ενημέρωση σχετικά με το ηλεκτρονικό ψάρεμα (phishing), την εφαρμογή ενημερώσεων λογισμικού και λειτουργικού συστήματος, αποφυγή μη εξουσιοδοτημένων συσκευών, συμπεριλαμβανομένου του IoT, και της χρήσης ισχυρών κωδικών πρόσβασης ή 504 B.R Payne και T.T. Abegaz φράσεις πρόσβασης ως μέρος ενός ολοκληρωμένου προγράμματος ευαισθητοποίησης για την ασφάλεια.
10. Προτεραιότητα στις συσκευές και προστασία όλων των τελικών σημείων κατάλληλα.Προστασία κάθε συσκευής στο δίκτυο ακομά και παλιούς υπολογιστές ειδικά όταν οι έξυπνες συσκευές είναι σε χρήση.Χρησιμοποίηση τέιχων προστασίας και λογισμικό προστασίας απο ιούς / κακόβουλο λογισμικό σε όλους τους διακομιστές , επιτραπέζιους υπολογιστές και φορητούς υπολογιστές και εφαρμογή κατάλληλης διαμόρφωσης σε ταμπλετ και smartphone ισχυροί κωδικοί πρόσβασης, έλεγχος ταυτότητας δύο βημάτων, αυτόματη απενεργοποίηση). (J. Wurm, 2016)

# 7. Πεδία Εφαρμογής

Το Διαδίκτυο των Πραγμάτων (IoT) ήρθε τόσο απο την εξέλιξη του ίντερνετ όσο και απο την αυξανόμενη ζήτηση πόρων στο διαδίκτυο.Ο συνδυασμός της τεχνολογίας IoT με το Cloud Computing , τις wearable συσκευές ,και τα Big Data δημιουργούν ένα πολύ έξυπνο σύστημα υπερσυνδεσιμότητας που φέρνει νέες υπηρεσίες και δυνατότητες τεχνολογίας.

Σήμερα οι δυνατότητες του IoT είναι αμέτρητες και μπορούν να χρησιμοποιηθούν σε όλους τους τομείς που απαρτίζουν μια κοινωνία όπως τομείς υγείας , εφοδιαστικής αλυσίδας , κτηνοτροφίας , γεωργίας ,μεταφορές , συγκοινωνίες , αυτοβιομηχανία κ.α.

## 7.1 Υγειονομική Περίθαλψη & Υπηρεσίες Υγείας

Η παρακολούθηση ενός ασθενή και το ιστορικό υγείας του είναι μια πτυχή του IoT.Πολλοί άνθρωποι παγκοσμίως φορούν wearables , smartwatches ή και άλλες ηλεκτρονικές συσκευές για να παρακολουθούν την κατάσταση της υγείας τους.Η τεχνολογία αυτή παρέχει πληροφορίες ζωτικής σημασίας σε πραγματικό χρόνο όπως σφιγμούς ,παλμούς ,θερμοκρασία κ.α.Παρέχει επίσης πληροφορίες για ταυτότητα του ασθενούς και το ιστορικό της υγείας του όπως φαρμακευτικές αγωγές .

Με αυτόν τον τρόπο βελτιώνονται οι υπηρεσίες υγείας και περίθαλψης , εξοικονομείται χρόνος που μπορεί να είναι ζωτικής σημασίας για τον επιβίωση του ασθενούς και μειώνει δραματικά το κόστος περιθαλψης του.Το σύστημα αυτό βρίσκει εφαρμογή στα νοσοκομεία και τα κέντρα υγείας καθώς και σε ιατρεία και κέντρα φροντίδας ηλικιωμένων.

## 7.2 Αλυσίδες Εφοδιασμού και Μεταφορές

Οι αλυσίδες εφοδιασμού είναι τόσο σημαντικές για τις επιχειρήσεις όσο η κυκλοφορία του αίματος στον άνθρωπο.Το IoT έχει επιφέρει δραματικές αλλαγές στον τρόπο που οι επιχειρήσεις διαχειρίζονται την αλυσίδα εφοδιασμού.

Μερικά θετικά χαρακτηριστικά :

- Καλύτερη λειτουργική ενημέρωση και προληπτική συντήρηση
- Καλύτερη διαχείρηση φορτίου με μηδαμινά λάθη
- Μείωση προβληματικών προιόντων και φορτίων

Θετικές αλλαγές έρχονται και στις έξυπνες μεταφορές :

- Καλύτερη διαχείρηση στόλου
- Παρακολούθηση εμπορευμάτων
- Έλεγχος των διαδρομών που ακολουθούν τα φορτία

## 7.3 Κτηνοτροφία & Γεωργία

Με την αυξανόμενο ρυθμό ανάπτυξης του πλυθησμού της γης και την αυξανόμενη ζήτηση κρέατος και λαχανικών οι ειδικοί καλούνται να δώσουν μια λύση με βιώσιμο τρόπο χώρις να καταστρέψουν το οικοσύστημα ή να ξεπεράσουν τους παγκόσμιους πόρους.

Η λύση έρχεται με την χρήση IoT στην κτηνοτροφία και την γεωργία.
Ο κύκλος που ακολουθείται με την βοήθεια της χρήσης του IoT είναι ο εξής :

1. Παρακολούθηση
2. Διάγνωση
3. Απόφαση
4. Ενέργεια

Στον τομέα της κτηνοτροφίας το IoT χρησιμεύει :

- Στην παρακολούθηση των αναγκών των ζώων
- Στην ρύθμιση της διατροφής τους για μεγαλύτερη παραγώγικοτητα και αποφυγή αρρωστιών παράλληλα με την υγεία του
- Στην παρακολούθηση της τοποθεσίας του

Στον τομέα της γεωργίας το IoT χρησιμεύει :

- Ακριβής γεωργία με την έννοια της απόδοσης μέγιστων θρεπτικών συστατικών
- Ακριβής μέτρηση των συστατικών και των χημικών στο έδαφος μειώνοντας την πιθανότητα αρρωστιών και αυξάνοντας την επίδραση των φαρμάκων και των λιπασμάτων.
- Καλύτερη χρήση του νερού με βάση τις ανάγκες της καλλιέργειας

## 7.4 Συγκοινωνίες

Το μέγεθος της αξιοποίησης των συγκοινωνιών με την χρήση του IoT είναι μεταβλητό. Απο πολύ μικρές εφαρμογές όσον αφορά των ιδιώτη αλλά και σε πολύ μεγαλύτερη κλίμακα που αφορά επιχειρήσεις μεταφορικών .Και στις δύο περιπτώσεις όμως οι εφαρμογές μπορεί να είνα αμέτρητες και η επίπτωση τεράστια .

1. Διατήρηση της υγείας των οχημάτων
2. Περιορισμός της κίνησης στους δρόμους
3. Βελτίωση της εφοδιαστικής στόλου+
4. Αυτοματοποίηση οδήγησης
5. Επικοινωνία οχημάτων προς αποφυγή ατυχημάτων,

## 7.5 Αυτοκινητοβιομηχανίες

Το IoT αλλάζει την αυτοκινητοβιομηχανία δημιουργώντας ένα οικοσύστημα αυτοκινήτων που μπορούν να επικοινωνήσουν μεταξύ τους αλλά και απευθείας με το ίντερνετ ενισχύοντας την αποδοτικότητα και την ασφάλεια του οδηγού αλλά και του οδικού δικτύου.Τα παραπάνω επιτυγχάνονται με εγκατεστημένους αισθητήρες και software στον εγκέφαλο αλλά και το αμάξωμα του αυτοκινήτου.Προσδιδεται έτσι :

- Ασφαλέστερη διαχείρηση στόλου.Οι αισθητήρες ειδοποιούν τον οδηγό με φωνητικές και μη εντολές για τον δρόμο και συμμορφώνεται με βάση τον κώδικα οδικής κυκλοφορίας
- Τηλεματική πραγματικού χρόνου ενημερωνόντας τον οδηγό για την λειτουργικότητα του αυτοκινήτου (έλεγχος λάστιχων ,έλεγχος οδοστρώματος κλπ)
- Καλύτερη απόδοση του οχήματος με βάση προηγούμενες ρυθμίσεις και προτιμήσεις του οδηγού με ροή απο το database του.

### 7.6 Έξυπνη ενέργεια

Το IoT συνεισφέρει και στην ίδια την πόλη εξοικονομώντας χρόνο και χρήμα καθώς και καλύτερη διαχείρηση της ενέργειας.Τροφοδοτώντας την πόλη με αισθητήρες σε όλα τα κρίσιμα σημεία της όπως αγωγούς νερού , κάδους σκουπιδιών , φανάρια , μετρητές κ.α οι αρμόδιοι ενημερώνονται εγκαίρα όταν υπάρχει ανάγκη επισκευάζοντας μια βλάβη σε λιγότερο χρόνο.

### 7.7 Βιομηχανική παραγωγή

Το διαδίκτυο των πραγμάτων στην βιομηχία παρέχει αυτόματη αναγνώριση προιόντων μέσω ετικετών ραδιοσυχνοτήτων RFID , παρακολούθηση των μηχανημάτων σε πραγματικό χρόνο για καλύτερη συντήρηση αυτών , αύξηση της αποδοτικότητας και της σωστής λειτουργίας των μηχανημάτων και των εξαρτημάτων που απαρτίζουν τους μηχανισμούς μιας επιχείρησης .

### 7.8 Περιβαλλοντική προστασία

Με την συλλογή και αξιοποίηση των πληροφοριών από :

- μετεωρολογικούς ελέγχους
- έλεγχος της θάλασσα για κύματα και τσουνάμι

- έλεγχος ρύπανσης των υπόγειων φορέων
- πυρανίχνευση δασών
- έλεγχος ηφαιστείων και σεισμογενών περιοχών (Bhuvaneswari, 2014)

# 8. Συγκριτική ανάλυση των πρωτοκόλλων Zigbee , 6LoWPAN και Thread

## 8.1 Ανάλυση του πρωτοκόλλου Zigbee

Το πρωτόκολλο ZigBee είναι μια ακολουθία υψηλού επιπέδου επικοινωνιακών πρωτοκόλλων που χρησιμοποιούνται για τη δημιουργία δικτύου προσωπικής περιοχής (personal area network) δημιουργημένο για μικρά, χαμηλής ενέργειας ψηφιακών ασυρμάτων (radios).

Το συγκεκριμένο πρωτόκολλο αναπτύσσεται με βάση το πρωτόκολλο IEEE 802.15.4 από την IEEE και την ZigBee Alliance. Είναι το μόνο παγκόσμιο πρότυπο ασύρματης δικτύωσης που επικεντρώνεται σε εφαρμογές παρακολούθησης, ελέγχου και αισθητήρων. Αν και χαμηλής ισχύος, οι zigbee συσκευές μπορούν να μεταδίδουν δεδομένα σε πολύ μεγάλες αποστάσεις στέλνωντας δεδομένα μέσω ενδιάμεσων συσκευών για να φτάσουν σε πιο απομακρυσμένες αποστάσεις, δημιουργώντας ένα δίκτυο χωρίς κεντρικό έλεγχο ή υψηλής ισχύος πομπό/ δέκτη, ικανό να φτάσει σε όλες τις δικτυακές συσκευές.

Το ZigBee εφαρμόζονται σε διάφορες εφαρμογές που απαιτούν μόνο ένα χαμηλό ρυθμό δεδομένων, μεγάλη διάρκεια ζωής της μπαταρίας και ασφαλή δικτύωση. Το ZigBee έχει ένα καθορισμένο ρυθμό 20-250 kbit/s, ταιριάζει καλύτερα για τα περιοδικά δεδομένα ή μία μόνο μετάδοση σήματος από έναν αισθητήρα ή τη συσκευή εισόδου. Η μετάδοση zigbee κυμαίνεται από 100m εσωτερικά και 1,5Km εξωτερικά (line-of-sight). Οι εφαρμογές περιλαμβάνουν ασύρματους διακόπτες φωτός, ηλεκτρικούς μετρητές με τις οθόνες στο σπίτι, συστήματα διαχείρισης της κυκλοφορίας και άλλο εξοπλισμό καταναλωτικών και βιομηχανικών που απαιτεί μικρής εμβέλειας ασύρματη μεταφορά δεδομένων σε σχετικά χαμηλές τιμές. Η τεχνολογία που ορίζεται από την προδιαγραφή ZigBee προορίζεται να είναι απλούστερη και λιγότερο δαπανηρή από οτι άλλες WPANs, όπως Bluetooth ή Wi-Fi.

Το ZigBee είναι χαμηλής ισχύος συσκευή που λειτουργεί στις βιομηχανικές, επιστημονικές και ιατρικές (ISM) ραδιοσυχνότητες: 868 MHz στην Ευρώπη, 915 MHz στις ΗΠΑ και την

Αυστραλία και 2,4 GHz στις περισσότερες χώρες σε όλο τον κόσμο. Ταχύτητες μετάδοσης δεδομένων κυμαίνονται από 20 kilobits/δευτερόλεπτο στη ζώνη συχνοτήτων 868 MHz έως 250 kilobits/δευτερόλεπτο στη ζώνη συχνοτήτων των 2,4 GHz.

Το επίπεδο δικτύου του zigbee υποστηρίζει εγγενώς τοπολογία αστέρα αλλά και tree τυπικά δίκτυα και γενικά δίκτυα πλέγματος. Καθώς το ZigBee μπορεί να χρησιμοποιηθεί σχεδόν οπουδήποτε, είναι εύκολο να εφαρμοστεί και χρειάζεται λίγη ενέργεια για να λειτουργήσει, η ευκαιρία για ανάπτυξη σε νέες αγορές, καθώς και η καινοτομία στις υπάρχουσες αγορές, είναι απεριόριστες.

Υπάρχουν τέσσερις κυκλοφορίες Zigbee, η εμφάνιση του zigbee ξεκίνησε το 2004 (Δεκέμβριος, 2004), έπειτα το ZigBee 2006 (Δεκέμβριος, 2006) και τέλος, το ZigBee 2007 και το ZigBee Pro (Οκτώβριος, 2007), (Baronti et al., 2007). Σε κάθε νέα έκδοση υπάρχει μια βελτίωση, σύμφωνα με τις προηγούμενες εκδόσεις. [32] (Khajenasiri, 2017)

## 8.2 Ανάλυση του πρωτοκόλλου 6Lowpan

Το 6LoWPAN είναι ένα αρκτικόλεξο, μια συντομογραφία του IPv6 (Low-power Wireless Personal Area Network), χαμηλής ισχύος στα ασύρματα προσωπικά δίκτυα (Wiley, 2009). Το 6LoWPAN είναι το όνομα μιας ομάδας εργασίας που συνάπτεται στο χώρο του Internet της IETF

Η έννοια 6LoWPAN προήλθε από την ιδέα ότι "το πρωτόκολλο του Διαδικτύου θα μπορούσε και θα έπρεπε να εφαρμοστεί ακόμη και στις μικρότερες συσκευές" (Mulligan, Geoff, 2007) και ότι οι συσκευές χαμηλής ισχύος με περιορισμένες δυνατότητες επεξεργασίας θα πρέπει να είναι σε θέση να συμμετάσχουν στο Ίντερνετ των πραγμάτων .

Όπως γνωρίζουμε, στο διαδίκτυο ένα πακέτο περνά μέσα από πολλά άλλα διαφορετικά διασυνδεδεμένα δίκτυα για να πάει από την πηγή στον προορισμό του. Έτσι, λαμβάνοντας υπόψη την τεχνολογία στρώματος ζεύξης του κάθε διασχισμένου δικτύου, πρέπει να υπάρχει μια

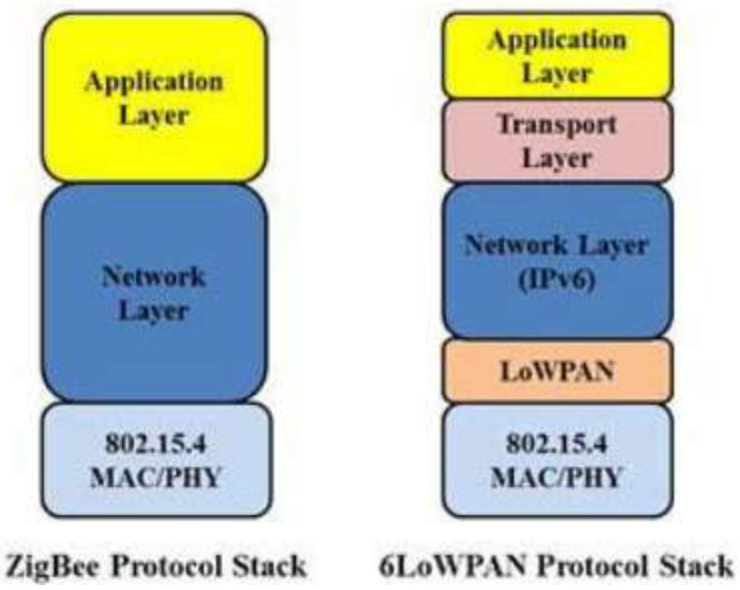
"IP διεύθυνση-πάνω από κάθε-X ", " IP-over-X", προδιαγραφή για να καθορίσει τον τρόπο που θα μεταφερθούν τα πακέτα IP.

Με λίγα λόγια, είναι ένα πρωτόκολλο δικτύου, που ορίζει μηχανισμούς ενθυλάκωσης και συμπίεσης κεφαλίδων (encapsulation and header compression mechanisms). Έτσι, έχοντας την ελευθερία της ζώνης συχνοτήτων και του φυσικού επιπέδου, μπορεί να χρησιμοποιηθεί σε πολλαπλές πλατφόρμες επικοινωνίας, συμπεριλαμβανομένων των Ethernet, Wi-Fi, 802.15.4 και ISM sub-1GHz. Το πιο βασικό χαρακτηριστικό του είναι η χρήση της στοίβας IPv6 (πρωτόκολλο Internet έκδοση 6), μιας πολύ σημαντικής εισαγωγής για να καταστεί δυνατή η χρησιμοποιήση του, στο IoT.

Το IPv6 έρχεται να σκεπάσει το IPv4, όπου προσφέρει 2διευθύνσεις, επιτρέποντας σε οποιοδήποτε ενσωματωμένο αντικείμενο ή συσκευή στον κόσμο να έχει τη δική του μοναδική διεύθυνση IP και να συνδεθεί στο Internet. Το IPv6παρέχει ένα βασικό μηχανισμό μεταφοράς, για την παραγωγή πολύπλοκων συστημάτων ελέγχου και την επικοινωνία συσκευών με οικονομικό τρόπο, μέσω ασυρμάτου δικτύου χαμηλής ισχύος (low-power wireless network).

Το IPv6 είναι σχεδιασμένο για να στέλνει πακέτα, μέσω δικτύων, που βασίζονται σε IEEE 802.15.4, και να εφαρμόζει ανοικτά πρότυπα IP, όπως TCP, UDP, HTTP, COAP, MQTT.Επίσης προσφέρει το end-to-end για διευθυνσιοδοτούμενους κόμβους, επιτρέποντας σε ένα δρομολογητή να συνδέει το δίκτυο με IP. Το 6LoWPAN είναι ένα δίκτυο πλέγματος ισχυρό, κλιμακωτό και αυτοθεραπεύσιμο(self-healing). Οι συσκευές δρομολόγησης πλέγματος (mesh) μπορούν να δρομολογήσουν δεδομένα προοριζόμενα για άλλες συσκευές, ενώ οι εξυπηρετητές (hosts) μπορούν να παραμένουν ανενεργοί για μεγάλες χρονικές περιόδους.

Το 6LoWPAN προτείνει μια προσαρμογή επιπέδου (layer) μεταξύ του MAC και του επιπέδου δικτύου (IPv6), προκειμένου να χειριστεί τη διαλειτουργικότητα μεταξύ IEEE 802.15.4 και IPv6. Η πιο ανταγωνιστική εναλλακτική λύση για το 6LoWPAN είναι το ZigBee, όπως φαίνεται και στην εικόνα παρακάτω. Και οι δύο χρησιμοποιούν το ίδιο πρωτόκολλο IEEE 802.15.4 στο φυσικό επίπεδο. [33] (Al-Sarawi, 2017)




**Εικόνα 10. Σύγκριση του ZigBeevs 6LoWPAN**

## 8.3 Ανάλυση του πρωτοκόλλου Thread

Το Thread είναι ένα νέο σχετικά πρωτόκολλο, δικτύωσης IPv6 βασισμένο σε IP, που στοχεύει στο περιβάλλον αυτοματισμού στο σπίτι βασισμένο στο 6LoWPAN. Ωστόσο, από την άποψη εφαρμογής, σχεδιάζεται πρωτίστως ως συμπλήρωμα του WiFi, καθώς αναγνωρίζει ότι, ενώ το WiFi είναι καλό για πολλές καταναλωτικές συσκευές, έχει περιορισμούς για χρήση σε μια εγκατάσταση αυτοματισμού στο σπίτι.

Ξεκίνησε στα μέσα του 2014 από την ομάδα Thread, είναι ανοικτό πρωτόκολλο και βασίζεται σε διάφορα πρότυπα, όπως το IEEE 802.15.4 (ως πρωτόκολλο ασύρματης διασύνδεσης), το IPv6, το 6LoWPAN. Υποστηρίζει ένα δίκτυο πλέγματος χρησιμοποιώντας πομποδέκτες IEEE 802.15.4 και είναι σε θέση να διαχειριστεί μέχρι 250 κόμβους, με υψηλά επίπεδα ελέγχου ταυτότητας (authentication) και κρυπτογράφησης (encryption). Μια σχετικά απλή αναβάθμιση λογισμικού θα πρέπει να επιτρέπει στους χρήστες να τρέχουν thread σε υπάρχουσες συσκευές με δυνατότητα IEEE 802.15.4. [34] (istu, 2019)

## 8.4 Διαφορές ZigBee vs Thread

Το ZigBeeμε το Threadθα λέγαμε ότι είναι παρόμοια αρκετά μεταξύ τους. Είναι και τα δύο δίκτυα τοπικών δικτύων. Χρησιμοποιούν το ίδιο πρωτόκολλο επιπέδου MAC χαμηλού επιπέδου-IEEE 802.15.4. Είναι και τα δύο ανοιχτά πρότυπα. Ακόμη και οι δύο έχουν στοχεύσει παρόμοιους τύπους εφαρμογών, όπως τα έξυπνα σπίτια.Και οι δύο λειτουργούν με το παγκόσμιο πρότυπο ζώνης συχνοτήτων 2,4 GHz. Τέλος, η κατανάλωση ενέργειας και η χρήση τους μπορεί να είναι πολύ παρόμοια.

Βέβαια πέρα από τις ομοιότητες, σίγουρα υπάρχουν και διαφορές, τι οποίες δεν θα μπορούσαμε να τις παραβλέψουμε. Παρακάτω γίνετε μία ανάλυση αυτών των διαφορών.

Το Thread ξεκίνησε από τηGoogle, τη Samsung και έναν αριθμό προμηθευτών που ήθελαν να αντιμετωπίσουν τους κόμβους με έναν πιο παραδοσιακό τρόπο. Χρησιμοποιεί το 6LoWPAN, το οποίο παρέχει σε κάθε κόμβο μια διεύθυνση IP. Η διεύθυνση με την οποία μιλάει το cloud πηγαίνει σε έναν δρομολογητή και στην συνέχεια στέλνει σε έναν κόμβο μέσω της διεύθυνσης IP του.Το ZigBee προσπάθησε να το κάνει αυτό με το ZigBee IP, αλλά δεν έχει κερδίσει σημαντική έλξη στην αγορά. Ένας άλλος τρόπος για την αντιμετώπιση των κόμβων ZigBee είναι η χρήση ενός δρομολογητή με το δίκτυο. Όταν μπαίνει η διεύθυνση, ο δρομολογητής πρέπει να έχει κάποιο είδος ‘ευφυΐας’ για να γνωρίζει ποιος κόμβος είναι συνδεδεμένος με αυτόν και πώς να μεταφράσει ένα συγκεκριμένο μήνυμα.

Το ZigBee δημιούργησε έτσι ένα επίπεδο εφαρμογής που υπαγορεύει τον τρόπο με τον οποίο οι εφαρμογές διασυνδέονται και λειτουργούν μέσα σε αυτό. Εάν δημιουργείτε μια εφαρμογή που πρόκειται να συνδεθεί με άλλη εφαρμογή ZigBee - όπως το ZigBee Light Link, το οποίο λειτουργεί με φωτισμό - αυτή είναι μια προφανής επιλογή. Αυτό όμως φέρνει και κάποια προβλήματα μαζί του.

Αντίθετα το Thread δεν ορίζει κάποιο επίπεδο εφαρμογής και επομένως δεν καθορίζει τον τρόπο αλληλεπίδρασης των συσκευών στο δίκτυο. Προσφέρει έναν γενικό τρόπο για να επικοινωνούν οι συσκευές με τους τελικούς κόμβους.

Επίσης, το λογισμικό για το ZigBee είναι μεγαλύτερο και πιο περίπλοκο,άρα έχει προβλήματα καθυστέρησης και μπορεί να χρησιμοποιεί περισσότερη ισχύ. Αυτό σημαίνει επίσης ότι χρησιμοποιεί περισσότερη μνήμη, η οποία μπορεί να απαιτεί μεγαλύτερο μικροελεγκτή (και συνεπώς να αυξήσει το κόστος).

| **ΛΕΙΤΟΥΡΓΙΕΣ** | **ZigBee** | **Thread** |
|---|---|---|
| Συχνότητα | 2.4 GHz | 2.4 GHz |
| Εύρος Ζώνης | 250kbps | 250kbps |
| Μέγεθος Δικτύου | 10-100 | 10-100 |
| Τύπος Τοπολογίας Δικτύου | Πλέγμα | Πλέγμα |
| Ισχύς | Χαμηλή | Χαμηλή |
| Επίπεδο Εφαρμογής | Ναι | Όχι |
| Υποστήριξη του IPv6 | Όχι | Ναι |
| Χρόνος ζωής | Λίγο καιρό | Λίγο καιρό |
| Πρόγραμμα πιστοποίησης και διαλειτουργικότητα | Πιστοποίηση του τελικού προϊόντος | Πιστοποίηση της στοίβας |
| Ασφάλεια | Κρυπτογράφηση και έλεγχος ταυτότητας σε όλο το δίκτυο μέσω κώδικα εγκατάστασης | Έλεγχος ταυτότητας με κωδικό πρόσβασης με DTLS (Ασφάλεια επιπέδου μεταφοράς δεδομένων) |
| Ενσωμάτωση στο cloud | Στην Πύλη Zigbee | Δρομολογητής του περιθωρίου νήματος |
| Απόδοση καθυστέρησης για πακέτα εφαρμογών | Η καλύτερη | Πολύ καλή |

**Πίνακας 2. Διαφορές ZigBee vs Thread**

## 8.5 Διαφορές ZigBee vs 6LoWPAN

Αναμφισβήτητα, όπως αναφέραμε και σε παραπάνω ενότητα, ο ZigBee είναι το πιο δημοφιλές πρωτόκολλο ασύρματης δικτύωσης χαμηλού κόστους και χαμηλής ισχύος που διατίθεται στις μέρες μας.

Η διαλειτουργικότητα είναι ένας από τους κύριους παράγοντες κατά την επιλογή ενός ασύρματου πρωτοκόλλου. Από τεχνική άποψη, η διαλειτουργικότητα σημαίνει ότι οι εφαρμογές δεν χρειάζεται να γνωρίζουν τους περιορισμούς των φυσικών συνδέσμων που φέρουν τα πακέτα τους. Το ZigBee ορίζει την επικοινωνία μεταξύ 802.15.4 κόμβων και στη συνέχεια ορίζει νέα ανώτερα επίπεδα μέχρι την εφαρμογή. Αυτό σημαίνει ότι οι συσκευές ZigBee μπορούν να λειτουργούν με άλλες συσκευές ZigBee, με την προϋπόθεση ότι χρησιμοποιούν το ίδιο προφίλ.

Το 6LoWPAN προσφέρει διαλειτουργικότητα με άλλες ασύρματες συσκευές 802.15.4 καθώς και με συσκευές σε οποιονδήποτε άλλο σύνδεσμο δικτύου IP (π.χ. Ethernet ή Wi-Fi) με μια απλή συσκευή γέφυρας. Η γεφύρωση μεταξύ δικτύων ZigBee και μη ZigBee απαιτεί μια πιο σύνθετη πύλη επιπέδου εφαρμογής. Η βασική απαίτηση για IPv6 άνω του 802.15.4 είναι ότι η μέγιστη μονάδα μετάδοσης (MTU) πρέπει να είναι τουλάχιστον 1280 πακέτα / byte (ανά RFC 2460). Δεδομένου ότι το τυπικό μέγεθος πακέτου IEEE 802.15.4 είναι 127 οκτάδες, πρέπει να εφαρμοστεί ένα επίπεδο προσαρμογής που θα επιτρέπει τη μετάδοση δεδομένων IPv6 σε 0,4 δίκτυα.

Επίσης, τόσο το ZigBee όσο και το 6LoWPAN επωφελούνται από την ενσωματωμένη κρυπτογράφηση AES128, η οποία αποτελεί μέρος του προτύπου IEEE 802.15.4.

Το 6LoWPAN είναι αρκετά ελκυστικό, (για τους λόγους που αναφέραμε παραπάνω) καθώς βασίζεται σε IP το τυπικό πρωτόκολλο εργασίας στο Διαδίκτυο. Ωστόσο, το ZigBee φαίνεται να είναι πιο δημοφιλές και έχει υιοθετηθεί από σημαντικούς παίκτες σε πολλούς κλάδους.

| **ΛΕΙΤΟΥΡΓΙΕΣ** | **ZigBee** | **6LoWPAN** |
|---|---|---|
| Μέγιστη Εμβέλεια σε Εξωτερικό χώρο | 500m | 200m |
| Εύρος Ζώνης | 250kbps | 200kbps |

| | | |
|---|---|---|
| Μέγεθος Δικτύου | 65536 | 100 |
| Μέση Κατανάλωση | 2mW | 2mW |
| Δυνατότητα Multi-Hop | Ναι | Ναι |
| Κόστος πιστοποίησης | Μέτριο | Χαμηλό |
| Αποδοχή αναπτυξιακής κοινότητας | Υψηλή | Μέτρια |
| Διαλειτουργικότητα | Υψηλή | Χαμηλή |

**Πίνακας 3.Διαφορές ZigBee vs 6LoWPAN**

## 8.6 Διαφορές Thread vs 6LoWPAN

Το Thread, όπως αναφέραμε και παραπάνω είναι μια δικτύωση πλέγματος που βασίζεται σε IPv6 στο Διαδίκτυο των Πραγμάτων. Για να δούμε όμως τι διαφορές έχουν μεταξύ τους αυτά τα δύο πρωτόκολλα αν και τοένα ενσωματώνεται μέσα στο άλλο.

Το Thread είναι ένα πρωτόκολλο δικτύωσης πλέγματος βασισμένο σε πρότυπα IPv6 που αναπτύχθηκε για άμεση και ασφαλή σύνδεση προϊόντων μεταξύ του σπιτιού μεταξύ τους, στο διαδίκτυο και στο cloud.Χτισμένο σε ανοιχτά πρότυπα και με πρωτόκολλα IPv6/6LoWPAN, η προσέγγιση του Thread στην ασύρματη δικτύωση προσφέρει ένα ασφαλές και αξιόπιστο δίκτυο ματιών χωρίς κανένα σημείο βλάβης και υποστήριξη για συσκευές χαμηλής κατανάλωσης

| **ΛΕΙΤΟΥΡΓΙΕΣ** | **Thread** | **6LoWPAN** |
|---|---|---|
| Φυσική Διέθυνση MAC | IEEE 802.15.4 | IEEE 802.11.1 |
| Εύρος ΖώνηςΣυχνοτήτων | 2.4 GHz | 2.4 GHz |
| Μέγεθος Δικτύου | 10-100 | 100 |
| Μέση Κατανάλωση | Χαμηλή | Υψηλή |

| | | |
|---|---|---|
| Μέγιστος ρυθμός Δεδομένων | 250Kbits | 54Mbits |
| Τοπολογία Δικτύου | Πλέγμα | Αστέρα |

**Πίνακας 4. Διαφορές ZigBee vs 6LoWPAN**

## 8.7 Συμπεράσματα

Οι ασύρματες τεχνολογίες δικτύωσης (πρωτόκολλα) που αναφέρθηκαν παραπάνω έχουν διαφορετικά χαρακτηριστικά, τα οποία καθορίζουν την χρησιμότητα σε συγκεκριμένες εφαρμογές.Το ZigBee και το Thread κατέχουν αμφότερα τον ίδιο χώρο μικρής εμβέλειας, χαμηλής ισχύος. Οι ζεύξεις πρωτοκόλλων ZigBee και Thread ορίζουν και χρησιμοποιούν και οι δύο, το ίδιο πρωτόκολλο φυσικής και στρώματος συνδέσμων στις στοίβες τους - IEEE 802.15.4. Στο Thread επίσης δεν έχει καθοριστεί ένα στρώμα εφαρμογής ενώ στο ZigBee έχει καθοριστεί για πολλά διαφορετικά προγράμματα.

Βέβαια τα πιο επικρατέστερα προς υλοποίηση είναι το 6LoWPAN και το Zigbee και όχι τόσο το Thread. Αυτό όμως που πρέπει να κρατήσουμε ως συμπέρασμα για τα παραπάνω τρία πρωτόκολλα ασύρματής δικτύωσης είναι ότι δεν μπορούμε να ορίσουμε πιο είναι καλύτερο ή χειρότερο. Ανάλογα, με τις απαιτήσεις που έχει κάθε δίκτυο και για ποια χρήση το θέλουμε μπορούμε να ορίσουμε εμείς πιο πρωτόκολλο θα χρησιμοποιήσουμε.

# 9. Προσομοιώσεις έξυπνου σπιτιού σε περιβάλλον Cisco Packet Tracer

## 9.1 Εισαγωγικά στοιχεία για το πρόγραμμα προσομοιώσεων

Το πρόγραμμα Cisco Packet Tracer είναι ένα πρόγραμμα προσομοιώσεων . το οποίο επιτρέπει στους χρήστες να χτίσουν δίκτυα διαφόρετικών κλιμάκων , ώστε να τις διαχειρίζονται σαν να ήταν πραγματικά δίκτυα υπολογιστών χρησιμοποιώντας πραγματικά πρωτόκολλα.Είναι προιόν της εταιρίας Cisco Systems και το γραφικό περιβάλλον παρέχει όλες τα απαραίτητα εργαλεία για έναν τεχνικό δικτύων η και απλούστερα έναν απλό σπουδαστή.

Τα εικονικά αυτά δίκτυα διαφορετικής κλίμακας μπορούν να αλληλεπιδρούν μεταξύ τους σε πραγματικό χρόνο.Το γραφικό περιβάλλον επιτρέπει στον χρήστη να προσθέσει ή να αφαίρεσει συσκευές στο δίκτυο αλλά και να τις παραμετροποιήσει σύμφωνα με τις ανάγκες του δικτύου.Η τροποποίηση των δικτύων γίνεται όπως ακριβώς θα γινόταν και σε πραγμακό δίκτυο , σώστη ρύθμιση IP ,μάσκα υποδικτύου , DHCP server ,DNS server,firewall .VPN και ότι άλλο είναι αναγκάιο και απαραίτητο για την σώστη επικοινωνία του δικτύου.

Από την έκδοση 7.x και μέτα το Cisco Packet Tracer έχει προσθέσει στην βιβλιοθήκη του έξυπνες συσκευές και αισθητήρες δίνοντας την δυνατότητα να δημιουργήσουμε ένα έξυπνο δίκτυο.Παρακάτω είναι οι έξυπνες συσκευές απο το πρόγραμμα προσομοίωση.

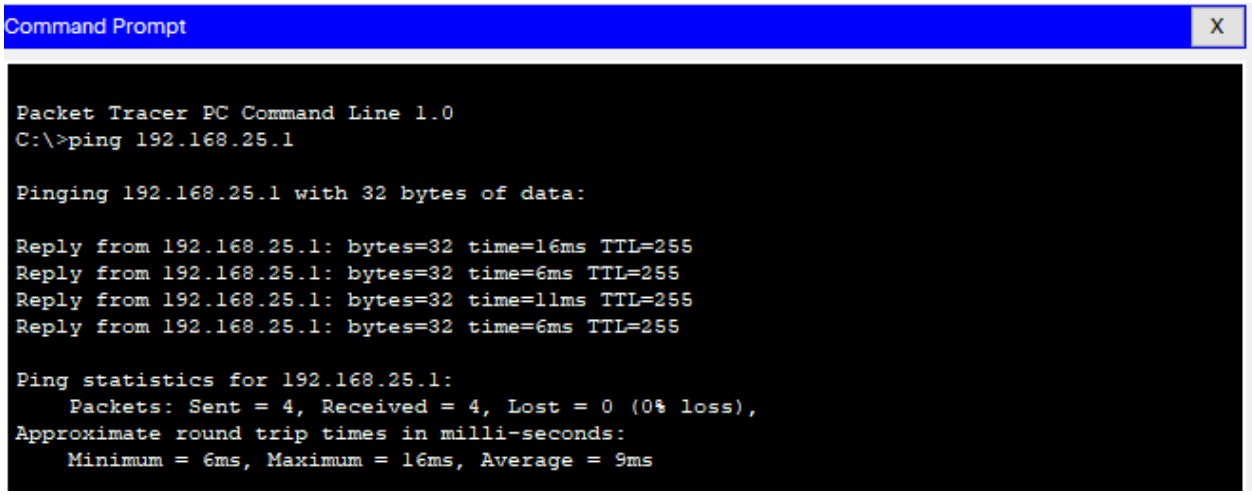

**Εικόνα 11. Έξυπνες συκευές και αισθητήρες Cisco Packet Tracer**

### 9.1.1 Σενάριο Προσομοίωσης 1

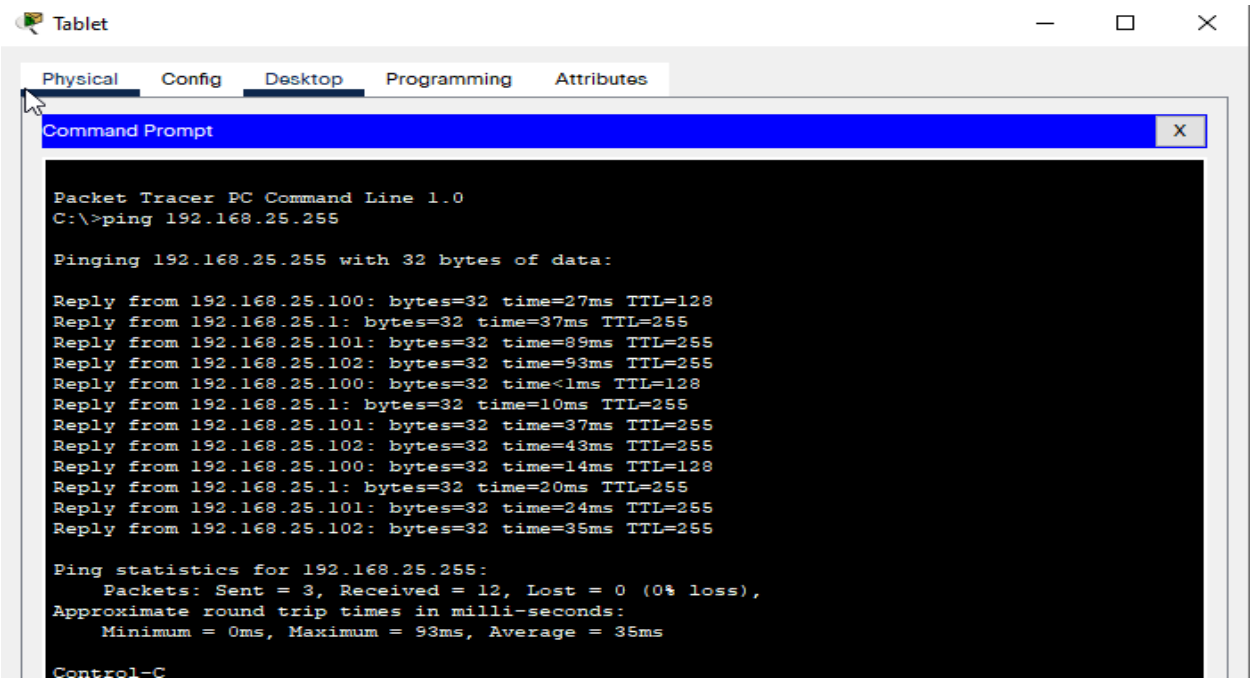
Το πρώτο σενάριο είναι ένα εισαγωγικό σενάριο αυτοματισμού για την εξοικείωση με το Cisco Packet Tracer .Στο σενάριο αυτό χρησιμοποιήθηκαν οι εξής συσκευές : a)ένα Home Gateway , b)ένα TabletPC-PT για τον έλεγχο των συσκυευών , c) ένας ανεμιστήρας και d)ένα φως. Εικόνα 9-1-1

Σε αυτό το σενάριο ο χρήστης έχει την δυνατότητα να ελέγξει τις παραπάνω συσκευές μέσα απο το interface του τάμπλετ, να ανάψει το φως η να θέσει σε λειτουργία τον ανεμιστήρα.Το Home Gateway λειτουργεί με DHCP διευθυνσιοδότηση.Το LAN IP του Gateway είναι 192.168.25.1

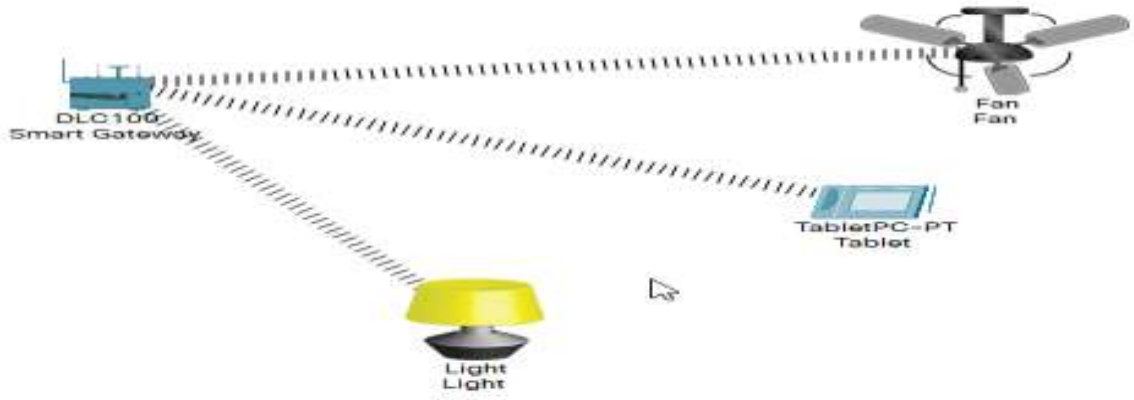
και οι συσκευές λαμβάνουν IP στο διάστημα 192.168.25.2-254 ( η IP 192.168.25.255 χρησιμοποιείται για broadcast μετάδοση. **Εικόνα 9-1-1 ,Εικόνα 9-1-2**




**Εικόνα 13. Ping απο το τάμπλετ στο Home Gateway για τον έλεγχο της επικοινωνίας μεταξύ τους επιτυχής**

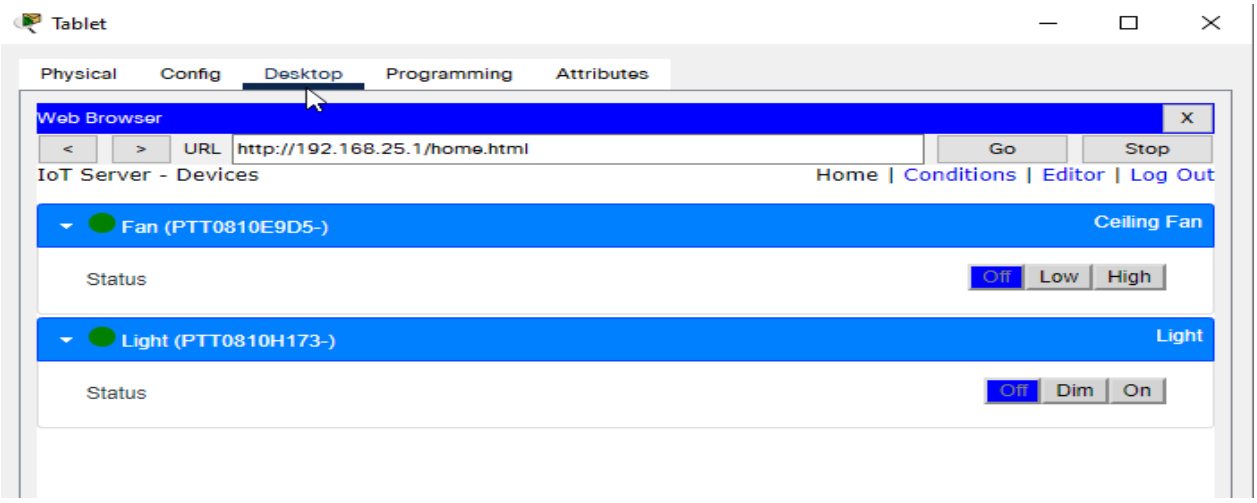



**Εικόνα 12. Broadcast ping απο το τάμπλετ σε όλες τις συσκευές συμπεριλαμβανομένου και του Gateway μας , επιτυχής**

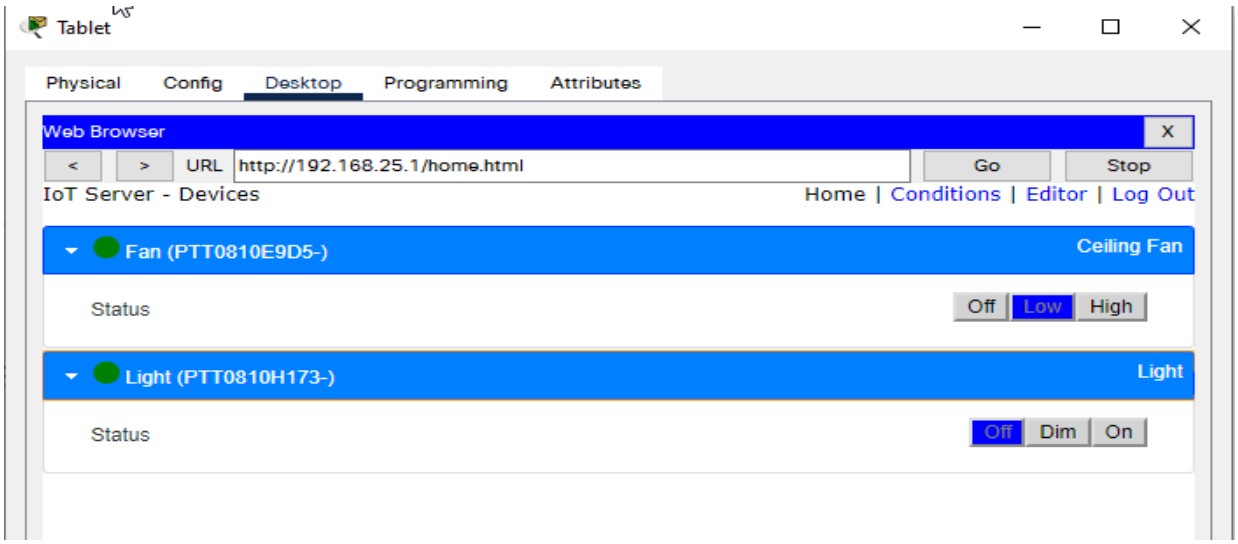



**Εικόνα 14.Σενάριο 1 : Στο σενάριο αυτό το δίκτυο αποτελείται απο ενα Home Gateway (DHCP:LAN-IP – 192.168.25.1) ,ένα φως (192.168.25.102) , ένα τάμπλετ (192.168.25.100) και έναν ανεμιστήρα(192.168.25.101) .Ο χρήστης μπορεί να ελέγξει τις συσκευές αυτές μέσα απο το**

Ο χρήστης έχει την δυνατότητα μέσα απο το GUI του τάμπλετ η πιο συγκεκριμένα απο το IoT monitor να κάνει είσοδο μέσω της διεύθυνσης IP και τα διαπιστευτήρια (credentials user/pass) και να μεταβάλλει την κατάσταση λειτουργίας των συσκευών που είναι εγγεγραμένες στο Home Gateway (Είκονα 15).

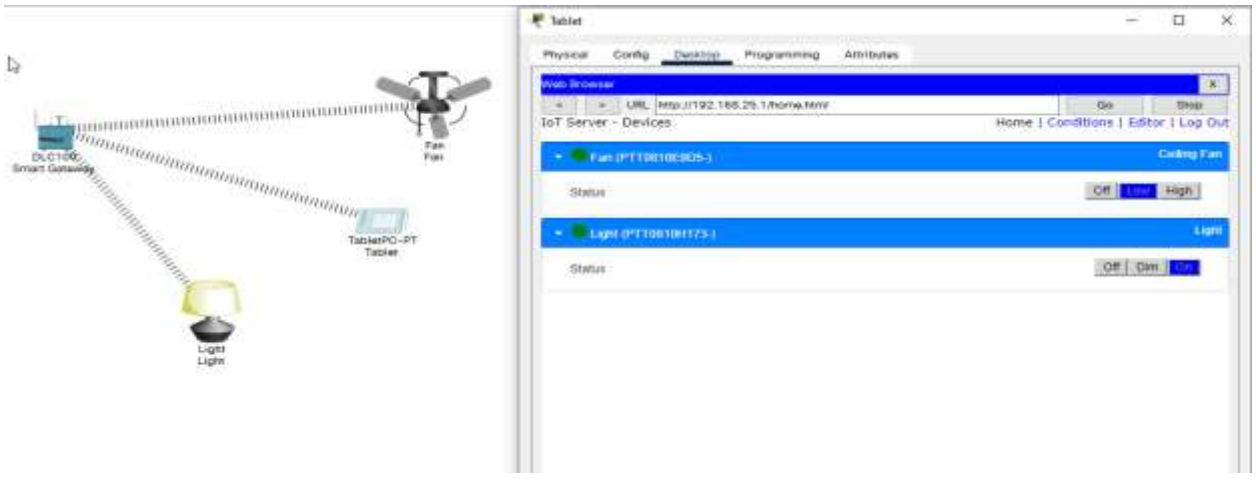



**Εικόνα 15. Κατάσταση λειτουργίας των συσκευών**




**Εικόνα 16. Είσοδος στο Gateway απο το IoT monitor της συσκευής τάμπλετ ,εισαγωγή διαπιστευτηρίων και παραμετροποίηση συσκευών.**

Στα πλαίσια της πρώτης προσομοίωσης και κατά της είσοδο στην σελίδα του Home Gateway ο χρήστης μπορεί να παραμετροποιήσει τις συσκευές που είναι register σ'αυτό.Στην συγκεκριμένη προσομοίωση έχουμε registered δυο συσκευές , τον ανεμιστήρα (Fan) και το φως (Light).Στον ανεμιστήρα επιτρέπονται τρεις καταστάσεις OFF,Low,High και στο φως OFF,Dim,ON.

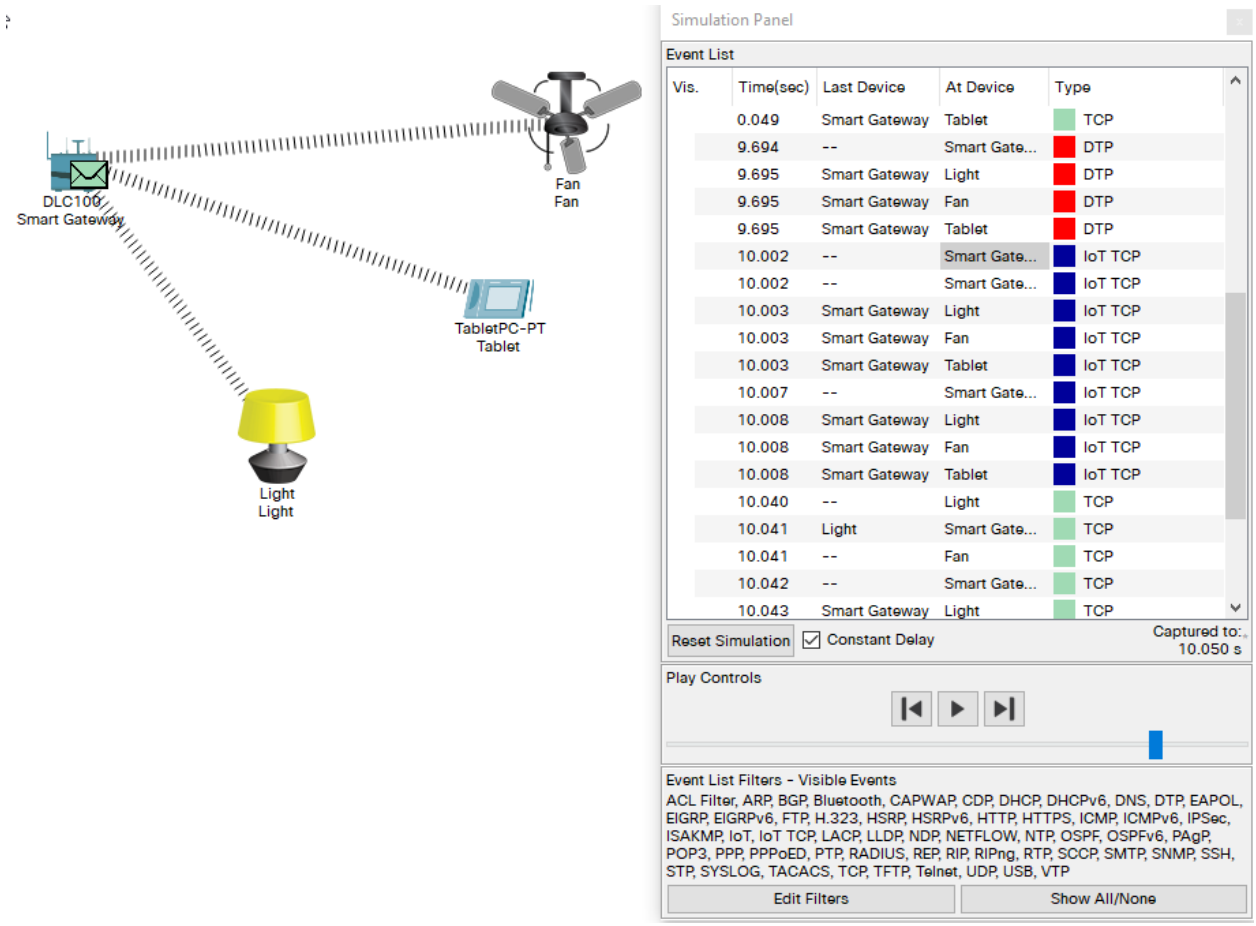


**Εικόνα 17. Θέση λειτουργίας του ανεμιστήρα σε Low και του φωτός σε ON**

Στο επίπεδο προσομοίωσης μπορούν να χρησιμοποιηθούν μια γκάμα πρωτοκόλλων αναλόγως με τις ανάγκες του δικτύου προσομοίωσης RP, DNS, ICMP, BGP, EIGRP, OSPF, DHCP, HSRP και RIP.

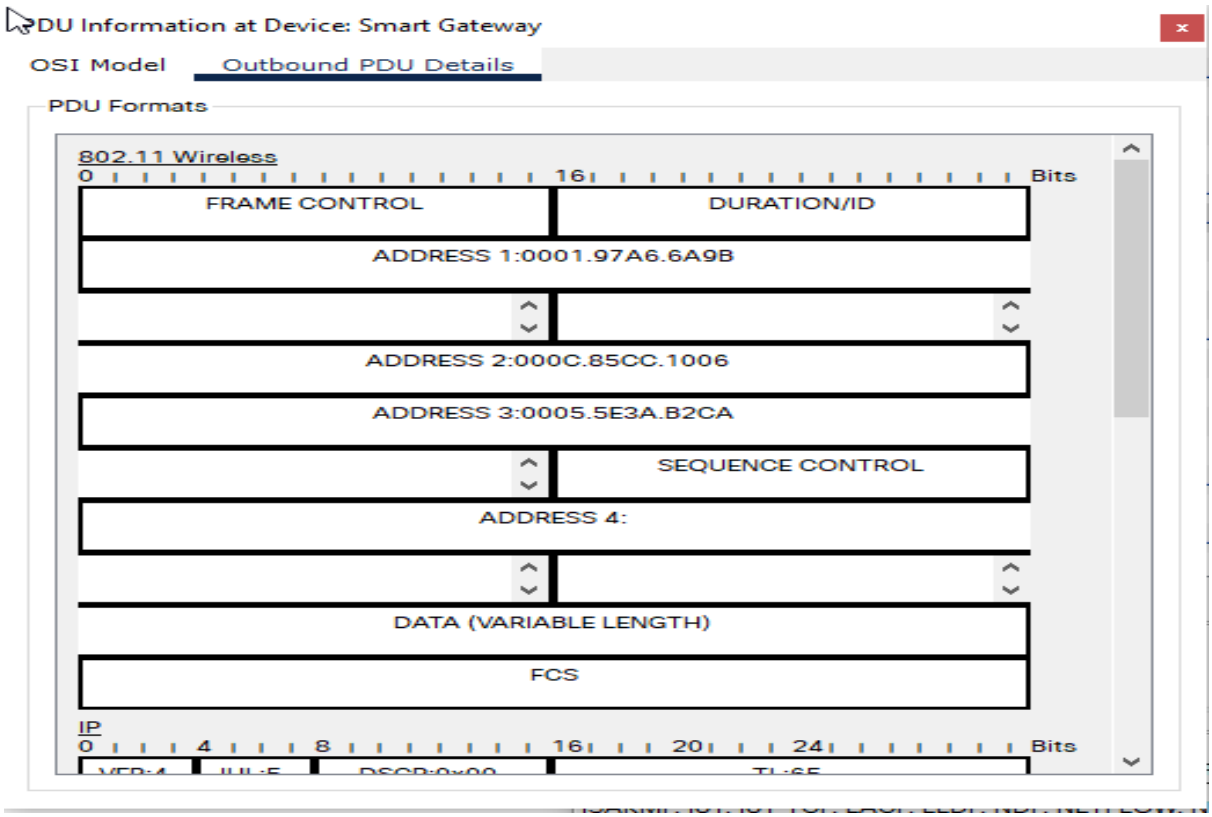

**Εικόνα 18. Λίστα πρωτοκόλλων περιβάλλοντος Cisco Packet Tracer**

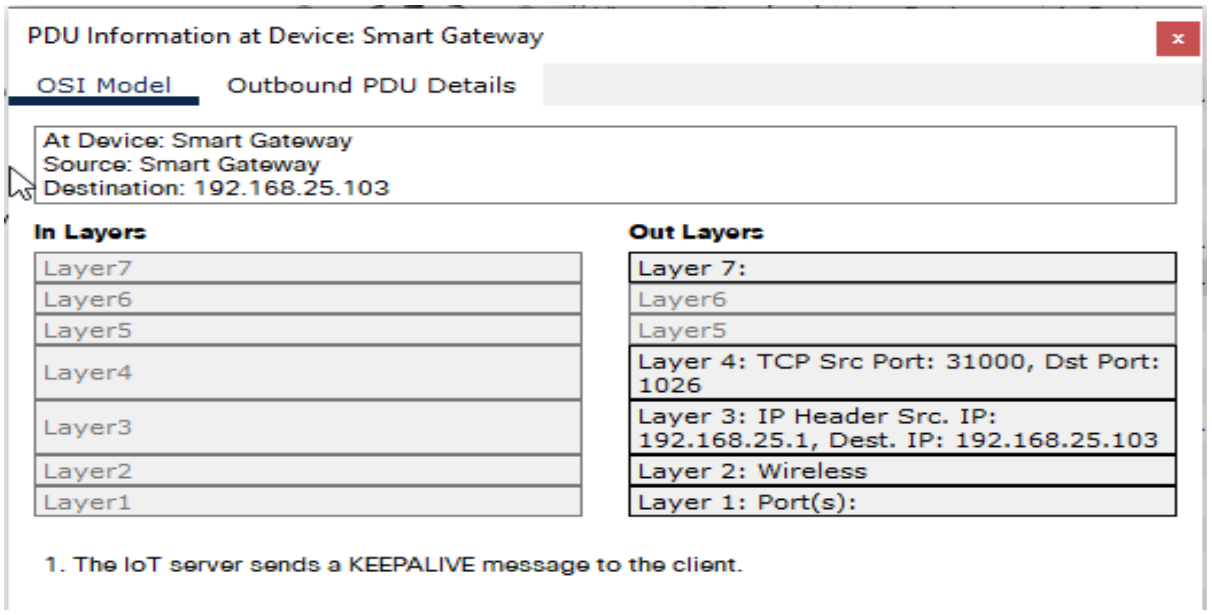
Στην διαδικασία προσομοίωσης μπορούμε να δούμε όλη την διαδικασία αποστολής πακέτων ,ποιά συσκευή έστειλε ποιό πακέτο και με ποιό χρησιμοποιούμενο πρωτόκολλο ,ποιά συσκευή το έλαβε και την χρονική στιγμή αποστολής και λήψης.




**Εικόνα 19. Διαδικασία προσομοίωσης.Αποστολή πακέτων με συγκεκριμένα πρωτόκολλα και λήψη απο τις χρησιμοποιούμενες συσκευές.**

Η προσομοίωση επίσης επιτρέπει να εξετάσουμε τις πληροφορίες για το επίπεδο OSI της κάθε συσκευής καθώς και το protocol data unit.




**Εικόνα 20. Πληροφορίες του protocol data unit του Home Gateway καθώς και πληροφορίες για το επίπεδο OSI**

### 9.1.2 Σενάριο προσομοίωσης 2

Στο δεύτερο σενάριο η προσομοίωση εκτυλίσσεται σε ένα smart home με τρεις διαφορετικούς χώρους όπου όλες οι συσκευές λειτουργούν αρμονικά καθώς και κάποιες απο αυτές λειτουργούν σε συνάρτηση με κάποιες (conditions).

Στο σενάριο αυτό χρησιμοποιήθηκαν οι εξής συσκευές a)ένα Smartphone , b)ένα Home Gateway c)ένα Bluetooth speaker , d) μία καφετιέρα , e) ένα παράθυρο, f) ένα Monitor θερμοκρασίας , g) ένα air-condition , h) δύο πόρτες και i)ένας αισθητήρας κίνησης.

Οι συσκευές βρίσκονται ανα χώρο :

| **Κουζίνα** | **Αιθουσα διαχείρησης** | **Δωμάτιο** | **Σαλόνι** |
|---|---|---|---|
| *Bluetooth Speaker* | *Temperature Monitor* | *AC* | *Smartphone* |
| *Appliance* | | *Motion Detector* | |
| *Door* | | *Door* | |
| *Window* | | | |

**Πίνακας 5. Συσκευές σεναρίου**

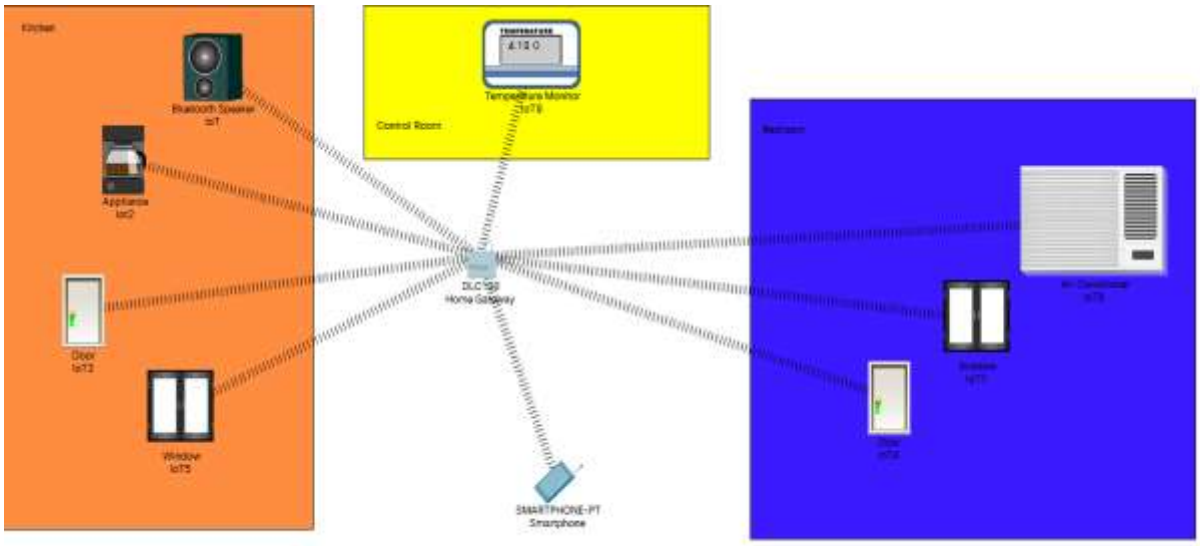
Σε αυτό το σενάριο ο χρήστης έχει την δυνατότητα να ελέγξει τις παραπάνω συσκευές μέσα απο το interface του smartphone , να θέσει σε λειτουργία όποια συσκευή επιθυμεί αλλά και να παραμετροποιήση τις συσκευές που λειτουργούν με συνθήκες.Το Home Gateway λειτουργεί με DHCP διευθυνσιοδότηση.Το LAN IP του Gateway είναι 192.168.25.1 και οι συσκευές λαμβάνουν IP στο διάστημα 192.168.25.2-254 ( η IP 192.168.25.255 χρησιμοποιείται για broadcast μετάδοση.

Οι συσκευές έχουν τις παρακάτω static IP για την καλύτερη διαχείρηση και έλεγχο τους.

| **Συσκευές** | **IP** |
|---|---|
| *Bluetooth Speaker* | 192.168.25.100 /24 |
| *Appliance* | 192.168.25.101 /24 |
| *Door* | 192.168.25.102 /24 |
| *Window* | 192.168.25.103 /24 |
| *Temperature Monitor* | 192.168.25.104 /24 |
| *AC* | 192.168.25.105 /24 |
| *Motion Detector* | 192.168.25.106 /24 |
| *Door* | 192.168.25.107 /24 |
| *Smartphone* | 192.168.25.108 /24 |

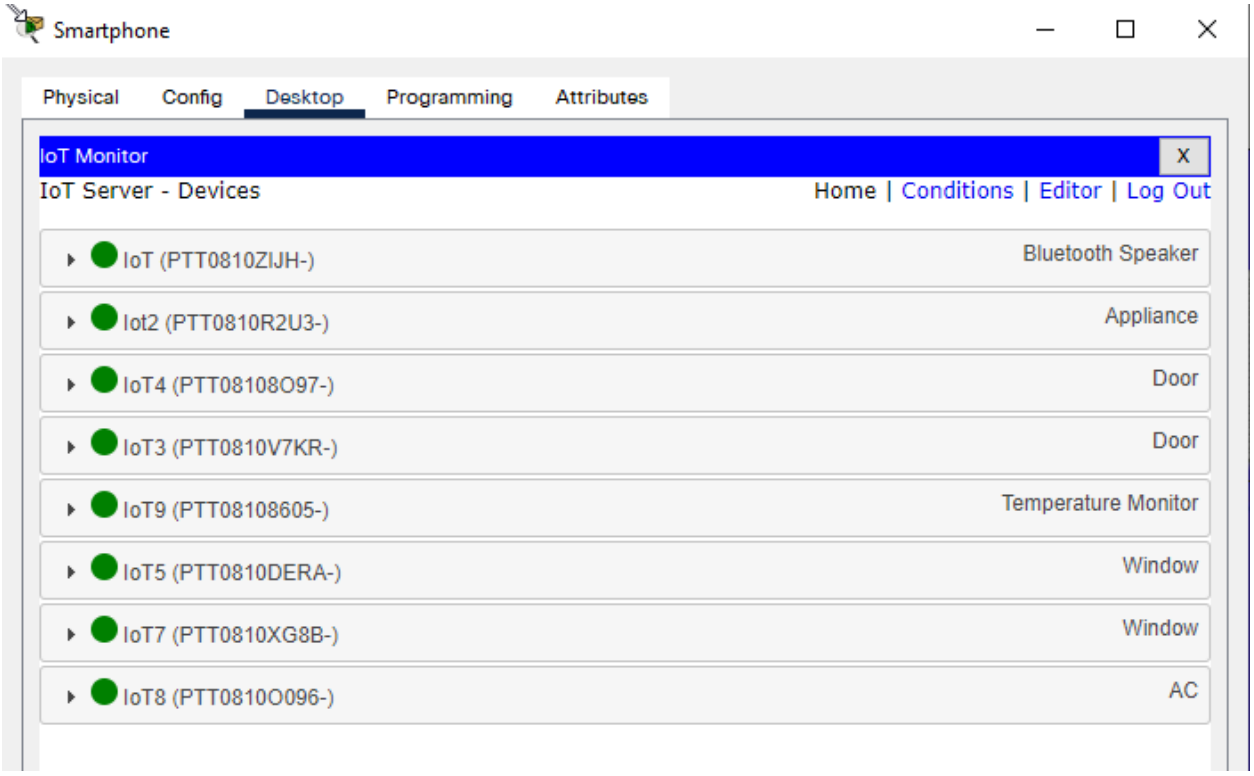
**Πίνακας 6. Διευθυνσιοδότηση συσκευών**

Παρακάτω βρίσκεται η προσομοίωση ,πως συνδέονται οι συσκευές μεταξύ τους και οι διάφοροι χώροι .



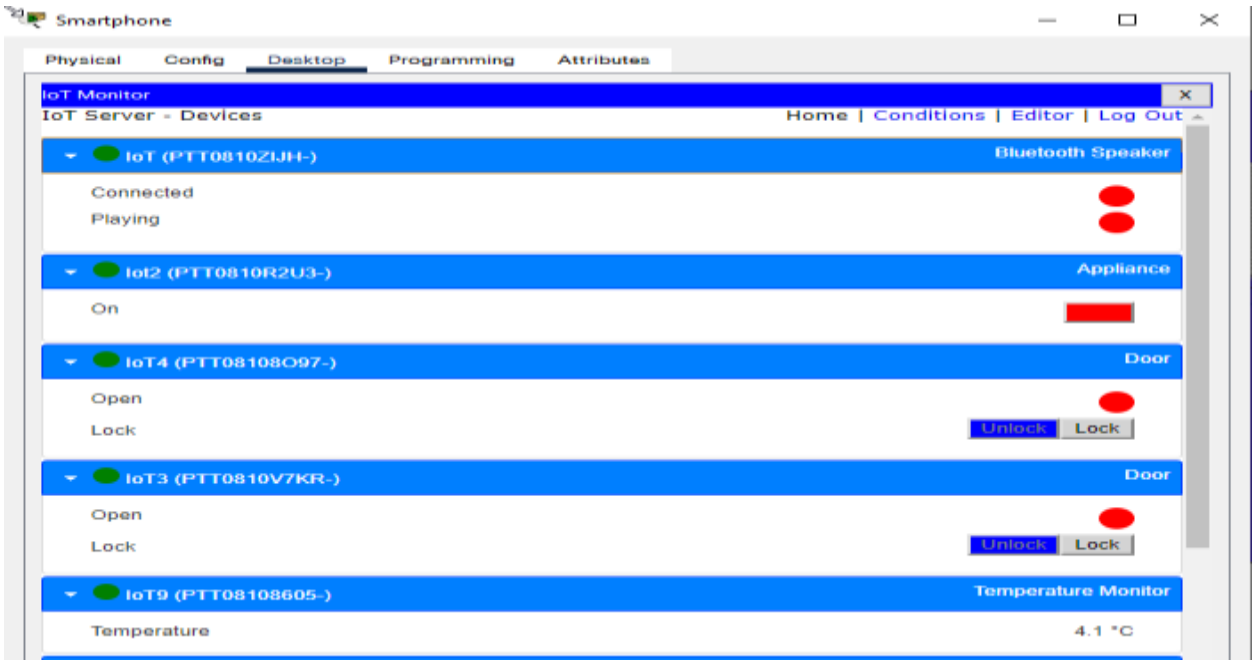
**Εικόνα 21. Σενάριο 2 –Προσοοίωση σεναρίου**

Ο χρήστης μπορεί με την εφαρμογή IoT monitor του smartphone να συνδεθεί στο interface του gateway και να συνδεθεί ως admin χρησιμοποιώντας πάντα τα σωστά διαπιστευτήρια για να κάνει τις απαραίτητες ρυθμίσεις στις συσκευές που είναι συνδεδεμένες.



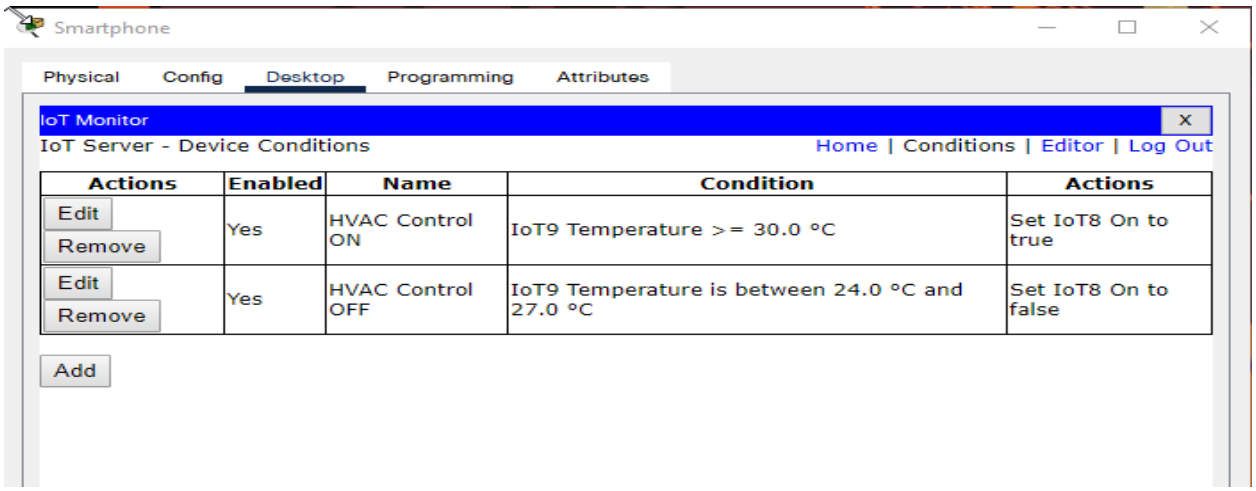

**Εικόνα 22. Είσοδος στην εφαρμογή παρακολούθησης των έξυπνων συσκευών**

Κατά την είσοδο ο χρήστης μπορεί να παραμετροποίησει τις συσκευές που είναι καταγεγραμμένες εκει  όπως πχ να ενεργοποιήσει το Bluetooth speaker η την μηχανή του καφέ.Βλέπουμε πως είναι registered όλες οι συσκευές της προσομοίωσης οπότε μπορούμε να τις παραμετροποιήσουμε.




**Εικόνα 23. Μέσα απο την εφαρμογή του smartphone θέτουμε το Bluetooth σε 'Playing' , την μηχανή του καφέ σε 'ON' , τις πόρτες 'Unlock'.**

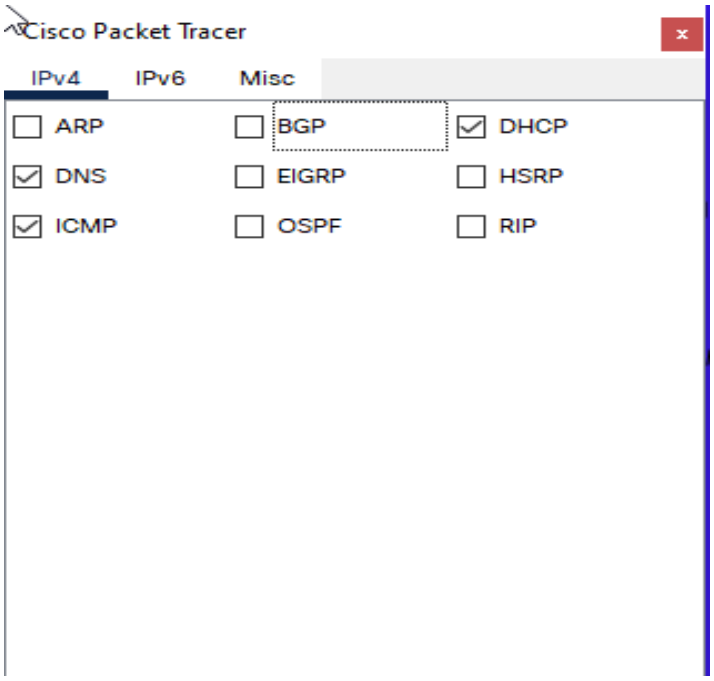
Στην συγκεκριμένη προσομοίωση έχει ενεργοποιηθεί και μια συνθήκη για δυο συσκευές. Η συνθήκη λέει πως όταν η θερμοκρασία ανέβει πολύ μέσα στο δωμάτιο να ανοίξει το κλιματιστικό για να δροσίσει.




**Εικόνα 24. Έλεγχος του κλιματισμού**

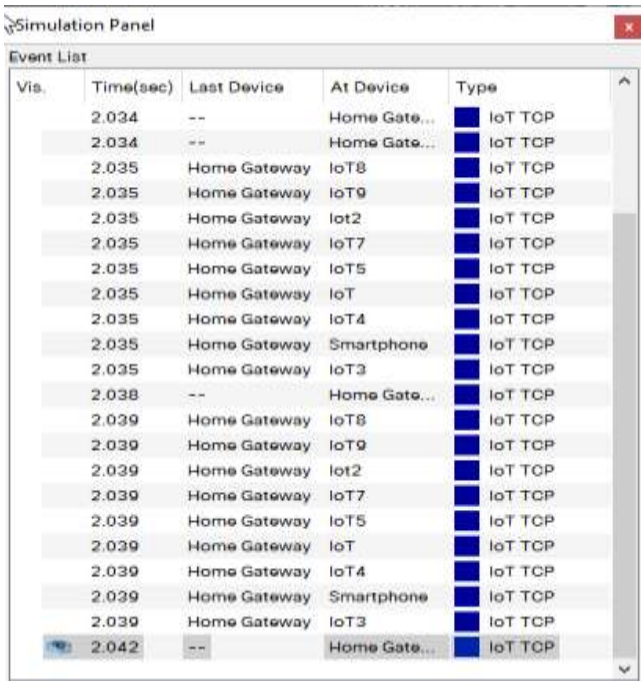
Πιο συγκεκριμένα η συνθήκη λέει πως όταν η θερμοκρασία στο δωμάτιο είναι μεγαλύτερη ή ίση των 30 βαθμών κελσίου να ενεργοποιηθεί το κλιματιστικό.Όταν η θερμοκρασία είναι ανάμεσα σε 24 και 27 βαθμούς κελσίου τότε το κλιματιστικό να σβήσει.Έχουμε φτιάξει έτσι ένα αυτόματο σύστημα κλιματισμού που κρατάει την θερμοκρασία πάντα σε επίπεδα που επιθυμεί ο χρήστης.

Στο επίπεδο προσομοίωσης μπορούν να χρησιμοποιηθούν μια γκάμα πρωτοκόλλων αναλόγως με τις ανάγκες του δικτύου προσομοίωσης ARP ,DNS , ICMP,BGP,EIGRP,OSPF,DHCP,HSRP και RIP.Για την προσομοίωση αυτήν επιλέχθηκαν μόνο τα πρωτόκολλα για DNS , ICMP και DHCP.



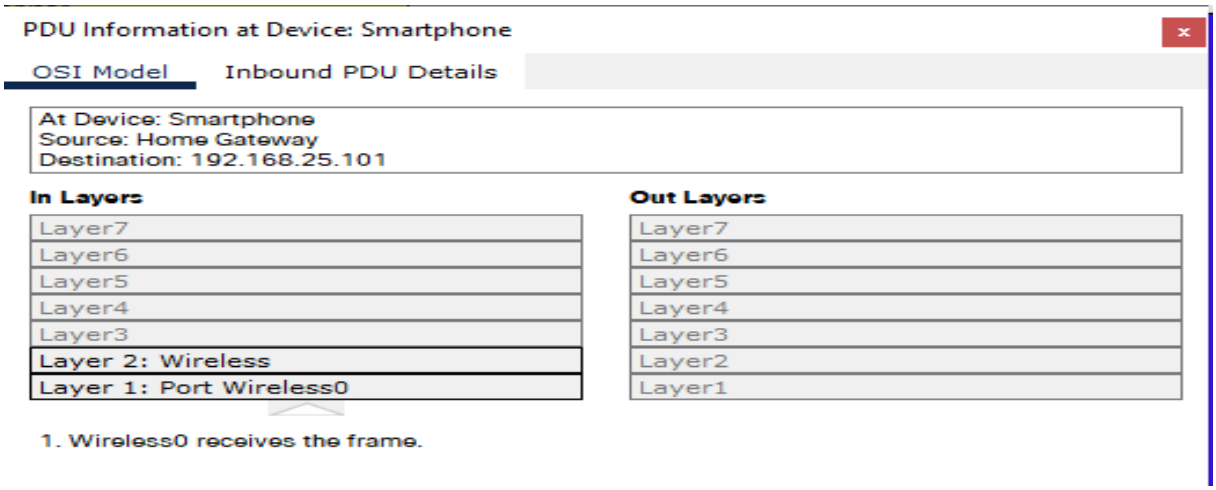

**Εικόνα 25. Πρωτόκολλα Cisco Packet Trace**

Στην διαδικασία προσομοίωσης μπορούμε να δούμε όλη την διαδικασία αποστολής πακέτων ,ποιά συσκευή έστειλε ποιό πακέτο και με ποιό χρησιμοποιούμενο πρωτόκολλο, ποιά συσκευή το έλαβε και την χρονική στιγμή αποστολής και λήψης.




**Εικόνα 26. Προσομοίωση σε πραγματικό χρόνο – Χρήση πρωτοκόλλων για την μεταφορά data**

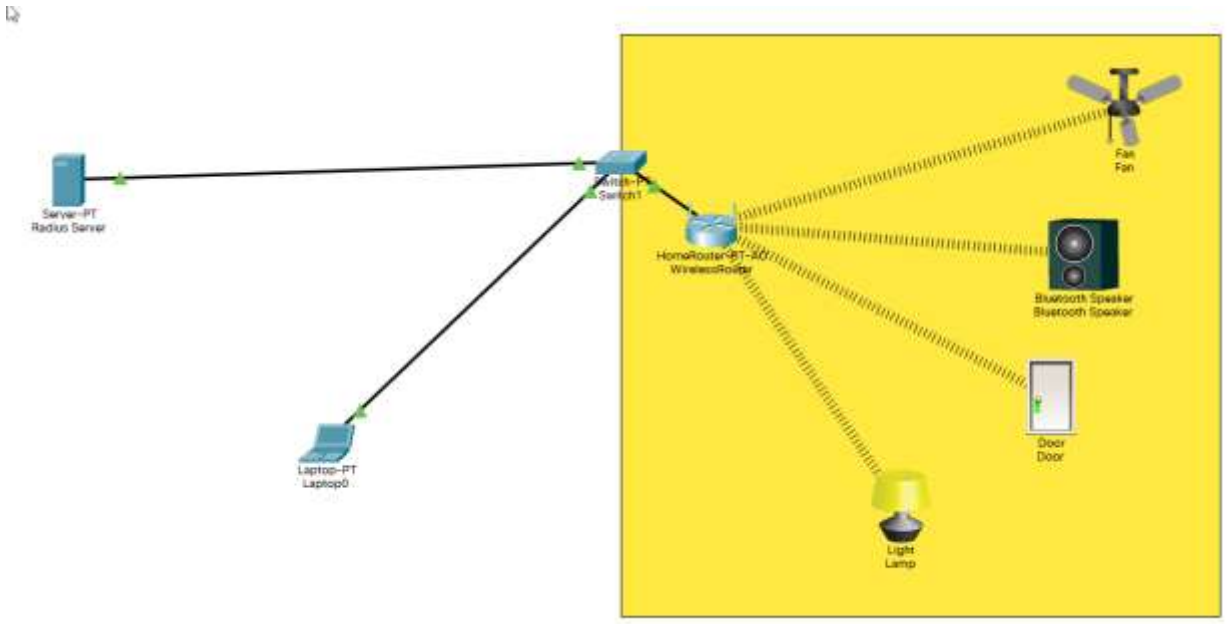
Η προσομοίωση επίσης επιτρέπει να εξετάσουμε τις πληροφορίες για το επίπεδο OSI της κάθε συσκευής καθώς και το protocol data unit.




**Εικόνα 27.Πληροφορίες σχετικά με protocol data unit και OSI frame format**

### 9.1.3 Σενάριο προσομοίωσης 3

Το 3$^{ο}$ σενάριο είναι μια προσομοίωση στην οποία οι IoT συσκευές συνδέονται και αλληλεπιδρούν μέσω ενός RADIUS server .Με την σύνδεση τους σε αυτό γίνεται η ταυτοποίηση με το πρωτόκολλο AAA(Authentication,Authorization,Accounting).Οι συσκευές συνδέονται ασύρματα σε ένα ασύρματο router.Οι συσκευές που χρησιμοποιήθηκαν είναι a)ένας RADIUS server, b)ένα λάπτοπ, c) ένα απλό switch-PT , d) ένα HomeRouter-PT-AC e) μία λάμπα , f)ένας ανεμιστήρας , g) ένα ηχείο Bluetooth Speaker ,h) και μία πόρτα.




**Εικόνα 28. Σενάριο προσομοίωσης 1**

Ο έλεγχος ταυτότητας και η εξουσιοδότηση μέσω του πρωτοκόλλου RADIUS Server είναι μια αξιόπιστη μέθοδος πρόληψης. Επιτρέπει σε ένα κεντρικό πρωτόκολλο εξουσιοδότησης , όλες οι αιτήσεις πρόσβασης περνούν από έναν μόνο διακομιστή. Ένας RADIUS server παρακολουθεί όλες τις ενέργειες των χρηστών για τη δημιουργία διαφάνειας μέσα στο δίκτυο.

## Τι είναι ένας RADIUS server;

Το RADIUS είναι ένα πρωτόκολλο δικτύωσης.Είναι υποκοριστικό στα αγγλικά για το Remote Authentication Dial-In User που είναι ο απομακρυσμένος έλεγχος ταυτοποίησης εισόδου χρήστη. Αυτό το πρωτόκολλο χρησιμοποιεί μια μέθοδο επικοινωνίας υπολογιστή-πελάτη-διακομιστή. Περιλαμβάνει διακομιστή και πελάτες.

Ένα πρόγραμμα-πελάτη RADIUS είναι μια συσκευή δικτύωσης, όπως ένας δρομολογητής, που χρησιμοποιείται για τη σύνδεση σε ένα δίκτυο ή ένας συμπυκνωτής VPN, ο οποίος δημιουργεί συνδέσεις VPN. Ο υπολογιστής-πελάτης ελέγχει τους χρήστες επικοινωνώντας με το διακομιστή.

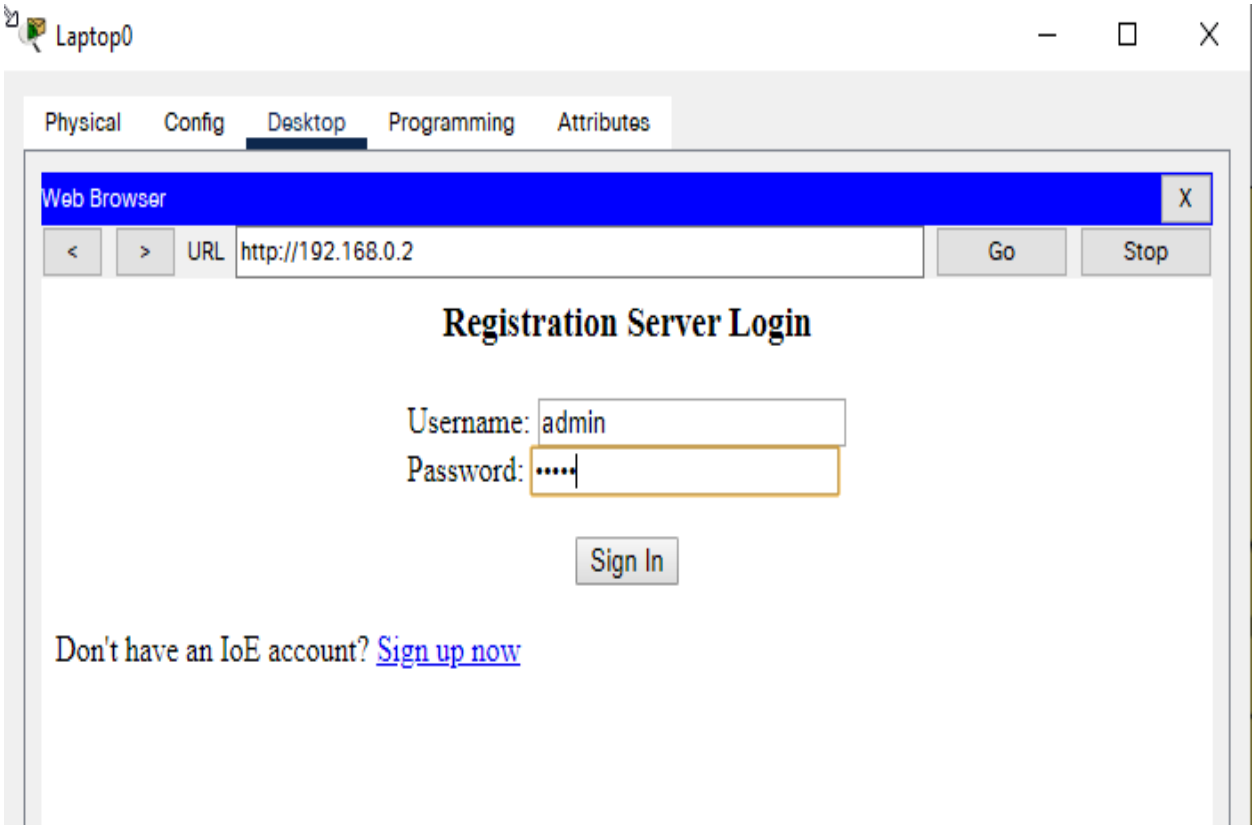
Το Radius Server είναι μια διαδικασία παρασκηνίου που εκτελείται σε μια εφαρμογή διακομιστή. Μπορεί να αποθηκεύσει και να διατηρήσει προφίλ χρηστών σε μια βάση δεδομένων, πράγμα που σημαίνει ότι ελέγχει κάθε πρόσβαση σε ένα δίκτυο. Όταν ένας χρήστης επιχειρεί να συνδεθεί με ένα πρόγραμμα-πελάτη RADIUS, στέλνει μια αίτηση στο διακομιστή. Μόνο αφού ο διακομιστής πραγματοποιήσει έλεγχο ταυτότητας και εξουσιοδοτήσει ένα χρήστη, ο διακομιστής θα εκχωρήσει σε ένα χρήστη πρόσβαση στο πρόγραμμα-πελάτη RADIUS.

## Τι είναι το AAA;

Η διαδικασία AAA έχει διευκολύνει τις εταιρείες να ελέγχουν και να εξουσιοδοτούν τους χρήστες. Πριν από την AAA, άλλα πρωτόκολλα χρησιμοποιούσαν μεμονωμένες συσκευές για έλεγχο ταυτότητας. Για παράδειγμα, ο σταθμός εργασίας ενός υπαλλήλου μπορεί να χρησιμοποιεί διαφορετική μέθοδο ελέγχου ταυτότητας σε σύγκριση με το smartphone του διευθυντή. Αυτό είναι προβληματικό για επεκτασιμότητα, επειδή κάποιος θα πρέπει να παρακολουθεί όλες τις μεθόδους ελέγχου ταυτότητας. Με την κεντρική διαδικασία AAA, οι χρήστες μπορούν να έχουν πρόσβαση σε έναν μόνο διακομιστή για έλεγχο ταυτότητας.

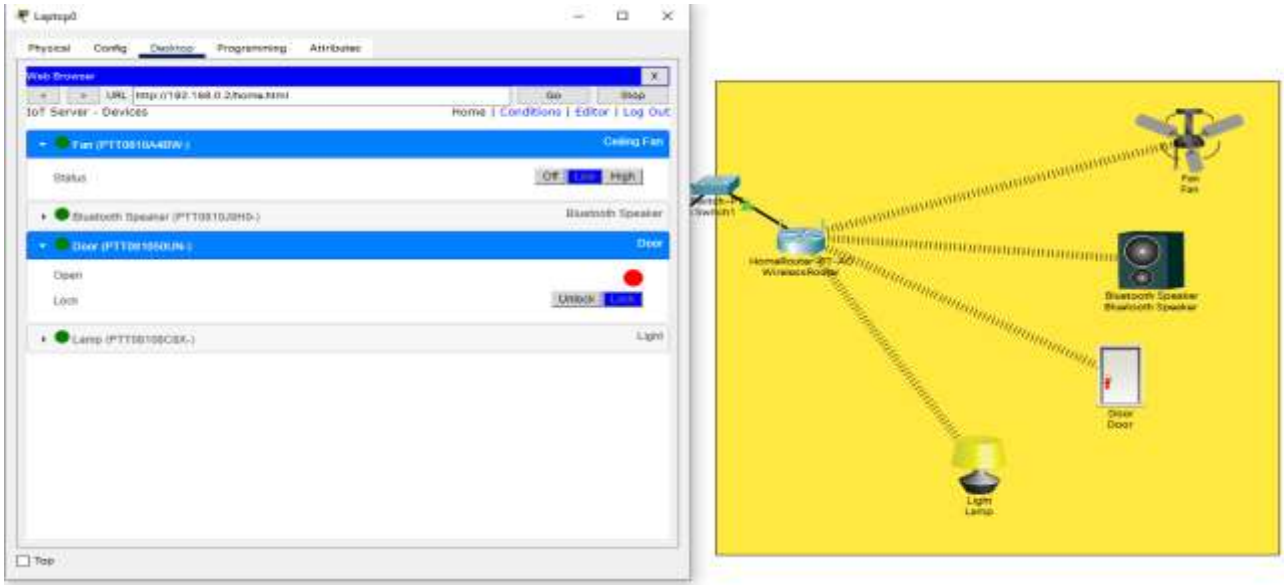
Στο τρέχον σενάριο , οι  IoT συσκευές συνδέονται στο ασύρματο ρούτερ με την διεπαφή PT-IOT-NM-1W-AC και πιστοποιείται η πρόσβαση τους.Το ρούτερ συνδέεται με ένα switch το οποίο και αυτό με την σειρά του είναι συνδεδεμένο στον RADIUS server μας.Στο switch είναι επίσης συνδεδεμένο και ένα λάπτοπ σε ενσύρματη σύνδεση.Για την διαχείρηση και

παραμετροποίηση των συσκευών ο χρήστης είναι αναγκαίο να συνδεθεί απο το λάπτοπ στον RADIUS σέρβερ πληκτρολογώντας την IP : 192.168.0.2 που αντιστοιχεί στον σέρβερ.Εκέι ταυτοποιώντας τα διαπιστευτήρια μπορεί να εισέλθει στον σέρβερ και να κάνει τις απαραίτητες ενέργειες.



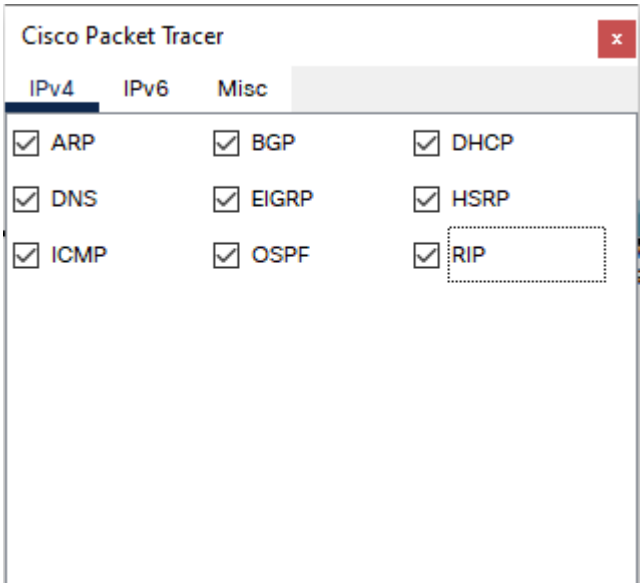

**Εικόνα 29. Είσαγωγή κωδικών πρόσβασης και ταυτοποίηση RADIUS server**

Κατά την είσοδο του μπορεί να αρχίσει να παραμετροποιεί τις IoT συσκευές όπως στην.



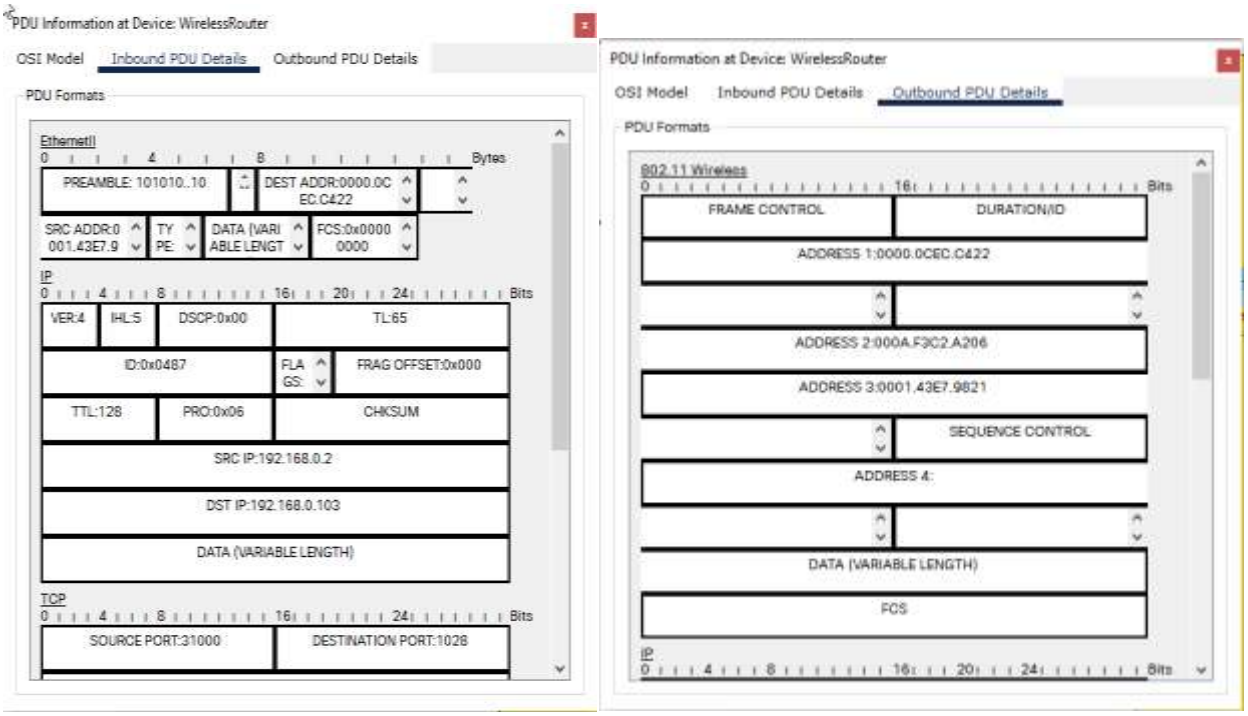
Εικόνα 30. Θέση του φωτιστικού σε “ON” και την πόρτα σε “Lock”

Στο επίπεδο προσομοίωσης μπορούν να χρησιμοποιηθούν μια γκάμα πρωτοκόλλων αναλόγως με τις ανάγκες του δικτύου προσομοίωσης  ARP, DNS, ICMP, BGP, EIGRP, OSPF,DHCP,HSRP και RIP.



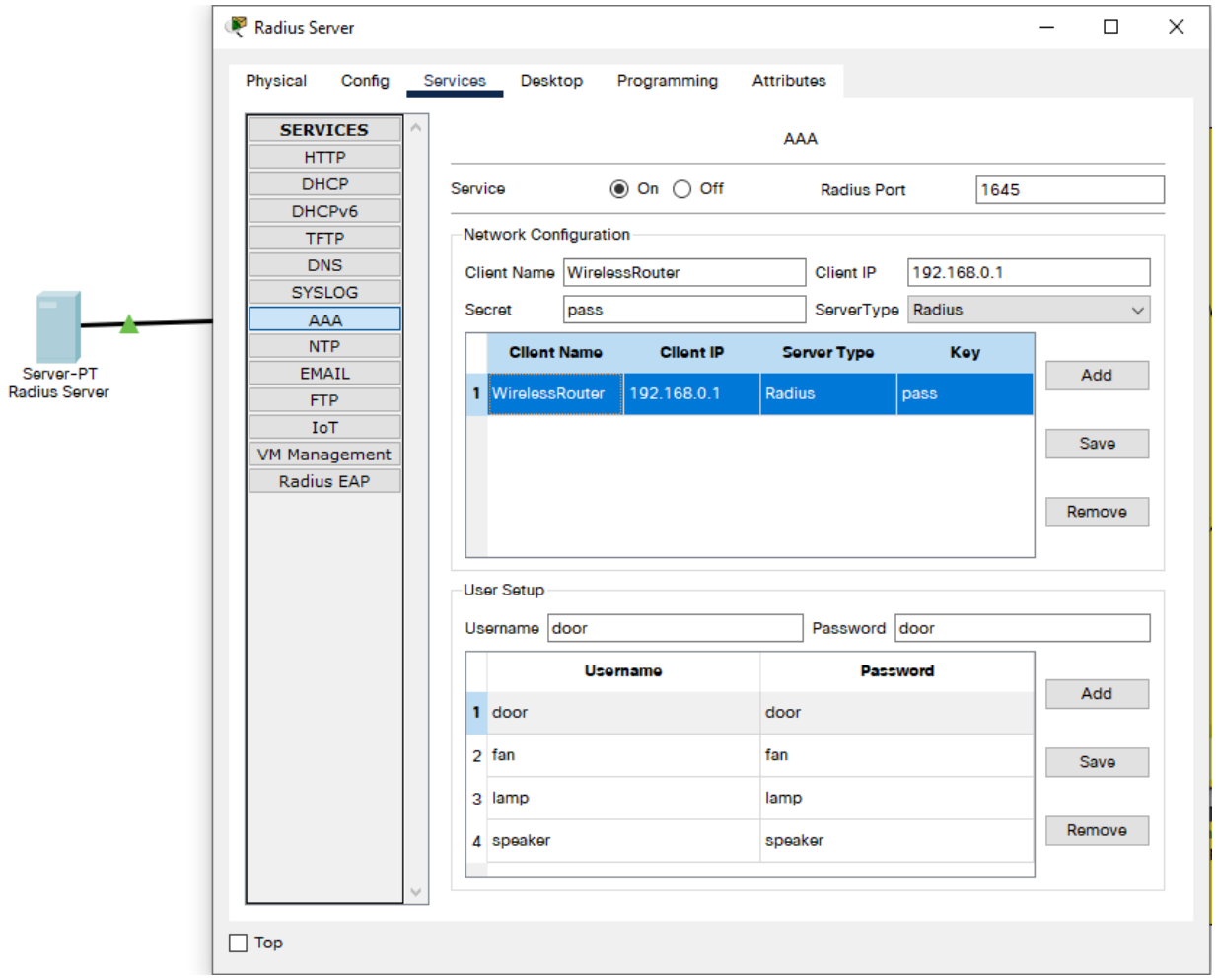

Εικόνα 31. Λίστα πρωτοκόλλων Cisco Packet Tracer

Στην διαδικασία προσομοίωσης μπορούμε να δούμε όλη την διαδικασία αποστολής πακέτων ,ποιά συσκευή έστειλε ποιό πακέτο και με ποιό χρησιμοποιούμενο πρωτόκολλο ,ποιά συσκευή το έλαβε και την χρονική στιγμή αποστολής και λήψης καθώς και πληροφορίες για τα επίπεδα OSI της κάθε συσκευής όπως και πληροφορίες για το protocol data unit.




**Εικόνα 32. Πληροφορίες επιπέδου OSI για το WirelessRouter και πληροφορίες για το PDU**

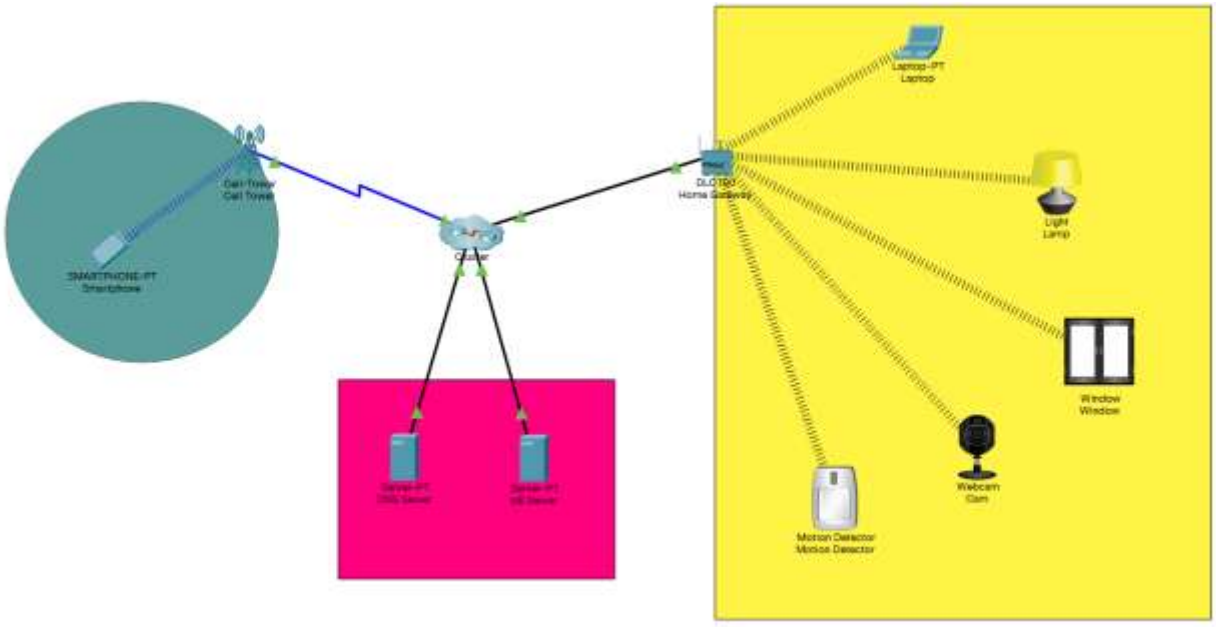
Τέλος βλέπουμε στον RADIUS server πως στην καρτέλα AAA έχουν γίνει οι απαραίτητες ρυθμίσεις για την ταυτοποίηση και καταγραφή των συσκευών καθώς και η παραμετροποιήση του Client (σαν client δουλεύει το WirelessRouter) στον οποίο θα συνδέονται όλες οι IoT συσκευές της προσομοίωσης για να γίνεται ταυτοποίηση στοιχείων.




**Εικόνα 33. Ρυθμίσεις δικτύου και παραμετροποίηση χρηστών που θα συνδέονται.Μόνο οι χρήστες που βρίσκονται στην εικόνα 9-3-6 μπορούν να συνδεθούν στον RADIUS server πχ η πόρτα , η λάμπα ,ο ανεμιστήρας , και το ηχείο.**

### 9.1.4 Σενάριο προσομοίωσης 4

Στο 4$^{ο}$ σενάριο οι IoT συσκευές αλληλεπιδρούν με το δίκτυο IoT και διαχειρίζονται μέσω μιας συσκευής smartphone.Η συσκευή αυτή συνδέεται με το δίκτυο μέσω μιας κεραίας 3G/4G και στην συνέχεια σε έναν ISP(cluster) που αναλαμβάνει όλο το διαχειριστικό κομμάτι του routing για να συνδέθει εν τέλη στο οικιακό δίκτυο IoT.Ο cluster της προσομοίωσης αποτελείται από a)ένα router cisco 2911 , b) ένα switch 2960 c)ένα cable-modem-PT , d)ένα Cloud-PT(WAN εξομοιωτής) και e)ένα Central-Office-Server.



**Εικόνα 34. Σενάριο 4 .Δημιουργία προσομοίωσης με DNS ,IoE server καθώς και τοποθέτηση κεραίας 3G/4G για την σύνδεση smartphone και απομακρυσμένου ελέγχου του IoT δικτύου.**

Για την σύνδεση των IoT και την ταυτοποιήση χρησιμοποιήθηκε ένας DNS server και ένας IoE server.Το DNS είναι υπεύθυνο να μετατρέπει μνημονικά ονόματα (domain names) στις σχετικές IP.Στο παρών σενάριο η IP του σερβερ (10.10.0.253) μετατρέπεται στο domain www.dimitfoun.com για την καλύτερη και ευκολότερη μνημονικά πρόσβαση στο IoT δίκτυο.Το υλοποιηθέν σενάριο φαίνεται στην εικόνα 34.

Παρακάτω είναι ο κώδικας του ISP για την δρομολόγηση όλης της κίνησης και της λειτούργιας του IoT δικτύου. Εικόνα 9-4-1

- **Διευθυνσιοδότηση για το DNS και IoE server**

**Router(config)#int g0/2**

**Router(config-if)#ip address 10.10.0.1 255.255.255.0**

**Router(config-if)#no shutdown**

**Interface GigabitEthernet0/2, changed state to up**

- **Διευθυνσιοδότηση για την κεράια**

  **Router(config)#int g0/0**

  **Router(config-if)#ip address 210.165.201.225 255.255.255.224**

  **Router(config-if)#no shut**

  **Interface GigabitEthernet0/0, changed state to up**

- **Διευθυνσιοδότηση για το IoT σπίτι**

  **Router(config-if)#int g0/1**

  **Router(config-if)#ip address 210.165.200.225 255.255.255.224**

  **Router(config-if)#no shut**

  **Interface GigabitEthernet0/1, changed state to up**

- **Δημιούργια DHCP pool-DNS server και default-router για όλες τις διευθνσιοδοτήσεις**

  **Router(config)#ip dhcp excluded-address 210.165.201.225 210.165.201.229**

  **Router(config)#ip dhcp pool CELL**

  **Router(dhcp-config)#network 210.165.201.224 255.255.255.224**

  **Router(dhcp-config)#default-router 210.165.201.225**

  **Router(dhcp-config)#dns-server 10.10.0.254**

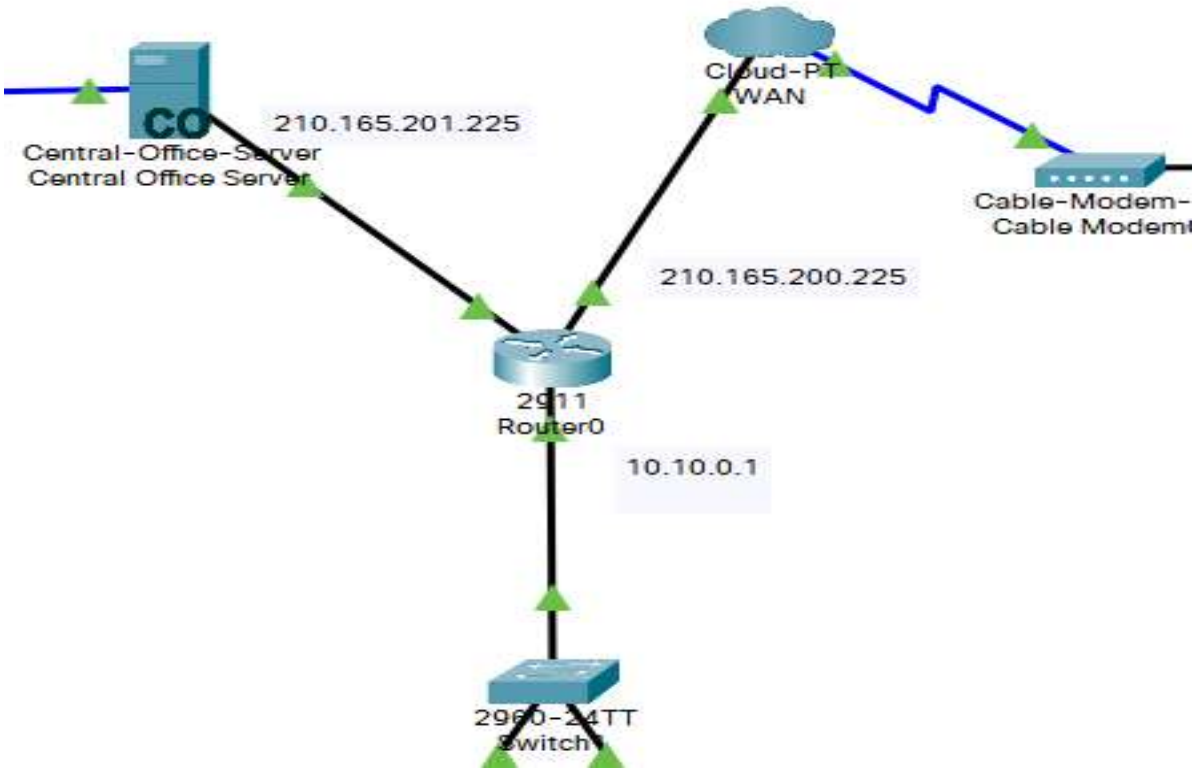
  **Router(config)#ip dhcp excluded-address 210.165.200.225 210.165.200.229**

  **Router(config)#ip dhcp pool WAN**

  **Router(dhcp-config)#network 210.165.200.224 255.255.255.224**

  **Router(dhcp-config)#default-router 210.165.200.225**

  **Router(dhcp-config)#dns-server 10.10.0.254**




**Εικόνα 35. Διευθυνσιοδοτήσεις για clients – Cluster σεναρίου**

Ένα σημαντικό κομμάτι που πρέπει να καλυφθεί για να λειτουργήσει το δυνατότερο καλύτερα το IoT δίκτυο ,είναι να γνωριζουμε το QoS.Το QoS είναι η χρήση μηχανισμών ή τεχνολογιών για τον έλεγχο της κυκλοφορίας και τη διασφάλιση της απόδοσης κρίσιμων εφαρμογών είναι η χρήση μηχανισμών ή τεχνολογιών για τον έλεγχο της κυκλοφορίας και τη διασφάλιση της απόδοσης κρίσιμων εφαρμογών. Επιτρέπει στους οργανισμούς να προσαρμόζουν τη συνολική κυκλοφορία του δικτύου τους δίνοντας προτεραιότητα σε συγκεκριμένες εφαρμογές υψηλής απόδοσης.Τα πιο σημαντικά QoS είναι :

- **Delay-** Λανθάνουσα κατάσταση είναι ο χρόνος που χρειάζεται ένα πακέτο δεδομένων για να ταξιδέψει από σημείο σε σημείο στο δίκτυο. Κάθε βήμα που κάνει η κυκλοφορία σας μέσω του δικτύου θα προσθέσει στον λανθάνοντα χρόνο του. Λανθάνουσα κατάσταση μεγαλύτερη από 150 χιλιοστά του δευτερολέπτου (ms) θα προκαλέσει αφύσικες καθυστερήσεις σε μια

συνομιλία ήχου. Σε μια βιντεοκλήση, ο υψηλός λανθάνων χρόνος θα μπορούσε να δημιουργήσει μια αποσύνδεση μεταξύ του ήχου και του βίντεο .Εάν ο λανθάνων χρόνος γίνει πολύ υψηλός, ενδέχεται να αντιμετωπίσετε περιόδους χωρίς ήχο ή βίντεο.

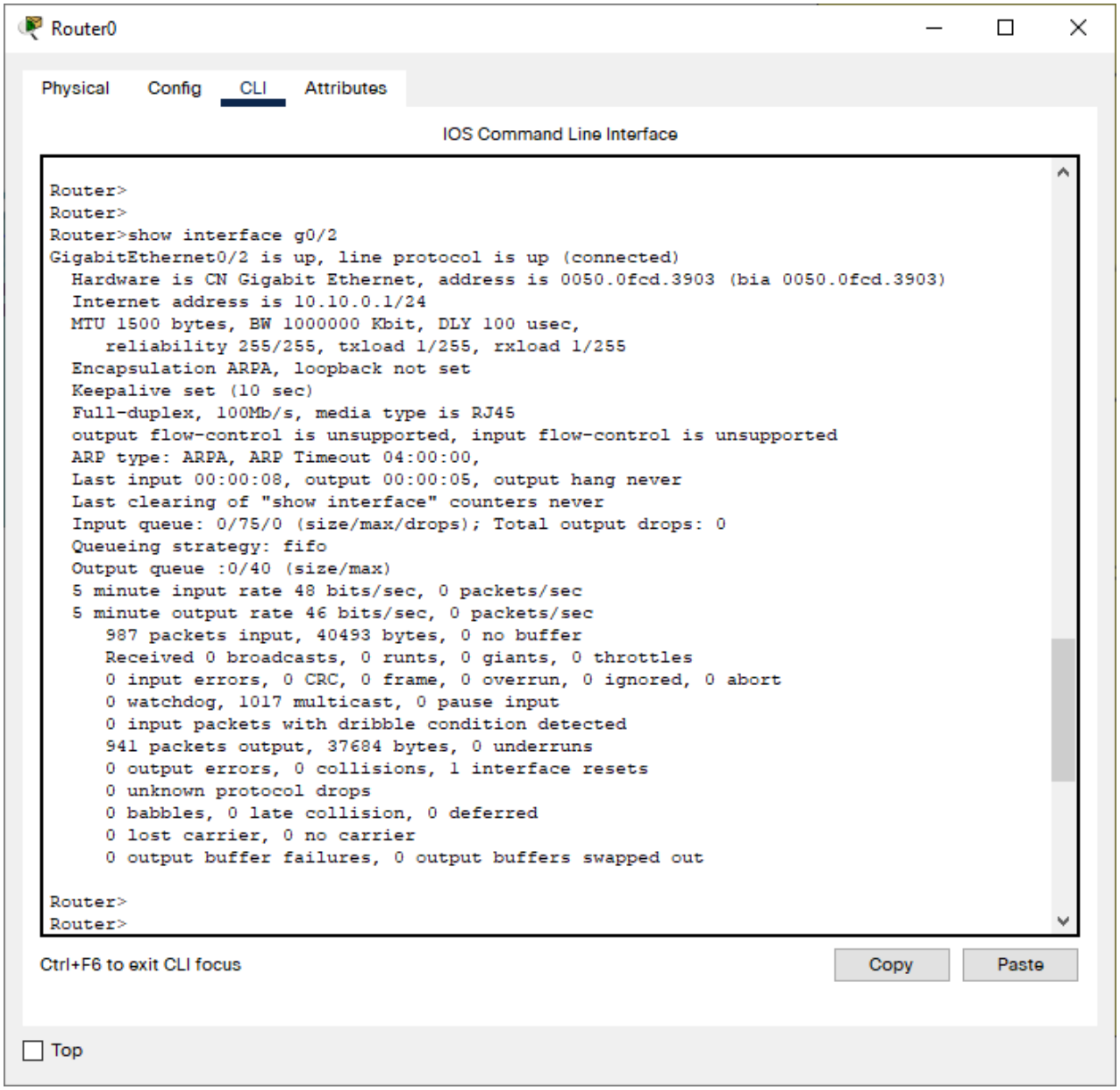
- **Jitter-**Το jitter είναι μια ασυνεπής άφιξη πακέτων μεταξύ δύο τελικών σημείων. Το Jitter άνω των 20 ms θα προκαλέσει καθυστερήσεις στην άφιξη πακέτων, οι οποίες, όπως η υψηλή καθυστέρηση, θα οδηγήσουν σε καθυστερήσεις στον ήχο ή το βίντεό σας.

- **Packet Loss-** Η απώλεια πακέτων συμβαίνει όταν ένα πακέτο δεν φτάνει, φτάνει εκτός λειτουργίας ή φτάνει πολύ αργά. Τα χαμένα πακέτα δεν πηγαίνουν σε ένα "πακέτο που χάθηκε και βρέθηκε", απλά απορρίπτονται. Η απώλεια πακέτων μέσω ενός δικτύου θα προκαλέσει ασταθή ήχο και βίντεο κακής ποιότητας. Θα πρέπει να υπάρχει ένα αρκετά υψηλό επίπεδο απώλειας πακέτων για να υποβαθμιστεί η υπηρεσία σε αυτή την κατάσταση.

- **Throughput**-Το throughput αναφέρεται στο πόσα δεδομένα μπορούν να μεταφερθούν μέσα σε ένα συγκεκριμένο χρονικό περιθώριο.Το throughput μετράει πόσα πακέτα φτάνουν στο προορισμό τους με επιτυχία.

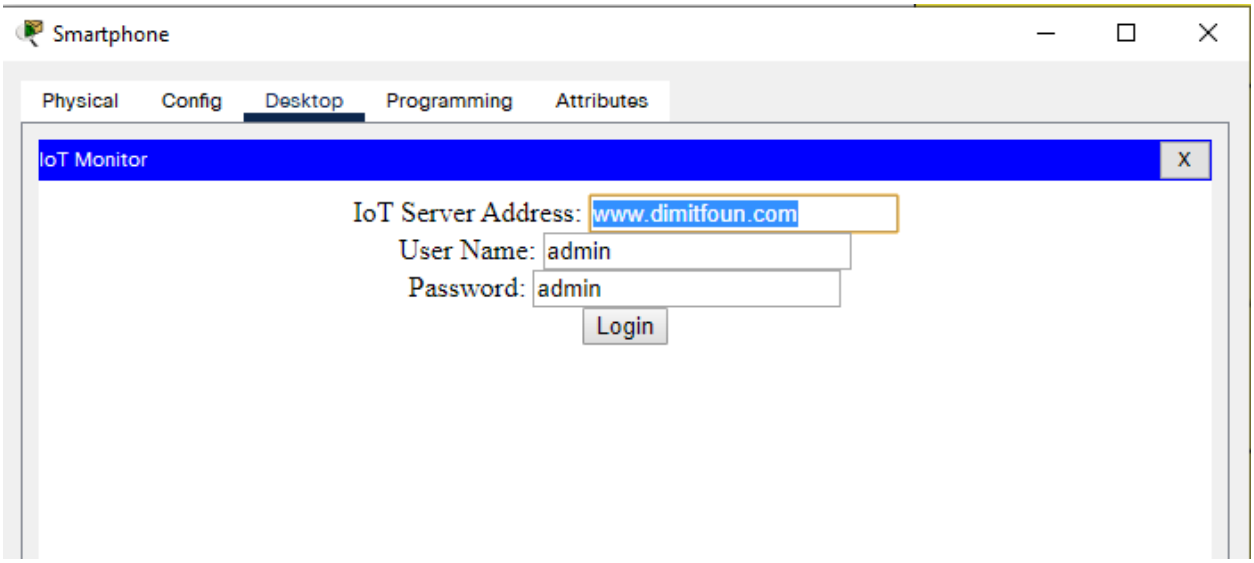
- Παράμετροι που επηρεάζουν τα παραπάνω QoS
- Ποιότητα του δικτύου
- Καθυστέρηση σειριοποίησης
- Καθυστερήσεις στο routing και switching
- Συμφόρηση
- Μη κατάλληλη τοπολογία δικτύου

Χρησιμοποιώντας την εντολή show ip interface g0/0 μπορούμε να δούμε κα τα χαρακτηριστικά απο για τις διεπαφές δικτύου των δικτυακών μας συσκευών **Εικόνα 9-4-3**



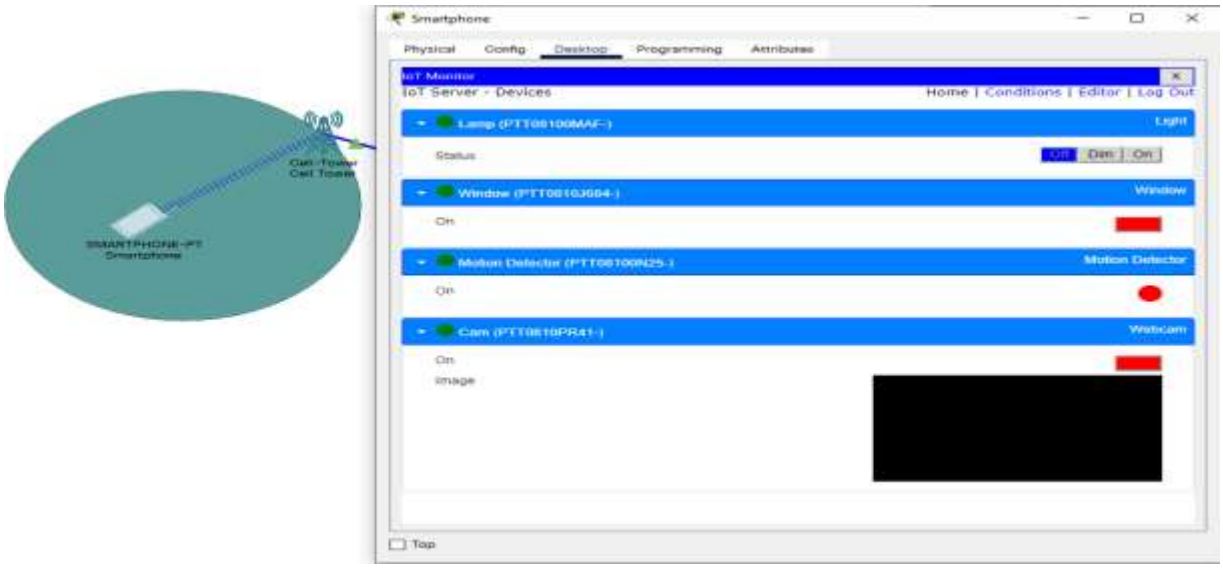

**Εικόνα 36. Χαρακτηριστηκά για την διεπαφή g0/2 (DNS-IoE server)**

Με την ολοκλήρωση της προσομοίωσης ο χρήστης μπορεί να συνδεθεί στην κέραια 3G/4G και να ελέγξει η να τροποιήσει το IoT δίκτυο. Ανοίγωντας την εφαρμογή IoT monitor πληκτρολογώντας την IP του DNS server (ή το domain name www.dimitfoun.com ) και των απαραίτητων διαπιστευτηρίων .




**Εικόνα 37. Ελέγχος διαπιστευτηρίων κατα την είσοδο στον server μέσω της σελίδας www.dimitfoun.com**

Κατά την είσοδο εμφανίζονται όλες οι εγγεγραμένες IoT συσκευές και ο χρήστης είναι εύκολο να τις παραμετροποιήσει.



**Εικόνα 38. Παραμετροποίηση των IoT συσκευών απομακρυσμένα με σύνδεση του κινητού τηλεφώνου σε κέραια κινητής τηλεφωνίας στο IoT δίκτυο.**

# Βιβλιογραφία


Al Sukkar, G. &. (2016). *Address Resolution Protocol (ARP): Spoofing Attack and Proposed Defense. Communications and Network.*

Al-Sarawi, S. A. (2017). *Internet of Things (IoT) communication protocols.*

Alshammari, A. (2019). *INTERNET OF THINGS OBJECTIVES, BENEFITS, AND APPLICATIONS.*

Bhuvaneswari, R. P. (2014). *The Internet of Things (IoT) Applications and Communication Enabling Technology Standards: An Overview.*

Chandrashekhar, K. (2016). *Internet of Things (IoT) Characteristics.* Linkedin.

Clarke, R. (2010). *User Requirements for Cloud Computing Architecture.* Melbourne: Proc. 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing.

D.Foote, K. (2018). *A Brief History of the Internet of Things.*

Domb, M. (2019). Smart Home Systems Based on Internet of Things. *Interchopen* .

Gandotra, P. &. (2016). *A Survey on Device-to-Device (D2D) Communication: Architecture and Security Issues. Journal of Network and Computer Applications.*

Harper, R. (2006). *Inside the Smart Home.* Springer Science & Business Media.

Husein, A. (2018). *Bellman Ford algorithm - in Routing Information Protocol (RIP).*

istu, S. &. (2019). *Performance Evaluation of Thread Protocol based Wireless Mesh Networks for Lighting Systems.*

J. Wurm, K. H. (2016). *Security analysis on consumer and industrial IoT devices," 2016 21st Asia and South Pacific Design Automation Conference.*

Jayapal, C. (2019). *Security Protocols for IoT.* Kumaraguru.

Khajenasiri, I. E. (2017). *A review on Internet of Things solutions for intelligent energy control in buildings for smart city applications.*

Malche, T. (2017). *Internet of Things (IoT) for building Smart Home System.*

Malche, T. (2017). *Internet of Things (IoT) for building Smart Home System.*

Michael Armbrust, A. F. (2010). *A view of cloud computing.* ACM.

N. Neshenko, E. B.-H. (2019). *Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations.*

Naveen, S. (2016). *Study of IoT: Understanding IoT Architecture, Applications, Issues and Challenges.*

Odii, J. &. (2016). *An Overview of Security Issues Relating to the Internet of Things.*

Qusay f. Hassan, P. ,. (2018). *Internet of Things A to Z: Technologies and Applications.* Hangzhou Dianzi Univercity.

R. Mahmoud, T. Y. (2015). *Internet of things (IoT) security: Current status, challenges and prospective measures.*

R. Mahmoud, T. Y. (2015). *Internet of things (IoT) security: Current status, challenges and prospective measures.*

Ragheb, A. &. (2015). *Green Architecture: A Concept of Sustainability. Procedia - Social and Behavioral Sciences.* Appraisal Institute.

S. Krčo, B. P. (2014). *Designing IoT architecture(s): A European perspective.* IEEE.

Sarawi, S. &. (2017). *Internet of Things (IoT) Communication Protocols.*

Sinha, r. G. (2001). *Introduction to IoT.*

Stergiou, C. &.-G. (2016). *Secure integration of IoT and Cloud Computing. Future Generation Computer Systems.*

Tadimety, P. R. (2015). *OSPF: A network routing protocol.*

Tim Mather, S. K. (2009). *Cloud Security and Privacy.* O'REILLY.