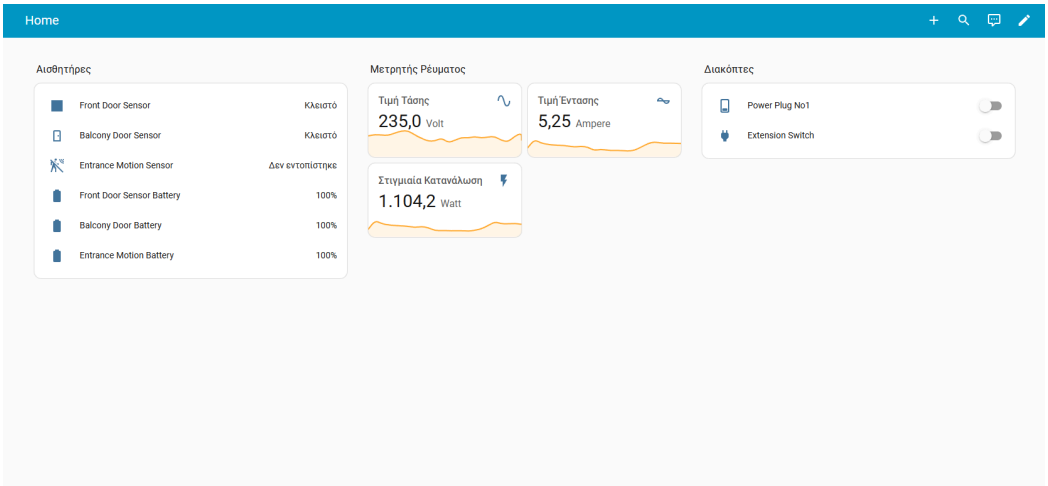
ΔΙΕΘΝΕΣ
ΠΑΝΕΠΙΣΤΗΜΙΟ
ΤΗΣ ΕΛΛΑΔΟΣ

ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Μελέτη, σχεδίαση και κατασκευή ενός έξυπνου σπιτιού (Smart Home) με τη χρήση Raspberry Pi»



Του φοιτητή
Γίδαρη Δημητρίου
Αρ. Μητρώου: 517019

Επιβλέπουσα
Μαρία Παπαδοπούλου
Επίκουρη Καθηγήτρια

Ημερομηνία 01-09-2025

Τίτλος Δ.Ε.: Μελέτη, σχεδίαση και κατασκευή ενός έξυπνου σπιτιού (Smart Home) με τη χρήση Raspberry Pi

Κωδικός Δ.Ε.: 24124

Ονοματεπώνυμο φοιτητή: Γίδαρης Δημήτριος

Ονοματεπώνυμο εισηγητή: Παπαδοπούλου Μαρία

Ημερομηνία ανάληψης Δ.Ε. 20-02-2024

Ημερομηνία περάτωσης Δ.Ε. 01-09-2025

Βεβαιώνω ότι είμαι ο συγγραφέας αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω καταγράψει τις όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών, εικόνων και κειμένου, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επιπλέον, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά, ειδικά ως διπλωματική εργασία, στο Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του ΔΙ.ΠΑ.Ε.

Η έγκριση της διπλωματικής εργασίας από το Τμήμα Μηχανικών Πληροφορικής και Ηλεκτρονικών Συστημάτων του Διεθνούς Πανεπιστημίου της Ελλάδος, δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα, εκ μέρους του Τμήματος.

Πρόλογος

Η καλπάζουσα ροή της τεχνολογίας, ολοένα και περισσότερο εισχωρεί στην καθημερινότητά μας, επηρεάζοντας τον τρόπο που ζούμε, εργαζόμαστε και αλληλεπιδρούμε με τον χώρο μας. Με την πάροδο του χρόνου, οι απαιτήσεις και οι ανάγκες που γεννιούνται γύρω από αυτήν αυξάνονται, οδηγώντας σε λύσεις που συνδυάζουν την ευκολία, την εξοικονόμηση πόρων και την ασφάλεια. Η παρούσα υλοποίηση της πτυχιακής εργασίας έρχεται να απαντήσει σε αυτές τις ανάγκες, καθώς στοχεύει στη δημιουργία αυτοματοποιημένων συνθηκών μέσα στον χώρο της οικίας, προσφέροντας σημαντικά πλεονεκτήματα. Από τη μία πλευρά, δίνεται η δυνατότητα για μείωση της κατανάλωσης ενέργειας, μέσω της βέλτιστης διαχείρισης συσκευών και φορτίων, ενώ από την άλλη ενισχύεται η άνεση και η διευκόλυνση της καθημερινής διαβίωσης.

Περίληψη

Η παρούσα πτυχιακή εργασία έχει ως αντικείμενο τη μελέτη, τον σχεδιασμό και την υλοποίηση ενός έξυπνου σπιτιού με χρήση του Raspberry Pi και της πλατφόρμας Home Assistant. Στόχος της ήταν η ανάπτυξη ενός ολοκληρωμένου συστήματος που επιτρέπει την απομακρυσμένη και ασφαλή πρόσβαση, την ενσωμάτωση αισθητήρων και συσκευών και τη δημιουργία αυτοματισμών για τη βελτίωση της καθημερινής διαβίωσης. Μέσα από την υλοποίηση αποδείχθηκε ότι με τη χρήση ανοικτού λογισμικού και οικονομικού εξοπλισμού μπορεί να επιτευχθεί ένα πλήρως λειτουργικό και αποδοτικό σύστημα έξυπνου σπιτιού. Το τελικό αποτέλεσμα περιλαμβάνει ένα κεντρικό ταμπλό παρακολούθησης και ελέγχου των συσκευών, την αξιοποίηση δεδομένων από αισθητήρες για την εξοικονόμηση ενέργειας και τη δυνατότητα δημιουργίας αυτοματισμών με βάση συνθήκες, όπως η τοποθεσία του χρήστη ή η κατανάλωση ρεύματος. Τα αποτελέσματα δείχνουν ότι η συγκεκριμένη υλοποίηση μπορεί να συμβάλει ουσιαστικά στη μείωση της ενεργειακής κατανάλωσης, στην αύξηση της ασφάλειας και στη διευκόλυνση της καθημερινότητας, επιβεβαιώνοντας ότι οι τεχνολογίες έξυπνου σπιτιού είναι πλέον εφαρμόσιμες σε πρακτικό και οικονομικό επίπεδο.

Design and implementation of a Smart Home System using Raspberry Pi

Dimitrios Gidaris

Abstract

This thesis focuses on the study, design, and implementation of a smart home using a Raspberry Pi and the Home Assistant platform. Its goal was to develop an integrated system that enables secure remote access, seamless integration of sensors and devices, and the creation of automations to improve everyday living.

Through the implementation, it was demonstrated that with open-source software and affordable hardware, it is possible to build a fully functional and efficient smart home system. The final result includes a central dashboard for monitoring and controlling devices, the utilization of sensor data for energy saving, and the ability to create automations based on conditions such as the user's location or the household's energy consumption.

The results show that this implementation can significantly contribute to reducing energy consumption, enhancing security, and facilitating daily life, confirming that smart home technologies are now practical and economically feasible.

Ευχαριστίες

Θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες στην οικογένειά μου και στη σύντροφό μου, οι οποίοι στάθηκαν αδιάκοπα δίπλα μου, προσφέροντάς μου ηθική, πνευματική και οικονομική στήριξη καθ' όλη τη διάρκεια της προσπάθειάς μου. Ιδιαίτερη ευγνωμοσύνη οφείλω στην επιβλέπουσα καθηγήτριά μου, κα. Μαρία Παπαδοπούλου, για την άριστη συνεργασία και την πολύτιμη καθοδήγησή της. Τέλος, θα ήθελα να ευχαριστήσω τον μέντορά μου, κ. Χαράλαμπο Τιφτικίδη, για την αστείρευτη γνώση και εμπειρία που απλόχερα μοιράστηκε μαζί μου.

Περιεχόμενα

Πρόλογος....3
Περίληψη....4
Design and implementation of a Smart Home System using Raspberry Pi....5
Abstract....5
Ευχαριστίες....6
Περιεχόμενα....7
Εισαγωγή....9
Κεφαλαιο 1ο: Τι ονομάζουμε Smart Home....10
1.1: ΚΑΤΗΓΟΡΙΕΣ ΔΙΚΤΥΩΝ....11
1.1.1: Personal Area Network (PAN)....11
1.1.2: Local Area Network (LAN)....11
1.1.3: Wireless Local Area Network (WLAN)....12
1.1.4: Wide Area Network (WAN)....15
1.1.5: Άλλες κατηγορίες δικτύων....15
1.2: Μοντελο OSI....16
1.3: Internet Protocol Version 4....17
1.4: Θύρες δικτύου....18
1.5: Virtual LAN....20
1.6: DHCP....21
1.7: Network Address Translation....23
1.8: Carrier Grade NAT....24
1.9: Zigbee....25
1.10: Υπέρυθρη Επικοινωνία....27
1.11: Ραδιοσυχνότητα....28
1.12: Bluetooth....30
1.13: Port Forwarding....32
1.14:Σύνδεση Μέσω Cloud....33
1.15: VPN (Virtual Private Network)....35
1.16: Transport Layer Security (TLS)....38
1.17:Cloudflare....40
1.18: Τείχος Προστασίας (Firewall)....41
1.19: Web Access Firewall....43
1.20: Conteinerization....44
1.21: Virtual Machine....45
1.23: Containerization Vs VM....46
Κεφάλαιο 2ο: Raspberry Pi....48
2.1: Home Assistant....50
2.2: YAML (YAML Ain’t Markup Language)....52
2.3: Passive Infrared Sensors (PIR)....54
2.4: Αισθητήρες Παρουσίας....55
2.5: Αισθητήρες Φωτεινότητας....56

2.7: Αισθητήρες Θυρών..... 57
2.8:Ενδιάμεσοι Διακόπτες..... 58
2.9: Μετρητές Τάσης, Κατανάλωσης και Ρεύματος..... 60
2.10: Φωνητική εντολή μέσω Google Home..... 62
2.11: Φωνητική εντολή μέσω Amazon Alexa..... 62
2.12: DNS Server..... 63
Κεφάλαιο 3ο: Εγκατάσταση και υλοποίηση ενος Smart Home χρησιμοποιώντας τον Home Assistant σε Raspberry Pi..... 65
3.1: Υλοποίηση VPN , DNS Server, Tunnel και μέτρων ασφαλείας..... 68
3.2: Παραμετροποίηση εξοπλισμού και ενεργοποίηση τελικού συστήματος..... 76
3.3: Παραμετροποίηση της αρχικης σελιδας (Lovelace)..... 81
3.4: Εφαρμογή για το κινητό και geotracking..... 85
3.5: Δημιουργία αυτοματισμών..... 86
Κεφάλαιο 4ο: Συμπέρασμα..... 89
Βιβλιογραφία..... 91

Εισαγωγή

Η συνεχής εξέλιξη των τεχνολογιών αυτοματισμού και του Διαδικτύου των Πραγμάτων (IoT) έχει καταστήσει εφικτή την ανάπτυξη ολοκληρωμένων συστημάτων «έξυπνης κατοικίας». Ένα «έξυπνο σπίτι» συνδυάζει αισθητήρες, ελεγκτές και λογισμικό διαχείρισης με στόχο την αυτοματοποίηση καθημερινών διαδικασιών, την ενεργειακή βελτιστοποίηση και την αύξηση της άνεσης των χρηστών. Στο πλαίσιο αυτό το Raspberry Pi αποτελεί έναν αξιόπιστο και οικονομικά προσιτό μικροϋπολογιστή, ικανό να λειτουργήσει ως κεντρικός ελεγκτής για την ολοκλήρωση ετερογενών συσκευών και πρωτοκόλλων. Η παρούσα πτυχιακή εργασία εστιάζει στη μελέτη, τον σχεδιασμό και την υλοποίηση ενός συστήματος έξυπνου σπιτιού με τη χρήση Raspberry Pi και της πλατφόρμας Home Assistant. Στην εργασία αξιοποιούνται συσκευές τεχνολογίας Zigbee και Wi-Fi, οι οποίες εντάσσονται σε ένα ενιαίο περιβάλλον ελέγχου και επιτήρησης, με δυνατότητα ασφαλούς απομακρυσμένης πρόσβασης μέσω Cloudflare Tunnel. Επιπλέον, αναπτύσσονται ταμπλό για την απεικόνιση μετρήσεων, την παρακολούθηση αισθητήρων και την άμεση διαχείριση διακοπτών, ενώ υλοποιούνται αυτοματισμοί που βασίζονται σε πραγματικά σενάρια χρήσης, όπως η ενεργειακή παρακολούθηση, η ασφάλεια του χώρου και η γεωεντοπισμένη αλληλεπίδραση.

Μέσα από την υλοποίηση αυτής της εργασίας αποδεικνύεται ότι η χρήση ανοικτού λογισμικού και οικονομικού εξοπλισμού μπορεί να οδηγήσει στη δημιουργία ενός αξιόπιστου, επεκτάσιμου και αποδοτικού συστήματος, το οποίο καλύπτει τις σύγχρονες ανάγκες ενεργειακής διαχείρισης και αυτοματοποίησης σε οικιακό περιβάλλον.

Κεφαλαιο 1ο: Τι ονομάζουμε Smart Home

Η έννοια του έξυπνου σπιτιού (Smart Home) αποτελεί έναν από τους πλέον χαρακτηριστικούς όρους της σύγχρονης ψηφιακής εποχής, όπου η καθημερινή ζωή του ανθρώπου διαπλέκεται με την τεχνολογία. Παρόλο που στην κοινή συνείδηση το "έξυπνο σπίτι" συχνά συνδέεται με φωνητικούς βοηθούς ή τηλεχειριστήρια για φώτα και ρολά, η πραγματικότητα είναι πολύ βαθύτερη και πιο δομημένη τεχνολογικά. Κατά βάση, ένα έξυπνο σπίτι είναι ένας χώρος διαβίωσης στον οποίο επιμέρους συσκευές και υποσυστήματα είναι διασυνδεδεμένα μεταξύ τους και μπορούν να αλληλεπιδρούν, να παρακολουθούνται ή και να ελέγχονται είτε τοπικά είτε εξ αποστάσεως, με σκοπό την αυτοματοποίηση λειτουργιών, την εξοικονόμηση ενέργειας, την ενίσχυση της ασφάλειας και τη βελτίωση της καθημερινής άνεσης των ενοίκων του. Ο όρος δεν παραπέμπει απλώς στη χρήση «έξυπνων» συσκευών με δυνατότητα σύνδεσης στο διαδίκτυο. Στην πραγματικότητα, πρόκειται για την ολοκλήρωση διαφορετικών τεχνολογιών, αισθητήρων, πρωτοκόλλων επικοινωνίας και κεντρικών συστημάτων ελέγχου, έτσι ώστε να δημιουργηθεί ένα ενιαίο ψηφιακό οικοσύστημα το οποίο μπορεί να "αντιλαμβάνεται" το περιβάλλον, να παίρνει αποφάσεις ή να ακολουθεί προκαθορισμένες εντολές από τον χρήστη του.

Η βασική αρχιτεκτονική ενός έξυπνου σπιτιού οργανώνεται γύρω από τρεις θεμελιώδεις άξονες, οι οποίοι συνεργάζονται αρμονικά ώστε να διασφαλίζεται η λειτουργικότητα, η αυτοματοποίηση και η απομακρυσμένη διαχείριση του συστήματος. Ο πρώτος άξονας περιλαμβάνει τους αισθητήρες, δηλαδή τα επιμέρους στοιχεία που έχουν ως ρόλο τη συλλογή πληροφοριών από το φυσικό περιβάλλον ή την άμεση αλληλεπίδραση με αυτό. Σε αυτήν την κατηγορία ανήκουν αισθητήρες θερμοκρασίας, υγρασίας, κίνησης, παγιδών πόρτας, καπνού, διοξειδίου του άνθρακα, φωτεινότητας, καθώς και διακόπτες κάθε είδους, όπως ρελέ, έξυπνοι λαμπτήρες, ηλεκτροκίνητα ρολά και πρίζες. Οι εν λόγω συσκευές επικοινωνούν με το υπόλοιπο σύστημα είτε μέσω ενσύρματων συνδέσεων είτε με χρήση ασύρματων πρωτοκόλλων, όπως Wi-Fi, Zigbee, Z-Wave και Bluetooth Low Energy. Ο δεύτερος άξονας αφορά το κεντρικό σύστημα ελέγχου (Home Automation Hub), το οποίο αποτελεί τον πυρήνα λειτουργίας του έξυπνου σπιτιού. Ο κόμβος αυτός είναι επιφορτισμένος με τη συλλογή των δεδομένων από τους αισθητήρες, την αποθήκευση, επεξεργασία και αξιολόγησή τους, καθώς και με τη λήψη αποφάσεων βάσει προκαθορισμένων σεναρίων ή δυναμικών κανόνων. Η υλοποίησή του μπορεί να γίνει μέσω ενός Raspberry Pi, ενός υπολογιστή, ενός εμπορικού Zigbee ή Z-Wave hub, ή ακόμα και μέσω ενός αποκλειστικού server. Παράλληλα, το κεντρικό σύστημα διασφαλίζει τη λειτουργία της διεπαφής χρήστη (UI), καθώς και τη δυνατότητα επικοινωνίας με εξωτερικά API ή υπηρεσίες cloud.

Τέλος, ο τρίτος άξονας σχετίζεται με τους μηχανισμούς ελέγχου και πρόσβασης, δηλαδή τα μέσα μέσω των οποίων ο χρήστης μπορεί να αλληλεπιδρά με το σύστημα. Ο έλεγχος πραγματοποιείται μέσω κινητών τηλεφώνων, tablet, προσωπικών υπολογιστών ή φωνητικών εντολών, ενώ για την ασφαλή απομακρυσμένη πρόσβαση αξιοποιούνται τεχνολογίες ασφαλείας που μάλιστα θα αναφέρουμε και παρακάτω. Οι τεχνολογίες αυτές διασφαλίζουν ότι η πρόσβαση γίνεται με ασφάλεια και ότι προστατεύονται τα δεδομένα του χρήστη από μη εξουσιοδοτημένες παρεμβάσεις. Σε πιο προχωρημένες υλοποιήσεις, ένα smart home δεν λειτουργεί απλώς με προσχεδιασμένους αυτοματισμούς (όπως «αν είναι νύχτα και ανιχνευθεί κίνηση, άναψε το φως»), αλλά εισάγει έννοιες προβλεπτικής συμπεριφοράς, μάθησης προτύπων, και ανάλυσης δεδομένων, ώστε να προσαρμόζεται στις συνήθειες των χρηστών. Μέσω της επεξεργασίας των ιστορικών δεδομένων και τη χρήση εργαλείων όπως machine learning, ένα έξυπνο σπίτι μπορεί να προτείνει αλλαγές, να ενεργεί προληπτικά ή να εντοπίζει ανωμαλίες (π.χ. ύποπτη χρήση ρεύματος ή παρατεταμένη απουσία κίνησης σε κρίσιμους χώρους). Ωστόσο, ένα από τα πιο κρίσιμα ζητήματα που αναδύονται με την εξάπλωση

των έξυπνων σπιτιών είναι το θέμα της ασφάλειας και της ιδιωτικότητας. Καθώς τα δεδομένα του χρήστη - είτε πρόκειται για ώρα επιστροφής στο σπίτι είτε για θερμοκρασιακά μοτίβα - διακινούνται και αποθηκεύονται, είναι θεμελιώδες να διασφαλίζεται η τοπική επεξεργασία των δεδομένων, η κρυπτογράφηση επικοινωνίας και η ελεγχόμενη απομακρυσμένη πρόσβαση. Το γεγονός αυτό καθιστά ιδιαίτερα σημαντική την επιλογή ελεύθερων, τοπικά εγκατεστημένων και πλήρως ελέγξιμων πλατφορμών, σε αντίθεση με πλήρως cloud-based λύσεις που διατηρούν τα δεδομένα στους servers τρίτων.

Τέλος, η έννοια του smart home δεν είναι στατική. Με την πρόοδο της τεχνολογίας, η έννοια εξελίσσεται σταδιακά σε smart living environment, όπου ενσωματώνονται ακόμη και στοιχεία της έξυπνης πόλης (smart city), του έξυπνου ενεργειακού δικτύου (smart grid) και της υγειονομικής παρακολούθησης (ambient assisted living), οδηγώντας σε ένα ολιστικό μοντέλο διαβίωσης που εστιάζει στην ενεργειακή αποδοτικότητα, την ασφάλεια, την υγεία και τη βιώσιμη καθημερινότητα.

1.1: ΚΑΤΗΓΟΡΙΕΣ ΔΙΚΤΥΩΝ

Οι κατηγορίες των δικτύων καθορίζονται κυρίως βάσει της γεωγραφικής έκτασης που καλύπτουν, του τρόπου σύνδεσης των συσκευών και της υποδομής που απαιτούν. Από τις πιο περιορισμένες τοπικά, μέχρι εκείνες που επεκτείνονται σε παγκόσμια κλίμακα, οι κατηγορίες αυτές εξυπηρετούν διαφορετικούς σκοπούς και ανάγκες επικοινωνίας. Στο πλαίσιο ενός έξυπνου σπιτιού, ιδιαίτερη σημασία έχουν τα δίκτυα **PAN**, **LAN**, **WLAN** και **WAN**, καθώς αλληλεπιδρούν άμεσα με τις συσκευές αυτοματισμού, τον τρόπο σύνδεσης στο διαδίκτυο και την απομακρυσμένη πρόσβαση.

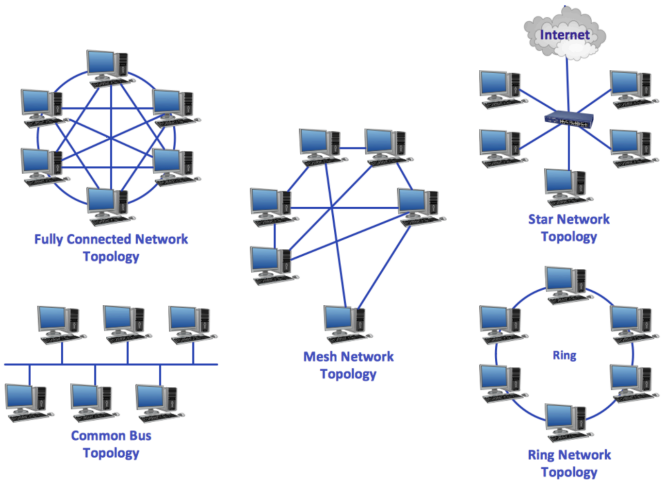
1.1.1: Personal Area Network (PAN)

Το PAN (Personal Area Network) είναι το πιο περιορισμένο από άποψης εμβέλειας δίκτυο, καθώς αφορά τη διασύνδεση συσκευών που βρίσκονται σε απόσταση μερικών εκατοστών έως λίγων μέτρων μεταξύ τους. Τέτοιες συσκευές μπορεί να είναι smartphone, smartwatch, ακουστικά Bluetooth, αισθητήρες σώματος και άλλα φορητά ή wearable τεχνολογικά μέσα. Τα PAN υλοποιούνται κυρίως με τεχνολογίες όπως Bluetooth, Zigbee, Infrared (IR) ή NFC. Στο πλαίσιο ενός smart home, το PAN αφορά για παράδειγμα τις συνδέσεις μεταξύ ενός Zigbee αισθητήρα θερμοκρασίας και ενός Zigbee coordinator, ή τη σύνδεση ενός κινητού με τον οικιακό υπολογιστή μέσω Bluetooth. Το σημαντικό πλεονέκτημα του PAN είναι η χαμηλή κατανάλωση ενέργειας, η απλότητα στη ζεύξη και η τοπική επικοινωνία χωρίς απαίτηση πρόσβασης σε εξωτερικά δίκτυα. [1]

1.1.2: Local Area Network (LAN)

Το LAN (Local Area Network) είναι η πλέον διαδεδομένη μορφή ενσύρματου (αλλα και ασύρματου δικτύου, βλ. WLAN) τοπικού δικτύου, και αφορά την καλωδιακή σύνδεση συσκευών μέσα σε έναν φυσικά περιορισμένο χώρο, όπως ένα σπίτι, ένα διαμέρισμα ή ένα γραφείο. Το LAN λειτουργεί συνήθως με τη χρήση τεχνολογιών Ethernet και απαιτεί τη χρήση επί το πλείστον switches, routers ή modems. Στα έξυπνα σπίτια, το LAN επιτρέπει τη σταθερή, αξιόπιστη και ταχύτατη σύνδεση συσκευών όπως το Raspberry Pi, οι NAS servers, οι κάμερες ασφαλείας IP, και οι έξυπνοι ελεγκτές. Το LAN διακρίνεται για τη σταθερότητα, την υψηλή ταχύτητα μετάδοσης δεδομένων και την ασφάλεια, αφού περιορίζεται εντός φυσικών συνδέσεων και δεν είναι άμεσα εκτεθειμένο σε εξωτερικές παρεμβάσεις.

Η χρήση LAN είναι ιδανική για συσκευές που απαιτούν συνεχή λειτουργία, μεγάλο εύρος μετάδοσης δεδομένων ή κριτική σημασία για την ασφάλεια, όπως οι αυτοματισμοί θέρμανσης ή οι συσκευές παρακολούθησης.[1]



Σχήμα 1.1: Τοπολογίες Δικτύων [1.α]

1.1.3: Wireless Local Area Network (WLAN)

Το WLAN (Wireless Local Area Network) αποτελεί την ασύρματη εκδοχή του LAN, δηλαδή ένα τοπικό δίκτυο που επιτρέπει τη σύνδεση συσκευών μέσω Wi-Fi χωρίς καλώδια. Η πιο κοινή μορφή WLAN είναι το οικιακό δίκτυο Wi-Fi, που βασίζεται σε τεχνολογίες του προτύπου IEEE 802.11. Στο έξυπνο σπίτι, το WLAN χρησιμοποιείται για τη σύνδεση κινητών τηλεφώνων, tablet, έξυπνων τηλεοράσεων, ασύρματων καμερών, θερμοστατών, διακοπτών και πλήθους άλλων IoT συσκευών. Παρόλο που προσφέρει μεγάλη ευελιξία και ευκολία εγκατάστασης, το WLAN υστερεί έναντι του ενσύρματου LAN ως προς την ασφάλεια, τη σταθερότητα και την αντοχή σε παρεμβολές, ιδίως όταν υπάρχουν πολλές ταυτόχρονες συνδέσεις ή εμπόδια στον χώρο. Εξαιτίας της φύσης του, το WLAN απαιτεί καλή διαχείριση καναλιών, χρήση ισχυρού κρυπτογραφικού πρωτοκόλλου (όπως WPA3) και συχνή επιτήρηση για εντοπισμό ευπαθειών. Το Wi-Fi, ακρωνύμιο του “Wireless Fidelity”, άρχισε να αναπτύσσεται στις αρχές της δεκαετίας του 1990, ενώ το πρώτο εμπορικό πρότυπο, το IEEE 802.11, εγκρίθηκε το 1997. Η αναγκαιότητά της αναδείχθηκε από την αυξανόμενη ανάγκη για κινητικότητα και την επιθυμία για ευκολότερη πρόσβαση σε δικτυακούς πόρους χωρίς τους περιορισμούς που επιβάλλει η ενσύρματη σύνδεση. Η αποδοχή της τεχνολογίας Wi-Fi εκτοξεύθηκε στις αρχές του 21ου αιώνα, καθιερώνοντάς την ως το πρότυπο για οικιακά και επαγγελματικά τοπικά ασύρματα δίκτυα. [1]

Το Wi-Fi λειτουργεί σε δύο κύριες ζώνες συχνοτήτων: Στα 2.4 GHz και στα 5 GHz, ενώ πιο πρόσφατα, με την εισαγωγή του Wi-Fi 6E και Wi-Fi 7, αξιοποιείται και το φάσμα των 6 GHz. Η ζώνη των 2.4 GHz προσφέρει μεγαλύτερη εμβέλεια, αλλά μικρότερες ταχύτητες και μεγαλύτερη ευαισθησία σε παρεμβολές, λόγω του κορεσμού της. Αντίθετα, η ζώνη των 5 GHz παρέχει υψηλότερες ταχύτητες και λιγότερες παρεμβολές, αλλά με μικρότερη εμβέλεια και δυσκολία διείσδυσης σε τοίχους και εμπόδια. Η επιλογή και χρήση καναλιών εντός αυτών των φασματικών ζωνών είναι κρίσιμη για τη σωστή λειτουργία ενός Wi-Fi δικτύου. Στο φάσμα των 2.4 GHz υπάρχουν 13 επικαλυπτόμενα κανάλια (στην Ευρώπη), εκ των οποίων μόνο τα 1, 6 και 11 είναι πλήρως μη επικαλυπτόμενα, κάτι που είναι απαραίτητο για την αποφυγή παρεμβολών. Στα 5 GHz, τα διαθέσιμα

κανάλια είναι περισσότερα και κατανεμημένα πιο αραιά, κάτι που διευκολύνει την αποδοτικότερη χρήση τους, ιδίως σε πυκνοκατοικημένα αστικά περιβάλλοντα.

Η διαδικασία σύνδεσης μίας συσκευής σε ένα Wi-Fi δίκτυο περιλαμβάνει ένα αρχικό handshake μέσω του λεγόμενου 4-way handshake, το οποίο διασφαλίζει την αυθεντικοποίηση του χρήστη και την κρυπτογράφηση της επικοινωνίας. Πιο συγκεκριμένα, το access point και η συσκευή-πελάτης ανταλλάσσουν πληροφορίες σχετικές με τα κλειδιά κρυπτογράφησης μέσω του πρωτοκόλλου WPA (Wi-Fi Protected Access), το οποίο στις σύγχρονες εκδοχές του (WPA2 & WPA3) χρησιμοποιεί εξελιγμένες μεθόδους όπως το AES (Advanced Encryption Standard) και τον μηχανισμό SAE (Simultaneous Authentication of Equals) για την πρόληψη επιθέσεων τύπου dictionary ή man-in-the-middle. Η συνολική ασφάλεια του Wi-Fi βασίζεται όχι μόνο στα πρωτόκολλα αυθεντικοποίησης και κρυπτογράφησης αλλά και στην κατάλληλη ρύθμιση του εξοπλισμού. Εσφαλμένες ρυθμίσεις ή η χρήση παρωχημένων μηχανισμών όπως το WEP (Wired Equivalent Privacy), που έχει αποδειχθεί ευάλωτο, μπορούν να εκθέσουν το δίκτυο σε σοβαρούς κινδύνους.

Στο τεχνικό επίπεδο, το Wi-Fi βασίζεται στο μοντέλο CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), προκειμένου να διαχειριστεί τη χρήση του ασύρματου μέσου μετάδοσης. Πριν μία συσκευή εκπέμψει δεδομένα, "ακούει" το κανάλι για πιθανή δραστηριότητα και, εφόσον αυτό είναι ελεύθερο, ξεκινά τη μετάδοση. Αν διαπιστωθεί συμφόρηση, καθυστερεί με τυχαίο τρόπο τη μετάδοση ώστε να μειωθεί η πιθανότητα σύγκρουσης πακέτων δεδομενογραματων..Τα πρότυπα του Wi-Fi έχουν εξελιχθεί σημαντικά με το πέρασμα του χρόνου. Ξεκινώντας από το 802.11b με μέγιστες ταχύτητες 11 Mbps, ακολούθησαν το 802.11a (54 Mbps, στα 5 GHz), το 802.11g (54 Mbps, στα 2.4 GHz), το 802.11n (Wi-Fi 4, έως 600 Mbps), το 802.11ac (Wi-Fi 5, έως και 3.5 Gbps) και το 802.11ax (Wi-Fi 6/6E), που εισήγαγε τεχνικές όπως το OFDMA (Orthogonal Frequency Division Multiple Access) και το MU-MIMO (Multi User - Multiple Input Multiple Output) για ταυτόχρονη εξυπηρέτηση πολλαπλών χρηστών. Το Wi-Fi 7 (802.11be), το οποίο βρίσκεται σε φάση υιοθέτησης, αναμένεται να φέρει ταχύτητες άνω των 30 Gbps, χαμηλό latency και προηγμένες δυνατότητες διαχείρισης φάσματος και ταυτοχρονα να αξιοποιησει την τεχνολογια MLO (Multi Link Operation) οπου η συγκεκριμένη, επιτρέπει την ταυτόχρονη χρήση των τριών διαφορετικών συχνοτήτων παράλληλα, μεγιστοποιόντας το διαθέσιμο έυρος ζώνης. [2]

Όπως αναφέραμε παραπάνω,η τεχνολογία Wi-Fi έχει εξελιχθεί μέσα από μια σειρά προτύπων του IEEE 802.11, τα οποία καθορίζουν τις τεχνικές παραμέτρους και τις δυνατότητες κάθε γενιάς ασύρματης δικτύωσης. Κάθε πρότυπο εισάγει βελτιώσεις ως προς τη χωρητικότητα, τη σταθερότητα, την εμβέλεια, την πολυπλεξία χρηστών και, φυσικά, την ασφάλεια. Το 802.11b, που κυκλοφόρησε το 1999, αποτέλεσε το πρώτο πρότυπο μαζικής αποδοχής, προσφέροντας ταχύτητες έως 11 Mbps στη ζώνη των 2.4 GHz. Την ίδια χρονιά εμφανίστηκε και το 802.11a, το οποίο λειτουργούσε στα 5 GHz και προσέφερε υψηλότερες ταχύτητες (έως 54 Mbps), αλλά με μικρότερη διείσδυση. Ακολούθησε το 802.11g (2003), το οποίο επανέφερε την ταχύτητα των 54 Mbps στη ζώνη των 2.4 GHz με καλύτερη συμβατότητα και σταθερότητα. Η σημαντική αναβάθμιση ήρθε με το 802.11n (γνωστό και ως Wi-Fi 4, 2009), που εισήγαγε τη χρήση πολλαπλών κεραιών (MIMO – Multiple Input Multiple Output), φτάνοντας θεωρητικά τα 600 Mbps, και παρέχει υποστήριξη τόσο για τα 2.4 GHz όσο και για τα 5 GHz. Το 802.11ac (Wi-Fi 5, 2013) εστίασε αποκλειστικά στην μπάντα των 5 GHz και εισήγαγε τεχνολογίες όπως το beamforming και το MU-MIMO (Multi-User MIMO), επιτρέποντας σε routers να εξυπηρετούν ταυτόχρονα πολλαπλές συσκευές χωρίς σημαντική απώλεια ταχύτητας. Οι ταχύτητες εκτοξεύθηκαν έως και 3.5 Gbps, σε ιδανικές συνθήκες. Η πιο δραστική και μοντέρνα αλλαγή ήρθε με το 802.11ax (Wi-Fi 6, 2019), που υποστηρίζει και τις δύο ζώνες (2.4 και 5 GHz), αλλά και επιπλέον δυνατότητες όπως το OFDMA (Orthogonal Frequency Division Multiple Access), το Target Wake

Time (για εξοικονόμηση ενέργειας σε IoT συσκευές) και εξελιγμένο MU-MIMO για ταυτόχρονη εξυπηρέτηση πολλών συσκευών. Το Wi-Fi 6E είναι επέκταση του Wi-Fi 6 στο απελευθερωμένο φάσμα των 6 GHz, που προσφέρει ευρύτερα κανάλια και μηδενικές παρεμβολές από παλιές συσκευές, γεγονός που το καθιστά ιδανικό για εφαρμογές με υψηλές απαιτήσεις. Το πιο πρόσφατο πρότυπο, το 802.11be (Wi-Fi 7), που βρίσκεται στη διαδικασία υλοποίησης, προσφέρει εντυπωσιακές ταχύτητες άνω των 30 Gbps, υποστηρίζει 320 MHz κανάλια, 4K-QAM για μεγαλύτερη πυκνότητα πληροφορίας και τεχνολογίες multi-link operation (MLO), οι οποίες επιτρέπουν σε μια συσκευή να συνδέεται ταυτόχρονα σε διαφορετικές συχνότητες για αυξημένη αξιοπιστία και απόδοση. Η προσέγγιση του Wi-Fi 7 δείχνει ξεκάθαρα τη στροφή της τεχνολογίας προς εφαρμογές με υψηλό throughput, ελάχιστο latency και υψηλή σταθερότητα [2]

Όσον αφορά την ασφάλεια, το πρωτόκολλο WEP (Wired Equivalent Privacy) υπήρξε η αρχική μορφή προστασίας, αλλά γρήγορα κρίθηκε ανεπαρκές λόγω σοβαρών αδυναμιών. Το WPA (Wi-Fi Protected Access) ήρθε ως ενδιάμεση λύση, μέχρι να θεσπιστεί το WPA2, το οποίο για χρόνια αποτελούσε το βασικό πρότυπο ασφάλειας για τα περισσότερα Wi-Fi δίκτυα. Το WPA2 εισήγαγε το AES (Advanced Encryption Standard) για ισχυρή συμμετρική κρυπτογράφηση, αλλά διατηρούσε κάποιες δομικές ευπάθειες, κυρίως στον τρόπο αυθεντικοποίησης. Το WPA3, που ανακοινώθηκε το 2018, αποτελεί τη νεότερη και πιο ασφαλή μορφή προστασίας. Εισάγει το SAE (Simultaneous Authentication of Equals) ως μηχανισμό handshake, ο οποίος είναι ανθεκτικός σε offline επιθέσεις λεξικού (dictionary attacks), καθώς και forward secrecy, που εξασφαλίζει ότι ακόμη και αν κάποιος αποκτήσει ένα session key, δεν μπορεί να αποκρυπτογραφήσει προηγούμενη κίνηση. Επιπλέον, το WPA3 υποστηρίζει το Enhanced Open, που προσφέρει κρυπτογράφηση ακόμα και σε ανοιχτά δίκτυα μέσω του Opportunistic Wireless Encryption (OWE), και προσθέτει μέτρα για την αποτροπή επιθέσεων μέσω IoT συσκευών. [2]

IEEE Standard	WiFi Gen	Year	Frequency	Max PHY Data Rate	Max Range
802.11	-	1997	2.4 GHz	2 Mbps	20m (indoor) 100m (outdoor)
802.11 a	-	1999	5 GHz	54 Mbps	35m (indoor) 120m (outdoor)
802.11 b	-	1999	2.4 GHz	11 Mbps	35m (indoor) 140m (outdoor)
802.11 g	-	2003	2.4 GHz	54 Mbps	38m (indoor) 140m (outdoor)
802.11 n	WiFi 4	2009	2.4/5 GHz	600 Mbps	70m (indoor) 250m (outdoor)
802.11 ac	WiFi 5	2013	5 GHz	6.9 Gbps	35m (indoor)
802.11 ad	-	2012	60 GHz	8.1 Mbps	3.3m (indoor)
802.11 ah	-	2017	Sub 1 GHz	347 Mbps	1km
802.11 ax	WiFi 6	2021	2.4/5/6 GHz	9.6 Gbps	30m (indoor) 120m (outdoor)
802.11 ay	-	2021	60 GHz	303 Gbps	10m (indoor) 100m (outdoor)
802.11 be	WiFi 7	2024	2.4/5/6 GHz	46.1 Gbps	30m (indoor) 120m (outdoor)

Εικόνα 1.2: Πρωτόκολλα Επικοινωνίας Wi-fi [2.α]

1.1.4: Wide Area Network (WAN)

Το WAN (Wide Area Network) είναι ένα δίκτυο μεγάλης εμβέλειας, το οποίο διασυνδέει επιμέρους LAN και WLAN δίκτυα σε γεωγραφικά κατανεμημένα σημεία, και το πλέον χαρακτηριστικό παράδειγμα του είναι το διαδίκτυο (Internet). Το WAN επιτρέπει την απομακρυσμένη πρόσβαση στο οικιακό δίκτυο από οποιοδήποτε σημείο του πλανήτη, υπό την προϋπόθεση ύπαρξης κατάλληλης δικτυακής υποδομής. Για ένα έξυπνο σπίτι, το WAN είναι ζωτικής σημασίας για τη διάγνωση προβλημάτων εξ αποστάσεως, την ειδοποίηση μέσω cloud, την πρόσβαση στον Home Assistant και γενικότερα για οποιαδήποτε μορφή έξυπνης απομακρυσμένης διαχείρισης. Η πρόκληση στη χρήση WAN για οικιακά δίκτυα είναι η ασφάλεια, καθώς η έκθεση συστημάτων στο διαδίκτυο δημιουργεί κινδύνους υποκλοπής ή επιθέσεων. Επομένως, η χρήση τεχνολογιών που θα αναφέρουμε παρακάτω είναι κρίσιμη για την αποφυγή αυτών των κινδύνων.[1]

1.1.5: Άλλες κατηγορίες δικτύων

Εκτός από τις παραπάνω βασικές κατηγορίες, υπάρχουν και άλλες μορφές δικτύωσης με ειδικότερο χαρακτήρα. Το Metropolitan Area Network (MAN) καλύπτει περιοχές μεγέθους πόλης και

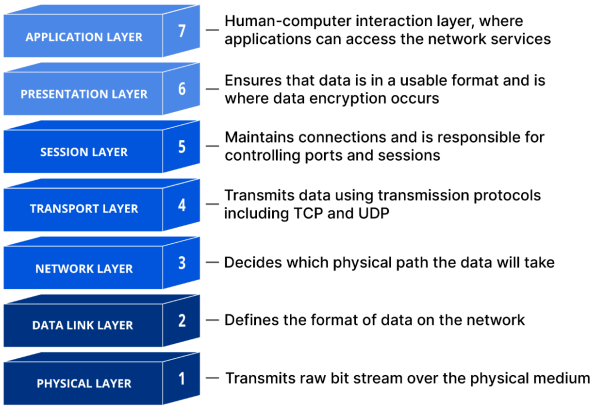
συναντάται σε δημόσιες υποδομές, πανεπιστήμια ή δήμους. Το Campus Area Network (CAN) αφορά πολλαπλά κτήρια ή υποδομές σε ένα πανεπιστημιακό ή βιομηχανικό συγκρότημα. Το Global Area Network (GAN) διασυνδέει WAN σε παγκόσμια κλίμακα, και χρησιμοποιείται συνήθως από πολυεθνικές εταιρείες ή δορυφορικά δίκτυα.[1]

1.2: Μοντελο OSI

Το μοντέλο OSI (Open Systems Interconnection) είναι ένα θεωρητικό πλαίσιο που δημιουργήθηκε από τον ISO για να περιγράψει και να τυποποιήσει τον τρόπο με τον οποίο επικοινωνούν τα δίκτυα υπολογιστών, χωρίζοντας τη διαδικασία σε επτά διακριτά επίπεδα. Στο πρώτο επίπεδο, το Physical Layer (Φυσικό Επίπεδο), μεταδίδονται τα πραγματικά bits μέσω φυσικών μέσων όπως καλώδια Ethernet, οπτικές ίνες ή ασύρματα σήματα, με παραδείγματα προτύπων όπως το Ethernet 100BASE-T ή το Wi-Fi 802.11. Στο δεύτερο επίπεδο, το Data Link Layer (Επίπεδο Σύνδεσης Δεδομένων), γίνεται η οργάνωση των δεδομένων σε frames και η διαχείριση της φυσικής διεύθυνσης (MAC address), με χαρακτηριστικά πρωτόκολλα όπως το Ethernet και το PPP (Point-to-Point Protocol). Το τρίτο επίπεδο, το Network Layer (Δικτυακό Επίπεδο), ασχολείται με τη δρομολόγηση των πακέτων μεταξύ διαφορετικών δικτύων, χρησιμοποιώντας πρωτόκολλα όπως το IPv4 και το IPv6. Στο τέταρτο επίπεδο, το Transport Layer (Επίπεδο Μεταφοράς), εξασφαλίζεται η αξιόπιστη ή μη αξιόπιστη μεταφορά των δεδομένων μεταξύ εφαρμογών, με πρωτόκολλα όπως το TCP (Transmission Control Protocol) για αξιόπιστη μεταφορά και το UDP (User Datagram Protocol) για ταχύτερη αλλά μη εγγυημένη μεταφορά. Το πέμπτο επίπεδο, το Session Layer (Επίπεδο Συνεδρίας), διαχειρίζεται τη δημιουργία, διατήρηση και τερματισμό συνεδριών επικοινωνίας, με παραδείγματα όπως το NetBIOS ή το RPC (Remote Procedure Call). Το έκτο επίπεδο, το Presentation Layer (Επίπεδο Παρουσίασης), φροντίζει για τη μορφοποίηση, τη συμπίεση και την κρυπτογράφηση των δεδομένων, με πρωτόκολλα και τεχνολογίες όπως το SSL/TLS για ασφάλεια ή το MPEG για συμπίεση πολυμέσων. Τέλος, το έβδομο επίπεδο, το Application Layer (Επίπεδο Εφαρμογής), είναι το πλησιέστερο στον χρήστη και περιλαμβάνει τα πρωτόκολλα που επιτρέπουν την άμεση αλληλεπίδραση, όπως το HTTP/HTTPS για ιστό, το SMTP για email και το FTP για μεταφορά αρχείων.

Η λογική του μοντέλου OSI είναι ότι κάθε επίπεδο προσφέρει συγκεκριμένες υπηρεσίες στο επίπεδο από πάνω του και χρησιμοποιεί τις λειτουργίες του επιπέδου από κάτω, επιτρέποντας έτσι τη modular ανάπτυξη και την ευκολότερη διάγνωση προβλημάτων. Για παράδειγμα, ένα πρόβλημα στο φυσικό επίπεδο (π.χ. κομμένο καλώδιο) μπορεί να απομονωθεί χωρίς να επηρεάσει την κατανόηση της λειτουργίας στα υψηλότερα επίπεδα, ενώ ένα πρόβλημα στο επίπεδο εφαρμογής (π.χ. σφάλμα HTTP) μπορεί να εντοπιστεί ανεξάρτητα από την υποδομή μεταφορά

Το μοντέλο OSI, πέρα από το ότι είναι θεωρητικό και δεν εφαρμόζεται αυτούσιο στην πράξη, λειτουργεί ως θεμελιώδης οδηγός κατανόησης της αρχιτεκτονικής των δικτύων και της διαστρωμάτωσης των λειτουργιών. Κάθε επίπεδο είναι αυστηρά καθορισμένο ώστε να επικοινωνεί μόνο με το ακριβώς πάνω ή κάτω από αυτό, κάτι που επιτρέπει την ανεξαρτησία της τεχνολογίας. Για παράδειγμα, μπορείς να αλλάξεις το φυσικό μέσο (από χαλκό σε οπτική ίνα) χωρίς να αλλάξεις τίποτα στα υψηλότερα επίπεδα, ή να αλλάξεις ένα πρωτόκολλο εφαρμογής (π.χ. από FTP σε HTTP) χωρίς να επηρεάσεις το πώς γίνεται η μετάδοση στο φυσικό επίπεδο.



Σχήμα 1.3: Επίπεδα του μοντέλου OSI [3.α]

Στην πράξη, το μοντέλο OSI συνδέεται στενά με το μοντέλο TCP/IP, το οποίο χρησιμοποιείται ευρέως στο διαδίκτυο. Στο TCP/IP, τα επτά επίπεδα του OSI συμπτύσσονται σε τέσσερα: Network Access (που περιλαμβάνει τα επίπεδα Physical και Data Link), Internet (που αντιστοιχεί στο Network Layer), Transport (ίδιο με του OSI) και Application (που περιλαμβάνει τα τρία υψηλότερα επίπεδα του OSI: Session, Presentation, Application). Η αντιστοίχιση αυτή βοηθά στην κατανόηση του γιατί πολλά πρωτόκολλα αναφέρονται ως “Layer 3” ή “Layer 4” — για παράδειγμα, το IPv4 είναι καθαρά πρωτόκολλο Layer 3, ενώ το TCP είναι Layer 4.

Ένα από τα σημαντικά πλεονεκτήματα της ύπαρξης του OSI είναι η τυποποίηση και η δυνατότητα troubleshooting. Στην ανάλυση προβλημάτων, οι τεχνικοί συχνά ακολουθούν την προσέγγιση "From Layer 1 to Layer 7", δηλαδή ελέγχουν πρώτα το φυσικό μέσο (καλώδια, σήμα), μετά τη συνδεσιμότητα (MAC addresses, switches), στη συνέχεια την IP δρομολόγηση, και προχωρούν μέχρι το επίπεδο εφαρμογής. Για παράδειγμα, αν ένας χρήστης δεν μπορεί να φορτώσει μια ιστοσελίδα, η ανάλυση μπορεί να ξεκινήσει από το Layer 1 (είναι συνδεδεμένο το καλώδιο;) και να φτάσει μέχρι το Layer 7 (είναι σωστά ρυθμισμένος ο web server;).

Επιπλέον, το OSI προσφέρει σαφή διαχωρισμό ρόλων σε συσκευές δικτύου. Τα switches λειτουργούν κυρίως στο Layer 2, οι routers στο Layer 3, τα firewalls μπορεί να λειτουργούν από Layer 3 μέχρι Layer 7 (ανάλογα με την πολυπλοκότητα), ενώ οι load balancers δουλεύουν κυρίως στα ανώτερα επίπεδα. Ορισμένες συσκευές, όπως τα Layer 3 switches, γεφυρώνουν λειτουργίες δύο επιπέδων [1]

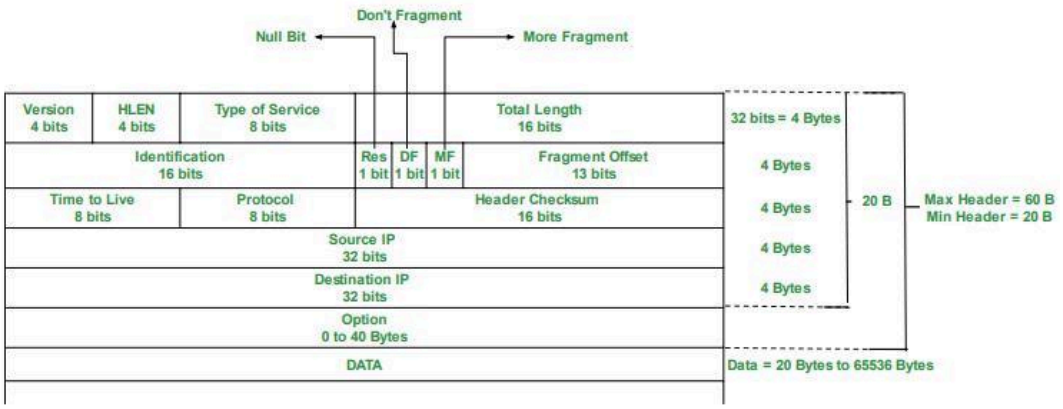
1.3: Internet Protocol Version 4

Το IPv4 (Internet Protocol version 4) αποτελεί την τέταρτη έκδοση του πρωτοκόλλου διαδικτύου και είναι μέχρι σήμερα η πλέον διαδεδομένη μορφή διευθυνσιοδότησης σε παγκόσμιο επίπεδο. Σχεδιάστηκε αρχικά τη δεκαετία του 1980 στο πλαίσιο του ARPANET και τέθηκε σε πλήρη λειτουργία κατά τη διάρκεια της δεκαετίας του 1990, αποτελώντας τη βάση για τη δημιουργία του σύγχρονου Διαδικτύου. Το IPv4 είναι ένα πρωτόκολλο δικτύου του επιπέδου δικτύου του μοντέλου TCP/IP, και βασική του λειτουργία είναι η παροχή μοναδικών διευθύνσεων σε κάθε συσκευή που συμμετέχει σε ένα δίκτυο, έτσι ώστε να είναι δυνατή η μετάδοση πακέτων μεταξύ αποστολέα και παραλήπτη.

Μια διεύθυνση IPv4 είναι 32-bit και συνήθως αναπαρίσταται με τέσσερις δεκαδικούς αριθμούς (οκτάδες) διαχωρισμένους με τελείες, όπως για παράδειγμα: 192.168.1.1. Το γεγονός ότι υπάρχουν 32 δυαδικά ψηφία συνεπάγεται θεωρητικά τη δυνατότητα ύπαρξης περίπου 4,3 δισεκατομμυρίων μοναδικών διευθύνσεων. Ωστόσο, στην πράξη, εξαιτίας της ανάγκης για ομαδοποιήσεις, broadcast διευθύνσεις και κρατημένες διευθύνσεις για ειδικούς σκοπούς, ο αριθμός των πραγματικά διαθέσιμων διευθύνσεων είναι σημαντικά μικρότερος. Αυτό το πρόβλημα της εξάντλησης των διαθέσιμων διευθύνσεων υπήρξε η αφορμή για την ανάπτυξη του IPv6, το οποίο χρησιμοποιεί 128-bit διευθύνσεις.

Για να αντιμετωπιστεί το ζήτημα της έλλειψης διαθέσιμων IPv4 διευθύνσεων χωρίς άμεση μετάβαση στο IPv6, εφαρμόστηκε η τεχνική του NAT (Network Address Translation). Το NAT επιτρέπει σε πολλές συσκευές μέσα σε ένα τοπικό δίκτυο (LAN) να χρησιμοποιούν ιδιωτικές, μη δρομολογήσιμες διευθύνσεις (όπως 192.168.x.x, 10.x.x.x, 172.16.x.x έως 172.31.x.x) και να μοιράζονται μία μόνο δημόσια διεύθυνση IP για να επικοινωνούν με το Διαδίκτυο. [13] Αυτό επιτυγχάνεται με τη μετάφραση των ιδιωτικών διευθύνσεων και των αντίστοιχων θυρών (ports) σε μία δημόσια διεύθυνση μέσω ενός NAT router ή firewall. Υπάρχουν διάφοροι τύποι NAT. Το πιο διαδεδομένο είναι το PAT (Port Address Translation), γνωστό και ως NAT Overload, όπου πολλές εσωτερικές συσκευές μοιράζονται μία δημόσια IP και διαχωρίζονται μεταξύ τους μέσω διαφορετικών αριθμών θύρας. Υπάρχουν επίσης το Static NAT, όπου μια εσωτερική διεύθυνση αντιστοιχίζεται μόνιμα σε μια δημόσια, και το Dynamic NAT, όπου οι εσωτερικές διευθύνσεις αντιστοιχίζονται προσωρινά από ένα pool δημόσιων διευθύνσεων.

Η ύπαρξη του NAT επιφέρει σημαντικές επιπτώσεις στην αρχιτεκτονική του Διαδικτύου. Από τη μία πλευρά, επιτρέπει την εξοικονόμηση δημόσιων διευθύνσεων και προσφέρει ένα επίπεδο ασφάλειας, καθώς οι εσωτερικές συσκευές δεν είναι άμεσα προσβάσιμες από το εξωτερικό. Από την άλλη, καθιστά πιο περίπλοκη τη δημιουργία συνδέσεων προς τα μέσα (inbound connections), απαιτώντας τεχνικές όπως port forwarding ή tunneling για να καταστεί δυνατή η πρόσβαση από το Διαδίκτυο σε εσωτερικές υπηρεσίες. Επίσης, δυσκολεύει την υλοποίηση end-to-end συνδέσεων, κάτι που ήταν θεμελιώδης στόχος στο αρχικό όραμα του Διαδικτύου. [1]



Σχήμα 1.4: Ενα Δεδομενογραμμα ενος πακέτου IPv4 [4.α]

1.4: Θύρες δικτύου

Οι θύρες δικτύου, γνωστές ως network ports, αποτελούν αναπόσπαστο στοιχείο της αρχιτεκτονικής επικοινωνίας στο Διαδίκτυο και στηρίζονται στο μοντέλο TCP/IP. Είναι αριθμητικοί αναγνωριστές μεγέθους 16-bit, που κυμαίνονται από το 0 έως το 65535, και χρησιμοποιούνται για να κατευθύνουν

την κυκλοφορία δεδομένων προς συγκεκριμένες εφαρμογές ή υπηρεσίες που εκτελούνται σε μια συσκευή δικτύου. Κάθε θύρα αντιστοιχεί σε ένα συγκεκριμένο πρωτόκολλο ή υπηρεσία, επιτρέποντας σε έναν υπολογιστή ή server να εξυπηρετεί πολλές εφαρμογές ταυτόχρονα, μέσω της ίδιας IP διεύθυνσης. Η σύνταξη που χρησιμοποιείται για να καθοριστεί μια συγκεκριμένη σύνδεση είναι της μορφής IP:θύρα, όπως για παράδειγμα 192.168.1.100:8123, όπου η διεύθυνση παραπέμπει στο web interface του Home Assistant, μιας πλατφόρμας έξυπνου αυτοματισμού.
Οι θύρες διακρίνονται σε τρεις βασικές κατηγορίες: Οι well-known ports, οι οποίες καταλαμβάνουν το εύρος από 0 έως 1023 και προορίζονται για θεμελιώδεις υπηρεσίες όπως το HTTP (θύρα 80), το HTTPS (443), το SSH (22), και το DNS (53),· οι registered ports, που βρίσκονται στο εύρος 1024 έως 49151 και προορίζονται για εφαρμογές τρίτων κατασκευαστών ή προσωποποιημένες υπηρεσίες· και οι dynamic ή ephemeral ports, από 49152 έως 65535, που χρησιμοποιούνται προσωρινά για την εξυπηρέτηση εξερχόμενων συνδέσεων. Στο πλαίσιο του οικιακού αυτοματισμού, μια ιδιαίτερα χαρακτηριστική θύρα είναι η 8123, η οποία αποτελεί την προεπιλεγμένη πόρτα για την πρόσβαση στη διεπαφή του Home Assistant. Μέσω αυτής της θύρας, οι χρήστες μπορούν να αλληλεπιδράσουν με το σύστημα αυτοματισμού τους μέσω browser ή εφαρμογών τρίτων. Οι θύρες είναι επίσης ουσιώδεις για την τεχνολογία προώθησης θυρών (port forwarding), όπου ο δρομολογητής ανακατευθύνει την εισερχόμενη κίνηση από το διαδίκτυο προς μια συγκεκριμένη συσκευή στο εσωτερικό δίκτυο, επιτρέποντας π.χ. την απομακρυσμένη πρόσβαση σε κάμερες, server ή το Home Assistant. Οι θύρες δικτύου δεν αποτελούν φυσικές διεπαφές, αλλά λογικούς αριθμητικούς προσδιορισμούς που χρησιμοποιούνται στο επίπεδο μεταφοράς του μοντέλου TCP/IP, κυρίως από τα πρωτόκολλα TCP (Transmission Control Protocol) και UDP (User Datagram Protocol). Με απλά λόγια, κάθε φορά που μια συσκευή συνδέεται σε μια υπηρεσία στο διαδίκτυο ή στο τοπικό δίκτυο, χρησιμοποιεί μια συγκεκριμένη θύρα για να επικοινωνήσει. Το λειτουργικό σύστημα παρακολουθεί αυτές τις θύρες, και κάθε εφαρμογή που χρειάζεται να δέχεται δεδομένα πρέπει να «ακούει» σε μία ή περισσότερες από αυτές.
Η διαχείριση των θυρών έχει ιδιαίτερη σημασία και για τους διαχειριστές συστημάτων, καθώς μπορεί να συνδεθεί με πολιτικές που εφαρμόζονται στα τείχη προστασίας (firewall). Για παράδειγμα, ένα τείχος προστασίας μπορεί να επιτρέπει μόνο τις θύρες 443 και 22 για ασφαλείς συνδέσεις (HTTPS και SSH αντίστοιχα), ενώ μπλοκάρει όλες τις υπόλοιπες, περιορίζοντας την επιφάνεια πιθανών επιθέσεων. Παράλληλα, πολλά προγράμματα ή υπηρεσίες καθορίζουν αυτόματα τις θύρες στις οποίες λειτουργούν. Αν μια θύρα είναι ήδη κατειλημμένη, η εφαρμογή θα αποτύχει να ξεκινήσει ή θα πρέπει να επαναρυθμιστεί με διαφορετικό αριθμό θύρας.
Μια ενδιαφέρουσα πτυχή αφορά τις θύρες UDP, οι οποίες συχνά χρησιμοποιούνται για υπηρεσίες που απαιτούν χαμηλή καθυστέρηση, όπως τα VoIP (Voice over IP), το video streaming και τα διαδικτυακά παιχνίδια. Σε αντίθεση με το TCP που εξασφαλίζει αξιόπιστη μετάδοση, το UDP προσφέρει ταχύτητα με μικρότερο έλεγχο, συνεπώς χρειάζεται ιδιαίτερη προσοχή στη χρήση του.
Η τεχνολογία των θυρών διαδραματίζει επίσης κεντρικό ρόλο στο Network Address Translation (NAT), όπου πολλές συσκευές σε ένα τοπικό δίκτυο χρησιμοποιούν μια κοινή δημόσια IP. Το NAT διαχειρίζεται αυτήν την πολυπλοκότητα αντιστοιχίζοντας τις εξερχόμενες συνδέσεις σε συγκεκριμένες θύρες, έτσι ώστε οι απαντήσεις από το διαδίκτυο να φτάσουν πίσω στη σωστή συσκευή. Αυτή η τεχνική επιτρέπει τη συνύπαρξη πολλών συσκευών πίσω από έναν μόνο δρομολογητή και είναι απολύτως εξαρτημένη από τη χρήση θυρών.
Τέλος, σε πιο σύγχρονες υλοποιήσεις και περιβάλλοντα, όπως τα containers ή τα virtual machines, η διαχείριση θυρών είναι κρίσιμη για τη δρομολόγηση της εσωτερικής και εξωτερικής κυκλοφορίας. Για παράδειγμα, σε ένα Docker container που τρέχει Home Assistant, μπορεί να γίνει map η εξωτερική θύρα 8123 του host στη θύρα 8123 του container, επιτρέποντας πλήρη πρόσβαση στη διεπαφή διαχείρισης του αυτοματισμού από το τοπικό ή και απομακρυσμένο δίκτυο. [1]

Port	Protocol	Name
7	TCP/UDP	echo
9	TCP/UDP	discard
19	TCP/UDP	chargen
20	TCP/SCTP	ftp-data
21	TCP/UDP/SCTP	ftp
22	TCP/UDP/SCTP	ssh/scp/sftp
23	TCP	telnet
25	TCP	smtp
42	TCP/UDP	wins replication
43	TCP/UDP	whois
49	UDP	tacacs
53	TCP/UDP	dns
67	UDP	dhcp/bootp
68	UDP	dhcp/bootp
69	UDP	tftp
70	TCP	gopher
79	TCP	finger
80	TCP/UDP/SCTP	http
88	TCP/UDP	kerberos
101	TCP	hostname
102	TCP	microsoft exchange iso-tsap
110	TCP	pop3
113	TCP	ident
119	TCP	nntp (usenet)
123	UDP	ntp
135	TCP/UDP	microsoft rpc epmap
137	TCP/UDP	netbios-ns
138	TCP/UDP	netbios-dgm
139	TCP/UDP	netbios-ssn
143	TCP/UDP	imap
161	UDP	snmp-agents (unencrypted)
162	UDP	snmp-trap (unencrypted)
177	UDP	xdmcp
179	TCP	bgp
194	UDP	irc
201	TCP/UDP	appletalk
264	TCP/UDP	bgmp
318	TCP/UDP	tsp
381	TCP/UDP	hp openview
383	TCP/UDP	hp openview
389	TCP/UDP	ldap
411	TCP/UDP	(multiple uses)
412	TCP/UDP	(multiple uses)
427	TCP	slp
443	TCP/UDP/SCTP	https (http over ssl)
445	TCP/UDP	microsoft ds smb
464	TCP/UDP	kerberos
465	TCP	smtp over tls/ssl
465	TCP	ssm
497	TCP/UDP	dantz retrospect
500	UDP	ipsec/isakmp/ike
512	TCP	rexec
513	TCP	rlogin
514	UDP	syslog/shell
515	TCP	lpd/lpr
520	UDP	rip
521	UDP	ripng (ipv6)
540	TCP	uucp
546	TCP/UDP	dhcpv6
547	TCP/UDP	dhcpv6
548	TCP	afp
554	TCP/UDP	rtsp
560	UDP	rmonitor
563	TCP/UDP	nntp over tls/ssl
587	TCP	smtp/submission
591	TCP	filemaker
593	TCP/UDP	microsoft dcom
596	TCP/UDP	smsd
631	TCP	ipp
636	TCP/UDP	ldap over tls/ssl
639	TCP	msdp (pim)
646	TCP/UDP	ldp (mpls)
691	TCP	microsoft exchange
860	TCP	iscsi
873	TCP	rsync
902	TCP/UDP	vmware server
989	TCP	ftps
990	TCP	ftps
992	TCP/UDP	telnets
993	TCP	imap over ssl (imaps)
995	TCP/UDP	pop3 over ssl (pop3s)
1025	TCP	microsoft rpc
1080	TCP/UDP	socks
1194	TCP/UDP	openvpn
1241	TCP/UDP	nessus
1311	TCP	dell openmanage
1433	TCP	ms-sql-s
1434	TCP/UDP	ms-sql-m
1494	TCP	ica
1512	TCP/UDP	wins
1524	TCP/UDP	ingreslock
1589	TCP/UDP	cisco vqp
1701	UDP	l2tp
1719	UDP	h323gatestat
1720	TCP	h323hostcall
1723	TCP/UDP	microsoft pptp
1725	UDP	steam
1755	TCP/UDP	mms
1812	TCP/UDP	radius
1813	TCP/UDP	radius-acct
1985	UDP	hsrp
2000	TCP	cisco sccp
2002	TCP	cisco acs
2008	TCP	teamspeak 3 accounting
2010	UDP	teamspeak 3 web list
2049	TCP/UDP	nfs
2082	TCP/UDP	cpanel
2083	TCP/UDP	radsec/cpanel
2100	TCP	amiganetfs
2102	TCP/UDP	zephyr-srv
2103	TCP/UDP	zephyr-clt
2104	TCP/UDP	zephyr-hm
2222	TCP	directadmin
2401	TCP	cvspserver
2483	TCP/UDP	oracle
2484	TCP/UDP	oracle
2809	TCP/UDP	corbaloc
2967	TCP/UDP	symantec av
3128	TCP/UDP	http proxy
3222	TCP/UDP	glbp
3260	TCP/UDP	iscsi target
3306	TCP/UDP	mysql
3389	TCP	rdp
3689	TCP	daap
3690	TCP/UDP	svn
4321	TCP	rwhois
4333	TCP	msql
4500	UDP	ipsec nat traversal
4899	TCP	radmin
5000	TCP	upnp
5001	TCP	iperf
5004-5005	UDP	rtp/rtsp
5060	TCP/UDP	sip
5061	TCP	sip-tls
5222-5223	TCP	xmpp
5353	UDP	mdns
5432	TCP	postresql
5800	TCP	vnc over http
5900-5999	TCP/UDP	rfb/vnc server
5999	TCP	cvsup
6000-6001	TCP	X11
6129	TCP	dameware
6379	TCP	redis
6588	TCP	analogx
6588	TCP	http proxy
8080	TCP	http proxy
8200	TCP/UDP	vmware server
8222	TCP/UDP	vmware server
8767	UDP	Teamspeak
9042	TCP	cassandra
9100	TCP	pdl
9800	TCP/UDP	webdav
10161	TCP	snmp-agents
10162	TCP	snmp-trap
13720	TCP/UDP	bprd
13721	TCP/UDP	bpdbm
13724	TCP/UDP	vnetd
13782	TCP/UDP	bpcd
13783	TCP/UDP	vopied
20000	TCP/UDP	usermin
22273	TCP/UDP	wnn6
23399	TCP/UDP	skype
25565	TCP	minecraft
27017	TCP/UDP	mongodb
33434	TCP/UDP	traceroute

NetworkProGuide.com

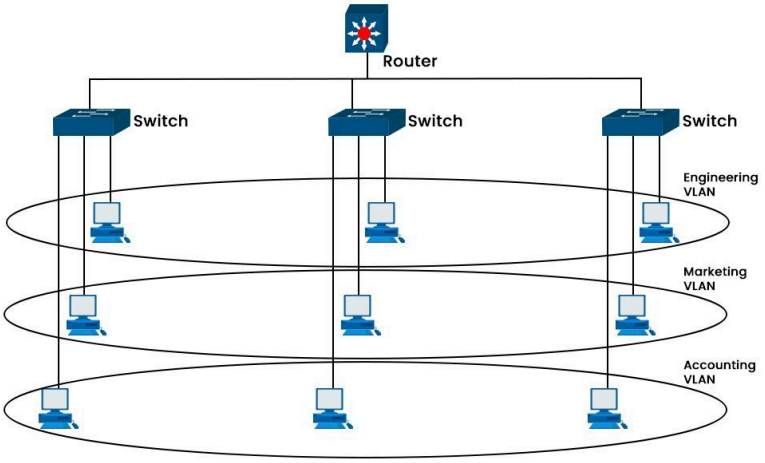
Σχήμα 1.5: Λίστα με τις Well-known θύρες απο τον IANA [5.α]

1.5: Virtual LAN

Τα VLAN (Virtual Local Area Networks) είναι μια τεχνολογία δικτύωσης που επιτρέπει τη λογική διαίρεση ενός φυσικού δικτύου σε πολλά ξεχωριστά, απομονωμένα τμήματα, χωρίς να απαιτείται η δημιουργία επιπλέον φυσικής υποδομής. Η λειτουργία τους βασίζεται στην προσθήκη μιας ετικέτας (tag) στα Ethernet frames, σύμφωνα με το πρότυπο IEEE 802.1Q, η οποία δηλώνει σε ποιο VLAN ανήκει κάθε πακέτο δεδομένων. Οι διαχειριστές μπορούν να ορίσουν VLANs πάνω σε switches και routers, απομονώνοντας έτσι την κίνηση διαφορετικών τμημάτων ενός οργανισμού, π.χ. το λογιστήριο, την τεχνική υποστήριξη ή τα συστήματα επισκεπτών, παρόλο που όλοι μοιράζονται την ίδια φυσική καλωδίωση.

Η χρήση VLAN προσφέρει πολλαπλά πλεονεκτήματα. Από πλευράς ασφάλειας, μειώνει την πιθανότητα μη εξουσιοδοτημένης πρόσβασης, καθώς η κίνηση περιορίζεται εντός του VLAN στο οποίο ανήκει. Από πλευράς απόδοσης, μειώνει την περιττή μετάδοση broadcast πακέτων, περιορίζοντας το μέγεθος κάθε broadcast domain. Επιπλέον, δίνει τη δυνατότητα ευελιξίας, αφού η αλλαγή της τοπολογίας του δικτύου μπορεί να γίνει απλώς με την ανακατανομή των VLAN tags, χωρίς να χρειάζεται φυσική μετακίνηση καλωδίων. Σε περιβάλλοντα όπως τα data centers ή οι μεγάλες επιχειρήσεις, τα VLAN αποτελούν βασικό στοιχείο για την απομόνωση υπηρεσιών, την

υλοποίηση διαφορετικών επιπέδων πρόσβασης, αλλά και την ενσωμάτωση τεχνολογιών όπως το Voice over IP (VoIP), όπου η φωνητική και η δεδομενική κίνηση πρέπει να διαχειρίζονται ξεχωριστά.
Κάθε VLAN σε ένα δίκτυο ταυτοποιείται από έναν μοναδικό αριθμό που ονομάζεται VLAN ID, ο οποίος μπορεί να κυμαίνεται από το 1 έως το 4094 σύμφωνα με το πρότυπο IEEE 802.1Q. Το VLAN ID χρησιμοποιείται για να μαρκάρει (tag) τα Ethernet frames, ώστε οι συσκευές δικτύου να γνωρίζουν σε ποιο εικονικό δίκτυο ανήκει κάθε πακέτο. Στα managed switches, κάθε φυσική θύρα μπορεί να ανήκει σε ένα ή περισσότερα VLANs και να έχει έναν προκαθορισμένο αριθμό VLAN που ονομάζεται PVID (Port VLAN ID). Το PVID καθορίζει ποιο VLAN ID θα αποδοθεί αυτόματα σε εισερχόμενα untagged frames, δηλαδή σε πακέτα που φτάνουν χωρίς VLAN tag. Με αυτόν τον τρόπο, ακόμα και συσκευές που δεν υποστηρίζουν VLAN tagging μπορούν να ενταχθούν σε ένα VLAN μέσω της αντιστοίχισης του PVID της θύρας τους.
Στη λειτουργία ενός VLAN υπάρχουν δύο βασικές έννοιες: Τα tagged και τα untagged δίκτυα. Τα tagged frames περιλαμβάνουν μέσα στο Ethernet frame header το VLAN ID τους, χάρη στο πρωτόκολλο 802.1Q, και επιτρέπουν την ταυτόχρονη μεταφορά πολλών VLANs μέσω μιας φυσικής σύνδεσης, κάτι που είναι απαραίτητο στα trunk ports. Από την άλλη, τα untagged frames δεν έχουν VLAN πληροφορία στο header τους και συνήθως μεταφέρονται σε access ports, που συνδέουν τελικές συσκευές όπως υπολογιστές, εκτυπωτές ή IP τηλέφωνα. Μια θύρα μπορεί να είναι untagged μόνο για ένα VLAN (το οποίο ορίζεται από το PVID της), ενώ μπορεί ταυτόχρονα να είναι tagged για άλλα VLANs, επιτρέποντας έτσι συνδυασμένη χρήση για ειδικές περιπτώσεις όπως VoIP ή guest δίκτυα. Αυτή η αρχιτεκτονική δίνει μεγάλη ευελιξία στη διαχείριση της δικτυακής κίνησης, επιτρέπει τη μεταφορά πολλαπλών εικονικών δικτύων πάνω στις ίδιες φυσικές υποδομές και συμβάλλει στην απομόνωση και στην ασφάλεια των δεδομένων, αρκεί η ρύθμιση των VLAN IDs, των PVIDs και των tagged/untagged θυρών να γίνει σωστά ώστε να αποφευχθούν διαρροές κίνησης μεταξύ διαφορετικών VLANs. [1]



Σχήμα 1.7: Οπτική απεικόνηση χωρισμού δικτύων μέσω VLAN [6.α]

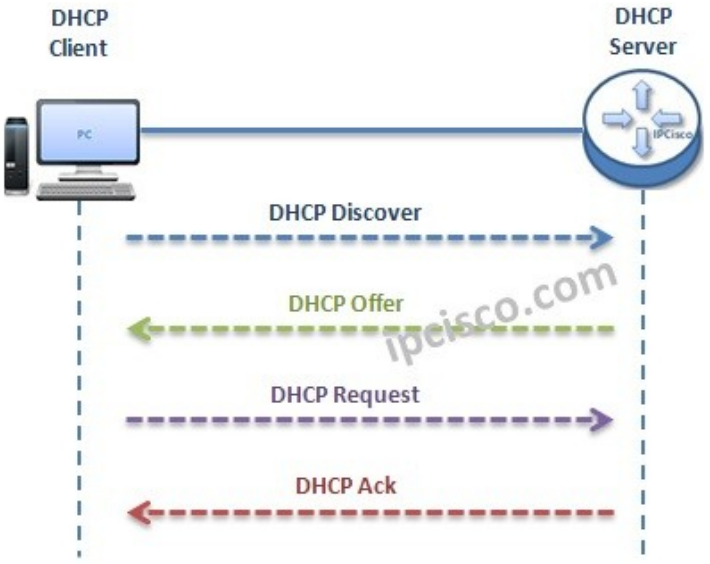
1.6: DHCP

Το DHCP (Dynamic Host Configuration Protocol) είναι ένα πρωτόκολλο δικτύου που αυτοματοποιεί τη διαδικασία απόδοσης διευθύνσεων IP και άλλων παραμέτρων διαμόρφωσης σε συσκευές μέσα σε ένα δίκτυο. Αντί ο διαχειριστής να ρυθμίζει χειροκίνητα κάθε συσκευή (στατική IP), το DHCP server αναλαμβάνει να εκχωρήσει δυναμικά μια διεύθυνση IP από ένα προκαθορισμένο εύρος (scope) σε κάθε συσκευή που συνδέεται, μαζί με πρόσθετες πληροφορίες όπως subnet mask, default gateway, DNS servers, ακόμη και το domain name. Η διαδικασία ξεκινά με το “DHCP Discover”, όπου η συσκευή εκπέμπει ένα broadcast πακέτο για να βρει διαθέσιμο server. Ο server απαντά με “DHCP

Offer" προτείνοντας μία IP, η συσκευή αποδέχεται με "DHCP Request" και τέλος ο server επιβεβαιώνει με "DHCP Acknowledgment" (ACK). Οι εκχωρημένες IP έχουν διάρκεια μίσθωσης (lease time), μετά την οποία η συσκευή πρέπει να ανανεώσει τη διεύθυνση. Το DHCP είναι θεμελιώδες για δίκτυα με πολλές συσκευές, καθώς μειώνει τον χρόνο διαχείρισης, αποφεύγει διπλές διευθύνσεις και επιτρέπει εύκολες αλλαγές στη δομή του δικτύου. Ωστόσο, από την πλευρά της ασφάλειας, χωρίς κατάλληλους περιορισμούς μπορεί να επιτρέψει σε μη εξουσιοδοτημένες συσκευές να αποκτήσουν πρόσβαση στο δίκτυο ή να δεχθεί επιθέσεις τύπου "rogue DHCP server", όπου κακόβουλοι servers εκχωρούν ψευδείς ρυθμίσεις, ανακατευθύνοντας την κίνηση σε επικίνδυνους προορισμούς. Για αυτό, σε επαγγελματικά περιβάλλοντα, χρησιμοποιούνται τεχνικές όπως DHCP snooping και MAC filtering για τον περιορισμό των κινδύνων.

Το DHCP ακολουθεί μια συγκεκριμένη διαδικασία τεσσάρων σταδίων για την ανάθεση μιας διεύθυνσης IP σε μια συσκευή, η οποία είναι γνωστή ως DORA (Discover, Offer, Request, Acknowledge). Αρχικά, στο στάδιο Discover, μια συσκευή που συνδέεται στο δίκτυο και δεν έχει ακόμη διεύθυνση IP στέλνει ένα broadcast μήνυμα DHCP Discover, αναζητώντας διαθέσιμο DHCP server. Στη συνέχεια, ο DHCP server που λαμβάνει αυτό το μήνυμα επιλέγει μια ελεύθερη IP από το προκαθορισμένο εύρος διευθύνσεων (scope) και απαντά με το στάδιο Offer, το οποίο περιλαμβάνει την προτεινόμενη IP, τη μάσκα υποδικτύου, το gateway και άλλες ρυθμίσεις δικτύου. Ακολουθεί το στάδιο Request, όπου η συσκευή απαντά επίσης με broadcast μήνυμα για να ζητήσει επίσημα την IP που της προτάθηκε, επιβεβαιώνοντας στον server ότι αποδέχεται την προσφορά. Τέλος, στο στάδιο Acknowledge, ο DHCP server αποστέλλει μήνυμα επιβεβαίωσης (DHCP ACK) που "κλειδώνει" τη συγκεκριμένη IP για τη συσκευή και ενημερώνει τη διάρκεια μίσθωσης (lease time). Αυτή η διαδικασία εξασφαλίζει ότι κάθε συσκευή λαμβάνει μοναδική IP στο δίκτυο, αποφεύγοντας συγκρούσεις διευθύνσεων και επιτρέποντας την ομαλή λειτουργία της επικοινωνίας. Επιπλέον, όταν πλησιάζει το τέλος της περιόδου μίσθωσης, η συσκευή μπορεί να επαναλάβει μέρος της διαδικασίας για να ανανεώσει την IP της χωρίς να χρειαστεί να αποσυνδεθεί από το δίκτυο

Το lease time στο DHCP είναι η χρονική περίοδος για την οποία μια διεύθυνση IP "ενοικιάζεται" σε μια συσκευή από τον DHCP server. Όταν το lease time λήγει, η συσκευή πρέπει να ανανεώσει τη μίσθωση είτε ζητώντας την ίδια IP είτε λαμβάνοντας νέα. Ένα μεγάλο lease time μειώνει την ανάγκη για συχνή ανανέωση, περιορίζοντας την κίνηση DHCP στο δίκτυο, αλλά μπορεί να οδηγήσει σε σπατάλη διευθύνσεων εάν συσκευές αποσυνδεθούν και δεν επιστρέψουν άμεσα. Αντίθετα, ένα μικρό lease time επιτρέπει την πιο δυναμική εκχώρηση IP, χρήσιμο σε δίκτυα με πολλούς περιστασιακούς χρήστες, αλλά αυξάνει την κίνηση DHCP traffic λόγω των συχνών αιτήσεων ανανέωσης. Ένα μειονέκτημα του να λειτουργούν όλες οι συσκευές αποκλειστικά μέσω DHCP είναι ότι δημιουργείται μεγαλύτερη εξάρτηση από τον DHCP server· αν αυτός πάψει να λειτουργεί, νέες συσκευές δεν θα μπορούν να πάρουν IP, ενώ και οι υπάρχουσες ίσως χάσουν συνδεσιμότητα μετά τη λήξη του lease. Επίσης, σε μεγάλα δίκτυα, ειδικά με μικρό lease time, μπορεί να προκληθεί DHCP flooding, δηλαδή σημαντική αύξηση broadcast πακέτων Discover και Request που καταναλώνουν bandwidth και επιβαρύνουν το latency, κάτι που γίνεται πιο έντονο σε ασύρματα δίκτυα ή δίκτυα με περιορισμένο εύρος ζώνης. [1]

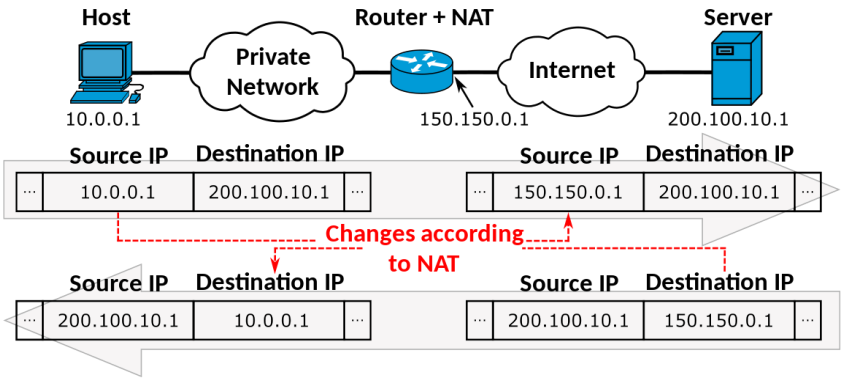


Σχήμα 1.8: Ροή λειτουργίας DHCP [7.α]

1.7: Network Address Translation

Το Network Address Translation (NAT) είναι ένας μηχανισμός που χρησιμοποιείται στα δίκτυα υπολογιστών για τη μετάφραση των ιδιωτικών διευθύνσεων IP σε δημόσιες και αντίστροφα. Δημιουργήθηκε ως λύση στην εξάντληση του διαθέσιμου χώρου διευθύνσεων του IPv4, δεδομένου ότι τα περίπου 4,3 δισεκατομμύρια μοναδικά IPv4 addresses δεν επαρκούν για τις σύγχρονες ανάγκες. Με το NAT, πολλές συσκευές σε ένα τοπικό δίκτυο μπορούν να μοιράζονται μία μόνο δημόσια IP διεύθυνση για την επικοινωνία τους με το διαδίκτυο. Η λειτουργία του NAT βασίζεται στην αντικατάσταση της ιδιωτικής διεύθυνσης και των θυρών μιας συσκευής με τη δημόσια διεύθυνση και κατάλληλη πόρτα επικοινωνίας που διαθέτει ο router. Αυτό καθιστά δυνατή όχι μόνο την εξοικονόμηση διευθύνσεων, αλλά και ένα επιπλέον επίπεδο ασφάλειας, καθώς οι εσωτερικές διευθύνσεις του τοπικού δικτύου δεν είναι ορατές από το διαδίκτυο.

Υπάρχουν διάφορες κατηγορίες NAT. Η πιο διαδεδομένη μορφή είναι το Port Address Translation (PAT), γνωστό και ως NAT Overload. Σε αυτή την περίπτωση, πολλές συσκευές μπορούν να χρησιμοποιούν την ίδια δημόσια IP διεύθυνση, αλλά διαφοροποιούνται με βάση τους αριθμούς θυρών (ports). Αυτός ο μηχανισμός επιτρέπει σε εκατοντάδες ή και χιλιάδες συσκευές να εξυπηρετούνται από μία μόνο δημόσια διεύθυνση.Όσον αφορά τη διάκριση σε Static NAT και Dynamic NAT, στο πρώτο η αντιστοίχηση μεταξύ μιας ιδιωτικής και μιας δημόσιας IP είναι μόνιμη και προκαθορισμένη, κάτι που χρησιμοποιείται συχνά για servers που πρέπει να είναι πάντα προσβάσιμοι από το διαδίκτυο. Αντίθετα, στο Dynamic NAT η αντιστοίχηση γίνεται δυναμικά από μια δεξαμενή διαθέσιμων δημόσιων διευθύνσεων, κάτι που προσφέρει μεγαλύτερη ευελιξία αλλά όχι εγγυημένη σταθερή διεύθυνση για κάθε συσκευή. [1], [14]



Σχήμα 1.9: Τρόπος λειτουργίας Network Address Translation [8.α]

1.8: Carrier Grade NAT

Το Carrier-Grade NAT (CGNAT), γνωστό επίσης και ως Large Scale NAT (LSN), αποτελεί μία εξέλιξη της τεχνικής του Network Address Translation που εφαρμόζεται από παρόχους υπηρεσιών διαδικτύου (ISPs) με σκοπό τη διατήρηση και επαναχρησιμοποίηση δημόσιων διευθύνσεων IPv4. Σε αντίθεση με το παραδοσιακό NAT, το οποίο υλοποιείται τοπικά στο δίκτυο ενός χρήστη ή επιχείρησης για να επιτρέψει σε πολλές εσωτερικές συσκευές να μοιραστούν μία δημόσια IP, το CGNAT υλοποιείται σε επίπεδο παρόχου και εφαρμόζεται ταυτόχρονα σε χιλιάδες ή εκατομμύρια συνδρομητές. Η εμφάνιση και εξάπλωση του CGNAT οφείλεται στην αυξανόμενη έλλειψη διαθέσιμων IPv4 διευθύνσεων, καθώς η μετάβαση στο IPv6 εξελίσσεται με αργούς ρυθμούς σε παγκόσμια κλίμακα. Οι πάροχοι, προκειμένου να συνεχίσουν να εξυπηρετούν νέες συνδέσεις και συσκευές, αναγκάζονται να τοποθετήσουν πολλαπλούς πελάτες πίσω από μία ενιαία δημόσια διεύθυνση, χρησιμοποιώντας τεχνικές παρόμοιες με το NAT αλλά σε πολύ μεγαλύτερη κλίμακα.

Αν και το CGNAT προσφέρει λειτουργική λύση στο πρόβλημα της διευθυνσιοδότησης, εισάγει σημαντικές περιοριστικές επιπτώσεις, κυρίως όσον αφορά την προσβασιμότητα και τη διαλειτουργικότητα. Ο σημαντικότερος περιορισμός είναι ότι οι χρήστες που βρίσκονται πίσω από CGNAT δεν μπορούν να δεχθούν εισερχόμενες συνδέσεις (inbound connections) από το Διαδίκτυο, εκτός αν εφαρμοστούν πολύπλοκες τεχνικές παρακάμψεων όπως reverse proxies, tunnels η port forwarding στο επίπεδο του παρόχου. Αυτό σημαίνει ότι δεν μπορούν εύκολα να φιλοξενήσουν εξωτερικά προσβάσιμες υπηρεσίες, όπως web servers, VPN endpoints, ή smart home εφαρμογές που απαιτούν άμεση επικοινωνία από έξω προς τα μέσα. Αυτοί οι περιορισμοί καθιστούν επιτακτική τη χρήση τεχνολογιών και πλατφορμών που βασίζονται σε cloud αρχιτεκτονικές. Για παράδειγμα, ένα smart home σύστημα που εκτελείται σε ένα τοπικό δίκτυο δεν μπορεί να προσφερθεί προς τον χρήστη απομακρυσμένα εάν βρίσκεται πίσω από CGNAT, εκτός εάν χρησιμοποιηθεί ένας ενδιάμεσος cloud-based μηχανισμός για την εξασφάλιση της σύνδεσης. Σε αυτό το σημείο έρχονται να καλύψουν το κενό λύσεις όπως το Cloudflare Tunnel, το ZeroTier, το Tailscale και αντίστοιχες τεχνολογίες VPN-over-cloud, οι οποίες εγκαθιστούν έναν ασφαλή, εξερχόμενο tunnel από το εσωτερικό του δικτύου προς το cloud, παρακάμπτοντας έτσι το φράγμα του CGNAT.

Η ανάγκη για αυτές τις λύσεις δεν περιορίζεται μόνο στα έξυπνα σπίτια, αλλά επεκτείνεται και σε επιχειρησιακά περιβάλλοντα, συστήματα IoT, remote access εφαρμογές και προσωπικά δίκτυα. Ουσιαστικά, η έλλειψη δυνατότητας στατικής διευθυνσιοδότησης και απευθείας πρόσβασης μέσω CGNAT υποχρεώνει τους χρήστες να εξαρτώνται ολοένα και περισσότερο από εξωτερικές, cloud-βασισμένες υπηρεσίες για λειτουργίες που παλαιότερα θα μπορούσαν να υλοποιηθούν τοπικά ή μέσω απλών ρυθμίσεων port forwarding.[3]

1.9: Zigbee

Η τεχνολογία Zigbee αποτελεί ένα πρότυπο ασύρματης επικοινωνίας το οποίο αναπτύχθηκε με σκοπό να καλύψει τις ανάγκες εφαρμογών χαμηλής ισχύος και χαμηλής κατανάλωσης, που απαιτούν σταθερή και αξιόπιστη μετάδοση μικρών ποσοτήτων δεδομένων. Δημιουργήθηκε το 2002 από την Zigbee Alliance, έναν οργανισμό που συστάθηκε με τη συνεργασία τεχνολογικών κολοσσών όπως η Philips, η Texas Instruments, η Siemens και η Motorola, μεταξύ άλλων. Το Zigbee βασίζεται στο πρότυπο IEEE 802.15.4, το οποίο καθορίζει τα φυσικά και MAC επίπεδα λειτουργίας, ενώ η Zigbee Alliance επέκτεινε το πρωτόκολλο για να καλύπτει τα ανώτερα επίπεδα, όπως η ασφάλεια, η δρομολόγηση, η δημιουργία δικτύου και η επικοινωνία εφαρμογών.

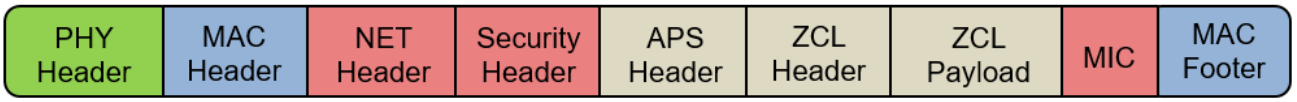
Η τεχνολογία λειτουργεί κυρίως στη συχνότητα των 2.4 GHz, η οποία είναι διαθέσιμη διεθνώς, ενώ υποστηρίζεται και η λειτουργία στις ζώνες των 868 MHz για την Ευρώπη και 915 MHz για τις Ηνωμένες Πολιτείες και την Αυστραλία. Το εύρος επικοινωνίας κυμαίνεται από 10 έως 100 μέτρα σε εσωτερικούς χώρους, ανάλογα με τα εμπόδια και τις συνθήκες, όμως χάρη στην αρχιτεκτονική τύπου mesh που χρησιμοποιεί, είναι δυνατό να επεκταθεί σημαντικά, καθώς κάθε συσκευή μπορεί να λειτουργεί και ως κόμβος αναμετάδοσης (router) για τις υπόλοιπες. Ο ρυθμός μετάδοσης δεδομένων φτάνει έως και τα 250 kbps στην συχνότητα των 2.4 GHz, ενώ είναι χαμηλότερος στις υπόλοιπες συχνότητες (40 kbps στα 915 MHz και 20 kbps στα 868 MHz), κάτι το οποίο δεν αποτελεί μειονέκτημα για τις εφαρμογές που εξυπηρετεί, δεδομένου ότι οι περισσότερες Zigbee συσκευές μεταδίδουν μικρά και σύντομα πακέτα δεδομένων, όπως είναι οι τιμές θερμοκρασίας ή η κατάσταση ενός διακόπτη. Το Zigbee χαρακτηρίζεται από εξαιρετικά χαμηλή κατανάλωση ενέργειας, γεγονός που το καθιστά ιδανικό για συσκευές που λειτουργούν με μπαταρία και απαιτούν αυτονομία πολλών μηνών ή και ετών. Η ασφάλεια αποτελεί επίσης βασικό στοιχείο της τεχνολογίας, με χρήση της κρυπτογράφησης AES 128-bit, μηχανισμών αυθεντικοποίησης και διασφάλισης της ακεραιότητας των πακέτων δεδομένων. Η τοπολογία του δικτύου είναι κατά βάση mesh, αν και υποστηρίζονται και άλλες μορφές, όπως του αστέρα η του δέντρου. Παρά τα περιορισμένα χαρακτηριστικά του σε ό,τι αφορά το εύρος ζώνης ή την ταχύτητα μετάδοσης, το Zigbee διακρίνεται για τη σταθερότητα, την επεκτασιμότητα και την ανεξαρτησία του από το διαδίκτυο. Χρησιμοποιείται εκτενώς σε προϊόντα μεγάλων εταιρειών όπως η Philips (Hue), η Aqara και η Sonoff. Για να λειτουργήσει σε περιβάλλον Home Assistant, απαιτείται η χρήση κατάλληλου coordinator (π.χ. USB dongle), και υποστηρίζονται διαφορετικές υλοποιήσεις όπως το ZHA (Zigbee Home Automation) και το Zigbee2MQTT να είναι τα πιο γνωστά, ανάλογα με τον τύπο της συσκευής και τις απαιτήσεις του χρήστη. Παράλληλα, το Zigbee αποτελεί μία από τις τεχνολογίες που συμβάλλουν στην μετάβαση προς το πρότυπο Matter, το οποίο αναπτύσσεται επίσης από τον ίδιο οργανισμό – πλέον γνωστό ως Connectivity Standards Alliance – και στοχεύει στη δημιουργία ενός ενιαίου διαλειτουργικού οικοσυστήματος για το Internet of Things.

Το πρωτόκολλο Zigbee αποτελεί ένα χαρακτηριστικό παράδειγμα δικτύου προσωπικής εμβέλειας (Personal Area Network – PAN) που σχεδιάστηκε ειδικά για εφαρμογές αυτοματισμού και αισθητήρων, με στόχο τη δημιουργία σταθερών, ασφαλών και αποδοτικών ασύρματων δικτύων χαμηλής κατανάλωσης ενέργειας. Ένα από τα βασικά του γνωρίσματα είναι η υποστήριξη τοπολογίας τύπου mesh, που του επιτρέπει να σχηματίζει δυναμικά επεκτάσιμα και αξιόπιστα δίκτυα, ακόμη και σε περιβάλλοντα με πολλαπλά φυσικά εμπόδια ή παρεμβολές. Σε αντίθεση με απλούστερες αρχιτεκτονικές τύπου αστέρα, η mesh τοπολογία του Zigbee δίνει τη δυνατότητα σε κάθε κόμβο να μεταβιβάζει δεδομένα όχι μόνο προς τον προορισμό τους αλλά και μέσω ενδιάμεσων διαδρομών, εξασφαλίζοντας έτσι εφεδρικές διαδρομές και υψηλή ανθεκτικότητα σε περιπτώσεις βλαβών ή αποσύνδεσης συσκευών.

Η αρχιτεκτονική ενός Zigbee δικτύου βασίζεται στην ύπαρξη τριών ειδών κόμβων: του συντονιστή (coordinator), των δρομολογητών (routers) και των τελικών συσκευών (end devices). Ο συντονιστής

αποτελεί το μοναδικό σημείο που έχει την ικανότητα να δημιουργήσει και να ξεκινήσει το δίκτυο. Είναι υπεύθυνος για την ανάθεση διευθύνσεων, τον συγχρονισμό, την ασφάλεια και την ολική διαχείριση της λειτουργίας του δικτύου. Δεν μπορεί να υπάρχουν δύο συντονιστές στο ίδιο δίκτυο Zigbee· η ύπαρξή του είναι μοναδική και θεμελιώδης για τη σταθερότητα του οικοσυστήματος. Ο συντονιστής συχνά υλοποιείται μέσω ενός USB dongle που συνδέεται στο σύστημα ελέγχου, που τρέχει το Home Assistant. Από τη στιγμή που το δίκτυο συσταθεί, μπορούν να ενταχθούν σε αυτό άλλες συσκευές, οι οποίες ανάλογα με τις δυνατότητές τους, αναλαμβάνουν είτε ρόλο δρομολογητή είτε σάν τερματική συσκευή. Οι δρομολογητές αποτελούν ενδιάμεσους κόμβους στο δίκτυο και είναι υπεύθυνοι για την αναμετάδοση πακέτων δεδομένων, εξυπηρετώντας τη σύνδεση μεταξύ συσκευών που βρίσκονται εκτός άμεσης εμβέλειας του συντονιστή ή άλλων κόμβων. Είναι κρίσιμο να σημειωθεί ότι μόνο οι Zigbee συσκευές που τροφοδοτούνται μόνιμα με ρεύμα (μέσω πρίζας ή USB) μπορούν να λειτουργήσουν ως δρομολογητές . Οι συσκευές που τροφοδοτούνται με μπαταρία δεν έχουν την τεχνική δυνατότητα να λειτουργούν διαρκώς ενεργές, καθώς η συνεχής επικοινωνία απαιτεί υψηλότερη ενεργειακή κατανάλωση. Συνεπώς, είναι υποχρεωτικά τερματικές συσκευές, δηλαδή τερματικοί κόμβοι που επικοινωνούν μόνο με τον συντονιστή ή με κάποιον κοντινό δρομολογητή, και συνήθως μεταβαίνουν σε λειτουργία ύπνου (low power state) όταν δεν μεταδίδουν δεδομένα, ώστε να παρατείνεται η διάρκεια ζωής της μπαταρίας τους. Η λειτουργία της mesh τοπολογίας στο Zigbee είναι τέτοια ώστε το δίκτυο να μπορεί να επεκτείνεται δυναμικά καθώς προστίθενται νέες συσκευές. Η κάθε συσκευή διατηρεί πληροφορίες για τις γειτονικές της και είναι σε θέση να επιλέξει την βέλτιστη διαδρομή για τη μετάδοση δεδομένων προς τον συντονιστή, ακόμη κι αν αυτό απαιτεί να διέλθουν τα πακέτα από πολλούς ενδιάμεσους κόμβους. Το δίκτυο προσαρμόζεται αυτόματα σε αλλαγές, όπως αποσύνδεση συσκευών ή προσθήκη νέων, διατηρώντας τη συνοχή του μέσω δυναμικής δρομολόγησης. Επιπλέον, επιτρέπει την απρόσκοπτη λειτουργία ακόμη και σε περιβάλλοντα με μεγάλο αριθμό συσκευών, κάτι που είναι ιδιαίτερα χρήσιμο σε εφαρμογές smart home όπου οι ανάγκες επεκτασιμότητας είναι αυξημένες. Η διαμόρφωση και η συντήρηση ενός Zigbee δικτύου πραγματοποιείται με ασφάλεια, καθώς το πρωτόκολλο ενσωματώνει μηχανισμούς κρυπτογράφησης AES 128-bit, πιστοποίησης συσκευών και ελέγχου ταυτότητας, ώστε να αποτρέπεται η παρείσφρηση μη εξουσιοδοτημένων στοιχείων. Τα χαρακτηριστικά αυτά, σε συνδυασμό με τη χαμηλή κατανάλωση ενέργειας, την ανθεκτικότητα της mesh τοπολογίας και την ευρεία διαλειτουργικότητα με χιλιάδες εμπορικά διαθέσιμες συσκευές, καθιστούν το Zigbee ένα από τα πιο αξιόπιστα και διαδεδομένα πρωτόκολλα για ασύρματη επικοινωνία στον τομέα των συστημάτων έξυπνου σπιτιού

Η διαδικασία σύνδεσης και επικοινωνίας μεταξύ των συσκευών σε ένα δίκτυο Zigbee, και ειδικότερα μεταξύ του συντονιστή, των routers και των end devices, βασίζεται σε μια συγκεκριμένη ακολουθία αλληλεπιδράσεων, η οποία αποσκοπεί στην ασφαλή και σταθερή ένταξη της εκάστοτε συσκευής στο mesh δίκτυο και στη συνεχιζόμενη επικοινωνία της εντός του. Αρχικά, όταν μια νέα Zigbee συσκευή ενεργοποιείται και επιχειρεί να ενταχθεί στο δίκτυο, ξεκινά με τη διαδικασία ανακάλυψης (discovery). Σε αυτό το στάδιο, η συσκευή σαρώνει τα διαθέσιμα κανάλια για να εντοπίσει την παρουσία ενός δικτύου Zigbee που είναι σε κατάσταση "permit join", δηλαδή επιτρέπει την προσθήκη νέων κόμβων. Μόλις εντοπίσει έναν τέτοιο κόμβο – συνήθως τον συντονιστή ή έναν δρομολογητή – αποστέλλει αίτημα σύνδεσης (association request). Ο κόμβος απαντά με ένα μήνυμα αποδοχής (association response), και κατά την ολοκλήρωση αυτής της διαδικασίας πραγματοποιείται το λεγόμενο “handshake”. Κατά τη διάρκεια του handshake γίνεται ανταλλαγή βασικών στοιχείων όπως η διεύθυνση MAC της συσκευής, η εκχώρηση μιας μοναδικής δικτυακής διεύθυνσης εντός του Zigbee δικτύου, καθώς και η επικύρωση της συμμετοχής βάσει του pre-shared network key, το οποίο διασφαλίζει την κρυπτογραφημένη επικοινωνία εντός του δικτύου.



Σχημα 1.10:Μορφή Δεδομενογράμματος ενός πακέτου Zigbee [9.α]

Η ασφάλεια είναι εγγενές χαρακτηριστικό του Zigbee και ενσωματώνεται από τα πρώτα βήματα του handshake. Πριν επιτραπεί η μόνιμη ένταξη μιας συσκευής στο δίκτυο, πρέπει να έχει προσπελάσει ή να της δοθεί το shared network key, με το οποίο γίνεται κρυπτογράφηση 128-bit σε όλα τα μηνύματα. Υπάρχουν δύο βασικά σενάρια σε αυτό το στάδιο: είτε το κλειδί παρέχεται μέσω pre-configuration, είτε προωθείται από τον συντονιστή κατά την ένταξη της συσκευής, εφόσον η ένταξη επιτρέπεται και η συσκευή θεωρείται αξιόπιστη. Αφού η συσκευή ενταχθεί, διατηρεί μια ενεργή λογική σύνδεση με τον γονικό κόμβο της – είτε αυτός είναι δρομολογητής είτε ο ίδιος ο Συντονιστής. Ωστόσο, το πρωτόκολλο Zigbee είναι σχεδιασμένο για εξαιρετικά χαμηλή κατανάλωση ενέργειας, ιδιαίτερα όσον αφορά τις μπαταριοκίνητες τερματικές συσκευές . Ως εκ τούτου, αυτές οι συσκευές δεν διατηρούν διαρκώς ανοιχτό δίαυλο επικοινωνίας, αλλά εισέρχονται σε κατάσταση «ύπνου» (sleep mode) για μεγάλα χρονικά διαστήματα και «ξυπνούν» περιοδικά για να επικοινωνήσουν. Για να διασφαλιστεί ότι η συσκευή παραμένει «ζωντανή» στο δίκτυο και ότι η σύνδεση της δεν θεωρείται απώλεια, χρησιμοποιείται ένας μηχανισμός που ονομάζεται keep-alive. Ο μηχανισμός αυτός λειτουργεί ως εξής: κάθε τερματική συσκευή οφείλει να στέλνει περιοδικά ένα πακέτο δεδομένων, ακόμη και εάν δεν έχει ενεργό φορτίο (payload), με στόχο να ενημερώσει τον γονικό κόμβο του ότι παραμένει ενεργό και συνδεδεμένο. Αν αυτό δεν συμβεί μέσα σε ένα προκαθορισμένο χρονικό όριο, τότε ο γονικός κόμβος (ειτε δρομολογητής ειτε ο συντονιστής) μπορεί να θεωρήσει ότι η συσκευή έχει αποσυνδεθεί και να αποδεσμεύσει τους πόρους που είχαν δεσμευτεί για αυτήν. Παράλληλα, οι δρομολογητές οφείλουν να διατηρούν σταθερά την ενεργή τους κατάσταση, καθώς είναι υπεύθυνες για τη δρομολόγηση δεδομένων και τη μετάδοση μηνυμάτων μεταξύ άλλων κόμβων του δικτύου. Η επικοινωνία σε ένα Zigbee δίκτυο είναι βασισμένη στο πρωτόκολλο IEEE 802.15.4, το οποίο χρησιμοποιεί ένα μοντέλο παρόμοιο με αυτό του OSI. Τα δεδομένα μεταδίδονται σε μικρά πακέτα (frames) με ενσωματωμένο μηχανισμό επιβεβαίωσης (acknowledgment), ώστε να διασφαλίζεται η παράδοση κάθε μηνύματος. Το ίδιο το δίκτυο διαχειρίζεται την επιλογή της βέλτιστης διαδρομής (routing) για τη μετάδοση δεδομένων, χρησιμοποιώντας αλγορίθμους που βασίζονται στο tree routing ή το source routing, ανάλογα με την εφαρμογή και τις δυνατότητες του firmware των συσκευών.
Η συνολική λειτουργία του δικτύου χαρακτηρίζεται από ευελιξία και ανθεκτικότητα, καθώς το mesh σύστημα επιτρέπει την αυτόματη επαναδρομολόγηση των πακέτων σε περίπτωση αλλαγών στη δομή του δικτύου ή αποσύνδεσης κόμβων. Αυτό επιτυγχάνεται μέσω της συνεχούς ανταλλαγής πληροφοριών μεταξύ των routers και του συντονιστή, με τους routing πίνακες να ενημερώνονται δυναμικά. Το αποτέλεσμα είναι ένα δίκτυο που μπορεί να αυτο-οργανώνεται, να αυτο-επουλώνεται και να προσαρμόζεται εύκολα σε μεταβαλλόμενες συνθήκες, με διατήρηση της σταθερότητας και της χαμηλής κατανάλωσης ενέργειας, καθιστώντας το Zigbee ιδανικό για εφαρμογές σε συστήματα έξυπνων κατοικιών.[6] [8] [9] [17] [21]

1.10: Υπέρυθρη Επικοινωνία

Η υπέρυθρη τεχνολογία (Infrared – IR) αποτελεί μια από τις παλαιότερες μορφές ασύρματης επικοινωνίας μικρής εμβέλειας και εξακολουθεί να χρησιμοποιείται εκτενώς σε εφαρμογές οικιακού αυτοματισμού, κυρίως για τον έλεγχο ηλεκτρονικών συσκευών όπως τηλεοράσεις, κλιματιστικά, ενισχυτές, αποκωδικοποιητές και άλλα καταναλωτικά προϊόντα. Η IR τεχνολογία βασίζεται στη μετάδοση παλμών υπέρυθρης ακτινοβολίας (με μήκος κύματος περίπου 850–950 nm) οι οποίοι είναι αόρατοι στο ανθρώπινο μάτι, αλλά ανιχνεύσιμοι από ειδικούς αισθητήρες.
Η πρώτη ευρεία υιοθέτηση της IR τεχνολογίας έγινε στις δεκαετίες του 1980 και 1990, κυρίως από κατασκευαστές συστημάτων ψυχαγωγίας και τηλεόρασης. Δεν πρόκειται για ένα ενιαίο πρωτόκολλο ή πρότυπο, αλλά για ένα γενικό μέσο επικοινωνίας μέσω φωτεινών σημάτων. Ωστόσο, έχουν αναπτυχθεί αρκετά πρότυπα IR πρωτοκόλλων, με πιο διαδεδομένα το NEC, το RC5/RC6 (της Philips) και το Sony SIRC. Κάθε πρωτόκολλο καθορίζει τη δομή των παλμών, τη διάρκεια, τη συχνότητα διαμόρφωσης (συνήθως 36–38 kHz) και τον τρόπο κωδικοποίησης των δεδομένων. Η μετάδοση μέσω IR απαιτεί απευθείας οπτική επαφή (line-of-sight) ανάμεσα στον πομπό και τον δέκτη. Ο πομπός, που είναι συνήθως ένα LED υπερύθρων, εκπέμπει διαμορφωμένους παλμούς φωτός με βάση τον δυαδικό κώδικα της εντολής που πρέπει να αποσταλεί (π.χ. “Power On” ή “Volume Up”). Ο δέκτης, συνήθως ένας φωτοτρανζίστορ IR ή ένας ολοκληρωμένος IR αισθητήρας, ανιχνεύει τους παλμούς και τους αποκωδικοποιεί με βάση το υποστηριζόμενο πρωτόκολλο.
Η εμβέλεια της IR επικοινωνίας είναι σχετικά περιορισμένη, κυμαινόμενη μεταξύ 5 και 10 μέτρων σε τυπικές οικιακές εφαρμογές, και εξαρτάται από την ισχύ του πομπού, την ευαισθησία του δέκτη, καθώς και από την απουσία εμποδίων μεταξύ τους. Η μετάδοση IR δεν μπορεί να διαπεράσει τοίχους ή αντικείμενα, γεγονός που περιορίζει τη χρήση της σε απλές, τοπικές επικοινωνίες. [22]

1.11: Ραδιοσυχνότητα

Η βασική αρχή λειτουργίας ενός Radio Frequency συστήματος έγκειται στην εκπομπή ενός διαμορφωμένου σήματος από έναν πομπό, το οποίο λαμβάνεται από τον δέκτη και αποδιαμορφώνεται ώστε να αναγνωριστεί η χρήσιμη πληροφορία. Η διαμόρφωση (modulation) αυτή μπορεί να είναι είτε απλή, όπως η ASK (Amplitude Shift Keying) και FSK (Frequency Shift Keying), είτε πιο εξελιγμένη, όπως η PSK (Phase Shift Keying) ή ακόμα και GFSK (Gaussian Frequency Shift Keying) σε περιπτώσεις που απαιτείται μεγαλύτερη αξιοπιστία ή απόδοση. Η αποστολή των εντολών σε RF συνήθως γίνεται σε μορφή κωδικοποιημένων bits, τα οποία περιλαμβάνουν ένα preamble (σειρά συγχρονισμού), ένα header, την κύρια πληροφορία (π.χ. on/off, ανοίγει/κλείνει) και ενδεχομένως κάποιο parity bit ή CRC για τον έλεγχο σφαλμάτων.
Ένα από τα σημαντικότερα χαρακτηριστικά των RF συστημάτων είναι ότι δεν απαιτούν σύνδεση σε δίκτυο, gateway ή οποιοδήποτε ενδιάμεσο επίπεδο λογισμικού για να λειτουργήσουν. Αυτή η ιδιότητα τα καθιστά εξαιρετικά απλά στην υλοποίηση, με σχεδόν άμεση και χωρίς καθυστερήσεις (latency-free) απόκριση, γεγονός που τα καθιστά κατάλληλα για κρίσιμες εφαρμογές όπως συναγερμοί, κουδούνια και απομακρυσμένοι διακόπτες. Ωστόσο, το γεγονός ότι πολλά από τα RF συστήματα λειτουργούν χωρίς διμερή επιβεβαίωση λήψης (acknowledgment) ή χωρίς κρυπτογράφηση καθιστά την ασφάλειά τους περιορισμένη. Είναι δυνατόν να υποκλαπεί ένα σήμα, να αναπαραχθεί (replay attack) και να εκτελεστεί ξανά χωρίς την έγκριση του χρήστη. Ορισμένα εξελιγμένα RF πρωτόκολλα χρησιμοποιούν rolling code, όπως αυτά των τηλεχειριστηρίων για γκαραζόπορτες, ώστε να αποφευχθεί αυτή η μορφή επίθεσης, αλλά η πλειοψηφία των φθηνών υλοποιήσεων παραμένει εκτεθειμένη. Όσον αφορά την τοπολογία της επικοινωνίας, τα RF συστήματα συνήθως ακολουθούν ένα μοντέλο point-to-point (ένας πομπός προς έναν δέκτη) ή

point-to-multipoint (ένας πομπός προς πολλούς δέκτες), χωρίς όμως ενδιάμεση δρομολόγηση δεδομένων, χωρίς mesh και χωρίς feedback, σε αντίθεση με τεχνολογίες όπως το Zigbee ή το Wi-Fi. Αυτό περιορίζει την ευελιξία τους αλλά παράλληλα μειώνει το κόστος και την πολυπλοκότητα.

Ένα σημαντικό πλεονέκτημα της RF τεχνολογίας είναι το πολύ χαμηλό ενεργειακό της αποτύπωμα. Οι RF πομποί και δέκτες καταναλώνουν ελάχιστη ενέργεια, γι' αυτό και βρίσκονται σε συσκευές που λειτουργούν με απλές μπαταρίες για χρόνια χωρίς επαναφόρτιση. Επίσης, η εμβέλειά τους είναι συνήθως αρκετά καλή, φτάνοντας τα 50-100 μέτρα σε ανοιχτό χώρο, και τα σήματα μπορούν να διαπεράσουν τοίχους και εμπόδια, αν και υπόκεινται σε εξασθένηση ανάλογα με το υλικό. Πέρα από τη βασική one-way αρχιτεκτονική, σε ορισμένες περιπτώσεις υπάρχουν πιο εξελιγμένα RF modules που επιτρέπουν bidirectional επικοινωνία, δίνοντας τη δυνατότητα σε μία συσκευή να απαντήσει πίσω στον πομπό, αν και αυτό παραμένει εξαίρεση και όχι ο κανόνας στις απλές consumer εφαρμογές.

Η συχνότητα στην οποία λειτουργεί ένα RF σύστημα επηρεάζει άμεσα την απόσταση που μπορεί να διανύσει το σήμα και την ικανότητά του να διαπερνά εμπόδια. Για παράδειγμα, χαμηλότερες συχνότητες όπως τα 315 MHz ή τα 433 MHz έχουν καλύτερη διείσδυση μέσα από τοίχους και δομικά υλικά αλλά προσφέρουν χαμηλότερο bandwidth και κατά συνέπεια μικρότερη ταχύτητα μετάδοσης δεδομένων. Από την άλλη πλευρά, υψηλότερες συχνότητες όπως τα 868 MHz και 915 MHz είναι πιο ευάλωτες στην απορρόφηση από το περιβάλλον αλλά επιτρέπουν πιο γρήγορη επικοινωνία και λιγότερη παρεμβολή από οικιακές συσκευές. Το εύρος ζώνης της RF επικοινωνίας, στις συνηθισμένες απλές υλοποιήσεις, είναι αρκετά περιορισμένο – συνήθως της τάξης των λίγων kilobits ανά δευτερόλεπτο – αλλά αυτό είναι απόλυτα επαρκές για εφαρμογές που απαιτούν μόνο την αποστολή μίας εντολής ή ενός ψηφιακού παλμού (π.χ. “άνοιγμα πόρτας”, “ενεργοποίηση φωτός”). Μια άλλη ενδιαφέρουσα πτυχή των RF συστημάτων είναι η χρήση τους σε «τυφλές» εγκαταστάσεις, όπου δεν υπάρχει cloud, router ή άλλο έξυπνο υποσύστημα. Ένα κλασικό παράδειγμα είναι η αντιστοίχιση ενός τηλεχειριστηρίου με έναν RF διακόπτη φωτισμού: το pairing γίνεται απλά με το πάτημα ενός πλήκτρου και η επικοινωνία παραμένει λειτουργική ακόμη και αν διακοπεί το τοπικό δίκτυο ή η πρόσβαση στο Internet. Αυτή η αυτονομία τα καθιστά εξαιρετικά αξιόπιστα σε περιβάλλοντα όπου η σταθερότητα της σύνδεσης δεν είναι εγγυημένη.

Ωστόσο, επειδή τα περισσότερα RF πρωτόκολλα δεν βασίζονται σε μοναδικές ταυτότητες (unique identifiers), προκύπτει ένα φλέγον ζήτημα σχεδόν σε όλες τις εφαρμογές: η πιθανότητα παρεμβολών από άλλες RF συσκευές ή ακόμα και η ακούσια ενεργοποίηση συσκευών από άλλους πομπούς. Το πρόβλημα αυτό έχει αντιμετωπιστεί εν μέρει με τη χρήση κωδικοποίησης rolling-code και encryption, όπως στο πρωτόκολλο Keeloq που εφαρμόζεται σε τηλεχειριστήρια γκαραζόπορτας, αλλά στις περισσότερες φθηνές υλοποιήσεις το σήμα εξακολουθεί να είναι plaintext και εύκολο στην αντιγραφή. Σε εφαρμογές έξυπνων σπιτιών, τα RF modules χρησιμοποιούνται κυρίως για να γεφυρώσουν το χάσμα μεταξύ «παραδοσιακών» και έξυπνων συσκευών. Πολλοί RF πομποί συνδέονται με κόμβους που υποστηρίζουν Home Assistant, ESPHome ή άλλες πλατφόρμες, οι οποίοι μέσω λογισμικού αντιστοιχίζουν το κάθε RF σήμα σε μια συγκεκριμένη ενέργεια.

Τέλος, αξίζει να σημειωθεί ότι η τεχνολογία RF δεν εξαρτάται από ένα συγκεκριμένο πρότυπο, όπως το Zigbee ή το Bluetooth, γεγονός που οδηγεί σε μια τεράστια ποικιλομορφία μεταξύ διαφορετικών συσκευών. Αυτή η έλλειψη τυποποίησης σημαίνει ότι κάθε κατασκευαστής μπορεί να χρησιμοποιήσει το δικό του πρωτόκολλο και format, κάτι που συχνά περιορίζει τη διαλειτουργικότητα. Παρ’ όλα αυτά, η τεχνολογία RF εξακολουθεί να έχει παρουσία λόγω του εξαιρετικά χαμηλού κόστους της, της ενεργειακής αποδοτικότητας και της απλότητας υλοποίησης

της, ιδίως σε περιπτώσεις που απαιτείται γρήγορη και απροβλημάτιστη επικοινωνία χωρίς τη μεσολάβηση περίπλοκων υποδομών. [23]

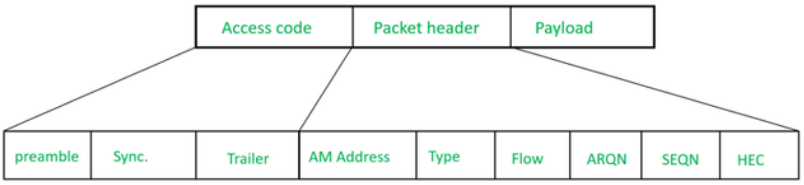
1.12: Bluetooth

Η τεχνολογία Bluetooth αποτελεί μία από τις πιο διαδεδομένες μορφές ασύρματης επικοινωνίας μικρής εμβέλειας, με βασική αποστολή τη μετάδοση δεδομένων μεταξύ συσκευών χωρίς τη χρήση καλωδίων. Αναπτύχθηκε αρχικά από την εταιρεία Ericsson το 1994 ως εσωτερικό ερευνητικό έργο για την αντικατάσταση των καλωδίων μεταξύ κινητών τηλεφώνων και περιφερειακών. Σταδιακά, εξελίχθηκε σε διεθνές πρότυπο υπό την επίβλεψη του οργανισμού Bluetooth Special Interest Group (Bluetooth SIG), που συστάθηκε το 1998 και στον οποίο συμμετέχουν πλέον πάνω από 30.000 εταιρείες από τον χώρο των τηλεπικοινωνιών, των υπολογιστών και των καταναλωτικών ηλεκτρονικών. Η τεχνολογία βασίζεται σε επικοινωνία στο φάσμα ISM (Industrial, Scientific and Medical) των 2.4 GHz, χρησιμοποιώντας frequency hopping spread spectrum (FHSS), δηλαδή μια τεχνική όπου το σήμα αλλάζει συνεχώς συχνότητες (μέχρι και 1600 φορές το δευτερόλεπτο) για να μειωθούν οι παρεμβολές και να αυξηθεί η ασφάλεια και αξιοπιστία της σύνδεσης. Ο τρόπος λειτουργίας είναι βασισμένος σε μια αρχιτεκτονική master-slave, όπου μία κύρια συσκευή (π.χ. smartphone ή υπολογιστής) διαχειρίζεται έως και επτά δευτερεύουσες (slaves), δημιουργώντας ένα μικρό ασύρματο δίκτυο που ονομάζεται piconet. Πολλαπλά piconets μπορούν να συνδεθούν μεταξύ τους σχηματίζοντας scatternets, αν και αυτό δεν υποστηρίζεται από όλες τις συσκευές.
Η μετάδοση δεδομένων μέσω Bluetooth καλύπτει εύρος λειτουργίας από περίπου 1 έως 100 μέτρα, ανάλογα με την κλάση ισχύος της συσκευής. Υπάρχουν τρεις βασικές κλάσεις: Class 1 (με μέγιστη ισχύ 100 mW και εμβέλεια έως 100 μέτρα), Class 2 (2.5 mW, έως 10 μέτρα, η πιο κοινή σε smartphones) και Class 3 (1 mW, έως 1 μέτρο). Η ταχύτητα μετάδοσης εξαρτάται από την έκδοση του Bluetooth. Οι πρώτες εκδόσεις (1.0 έως 2.0) παρείχαν ταχύτητες έως 1 Mbps, ενώ το Bluetooth 2.1 + EDR αύξησε τον ρυθμό σε περίπου 3 Mbps. Με την έλευση του Bluetooth 4.0 και της τεχνολογίας Bluetooth Low Energy (BLE), δόθηκε έμφαση στη μείωση της κατανάλωσης ενέργειας, επιτρέποντας τη λειτουργία συσκευών με μικρές μπαταρίες για μήνες ή ακόμα και χρόνια, σε βάρος της ταχύτητας (που περιορίζεται γύρω στα 1 Mbps). Η έκδοση 5.0 και μεταγενέστερες (5.1, 5.2, 5.3) βελτίωσαν σημαντικά την εμβέλεια (έως 240 μέτρα θεωρητικά), την ταχύτητα (έως 2 Mbps σε BLE) και την ακρίβεια στον προσδιορισμό θέσης.

Bluetooth Version	Adoption Year	Maximum rate		Theoretical Range	Features
		Classic	Low Energy		
Bluetooth 1.0	1999	723Kbps	N/A	10 m	Basic Rate Mode (BR), used to replace RS-232 serial connection.
Bluetooth 2.0+EDR	2004	2.1 Mbps	N/A	10 m	Enhanced Data Rate (EDR), increases transmission speed, supports full-duplex communication.
Bluetooth 3.0+HS	2009	24 Mbps (only high speed mode)	N/A	10 m	High Speed (HS) mode, uses Wi-Fi technology for higher transmission speeds.
Bluetooth 4.0-4.2	2010/2013/2014	3 Mbps	1 Mbps	60 m	Low Energy (LE), optimized for IoT devices.
Bluetooth 5.0	2016	50 Mbps	2 Mbps	240 m	Increased transmission speed and range, supports indoor positioning.
Bluetooth 5.1	2019	50 Mbps	2 Mbps	240 m	Angle of Arrival (AoA) and Angle of Departure (AoD) for improved positioning accuracy.
Bluetooth 5.2	2020	50 Mbps	2 Mbps	240 m	Enhanced audio features, supports LE Audio and other communications.
Bluetooth 5.3	2021	50 Mbps	2 Mbps	240 m	Further optimized transmission efficiency, stable connection security.
Bluetooth 5.4	2023	50 Mbps	2 Mbps	240 m	Further optimized transmission features, improves device interaction.
Bluetooth 6.0	2024	Unknown	3 Mb/s	300 m	Bluetooth Channel Sounding for secure, fine-ranging

Σχήμα 1.11: Γενιές του Bluetooth πρωτόκολλου [10.α]

Ο τρόπος με τον οποίο δημιουργείται μια σύνδεση Bluetooth περιλαμβάνει τη διαδικασία του pairing, δηλαδή του αρχικού «χειραψίας» (handshake) μεταξύ δύο συσκευών, με στόχο την ανταλλαγή κρυπτογραφημένων κλειδιών και την επαλήθευση ταυτότητας. Το pairing μπορεί να γίνει με διάφορους τρόπους (PIN, passkey, NFC ή Just Works), ανάλογα με την έκδοση του Bluetooth και τις δυνατότητες των συσκευών. Αφού ολοκληρωθεί το pairing, οι συσκευές παραμένουν σε bonded κατάσταση, ώστε να μην χρειάζεται να επαναλάβουν τη διαδικασία σε επόμενες συνδέσεις. Κατά τη διάρκεια λειτουργίας της σύνδεσης, οι συσκευές στέλνουν περιοδικά keep-alive μηνύματα (γνωστά και ως supervision timeouts) για να επιβεβαιώνουν τη σταθερότητα του συνδέσμου και να αποτρέπουν τη διακοπή λόγω απουσίας δραστηριότητας. Η ασφάλεια στη μετάδοση δεδομένων επιτυγχάνεται μέσω ενσωματωμένης κρυπτογράφησης 128-bit και authentication mechanisms, ιδιαίτερα στις εκδόσεις 4.2 και άνω, που συμμορφώνονται και με πρότυπα ασφάλειας IoT. Ωστόσο, παλαιότερες εκδόσεις του Bluetooth (1.x και 2.x) παρουσίαζαν σημαντικά κενά ασφαλείας, τα οποία στο παρελθόν εκμεταλλεύτηκαν κακόβουλοι χρήστες σε επιθέσεις τύπου bluejacking, bluesnarfing και man-in-the-middle.



Σχήμα 1.12: Δεδομενόγραμμα Bluetooth [11.α]

Όσον αφορά την τοπολογία ενός έξυπνου σπιτιού, το Bluetooth συναντάται κυρίως σε περιφερειακές συσκευές μικρής ισχύος και χαμηλής κατανάλωσης, όπως έξυπνα λουκέτα, αισθητήρες παρουσίας, συσκευές fitness ή ιατρικά wearables. Ειδικά το Bluetooth Low Energy είναι κατάλληλο για εφαρμογές όπου απαιτείται περιστασιακή μετάδοση μικρών ποσοτήτων δεδομένων και μεγάλη αυτονομία. Αν και το Bluetooth δεν υποστηρίζει mesh δικτύωση σε παλαιότερες εκδόσεις, από το 2017 και έπειτα, με την καθιέρωση του Bluetooth Mesh Profile, καθίσταται δυνατή η δημιουργία

επεκτάσιμων mesh δικτύων όπου κάθε συσκευή μπορεί να αναμεταδίδει πακέτα άλλων συσκευών. Αυτή η δυνατότητα, όμως, εφαρμόζεται κυρίως σε σταθερές και συνεχώς τροφοδοτούμενες συσκευές, καθώς απαιτεί μεγαλύτερη επεξεργαστική ισχύ και ενεργειακή απόδοση. Οι συσκευές με μπαταρία παραμένουν κατά κανόνα σε ρόλο απλού κόμβου (end device). Η διαδικασία σύνδεσης μεταξύ δύο συσκευών Bluetooth βασίζεται στη θεμελιώδη έννοια του handshake, το οποίο αποτελεί το αρχικό στάδιο επικοινωνίας και εμπιστοσύνης μεταξύ των συσκευών. Στο στάδιο αυτό, γίνεται η αναγνώριση των συσκευών, η διαπραγμάτευση παραμέτρων ασφαλείας και η δημιουργία του λεγόμενου trust relationship, με απώτερο στόχο τη διασφάλιση της ασφαλούς ανταλλαγής δεδομένων. Το handshake πραγματοποιείται στο πλαίσιο της διαδικασίας pairing, η οποία εξελίσσεται σε τρία βασικά βήματα: την ανακάλυψη (discovery), την αυθεντικοποίηση (authentication) και την εγκαθίδρυση ασφαλούς καναλιού επικοινωνίας. Αρχικά, μια συσκευή μεταδίδει ένα inquiry πακέτο στο ραδιοφάσμα των 2.4 GHz, αναζητώντας κοντινές διαθέσιμες συσκευές. Μόλις βρεθεί συμβατή συσκευή, ανταλλάσσονται πληροφορίες ταυτοποίησης όπως η διεύθυνση MAC, το όνομα της συσκευής και οι υποστηριζόμενες υπηρεσίες.

Κατά τη δεύτερη φάση, ενεργοποιούνται οι μηχανισμοί ασφαλείας. Ανάλογα με την έκδοση του πρωτοκόλλου, η διαδικασία μπορεί να περιλαμβάνει χρήση PIN code, passkey, Numeric Comparison, Out of Band pairing ή τη λεγόμενη Just Works μέθοδο. Το είδος του pairing που θα επιλεγεί εξαρτάται από τις δυνατότητες των συσκευών και την υποστήριξη από τη συγκεκριμένη έκδοση Bluetooth. Για παράδειγμα, από την έκδοση 2.1 και μετά, χρησιμοποιείται το πρωτόκολλο Secure Simple Pairing (SSP), το οποίο προσφέρει βελτιωμένη ασφάλεια με χρήση Elliptic Curve Diffie-Hellman (ECDH) για ανταλλαγή κλειδιών, εξαλείφοντας την ανάγκη για αποθήκευση ή μετάδοση ευαίσθητων δεδομένων σε μη κρυπτογραφημένη μορφή. Με την επιτυχή ολοκλήρωση του pairing, δημιουργείται μια ασφαλής σύνδεση, γνωστή ως bond, μέσω της οποίας οι συσκευές μπορούν να συνδέονται στο μέλλον χωρίς επανάληψη της διαδικασίας. Από εκεί και πέρα, κάθε πακέτο που μεταδίδεται κρυπτογραφείται με δυναμικά παραγόμενα κλειδιά 128-bit, ενώ χρησιμοποιούνται και message integrity checks για την προστασία από τροποποίηση ή παρεμβολή. Η ανταλλαγή πληροφοριών σε επίπεδο δεδομένων γίνεται μέσω προκαθορισμένων προφίλ Bluetooth, που περιγράφουν τη μορφή και τα χαρακτηριστικά των υπηρεσιών που υποστηρίζει η κάθε συσκευή. Ενδεικτικά, υπάρχουν τα προφίλ HID (για πληκτρολόγια και ποντίκια), A2DP (για ήχο), GATT (για BLE αισθητήρες), SPP (για σειριακή επικοινωνία) κ.ά. Κάθε προφίλ βασίζεται σε συγκεκριμένα services και characteristics, που λειτουργούν ως κανάλια ανταλλαγής δεδομένων.

Στο επίπεδο διατήρησης της σύνδεσης, η τεχνολογία Bluetooth ενσωματώνει μηχανισμούς όπως τα keep-alive packets και supervision timeouts. Αυτά εξασφαλίζουν ότι η σύνδεση παραμένει ενεργή, ενώ παράλληλα επιτρέπουν στις συσκευές να ανιχνεύσουν πότε μια σύνδεση έχει χαθεί ή πότε απαιτείται επανασύνδεση. Ιδιαίτερα στο Bluetooth Low Energy, τα keep-alive πακέτα είναι αραιότερα για εξοικονόμηση ενέργειας, ενώ υποστηρίζονται connection intervals και sleep modes που επιτρέπουν στις συσκευές να μπαίνουν σε κατάσταση χαμηλής κατανάλωσης όταν δεν υπάρχει ανάγκη για συνεχή επικοινωνία. Η ασφάλεια της τεχνολογίας Bluetooth έχει εξελιχθεί σημαντικά με την πάροδο των ετών. Παρότι οι πρώτες εκδόσεις (π.χ. 1.0 ή 2.0) είχαν σοβαρές αδυναμίες που επέτρεπαν επιθέσεις τύπου bluejacking, bluesnarfing και man-in-the-middle, οι πιο σύγχρονες εκδόσεις (4.2, 5.0 και 5.1) ενσωματώνουν ισχυρούς μηχανισμούς όπως AES-CCM encryption, key refreshing, καθώς και δυνατότητα προστασίας της ιδιωτικότητας μέσω random address generation, ώστε οι συσκευές να μη γίνονται εύκολα ιχνηλάσιμες.

Στο πλαίσιο ενός έξυπνου σπιτιού, η τεχνολογία Bluetooth παραμένει πολύτιμη όταν απαιτείται η σύνδεση χαμηλής ισχύος, μικρής εμβέλειας και με ελάχιστο κόστος. Συχνά χρησιμοποιείται σε έξυπνες κλειδαριές, θερμόμετρα, συσκευές fitness, αισθητήρες πόρτας ή κίνησης, αλλά και σε συνδυασμό με gateways, τα οποία συγκεντρώνουν δεδομένα από πολλαπλές συσκευές BLE (Bluetooth Low Energy). Με την ωρίμανση των Bluetooth Mesh δικτύων, η τεχνολογία αποκτά και

τη δυνατότητα επεκτασιμότητας, αν και αυτό εξακολουθεί να είναι περιορισμένο σε πολύ συγκεκριμένες εφαρμογές όπου οι συσκευές είναι συνεχώς τροφοδοτούμενες και διαθέτουν τις απαιτούμενες δυνατότητες επεξεργασίας και μνήμης. [18] [24]

1.13: Port Forwarding

Το port forwarding αποτελεί μια τεχνική που επιτρέπει τη δρομολόγηση εισερχόμενης κίνησης από το διαδίκτυο προς συγκεκριμένες συσκευές ή υπηρεσίες εντός ενός ιδιωτικού δικτύου. Η τεχνική αυτή καθιστά δυνατή την πρόσβαση σε τοπικές υπηρεσίες πίσω από έναν δρομολογητή ή από ενα τοίχος προστασίας, οι οποίες κανονικά δεν είναι ορατές ή προσβάσιμες από το εξωτερικό δίκτυο. Στην πράξη, η μέθοδος χρησιμοποιείται εκτενώς για την απομακρυσμένη πρόσβαση σε διακομιστές (π.χ. web servers, FTP, SSH), σε συστήματα αυτοματισμού, κάμερες επιτήρησης, και άλλες υπηρεσίες IoT, ιδιαίτερα σε περιβάλλοντα όπως ένα έξυπνο σπίτι.
Η βασική αρχή πάνω στην οποία στηρίζεται το port forwarding προκύπτει από τη λειτουργία του NAT (Network Address Translation), ενός μηχανισμού που χρησιμοποιείται στους routers ώστε να επιτρέπεται σε πολλαπλές τοπικές (ιδιωτικές) IP διευθύνσεις να μοιράζονται μία δημόσια IP όταν συνδέονται στο διαδίκτυο. Το NAT, ωστόσο, παρουσιάζει ένα πρόβλημα: ενώ επιτρέπει στις τοπικές συσκευές να ξεκινούν συνδέσεις προς το εξωτερικό, δεν επιτρέπει εξ ορισμού σε εξωτερικές συσκευές να ξεκινούν συνδέσεις προς μια εσωτερική IP, καθώς η μετάφραση διευθύνσεων δεν γνωρίζει σε ποια εσωτερική συσκευή να προωθήσει τα εισερχόμενα πακέτα. Το port forwarding έρχεται να λύσει αυτό ακριβώς το πρόβλημα με έναν σαφή και μηχανιστικό τρόπο. Όταν διαμορφώνεται ένας κανόνας port forwarding στον δρομολογητή, αυτός ορίζει ότι κάθε εισερχόμενη σύνδεση στην εξωτερική (public) IP διεύθυνση του δρομολογητή σε μία συγκεκριμένη θύρα (π.χ. TCP 8123) πρέπει να προωθείται προς μια συγκεκριμένη εσωτερική IP και θύρα (π.χ. 192.168.1.100:8123). Ο δρομολογητής καταγράφει αυτόν τον κανόνα στον πίνακα NAT και εκτελεί δυναμικά την ανακατεύθυνση κάθε σχετικού πακέτου. Η αρχιτεκτονική του port forwarding βασίζεται σε επίπεδα του μοντέλου TCP/IP, συγκεκριμένα στα επίπεδα μεταφοράς (transport) και δικτύου (network). Στο επίπεδο δικτύου, χρησιμοποιούνται IP διευθύνσεις για τη δρομολόγηση των πακέτων, ενώ στο επίπεδο μεταφοράς αξιοποιούνται οι αριθμοί θυρών (ports) για τη διάκριση μεταξύ διαφορετικών υπηρεσιών στον ίδιο υπολογιστή. Ο συνδυασμός διεύθυνσης IP και θύρας (π.χ. 203.0.113.1:8080) επιτρέπει τον προσδιορισμό της ακριβούς υπηρεσίας που πρέπει να δρομολογηθεί.
Ωστόσο, η χρήση του port forwarding συνοδεύεται από ορισμένες κρίσιμες επιπτώσεις, κυρίως στον τομέα της ασφάλειας. Όταν μια θύρα προωθείται προς μια εσωτερική συσκευή, αυτή γίνεται ουσιαστικά εκτεθειμένη στο διαδίκτυο. Εάν η υπηρεσία αυτή δεν είναι επαρκώς ασφαλισμένη — για παράδειγμα, αν δεν χρησιμοποιεί κρυπτογράφηση, εάν έχει ευάλωτο λογισμικό ή αδύναμους κωδικούς πρόσβασης — τότε αποτελεί δυνητικό στόχο για κακόβουλους χρήστες ή αυτοματοποιημένα bots. Πολλές επιθέσεις τύπου brute-force, port scanning ή ακόμα και remote code execution έχουν τις ρίζες τους σε κακώς διαμορφωμένα port forwardings.
Επιπλέον, από την πλευρά της ιδιωτικότητας, το port forwarding καθιστά ένα εσωτερικό σύστημα προσβάσιμο, καταργώντας την "φυσική" απομόνωση που παρέχει το NAT. Αυτό σημαίνει ότι ένας υπολογιστής ή ένας διακομιστής εντός του τοπικού δικτύου μπορεί πλέον να εμφανίζεται δημοσίως και να ανταλλάσσει δεδομένα χωρίς να είναι ορατό στους χρήστες αν κάτι πηγαίνει στραβά. Σε κάποιες περιπτώσεις, αυτό μπορεί να παραβιάζει πολιτικές δικτύου ή να έρχεται σε αντίθεση με τις προϋποθέσεις του παρόχου υπηρεσιών διαδικτύου. [1] [15]

1.14:Σύνδεση Μέσω Cloud

Η αρχιτεκτονική των cloud-based εφαρμογών αποτελεί σήμερα το θεμέλιο για την υλοποίηση και λειτουργία πολλών σύγχρονων τεχνολογιών, ιδίως σε περιβάλλοντα όπου η άμεση επικοινωνία μέσω κλασικού port forwarding ή one-to-one συνδέσεων δεν είναι εφικτή λόγω περιορισμών όπως το Carrier-Grade NAT (CGNAT) ή οι φραγμένες θύρες από τον πάροχο. Η βασική ιδέα πίσω από τις cloud υπηρεσίες είναι ότι η εφαρμογή, το σύστημα ή η συσκευή αντί να είναι άμεσα προσβάσιμα από το εξωτερικό δίκτυο μέσω της δημόσιας IP του χρήστη, επικοινωνούν πρώτα με έναν απομακρυσμένο εξυπηρετητή (cloud server) μέσω εξερχόμενης σύνδεσης, η οποία επιτρέπεται πάντα από οποιοδήποτε δίκτυο NAT. Σε αυτό το μοντέλο αρχιτεκτονικής, οι τοπικές συσκευές, είτε πρόκειται για αισθητήρες, είτε για έξυπνα hub, είτε για συστήματα όπως ένα Raspberry Pi, πραγματοποιούν μια εξερχόμενη σύνδεση (outbound HTTPS/TLS session) προς το cloud. Από τη στιγμή που αυτή η σύνδεση καθιερωθεί, μπορεί να παραμείνει "ανοιχτή" και σταθερή, ώστε να επιτρέπει στον server να στέλνει εντολές ή δεδομένα πίσω στη συσκευή, μέσω αυτού του ήδη καθιερωμένου καναλιού. Έτσι, παρακάμπτεται πλήρως η ανάγκη για εισερχόμενο port forwarding, διευκολύνοντας την επικοινωνία ακόμα και σε δίκτυα με αυστηρούς περιορισμούς.
Η αρχιτεκτονική αυτή είναι ιδιαίτερα σημαντική σε περιβάλλοντα όπου οι χρήστες δεν έχουν πρόσβαση στις ρυθμίσεις του router (π.χ. σε πολυκατοικίες, σε εταιρικά δίκτυα ή σε κινητές συνδέσεις), ή όταν η δημόσια IP που τους έχει αποδοθεί είναι πίσω από CGNAT και επομένως δεν μπορεί να χρησιμοποιηθεί για να κατευθύνει εισερχόμενη κίνηση σε συγκεκριμένες τοπικές συσκευές. Παράλληλα, οι cloud λύσεις προσφέρουν υψηλή διαθεσιμότητα, επεκτασιμότητα και συνήθως αυξημένα επίπεδα ασφάλειας μέσω κρυπτογράφησης των επικοινωνιών, πολιτικών ελέγχου πρόσβασης και ενσωματωμένων μηχανισμών ταυτοποίησης. Η συγκεκριμένη αρχιτεκτονική αποτελεί τη βάση για την πλειονότητα των "plug and play" έξυπνων συσκευών της αγοράς, όπως κάμερες ασφαλείας, έξυπνα φώτα, και φωνητικοί βοηθοί, τα οποία επικοινωνούν με τις αντίστοιχες υπηρεσίες cloud (π.χ. Google, Amazon, Tuya) και από εκεί διαχειρίζονται είτε από το κινητό του χρήστη, είτε από τρίτες εφαρμογές. Η μετάβαση στο cloud εξαλείφει την πολυπλοκότητα του παραδοσιακού δικτύου και καθιστά την εμπειρία χρήσης πιο απλή, καθολική και ασφαλή για το ευρύ κοινό. Η αρχιτεκτονική cloud-based εφαρμογών έχει εξελιχθεί ώστε να καλύψει όχι μόνο την ανάγκη για συνδεσιμότητα σε περιβάλλοντα με περιορισμούς, αλλά και για ένα πιο ολοκληρωμένο, αξιόπιστο και επεκτάσιμο οικοσύστημα υπηρεσιών που απλοποιεί σημαντικά τη διαχείριση των τοπικών συσκευών. Ο πυρήνας αυτής της προσέγγισης βασίζεται στην έννοια του intermediary server (διαμεσολαβητή), ο οποίος λειτουργεί σαν ενδιάμεσος κόμβος μεταξύ των συσκευών του χρήστη και των εφαρμογών διαχείρισης ή του ίδιου του χρήστη εξ αποστάσεως. Με άλλα λόγια, οι τοπικές συσκευές δεν είναι πλέον απευθείας εκτεθειμένες στο διαδίκτυο – κάτι που απαιτούσε μέχρι πρότινος τη ρύθμιση του router, την παραχώρηση στατικής IP ή δυναμικής DNS υπηρεσίας και το άνοιγμα θυρών μέσω port forwarding.

Αντίθετα, μέσω της cloud αρχιτεκτονικής, οι συσκευές δημιουργούν μόνες τους ασφαλείς, εξερχόμενες συνδέσεις (συνήθως μέσω HTTPS, MQTT over TLS, WebSockets ή άλλων κρυπτογραφημένων πρωτοκόλλων) με τους διακομιστές της εταιρείας ή του παρόχου της υπηρεσίας. Μόλις η σύνδεση εγκατασταθεί, παραμένει ενεργή, επιτρέποντας δύο κατευθύνσεις δεδομένων – ακόμα κι αν ο χρήστης θελήσει να αλληλεπιδράσει με το σύστημα από μακριά. Ένα απλό παράδειγμα είναι η χρήση μιας εφαρμογής στο κινητό, η οποία δεν συνδέεται απευθείας με το τοπικό δίκτυο του χρήστη, αλλά με το cloud της υπηρεσίας. Από εκεί, το cloud server προωθεί εντολές προς τη συσκευή μέσα από το ανοιχτό κανάλι επικοινωνίας. Αυτό το μοντέλο είναι εξαιρετικά ανθεκτικό σε δικτυακούς περιορισμούς όπως το CGNAT, όπου πολλοί χρήστες μοιράζονται την ίδια δημόσια IP και δεν μπορούν να λάβουν εισερχόμενη κίνηση ή να εκθέσουν τις τοπικές τους συσκευές. Ταυτόχρονα,

παρακάμπτει εντελώς την ανάγκη για port forwarding, το οποίο εγκυμονεί και ζητήματα ασφαλείας, καθώς οποιαδήποτε θύρα ανοιχτεί δημόσια στο διαδίκτυο αποτελεί πιθανό στόχο επιθέσεων. Το cloud λειτουργεί ως buffer ασφαλείας: η συσκευή συνδέεται μόνο προς τα έξω και όχι αντίστροφα, μειώνοντας έτσι σημαντικά την επιφάνεια επίθεσης. Επιπλέον, το μοντέλο αυτό κλιμακώνεται ευκολότερα, αφού μπορεί να διαχειριστεί χιλιάδες συσκευές ανά χρήστη και να εφαρμόσει πολιτικές κεντρικά, χωρίς να απαιτούνται ξεχωριστές τοπικές ρυθμίσεις για κάθε περιβάλλον. Στην πράξη, αυτό σημαίνει ότι η εγκατάσταση μιας συσκευής μπορεί να γίνει με ένα απλό QR scan ή login, χωρίς να χρειάζεται τεχνική γνώση για παραμετροποίηση του router ή του firewall. Επίσης, το cloud επιτρέπει πρόσβαση από οπουδήποτε, χωρίς VPN, αρκεί η εφαρμογή και η συσκευή να συνδέονται στον ίδιο πάροχο.

Τέλος, πρέπει να σημειωθεί πως οι cloud-based λύσεις ενισχύουν και τη διαθεσιμότητα: σε περίπτωση αποτυχίας ή αποσύνδεσης μιας συσκευής, ο cloud server μπορεί να αποθηκεύσει logs, να ενεργοποιήσει ειδοποιήσεις, να τρέξει απομακρυσμένα σενάρια ή να συγχρονίσει με άλλα API – κάτι που θα ήταν δύσκολο σε αποκλειστικά τοπική αρχιτεκτονική. Ωστόσο, αυτή η ευκολία συνοδεύεται και από το μειονέκτημα της εξάρτησης από τρίτους, καθώς κάθε απώλεια σύνδεσης με το cloud (λόγω διακοπής υπηρεσίας, αλλαγής πολιτικής, ή hacking) μπορεί να επηρεάσει δραστικά τη λειτουργικότητα του συστήματος. Παρ’ όλα αυτά, για τον μέσο χρήστη και για πολλές εταιρικές εφαρμογές, το πλεονέκτημα της ευκολίας, της ασφάλειας και της προσβασιμότητας υπερτερεί ξεκάθαρα, γι’ αυτό και η μετάβαση προς το cloud θεωρείται πλέον δεδομένη για το μεγαλύτερο μέρος των "έξυπνων" λύσεων.[11] [12]

1.15: VPN (Virtual Private Network)

Ένα VPN (Virtual Private Network – Εικονικό Ιδιωτικό Δίκτυο) είναι μια τεχνολογία που επιτρέπει την ασφαλή και κρυπτογραφημένη σύνδεση ενός υπολογιστή ή δικτύου με κάποιο απομακρυσμένο δίκτυο μέσω του διαδικτύου. Σκοπός ενός VPN είναι η δημιουργία ενός ασφαλούς “τούνελ” (tunnel) δεδομένων, μέσω του οποίου η επικοινωνία ανάμεσα σε δύο ή περισσότερους κόμβους αποκτά χαρακτηριστικά εμπιστευτικότητας, ακεραιότητας και ταυτοποίησης, σαν να επρόκειτο για άμεση σύνδεση σε τοπικό δίκτυο. Η τεχνολογική βάση ενός VPN στηρίζεται στην αρχιτεκτονική της σήραγγας (tunneling), κατά την οποία τα πακέτα ενός πρωτοκόλλου (π.χ. TCP/IP) εγκιβωτίζονται (encapsulated) μέσα σε άλλα πακέτα ώστε να μεταφερθούν μέσω δικτύων τρίτων, όπως το δημόσιο διαδίκτυο. Αυτή η σήραγγα μπορεί να είναι είτε point-to-point (για παράδειγμα, σύνδεση ενός client με έναν server) είτε site-to-site (για διασύνδεση δύο απομακρυσμένων δικτύων μεταξύ τους). Η διαδικασία αυτή συνδυάζεται με μηχανισμούς κρυπτογράφησης των δεδομένων, επιτρέποντας ασφαλή μεταφορά ακόμα και μέσω επισφαλών δικτύων.

Η υλοποίηση ενός VPN βασίζεται σε λογισμικό ή εξειδικευμένο υλικό (VPN appliances) και περιλαμβάνει δύο βασικά μέρη: τον client (πελάτη) και τον server. Ο client εγκαθίσταται στον υπολογιστή, smartphone ή router του χρήστη, ενώ ο server βρίσκεται στο απομακρυσμένο σημείο (π.χ. το σπίτι, το πανεπιστήμιο, ο εταιρικός κόμβος). Κατά την εγκαθίδρυση της σύνδεσης, πραγματοποιείται διαδικασία ταυτοποίησης, ανταλλαγής κλειδιών και συμφωνίας επί των κρυπτογραφικών παραμέτρων (handshake), ώστε η σύνδεση να εξασφαλίσει ιδιωτικότητα και ασφάλεια. Τα VPN χρησιμοποιούνται ευρέως για διάφορους σκοπούς. Στο πλαίσιο ενός έξυπνου σπιτιού, επιτρέπουν την απομακρυσμένη πρόσβαση στο οικιακό δίκτυο σαν να ήταν ο χρήστης τοπικά συνδεδεμένος, χωρίς να απαιτείται επικίνδυνο port forwarding. Σε επιχειρησιακά περιβάλλοντα, διευκολύνουν την ασφαλή πρόσβαση υπαλλήλων σε εταιρικά δίκτυα. Επιπλέον,

χρησιμοποιούνται για την προστασία της ιδιωτικότητας σε δημόσια δίκτυα Wi-Fi, την παράκαμψη γεωγραφικών περιορισμών περιεχομένου και τη γενικότερη ενίσχυση της διαδικτυακής ανωνυμίας.

Υπάρχουν αρκετά πρωτόκολλα υλοποίησης VPN, καθένα από τα οποία προσφέρει διαφορετικά χαρακτηριστικά ασφαλείας, απόδοσης και συμβατότητας. Το OpenVPN είναι ανοιχτού κώδικα και βασίζεται στο πρωτόκολλο SSL/TLS, προσφέροντας ισχυρή κρυπτογράφηση και μεγάλη ευελιξία. Το WireGuard, επίσης ανοιχτού κώδικα, είναι νεότερο, πιο ελαφρύ και εξαιρετικά αποδοτικό, με μοντέρνα αρχιτεκτονική και μικρότερο attack surface. Το IPSec χρησιμοποιείται σε συνδυασμό με πρωτόκολλα όπως το IKEv2 και είναι ιδιαίτερα διαδεδομένο σε επαγγελματικές εγκαταστάσεις, ενώ το L2TP/IPSec παρέχει σήραγγα χωρίς κρυπτογράφηση (L2TP) η οποία συνδυάζεται με το IPSec για την ασφάλεια. Άλλα, πιο παλαιά πρωτόκολλα, όπως το PPTP, θεωρούνται πλέον ανασφαλή και καταργούνται σταδιακά. Η αρχιτεκτονική ενός VPN μπορεί να διαφέρει ανάλογα με το μοντέλο που υιοθετείται. Σε κεντρικοποιημένα VPN, υπάρχει ένας κεντρικός server στον οποίο συνδέονται όλοι οι clients, καθιστώντας τον κόμβο αυτό το σημείο εισόδου και εξόδου των δεδομένων. Αντιθέτως, σε peer-to-peer ή mesh VPNs, όπως υλοποιούνται μέσω τεχνολογιών όπως το Tailscale (βασισμένο στο WireGuard), οι κόμβοι μπορούν να επικοινωνούν απευθείας μεταξύ τους με αποκλειστικά end-to-end κρυπτογράφηση, χωρίς να χρειάζεται κεντρική δρομολόγηση της κίνησης.

Τα πλεονεκτήματα των VPN είναι πολυάριθμα. Παρέχουν ισχυρή κρυπτογράφηση και ασφάλεια, εξασφαλίζουν ιδιωτικότητα και αποφυγή καταγραφής της δραστηριότητας από παρόχους υπηρεσιών διαδικτύου, προσφέρουν γεωγραφική ανεξαρτησία πρόσβασης, και εξαλείφουν την ανάγκη για port forwarding, μειώνοντας τον κίνδυνο εκμετάλλευσης ευπαθειών. Παράλληλα, υπάρχουν και μειονεκτήματα που πρέπει να ληφθούν υπόψη. Η χρήση VPN επιφέρει γενικά μείωση της ταχύτητας λόγω κρυπτογράφησης και δρομολόγησης, απαιτεί πιο σύνθετη ρύθμιση σε σχέση με απλές συνδέσεις, και σε κάποιες περιπτώσεις υπόκειται σε περιορισμούς από παρόχους ή κρατικές αρχές. Η τεχνολογία των VPN στηρίζεται σε πληθώρα πρωτοκόλλων, καθένα από τα οποία προσφέρει διαφορετικές προσεγγίσεις σε ζητήματα ασφάλειας, απόδοσης και συμβατότητας με υποδομές και λειτουργικά συστήματα. Ορισμένα από αυτά έχουν εξελιχθεί μέσα από δεκαετίες χρήσης σε εταιρικά και προσωπικά δίκτυα, ενώ άλλα είναι πιο σύγχρονες υλοποιήσεις που εστιάζουν στην απλότητα και τη βελτιστοποίηση. Παρακάτω θα γινει αναφορά σε ορισμενα απο τα σημαντικοτερα πρωτόκολλα.

Το IPSec (Internet Protocol Security) αποτελεί ένα από τα πιο διαδεδομένα και ώριμα πρωτόκολλα για τη δημιουργία ασφαλών σήραγγων σε επίπεδο δικτύου (Layer 3). Εφαρμόζεται κυρίως σε εταιρικά περιβάλλοντα και router-to-router συνδέσεις και χρησιμοποιεί μηχανισμούς όπως ESP (Encapsulating Security Payload) και AH (Authentication Header) για να διασφαλίσει την εμπιστευτικότητα, την ακεραιότητα και την αυθεντικότητα των δεδομένων. Η λειτουργία του IPSec μπορεί να είναι είτε σε transport mode, όπου μόνο το ωφέλιμο φορτίο (payload) κρυπτογραφείται, είτε σε tunnel mode, όπου ολόκληρο το IP πακέτο ενθυλακώνεται και προστατεύεται. Στενά συνδεδεμένο με το IPSec είναι το IKE (Internet Key Exchange), και πιο συγκεκριμένα η δεύτερη του έκδοση, IKEv2. Το πρωτόκολλο αυτό αναλαμβάνει τη διαπραγμάτευση των παραμέτρων ασφάλειας μεταξύ των δύο άκρων της σύνδεσης, τη δημιουργία και ανανέωση κλειδιών, καθώς και τη διαδικασία ταυτοποίησης. Το IKEv2 θεωρείται ιδιαίτερα ασφαλές και σταθερό, με ενσωματωμένους μηχανισμούς επανασύνδεσης, κάτι που το καθιστά ιδανικό για mobile περιβάλλοντα. Συχνά χρησιμοποιείται σε συνδυασμό με IPSec για τη δημιουργία πλήρως κρυπτογραφημένων VPN συνδέσεων.

Το OpenVPN αποτελεί μία από τις πιο δημοφιλείς και διαδεδομένες λύσεις υλοποίησης εικονικών ιδιωτικών δικτύων (VPN), ειδικά σε περιβάλλοντα όπου απαιτείται υψηλό επίπεδο

παραμετροποίησης, ασφάλειας και διαλειτουργικότητας με διάφορα λειτουργικά συστήματα και δικτυακές αρχιτεκτονικές. Αναπτύχθηκε από τον James Yonan το 2001, και από τότε εξελίχθηκε σε ανοιχτού κώδικα (open-source) λογισμικό υπό την επίβλεψη της OpenVPN Inc., με τεράστια κοινότητα χρηστών και υποστηρικτών.

Σε αντίθεση με άλλα VPN πρωτόκολλα που λειτουργούν σε επίπεδο IP (όπως το IPSec), το OpenVPN βασίζεται στην αρχιτεκτονική του πρωτοκόλλου SSL/TLS (Secure Sockets Layer / Transport Layer Security), το οποίο χρησιμοποιείται ευρέως και στον παγκόσμιο ιστό για την ασφαλή μεταφορά δεδομένων. Μέσω αυτής της αρχιτεκτονικής, το OpenVPN δημιουργεί έναν ασφαλή κρυπτογραφημένο δίαυλο ανάμεσα στον client και τον server, αξιοποιώντας συμμετρική κρυπτογράφηση (AES, ChaCha20), έλεγχο ταυτότητας με δημόσια και ιδιωτικά κλειδιά, καθώς και πιστοποιητικά X.509. Η ασφάλεια που παρέχει είναι εφάμιλλη – και σε πολλές περιπτώσεις ανώτερη – από παραδοσιακά πρωτόκολλα όπως το L2TP/IPSec.

Ένα από τα βασικά πλεονεκτήματα του OpenVPN είναι η ευελιξία του στη χρήση των μεταφορικών επιπέδων. Μπορεί να λειτουργεί είτε μέσω TCP είτε UDP, προσφέροντας τη δυνατότητα παράκαμψης περιοριστικών firewall και NAT (Network Address Translation), ακόμη και μέσω της θύρας 443, που χρησιμοποιείται από το HTTPS. Αυτό του επιτρέπει να διεισδύει σε δίκτυα που μπλοκάρουν άλλες VPN λύσεις, καθιστώντας το ιδανικό για δύσκολα περιβάλλοντα ή δίκτυα με περιορισμούς.

Η διαδικασία δημιουργίας σύνδεσης στο OpenVPN περιλαμβάνει handshake μέσω TLS, ανταλλαγή κρυπτογραφικών κλειδιών και στη συνέχεια σύναψη ενός ασφαλούς καναλιού δεδομένων. Η υποστήριξη Perfect Forward Secrecy (PFS) διασφαλίζει ότι ακόμη και σε περίπτωση υποκλοπής παλαιών κλειδιών, οι μελλοντικές ή παρελθοντικές επικοινωνίες δεν είναι δυνατόν να αποκρυπτογραφηθούν. Επιπλέον, παρέχει δυνατότητα χρήσης HMAC για την προστασία της ακεραιότητας των πακέτων και προαιρετικά χρησιμοποιεί συμπίεση δεδομένων μέσω του αλγορίθμου LZO (αν και πλέον συστήνεται η απενεργοποίησή της για λόγους ασφάλειας).

Η χρήση του OpenVPN συναντάται σε πληθώρα περιβαλλόντων: από οικιακές υλοποιήσεις σε Raspberry Pi ή μικρούς servers, μέχρι εταιρικές εγκαταστάσεις υψηλής διαθεσιμότητας με clustering και failover. Η υποστήριξή του επεκτείνεται σε Windows, Linux, macOS, Android, iOS και πλήθος embedded συσκευών. Παράλληλα, προσφέρεται και με γραφικά περιβάλλοντα ή μέσω CLI, ενώ υποστηρίζει σενάρια multi-client, bridge mode και routing mode, με λεπτομερή έλεγχο μέσω αρχείων παραμετροποίησης.

Το WireGuard είναι ένα νεότερο VPN πρωτόκολλο, που σχεδιάστηκε με στόχο την απλότητα, την ταχύτητα και την ασφάλεια. Γραμμένο αρχικά για τον πυρήνα του Linux, βασίζεται σε σύγχρονους αλγορίθμους κρυπτογράφησης όπως ChaCha20, Poly1305 και Curve25519, και ακολουθεί μία μινιμαλιστική σχεδίαση με μόλις ~4.000 γραμμές κώδικα – σημαντικά λιγότερες σε σχέση με τα παραδοσιακά IPSec ή OpenVPN. Το WireGuard δεν υποστηρίζει παραδοσιακή διαπραγμάτευση κλειδιών όπως το IKE, αλλά λειτουργεί μέσω ενός απλού μηχανισμού ανταλλαγής δημοσίων κλειδιών, καθιστώντας το ιδιαίτερα γρήγορο και αξιόπιστο. Παρά το ότι θεωρείται ακόμη σχετικά νέο, έχει ενσωματωθεί στους πυρήνες των σύγχρονων λειτουργικών συστημάτων και υιοθετείται ευρέως, ειδικά σε προσωπικά και οικιακά VPN.

Ένα άλλο ευρέως γνωστό και υποστηριζόμενο πρωτόκολλο είναι το L2TP (Layer 2 Tunneling Protocol), το οποίο συχνά συνδυάζεται με IPSec για την κρυπτογράφηση των δεδομένων, αφού από μόνο του δεν προσφέρει κρυπτογράφηση. Το ζεύγος L2TP/IPSec θεωρείται σχετικά ασφαλές, αλλά παρουσιάζει περιορισμούς σε σύγχρονες απαιτήσεις όπως mobile switching ή χρήση σε restrictive

δίκτυα, λόγω της εξάρτησής του από συγκεκριμένες θύρες (UDP 500, 1701, 4500) που συχνά μπλοκάρονται από firewalls ή NAT. Το παλαιότερο PPTP (Point-to-Point Tunneling Protocol), αν και αποτέλεσε μία από τις πρώτες υλοποιήσεις VPN, θεωρείται πλέον ανεπαρκές από άποψη ασφάλειας και έχει καταργηθεί από πολλά λειτουργικά συστήματα. Οι γνωστές του ευπάθειες, η απουσία ισχυρής κρυπτογράφησης και η εύκολη παραβίασή του καθιστούν την χρήση του απαγορευτική σε οποιοδήποτε περιβάλλον που απαιτεί βασική προστασία. Σε επίπεδο ευρείας διασύνδεσης επιχειρησιακών δικτύων, η τεχνολογία MPLS (Multiprotocol Label Switching) συχνά συγχέεται με τα VPN, παρότι δεν είναι αμιγώς VPN πρωτόκολλο. Πρόκειται για μία τεχνική δρομολόγησης που χρησιμοποιείται από παρόχους για τη δημιουργία εικονικών ιδιωτικών κυκλωμάτων μεταξύ διαφορετικών γεωγραφικών σημείων ενός οργανισμού. Το MPLS VPN προσφέρει υψηλή απόδοση, εγγυημένο QoS (Quality of Service) και αξιοπιστία, όμως η ασφάλεια του δεν είναι end-to-end και συνήθως βασίζεται στην εμπιστοσύνη στον πάροχο, κάτι που το διαφοροποιεί θεμελιωδώς από λύσεις όπως το WireGuard ή το IPSec.

Εν κατακλείδι, η επιλογή του κατάλληλου πρωτοκόλλου VPN εξαρτάται από τις ανάγκες του εκάστοτε περιβάλλοντος: απόδοση, ευκολία εγκατάστασης, συμβατότητα, δυνατότητα mobility και φυσικά επίπεδο ασφάλειας. Σε προσωπικά και οικιακά περιβάλλοντα, το WireGuard ξεχωρίζει για τη μοντέρνα και αποδοτική του προσέγγιση, ενώ σε μεγάλες επιχειρήσεις το IPSec με IKEv2 παραμένει ένα σταθερό και αξιόπιστο θεμέλιο για την προστασία της δικτυακής υποδομής.

Ωστόσο, η ευελιξία και η ισχύς του OpenVPN συνοδεύονται από μια σχετική πολυπλοκότητα στη ρύθμιση, ειδικά για χρήστες χωρίς εμπειρία σε δίκτυα και κρυπτογραφία. Η δημιουργία έγκυρων πιστοποιητικών, η διαχείριση των TLS parameters και η ορθή ρύθμιση των firewalls απαιτούν προσοχή και γνώση, γι’ αυτό και πολλές διανομές (όπως το Home Assistant OS ή έτοιμα scripts όπως το PiVPN) προσφέρουν αυτοματοποιημένες λύσεις για την εγκατάστασή του. [25]

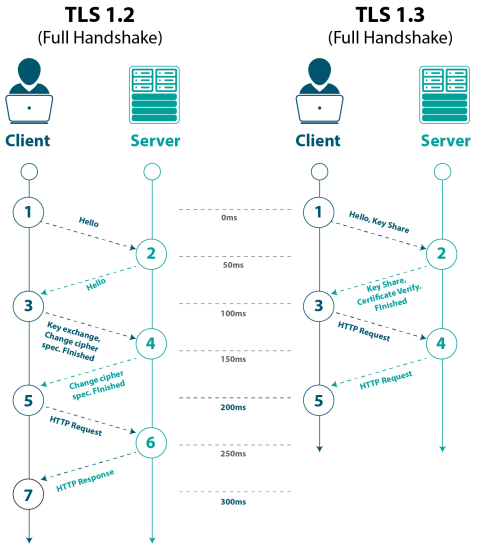
1.16: Transport Layer Security (TLS)

Το TLS (Transport Layer Security) είναι ένα πρωτόκολλο κρυπτογράφησης που χρησιμοποιείται για την εξασφάλιση ασφαλούς επικοινωνίας μέσω δικτύων, κυρίως στο διαδίκτυο. Αποτελεί τον διάδοχο του SSL (Secure Sockets Layer), από το οποίο εξελίχθηκε, και έχει σχεδιαστεί ώστε να παρέχει εμπιστευτικότητα (confidentiality), ακεραιότητα (integrity) και αυθεντικότητα (authentication) κατά την ανταλλαγή δεδομένων μεταξύ δύο μερών, όπως ενός browser και ενός web server. Το TLS λειτουργεί «πάνω» από πρωτόκολλα μεταφοράς όπως το TCP, και κρυπτογραφεί το περιεχόμενο των δεδομένων που διακινούνται, εμποδίζοντας τρίτους (man-in-the-middle) να παρακολουθήσουν ή να αλλοιώσουν τις πληροφορίες που ανταλλάσσονται. Η διαδικασία έναρξης ασφαλούς επικοινωνίας μέσω TLS ξεκινά με το TLS handshake, κατά το οποίο ο πελάτης (π.χ. ένας browser) και ο εξυπηρετητής συμφωνούν σε κρίσιμες παραμέτρους, ποια κρυπτογραφικά πρωτόκολλα θα χρησιμοποιήσουν (αλγόριθμοι συμμετρικής και ασύμμετρης κρυπτογράφησης, hash functions κ.λπ.), ποια θα είναι τα κλειδιά κρυπτογράφησης και ποιος είναι ο έμπιστος εξυπηρετητής. Ο εξυπηρετητής αποστέλλει στον πελάτη το ψηφιακό του πιστοποιητικό, το οποίο έχει εκδοθεί από μια έγκυρη αρχή πιστοποίησης (CA – Certificate Authority) και περιέχει το δημόσιο κλειδί του. Ο πελάτης ελέγχει την εγκυρότητα του πιστοποιητικού και, εφόσον την επιβεβαιώσει, δημιουργεί ένα κλειδί συνεδρίας (session key) το οποίο κρυπτογραφεί με το δημόσιο κλειδί του εξυπηρετητή και του το αποστέλλει. Από εκεί και πέρα, και τα δύο μέρη χρησιμοποιούν αυτό το συμμετρικό κλειδί για την ανταλλαγή των δεδομένων.

Το πρωτόκολλο TLS έχει γνωρίσει πολλές εκδόσεις, με την πιο σύγχρονη και ασφαλή να είναι η TLS 1.3, η οποία βελτιώνει την ταχύτητα του handshake, μειώνει τον αριθμό των βημάτων, και αφαιρεί παλαιότερους αλγόριθμους που κρίθηκαν ανασφαλείς. Σε σχέση με τις προηγούμενες εκδόσεις, το TLS 1.3 ελαχιστοποιεί τη δυνατότητα παρεμβολής ή παρακολούθησης, ενώ επιτρέπει και τη χρήση πρωτοκόλλων όπως το 0-RTT (zero round-trip time) για ακόμα ταχύτερες συνδέσεις. Το TLS χρησιμοποιείται ευρέως σε εφαρμογές όπως το HTTPS (HTTP over TLS), σε πρωτόκολλα ηλεκτρονικού ταχυδρομίου (IMAP, SMTP), VPNs, VoIP, και γενικά όπου υπάρχει ανάγκη για προστασία ευαίσθητων πληροφοριών. Ένα από τα μεγαλύτερα πλεονεκτήματα του είναι ότι είναι διαφανές για τον τελικό χρήστη, δεν απαιτεί πρόσθετη ενέργεια και είναι πλέον σχεδόν υποχρεωτικό για κάθε σοβαρή διαδικτυακή υπηρεσία που χειρίζεται προσωπικά ή κρίσιμα δεδομένα. Στο πλαίσιο του IoT και των έξυπνων σπιτιών, το TLS είναι εξαιρετικά σημαντικό γιατί διασφαλίζει ότι η επικοινωνία των συσκευών με cloud υπηρεσίες ή mobile εφαρμογές δεν μπορεί να υποκλαπεί, ειδικά σε περιβάλλοντα όπου η φυσική ασφάλεια δεν είναι εγγυημένη. Παρότι επιβαρύνει ελαφρώς τη συσκευή με επεξεργαστικό φόρτο, ο σωστός σχεδιασμός λογισμικού και η χρήση hardware acceleration επιτρέπει την ευρεία υιοθέτησή του ακόμα και σε ενσωματωμένα συστήματα όπως αυτά που βασίζονται σε Raspberry Pi ή ESP32.

Το TLS αποτελεί έναν από τους πιο κρίσιμους πυλώνες της σύγχρονης ψηφιακής ασφάλειας και είναι τόσο θεμελιώδες στην υποδομή του διαδικτύου, ώστε πρακτικά κάθε σοβαρή υπηρεσία που διακινεί προσωπικά δεδομένα στηρίζεται σε αυτό. Η ευελιξία του, η δυνατότητα κλιμάκωσης και οι συνεχείς βελτιώσεις το έχουν εδραιώσει ως το de facto πρότυπο για ασφαλή επικοινωνία σε περιβάλλοντα όπου το απόρρητο και η ακεραιότητα των δεδομένων έχουν ζωτική σημασία. Ένα βασικό χαρακτηριστικό του TLS είναι η υποστήριξη για **forward secrecy** (εμπιστευτικότητα προς τα εμπρός), ιδιότητα που εξασφαλίζει ότι ακόμα και αν στο μέλλον παραβιαστεί ένα κλειδί κρυπτογράφησης, δεν μπορούν να αποκρυπτογραφηθούν προηγούμενες επικοινωνίες, γιατί κάθε συνεδρία έχει μοναδικό προσωρινό κλειδί. Αυτή η δυνατότητα προστατεύει ακόμα και σε σενάρια όπου ένας επιτιθέμενος καταγράφει την κυκλοφορία σήμερα και προσπαθεί να την αποκρυπτογραφήσει αργότερα. Επιπλέον, το TLS επιτρέπει και **αμοιβαία αυθεντικοποίηση**, όχι μόνο του εξυπηρετητή προς τον πελάτη αλλά και του πελάτη προς τον εξυπηρετητή, μέσω client-side certificates. Αυτή η προσέγγιση είναι ιδιαίτερα σημαντική σε εταιρικά περιβάλλοντα, συστήματα ελέγχου πρόσβασης ή εφαρμογές IoT, όπου χρειάζεται να επιβεβαιωθεί η ταυτότητα και των δύο πλευρών.

Από την άποψη των επιδόσεων, το TLS έχει γίνει πολύ πιο αποδοτικό με την πάροδο του χρόνου. Παλαιότερες εκδόσεις όπως το TLS 1.0 και 1.1 χαρακτηρίζονταν από αργά handshakes και μεγάλα round-trips, ενώ οι νεότερες εκδόσεις, ειδικά το TLS 1.3, έχουν βελτιστοποιηθεί ώστε να μειώνουν σημαντικά την καθυστέρηση και να απαιτούν λιγότερους πόρους. Αυτή η εξέλιξη είναι ιδιαίτερα σημαντική για εφαρμογές real-time ή για συσκευές περιορισμένων δυνατοτήτων, όπως οι περισσότερες IoT πλατφόρμες Σε επίπεδο εφαρμογής, η ενεργοποίηση του TLS δεν είναι μόνο θέμα εγκατάστασης ενός πιστοποιητικού. Προϋποθέτει την σωστή παραμετροποίηση του εξυπηρετητή , την επιλογή κατάλληλων cipher suites, την απόρριψη παλαιών και ευάλωτων αλγορίθμων (όπως RC4, SHA-1 ή SSL), και τη διαρκή ανανέωση των πιστοποιητικών μέσω έγκυρων CA (π.χ. Let's Encrypt).



Σχημα 1.13: Διάγραμμα ροής TLS [12.α]

Αξίζει επίσης να σημειωθεί ότι με το TLS ενσωματώνεται πλέον και η SNI (Server Name Indication), η οποία επιτρέπει τη χρήση πολλαπλών πιστοποιητικών σε έναν server με μία μόνο IP – κάτι που είναι κρίσιμο για shared hosting περιβάλλοντα ή proxies. Υπάρχει και υποστήριξη για ALPN (Application-Layer Protocol Negotiation) που χρησιμοποιείται για την επιλογή εφαρμογών όπως HTTP/2 ή QUIC πάνω από TLS. Τέλος, σε περιβάλλοντα smart home και edge computing, το TLS προσφέρει τη δυνατότητα να ασφαλίζονται όλα τα δεδομένα που διακινούνται μεταξύ τοπικών συσκευών και των cloud υπηρεσιών τους, π.χ. όταν ένας αισθητήρας μεταδίδει δεδομένα θερμοκρασίας ή όταν ένας διακόπτης στέλνει σήμα. Ακόμα και εσωτερικά APIs σε ένα δίκτυο μπορούν να προστατευθούν με TLS για να αποτραπούν επιθέσεις μέσα από μη έμπιστες τοπικές συσκευές. [1]

1.17:Cloudflare

Η Cloudflare είναι μια αμερικανική εταιρεία τεχνολογίας που εξειδικεύεται στην παροχή υπηρεσιών διαδικτυακής ασφάλειας, ταχύτητας και αξιοπιστίας για ιστότοπους και εφαρμογές. Ιδρύθηκε το 2009 από τους Matthew Prince, Michelle Zatlyn και Lee Holloway, με την αποστολή να βοηθήσει στη δημιουργία ενός καλύτερου και ασφαλέστερου διαδικτύου. Από την ίδρυσή της μέχρι σήμερα, η Cloudflare έχει εξελιχθεί σε έναν από τους σημαντικότερους παρόχους υποδομών στο διαδίκτυο, εξυπηρετώντας εκατομμύρια domains παγκοσμίως και υποστηρίζοντας τόσο μικρές επιχειρήσεις όσο και μεγάλους οργανισμούς και κυβερνητικές υπηρεσίες. Η Cloudflare εδρεύει στο Σαν Φρανσίσκο και από το 2019 είναι εισηγμένη στο Χρηματιστήριο της Νέας Υόρκης (NYSE), γεγονός που αποδεικνύει τη σταθερή ανάπτυξή της και τη σημασία της στον παγκόσμιο ψηφιακό χάρτη. Με μια ευρεία γκάμα υπηρεσιών που καλύπτει σχεδόν κάθε ανάγκη ασφάλειας και επιτάχυνσης ιστοσελίδων και εφαρμογών, η Cloudflare παραμένει ένας από τους βασικούς παρόχους υποδομών και προστασίας του σύγχρονου διαδικτύου.

Η εταιρεία έγινε ιδιαίτερα γνωστή για τις υπηρεσίες προστασίας από επιθέσεις DDoS (Distributed Denial of Service), καθώς και για το Content Delivery Network (CDN) που διαθέτει, το οποίο βοηθά τους ιστότοπους να φορτώνουν πιο γρήγορα, χρησιμοποιώντας servers κατανεμημένους σε δεκάδες χώρες. Η τεχνολογία της Cloudflare λειτουργεί ως ενδιάμεσος μεταξύ του τελικού χρήστη και του

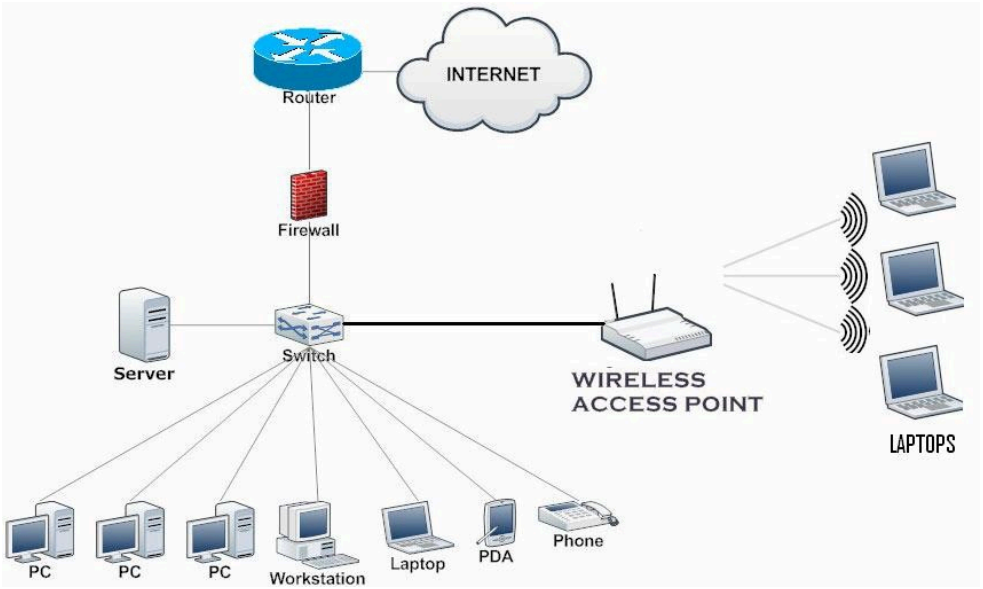
εξυπηρετητή (origin server), φιλτράροντας την κακόβουλη κυκλοφορία, αποθηκεύοντας προσωρινά περιεχόμενο για μείωση του φορτίου στον διακομιστή, και επιταχύνοντας τη μετάδοση των δεδομένων χάρη στην παγκόσμια υποδομή της. Εκτός από τις υπηρεσίες CDN και προστασίας DDoS, η Cloudflare παρέχει και ένα πλήρες Web Application Firewall (WAF), εργαλεία για την παρακολούθηση και τον έλεγχο της κίνησης, διαχείριση DNS μέσω της δικής της υποδομής, καθώς και προηγμένες λύσεις ασφαλούς πρόσβασης με τεχνολογίες Zero Trust. Ιδιαίτερα σημαντική είναι η προσφορά του Cloudflare Tunnel (παλαιότερα γνωστό ως Argo Tunnel), μέσω του οποίου μπορεί κάποιος να δημοσιεύσει υπηρεσίες και εφαρμογές στο διαδίκτυο χωρίς να εκθέτει άμεσα την IP του server του ή να ανοίγει θύρες στον router του. Αυτό είναι εξαιρετικά σημαντικό για προσωπικές και επαγγελματικές υποδομές, καθώς ενισχύει την ασφάλεια μειώνοντας την επιφάνεια επίθεσης. Η Cloudflare έχει επίσης επεκταθεί στον χώρο των λύσεων DNS με την υπηρεσία 1.1.1.1, έναν από τους ταχύτερους και πιο ασφαλείς DNS resolvers, που δίνει έμφαση στην προστασία της ιδιωτικότητας. Παράλληλα, παρέχει λύσεις ασφαλούς πλοήγησης μέσω του WARP VPN client, που βασίζεται στην τεχνολογία WireGuard, με στόχο τη βελτίωση της ταχύτητας και της ασφάλειας των συνδέσεων από κινητές συσκευές ή προσωπικούς υπολογιστές. Η ανάγκη για τις υπηρεσίες που προσφέρει η Cloudflare είναι πιο έντονη από ποτέ, λόγω της συνεχώς αυξανόμενης πολυπλοκότητας των κυβερνοεπιθέσεων, της αύξησης της παγκόσμιας διαδικτυακής κίνησης, καθώς και της επιτακτικής ανάγκης για ασφάλεια, απόδοση και διαθεσιμότητα. Ειδικά για μικρές και μεσαίες επιχειρήσεις ή ανεξάρτητους δημιουργούς περιεχομένου, η Cloudflare προσφέρει πρόσβαση σε τεχνολογίες που παλαιότερα ήταν διαθέσιμες μόνο σε μεγάλες εταιρείες με σημαντικούς πόρους.[10]

1.18: Τείχος Προστασίας (Firewall)

Το firewall είναι ένα σύστημα ασφαλείας, είτε υλικό είτε λογισμικό, που ελέγχει και φιλτράρει την κίνηση δεδομένων μεταξύ διαφορετικών δικτυακών τμημάτων, συνήθως ανάμεσα σε ένα ιδιωτικό εσωτερικό δίκτυο και το Διαδίκτυο, λειτουργώντας ως φράγμα που αποφασίζει ποια πακέτα δεδομένων επιτρέπονται και ποια απορρίπτονται βάσει προκαθορισμένων κανόνων. Στόχος του είναι η προστασία των συστημάτων από μη εξουσιοδοτημένη πρόσβαση, ο περιορισμός επιθέσεων και ο έλεγχος της ροής πληροφοριών. Η τοπολογία του μπορεί να ποικίλει, από ένα περιμετρικό firewall στην περιφέρεια του δικτύου που ελέγχει όλη την κίνηση, έως εσωτερικά firewalls που απομονώνουν τμήματα του ίδιου οργανισμού ή layered αρχιτεκτονικές με πολλαπλά firewalls για αυξημένη ασφάλεια, καθώς και ειδικές ζώνες όπως η DMZ (Demilitarized Zone) όπου απομονώνονται δημόσιοι servers ώστε να μην επηρεάζουν το εσωτερικό δίκτυο σε περίπτωση επίθεσης. Στην πράξη, το firewall χρησιμοποιείται για την προστασία από μη εξουσιοδοτημένη πρόσβαση μέσω φιλτραρίσματος θυρών και IP διευθύνσεων, τον περιορισμό επιθέσεων όπως DDoS (Distributed Denial Of Service) ή brute force, τον έλεγχο και καταγραφή της κίνησης, την εφαρμογή πολιτικών ασφαλείας και την απομόνωση δικτυακών ζωνών για την αποτροπή διάδοσης επιθέσεων. Η λειτουργία του βασίζεται σε τεχνικές όπως το packet filtering, το stateful inspection και το application layer filtering, εξασφαλίζοντας ότι η επικοινωνία στο δίκτυο γίνεται μόνο υπό ελεγχόμενες και ασφαλείς συνθήκες.

Το firewall, σε τοπικό επίπεδο (local firewall) σε ένα bare metal σύστημα, δεν είναι απλώς ένα «φράγμα» αλλά ένας ενεργός μηχανισμός ελέγχου που μπορεί να λειτουργεί είτε σε επίπεδο hardware είτε ως ενσωματωμένο λογισμικό στο λειτουργικό σύστημα. Η βασική του λειτουργία είναι να παρακολουθεί και να φιλτράρει πακέτα δεδομένων σε πραγματικό χρόνο, χρησιμοποιώντας κανόνες που μπορεί να βασίζονται σε IP διευθύνσεις, MAC διευθύνσεις, αριθμούς θυρών, πρωτόκολλα (TCP, UDP, ICMP), ακόμη και στο περιεχόμενο της εφαρμογής (application layer filtering). Ένα ισχυρό firewall δεν σταματά απλώς μη εξουσιοδοτημένη κίνηση, αλλά μπορεί να εντοπίσει ύποπτα μοτίβα,

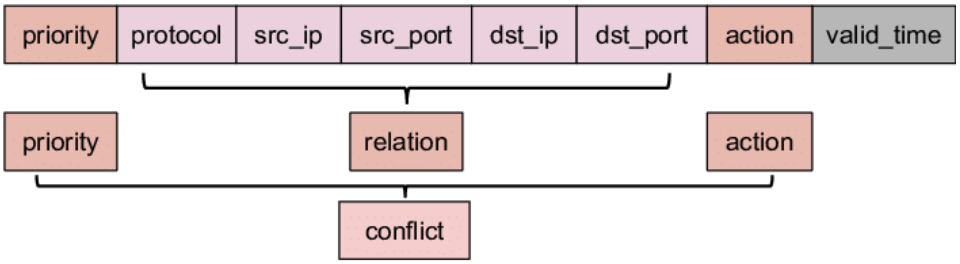
να μπλοκάρει επιθέσεις που εκμεταλλεύονται γνωστά κενά ασφαλείας, να καταγράψει κάθε συμβάν για μελλοντική ανάλυση (logging), καθώς και να ενεργοποιεί μηχανισμούς alerting όταν διαπιστωθεί παραβίαση. Η τοπολογία του μπορεί να ποικίλει σημαντικά. Σε απλά δίκτυα, βρίσκεται στο ίδιο το μηχάνημα, λειτουργώντας σαν φίλτρο πριν φτάσουν τα πακέτα στο λειτουργικό. Σε πιο σύνθετα περιβάλλοντα, μπορεί να τοποθετείται μεταξύ εσωτερικών υποδικτύων, να χρησιμοποιείται σε συνδυασμό με IDS/IPS (Intrusion Detection System / Intrusion Prevention System) συστήματα για άμεση ανίχνευση και απόκριση σε απειλές, ή να δημιουργεί «ζώνες ασφαλείας» όπως η DMZ για τον διαχωρισμό των συστημάτων που έχουν δημόσια έκθεση. Μπορεί επίσης να υποστηρίζει NAT, VPN passthrough, rate limiting και geo-blocking, προσφέροντας έτσι επιπλέον επίπεδα ελέγχου.



Σχήμα:1.14: Τοπολογία δικτύου με τείχος προστασίας [13.α]

Η χρησιμότητά του δεν περιορίζεται μόνο στην προστασία από εξωτερικές επιθέσεις, αλλά επεκτείνεται και στον εσωτερικό έλεγχο — όπως το να εμποδίζει συγκεκριμένες εφαρμογές από το να συνδεθούν στο διαδίκτυο, να περιορίζει την πρόσβαση σε υπηρεσίες μόνο σε συγκεκριμένα τμήματα του δικτύου, να αποκλείει spam ή command-and-control servers και να εφαρμόζει πολιτικές συμμόρφωσης ασφαλείας. Ειδικά σε bare metal μηχανές που φιλοξενούν κρίσιμες υπηρεσίες, ένα σωστά ρυθμισμένο τοπικό firewall αποτελεί την πρώτη και πιο άμεση γραμμή άμυνας πριν οποιαδήποτε απειλή φτάσει σε επίπεδο εφαρμογής.Ένα από τα πιο σημαντικά τεχνικά χαρακτηριστικά των σύγχρονων firewall είναι η διάκριση μεταξύ stateless και stateful λειτουργίας.
Τα stateless firewalls εξετάζουν κάθε πακέτο μεμονωμένα, βασιζόμενα αποκλειστικά στα στατικά κριτήρια των κανόνων (π.χ. IP διεύθυνση, θύρα, πρωτόκολλο). Δεν διατηρούν πληροφορία για προηγούμενα πακέτα και έτσι είναι ταχύτερα αλλά λιγότερο έξυπνα, καθώς δεν μπορούν να αναγνωρίσουν αν ένα πακέτο είναι μέρος μιας έγκυρης, ήδη εγκατεστημένης σύνδεσης. Αντίθετα, τα stateful firewalls παρακολουθούν την «κατάσταση» κάθε σύνδεσης, δημιουργώντας έναν πίνακα καταστάσεων (state table) όπου καταγράφονται οι ενεργές συνδέσεις και η σχετική τους δραστηριότητα. Με αυτόν τον τρόπο, μπορούν να επιτρέπουν αυτόματα την επιστροφή πακέτων από έγκυρες συνδέσεις, ενώ μπλοκάρουν πακέτα που δεν ταιριάζουν με κάποιο γνωστό session, αυξάνοντας έτσι την ασφάλεια χωρίς να απαιτείται περίπλοκη διαχείριση κανόνων. Προχωρώντας ακόμη βαθύτερα, υπάρχει η τεχνολογία Deep Packet Inspection (DPI), η οποία δίνει τη δυνατότητα στο firewall να εξετάζει όχι μόνο τα μεταδεδομένα του πακέτου (headers) αλλά και το ίδιο το περιεχόμενο (payload). Αυτό σημαίνει ότι μπορεί να αναλύσει εφαρμογές και πρωτόκολλα σε επίπεδο 7 του OSI (application layer), αναγνωρίζοντας αν π.χ. η κίνηση ενός πακέτου που μοιάζει με HTTP

στην πραγματικότητα περιέχει κακόβουλο κώδικα, προσπάθεια SQL injection ή ακόμα και παραβίαση πολιτικών περιεχομένου. Το DPI μπορεί να χρησιμοποιηθεί για να μπλοκάρει peer-to-peer κίνηση, να αποτρέψει την πρόσβαση σε ακατάλληλο περιεχόμενο, να ανιχνεύσει malware ή command-and-control επικοινωνία, αλλά απαιτεί περισσότερη επεξεργαστική ισχύ και μπορεί να αυξήσει την καθυστέρηση (latency).



Σχημα 1.15: Δομή σύνταξης ενός κανόνα σε firewall [14.α]

Στη σύγχρονη αρχιτεκτονική ασφαλείας, τα stateful firewalls σε συνδυασμό με DPI αποτελούν μια ολοκληρωμένη λύση, καθώς προσφέρουν τόσο ευφυΐα στην κατανόηση της ροής δεδομένων όσο και τη δυνατότητα επιθεωρήσεων σε βάθος για τον εντοπισμό προηγμένων απειλών. Σε bare metal μηχανές που παρέχουν κρίσιμες υπηρεσίες, μια τέτοια υλοποίηση μπορεί να προστατεύσει αποτελεσματικά από επιθέσεις που δεν θα σταματούσαν με παραδοσιακά, απλά, stateless φίλτρα. [26]

1.19: Web Access Firewall

Το Web Application Firewall (WAF) αποτελεί έναν εξειδικευμένο τύπο firewall που είναι σχεδιασμένος για να προστατεύει εφαρμογές ιστού από ένα ευρύ φάσμα απειλών, εκτελώντας λεπτομερή έλεγχο των HTTP/HTTPS αιτημάτων που εισέρχονται ή εξέρχονται από μια web εφαρμογή. Σε αντίθεση με τα παραδοσιακά firewalls, τα οποία επικεντρώνονται στην προστασία του δικτύου μέσω ελέγχου θύρων, διευθύνσεων IP και πρωτοκόλλων, το WAF εστιάζει στην αναγνώριση και αποτροπή επιθέσεων σε επίπεδο εφαρμογής, όπως SQL injection, cross-site scripting (XSS), file inclusion, session hijacking και άλλα είδη κακόβουλων αιτημάτων που εκμεταλλεύονται ευπάθειες στον κώδικα ή την αρχιτεκτονική μιας εφαρμογής. Η λειτουργία του WAF βασίζεται στη δημιουργία και εφαρμογή ενός συνόλου κανόνων (rulesets), που ορίζουν μοτίβα κακόβουλης συμπεριφοράς ή επικίνδυνων αιτημάτων. Αυτοί οι κανόνες μπορούν να είναι είτε στατικοί είτε δυναμικοί, ανάλογα με την πλατφόρμα και τη φιλοσοφία σχεδίασης του WAF. Το WAF μπορεί να λειτουργεί σε τρεις βασικές λειτουργίες: σε λειτουργία ανίχνευσης (monitoring), όπου δεν αποκλείει την κίνηση αλλά παρακολουθεί για ύποπτες συμπεριφορές, σε λειτουργία προστασίας (blocking), όπου απορρίπτει ενεργά κακόβουλα αιτήματα, και σε λειτουργία hybrid/learning, όπου το σύστημα προσαρμόζεται δυναμικά στα δεδομένα της εφαρμογής. Η υλοποίηση μπορεί να είναι τοπική (on-premises), να βασίζεται σε cloud (cloud-based WAF), ή να γίνεται μέσω αντιπροσώπευσης (reverse proxy), όπως συμβαίνει με την Cloudflare ή την AWS. Το WAF τοποθετείται συνήθως μπροστά από την web εφαρμογή και αναλαμβάνει τη διεκπεραίωση όλων των εισερχόμενων αιτημάτων πριν αυτά φτάσουν στον server. Αυτό του δίνει τη δυνατότητα να ελέγχει κάθε πακέτο δεδομένων για ύποπτα πρότυπα. Οι σύγχρονες υλοποιήσεις βασίζονται σε τεχνικές deep packet inspection, συμπεριλαμβανομένων μεθόδων ταυτοποίησης βάσει υπογραφών (signatures), τεχνικών machine learning, heuristics και κατηγοριοποίησης συμπεριφοράς.

Η χρησιμότητα ενός WAF είναι κρίσιμη για την αποτροπή επιθέσεων που δεν μπορούν να αναγνωριστούν ή να αποτραπούν από τα συμβατικά firewalls ή τα συστήματα IDS/IPS. Ειδικά για δημόσια προσβάσιμες εφαρμογές, η ύπαρξη ενός WAF προσφέρει ένα επιπλέον επίπεδο άμυνας στο

πλαίσιο της αρχιτεκτονικής άμυνας βάθους (defense-in-depth). Ωστόσο, η αποτελεσματικότητα ενός WAF εξαρτάται σε μεγάλο βαθμό από τη σωστή παραμετροποίησή του. Υπερβολικά αυστηροί κανόνες μπορούν να οδηγήσουν σε false positives και διακοπή νόμιμων αιτημάτων, ενώ ελλιπής ρύθμιση μπορεί να αφήσει ευάλωτα σημεία μη προστατευμένα. Οι υπηρεσίες WAF που προσφέρονται από παρόχους όπως η Cloudflare, η AWS (AWS WAF), και η Imperva, επεκτείνουν τη λειτουργία τους με συνεχή ενημέρωση για νέες απειλές, αυτόματη προσαρμογή των κανόνων και δυνατότητες ενσωμάτωσης με συστήματα SIEM και log analysis. Σε πολλές περιπτώσεις, το WAF συνοδεύεται από άλλες υπηρεσίες όπως rate limiting, bot protection, API shielding και DDoS mitigation, καθιστώντας το βασικό εργαλείο στην ολιστική προσέγγιση ασφάλειας μιας εφαρμογής ιστού [16] [26].

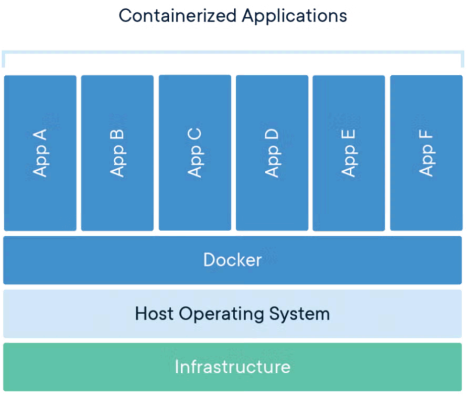
1.20: Conteinerization

Η έννοια του containerization αναφέρεται σε μια μέθοδο απομόνωσης και εκτέλεσης εφαρμογών μέσα σε ελαφριά, ανεξάρτητα και φορητά περιβάλλοντα που ονομάζονται containers. Πρόκειται για μια τεχνολογική προσέγγιση που επιτρέπει την ανάπτυξη και λειτουργία λογισμικού με συνέπεια, ανεξάρτητα από τις διαφορές του υποκείμενου υπολογιστικού περιβάλλοντος. Η βασική ιδέα είναι ότι κάθε εφαρμογή, μαζί με όλες τις βιβλιοθήκες, εξαρτήσεις, ρυθμίσεις και αρχεία συστήματος που απαιτούνται για την εκτέλεσή της, πακετάρεται σε μια ενιαία οντότητα που μπορεί να εκτελεστεί σε οποιονδήποτε συμβατό υπολογιστή ή server. Η αρχιτεκτονική του containerization βασίζεται στην αρχή της απομόνωσης διεργασιών και πόρων. Σε επίπεδο λειτουργικού συστήματος, αυτό επιτυγχάνεται μέσω τεχνολογιών όπως τα namespaces και τα control groups (cgroups), τα οποία επιτρέπουν τη διαχείριση των διεργασιών, του χώρου διευθύνσεων, της πρόσβασης στο δίκτυο, της χρήσης του συστήματος αρχείων και των διαθέσιμων πόρων υπολογιστικής ισχύος. Οι containers, σε αντίθεση με τις παραδοσιακές εικονικές μηχανές, δεν απαιτούν τη δημιουργία πλήρους εικονικού λειτουργικού συστήματος. Αντιθέτως, μοιράζονται τον ίδιο πυρήνα (kernel) του host λειτουργικού, με αποτέλεσμα να είναι σημαντικά πιο ελαφριοί, ταχύτεροι στην εκκίνηση και αποδοτικότεροι στη χρήση των πόρων.

Η προσέγγιση αυτή προσφέρει σημαντικά πλεονεκτήματα για την ανάπτυξη και την κλιμάκωση σύγχρονων πληροφοριακών συστημάτων. Πρώτον, καθιστά τη διαδικασία της ανάπτυξης ανεξάρτητη από το εκτελεστικό περιβάλλον, αφού ο container μπορεί να τρέξει με τον ίδιο τρόπο τοπικά στον υπολογιστή του προγραμματιστή, σε έναν server ελέγχου ποιότητας ή σε ένα περιβάλλον παραγωγής. Δεύτερον, ενισχύει την ασφάλεια, καθώς κάθε container είναι απομονωμένος από τους υπόλοιπους και από το λειτουργικό του host, περιορίζοντας τις πιθανές επιπτώσεις από κακόβουλη δραστηριότητα ή σφάλματα. Τρίτον, διευκολύνει την υλοποίηση αρχιτεκτονικών βασισμένων σε μικροϋπηρεσίες (microservices), καθώς κάθε υπηρεσία μπορεί να τρέχει σε δικό της container, ανεξάρτητα από τις υπόλοιπες. Από άποψη διαχείρισης, το containerization επιτρέπει τη δημιουργία επαναχρησιμοποιήσιμων και αναπαραγώγιμων images, που μπορούν να αποθηκευτούν σε αποθετήρια και να αναπτυχθούν μαζικά ή αυτοματοποιημένα μέσω μηχανισμών συνεχούς ενσωμάτωσης και ανάπτυξης . Επιπλέον, σε περιβάλλοντα υψηλής κλίμακας, το containerization καθίσταται απαραίτητο για την αποδοτική αξιοποίηση των υπολογιστικών υποδομών, κυρίως σε cloud συστήματα ή κατανεμημένα clusters, όπου μπορεί να συνδυαστεί με συστήματα ορχήστρωσης που αυτοματοποιούν την εκκίνηση, κατανομή, παρακολούθηση και επανεκκίνηση των containers.

Παρά τα πλεονεκτήματα, η τεχνολογία αυτή ενέχει και προκλήσεις, όπως η ανάγκη προσεκτικής διαχείρισης των δικαιωμάτων πρόσβασης μεταξύ containers και του host, η αντιμετώπιση της πολυπλοκότητας σε περιβάλλοντα με εκατοντάδες containers, και η σωστή παρακολούθηση της

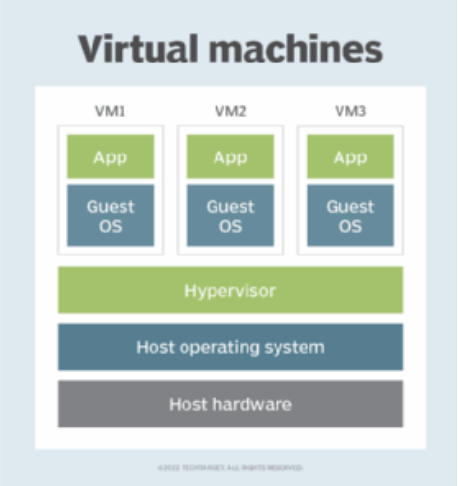
κατανάλωσης πόρων. Παρόλα αυτά, η καθιέρωση του containerization θεωρείται μια από τις σημαντικότερες εξελίξεις στη σύγχρονη πληροφορική, καθώς προσφέρει ένα ενοποιημένο μοντέλο για τη φορητότητα, ασφάλεια και αποδοτικότητα των εφαρμογών σε ένα ευρύ φάσμα περιβαλλόντων.[27]



Σχήμα 1.16: Δομή ενός Docker Συστήματος [15.a]

1.21: Virtual Machine

Οι εικονικές μηχανές (Virtual Machines – VMs) αποτελούν μία από τις θεμελιώδεις τεχνολογίες εικονικοποίησης (virtualization), μέσω της οποίας παρέχεται η δυνατότητα εκτέλεσης πολλαπλών ανεξάρτητων λειτουργικών συστημάτων πάνω στον ίδιο φυσικό υπολογιστή ή διακομιστή (host). Ουσιαστικά, μια εικονική μηχανή είναι ένα απομονωμένο, πλήρως λειτουργικό περιβάλλον το οποίο προσομοιώνει το υλικό ενός υπολογιστή (CPU, RAM, σκληρός δίσκος, κάρτα δικτύου, BIOS κ.λπ.), επιτρέποντας σε ένα λειτουργικό σύστημα (guest OS) να εγκατασταθεί και να εκτελείται ως αν επρόκειτο για φυσικό υλικό. Η υλοποίηση των εικονικών μηχανών βασίζεται στην ύπαρξη ενός λογισμικού που ονομάζεται hypervisor. Ο hypervisor λειτουργεί ως διαμεσολαβητής ανάμεσα στο υλικό του host συστήματος και στα λειτουργικά συστήματα των VMs. Υπάρχουν δύο βασικοί τύποι hypervisors. Οι hypervisors τύπου 1 (bare-metal) εγκαθίστανται απευθείας στο υλικό του συστήματος και χρησιμοποιούνται σε περιβάλλοντα υψηλής απόδοσης και παραγωγής, όπως το VMware ESXi, το Microsoft Hyper-V και το Xen. Οι hypervisors τύπου 2 (hosted) λειτουργούν πάνω από ένα υπάρχον λειτουργικό σύστημα (όπως π.χ. ο VirtualBox ή το VMware Workstation) και χρησιμοποιούνται κυρίως για ανάπτυξη, δοκιμές ή εκπαιδευτικούς σκοπούς.



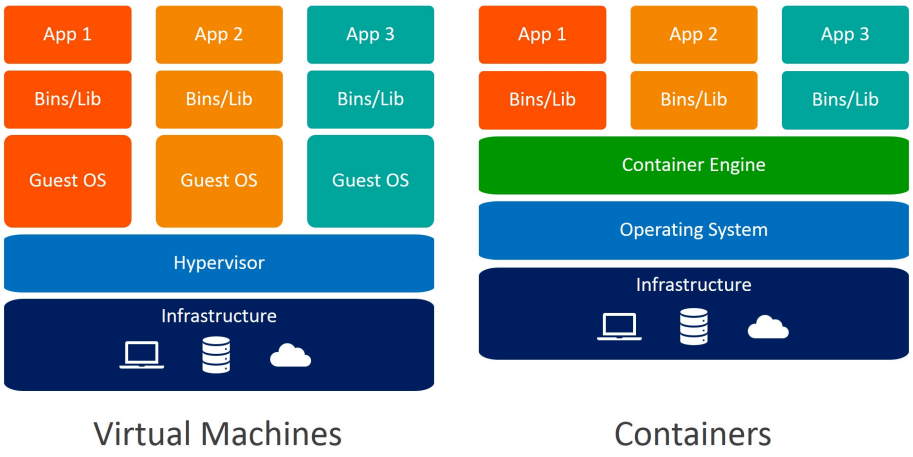
Σχήμα 1.16: Δομή ενός virtual machine [16.α]

Η βασική αρχιτεκτονική μιας εικονικής μηχανής περιλαμβάνει τη δημιουργία ενός εικονικού δίσκου (συνήθως σε μορφή αρχείου στον host), την εκχώρηση ενός ποσοστού των φυσικών πόρων (π.χ. CPU πυρήνων, RAM) και τη διαμόρφωση της σύνδεσης με το δίκτυο (μέσω bridged, NAT ή host-only λειτουργιών). Μόλις εγκατασταθεί το λειτουργικό σύστημα στη VM, αυτό μπορεί να λειτουργεί όπως και σε ένα φυσικό μηχάνημα, χωρίς να γνωρίζει ότι εκτελείται σε εικονικό περιβάλλον. Ένα από τα κυριότερα πλεονεκτήματα των εικονικών μηχανών είναι η πλήρης απομόνωση που προσφέρουν. Κάθε VM είναι ανεξάρτητη και απομονωμένη από τις υπόλοιπες και από το host, γεγονός που ενισχύει την ασφάλεια και τη σταθερότητα του συστήματος. Επιπλέον, η δυνατότητα δημιουργίας snapshots, δηλαδή στιγμιότυπων κατάστασης μιας VM, διευκολύνει την ανάκτηση συστημάτων, τον πειραματισμό και την ελαχιστοποίηση του downtime σε περίπτωση σφάλματος. Τα VMs χρησιμοποιούνται ευρύτατα σε datacenters, σε περιβάλλοντα δοκιμών, σε ανάπτυξη λογισμικού και σε σενάρια disaster recovery. Ωστόσο, οι εικονικές μηχανές έχουν και σημαντικά μειονεκτήματα σε σχέση με τις πιο πρόσφατες τεχνολογίες containerization. Λόγω του γεγονότος ότι κάθε VM απαιτεί την εκτέλεση ενός πλήρους λειτουργικού συστήματος, η κατανάλωση πόρων (RAM, CPU, δίσκου) είναι σημαντικά αυξημένη. Η εκκίνηση μιας VM είναι βραδύτερη σε σύγκριση με έναν container, και η απόδοση συχνά υπολείπεται, ιδίως όταν πολλές VMs συνυπάρχουν στον ίδιο host. Παρόλα αυτά, εξακολουθούν να είναι απαραίτητες σε περιπτώσεις όπου απαιτείται πλήρης απομόνωση, λειτουργία διαφορετικών λειτουργικών συστημάτων ή εκτέλεση εφαρμογών που δεν μπορούν να ενταχθούν σε ένα σύστημα container.

Η τεχνολογία των εικονικών μηχανών αποτελεί το θεμέλιο πάνω στο οποίο οικοδομήθηκαν πολλές από τις σύγχρονες υπηρεσίες cloud. Πλατφόρμες όπως το Amazon EC2, το Microsoft Azure Virtual Machines και το Google Compute Engine βασίζονται στην εικονικοποίηση για να προσφέρουν υποδομές ως υπηρεσία (IaaS), δίνοντας στους χρήστες τη δυνατότητα να δημιουργούν και να διαχειρίζονται εικονικά περιβάλλοντα χωρίς την ανάγκη φυσικής υποδομής. Η εξέλιξη των VMs σε συνδυασμό με τις νεότερες τεχνολογίες όπως τα containers και οι μικροϋπηρεσίες έχει μεταμορφώσει τον τρόπο με τον οποίο αναπτύσσεται, εκτελείται και κλιμακώνεται το λογισμικό στον 21ο αιώνα. [27]

1.23: Containerization Vs VM

Η βασική διαφορά εντοπίζεται στο επίπεδο στο οποίο υλοποιείται η απομόνωση. Οι εικονικές μηχανές απομονώνουν σε επίπεδο υλικού, εφόσον κάθε VM προσομοιώνει ένα πλήρες υπολογιστικό σύστημα, το οποίο περιλαμβάνει τον δικό του πυρήνα λειτουργικού συστήματος. Αυτό σημαίνει ότι κάθε VM «κουβαλάει» το δικό της πλήρες λειτουργικό σύστημα (όπως Linux, Windows κ.λπ.), δημιουργώντας μια μονάδα απολύτως ανεξάρτητη αλλά και πιο βαριά από άποψη πόρων. Η επικοινωνία με το φυσικό υλικό (host) γίνεται μέσω του hypervisor, ο οποίος διαχειρίζεται την κατανομή των διαθέσιμων πόρων και φροντίζει για την απομόνωση και τη σταθερότητα του συστήματος. Αντίθετα, το containerization εφαρμόζει την απομόνωση σε επίπεδο λειτουργικού συστήματος. Όλοι οι containers εκτελούνται απευθείας πάνω στον πυρήνα του host OS, χωρίς να απαιτείται ξεχωριστός πυρήνας ή πλήρες λειτουργικό για κάθε container. Αυτό σημαίνει ότι οι containers είναι σημαντικά πιο ελαφροί, γρηγορότεροι στην εκκίνηση, καταναλώνουν λιγότερους πόρους και κλιμακώνονται ευκολότερα. Χάρη σε τεχνολογίες όπως τα namespaces και τα control groups (cgroups) στο Linux, διασφαλίζεται η απομόνωση της κάθε containerized εφαρμογής χωρίς να θυσιάζεται η απόδοση. Η πρακτική συνέπεια αυτών των διαφορών είναι ότι οι containers είναι ιδανικοί για τη φιλοξενία μικροϋπηρεσιών, cloud-native εφαρμογών, pipelines ανάπτυξης λογισμικού και ευέλικτων αρχιτεκτονικών. Παρέχουν επίσης υψηλό βαθμό φορητότητας: ένας container που δημιουργήθηκε σε ένα περιβάλλον μπορεί να εκτελεστεί με τον ίδιο τρόπο σε οποιοδήποτε άλλο σύστημα που υποστηρίζει την ίδια μηχανή container (όπως το Docker). Οι εικονικές μηχανές, από την άλλη πλευρά, είναι πιο κατάλληλες για εφαρμογές που απαιτούν απομόνωση σε βάθος, συμβατότητα με διαφορετικά λειτουργικά συστήματα ή τη δυνατότητα εκτέλεσης legacy λογισμικού που δεν μπορεί να τρέξει σε container.



Σχημα 1.17: Απεικόνιση διαφορών των δύο συστημάτων [17.α]

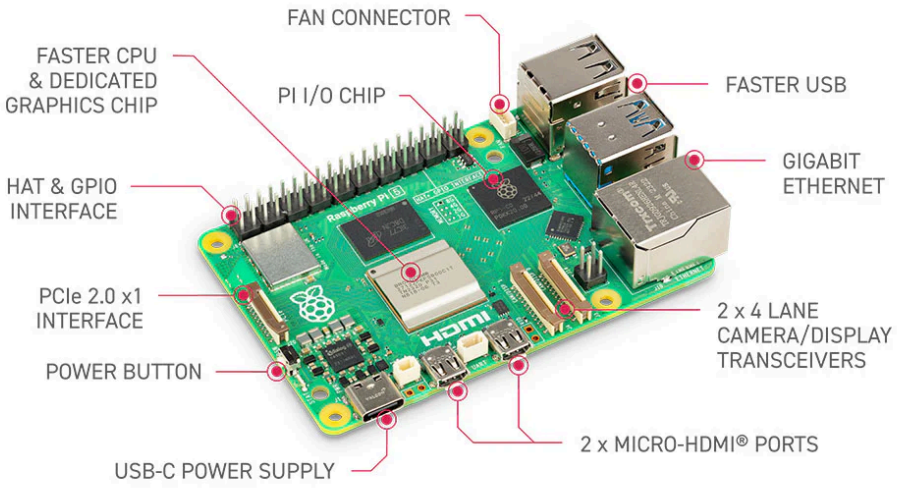
Όσον αφορά την ασφάλεια, τα VMs τείνουν να προσφέρουν υψηλότερο επίπεδο απομόνωσης από πλευράς συστήματος, καθώς οποιαδήποτε επίθεση περιορίζεται εντός της συγκεκριμένης VM. Οι containers, ενώ είναι απομονωμένοι λογικά, μοιράζονται τον ίδιο πυρήνα με τον host και επομένως, θεωρητικά, μια ευπάθεια στον πυρήνα θα μπορούσε να επηρεάσει όλους τους containers. Αν και η τεχνολογία container έχει σημειώσει τεράστια πρόοδο στο ζήτημα της ασφάλειας, σε ορισμένες περιπτώσεις εξακολουθούν να υπάρχουν περιορισμοί σε περιβάλλοντα με αυστηρές απαιτήσεις απομόνωσης. Τέλος, από άποψη συντήρησης και διαχείρισης, οι containers είναι πιο απλοί και ευέλικτοι. Η διαχείριση των εξαρτήσεων, η ανάπτυξη ενημερώσεων και η επαναδημιουργία

περιβαλλόντων γίνεται ταχύτερα και με μεγαλύτερη διαφάνεια. Οι εικονικές μηχανές, αντίθετα, έχουν υψηλότερο λειτουργικό κόστος και πιο βαρύ αποτύπωμα, γεγονός που καθιστά τη διαχείρισή τους πιο απαιτητική.

Συνολικά, και οι δύο τεχνολογίες διαδραματίζουν κρίσιμο ρόλο στη σύγχρονη πληροφορική. Οι εικονικές μηχανές εξακολουθούν να έχουν ζωτικό ρόλο σε υποδομές με συγκεκριμένες ανάγκες απομόνωσης, ενώ οι containers κυριαρχούν στο cloud computing, τη συνεχή ενσωμάτωση και ανάπτυξη , και τη δημιουργία ευέλικτων, αποκεντρωμένων συστημάτων. Η κατανόηση των διαφορών τους είναι καθοριστική για την επιλογή της κατάλληλης τεχνολογίας, ανάλογα με το εκάστοτε πλαίσιο εφαρμογής.[27]

Κεφάλαιο 2ο: Raspberry Pi

Το Raspberry Pi αποτελεί μία από τις πιο επαναστατικές και προσιτές υπολογιστικές πλατφόρμες των τελευταίων δεκαετιών, έχοντας μεταβάλει ριζικά τον τρόπο με τον οποίο προσεγγίζονται η εκπαίδευση, η καινοτομία και η χαμηλού κόστους υπολογιστική ισχύς. Πρόκειται για μία πλακέτα υπολογιστή (single-board computer) που αναπτύχθηκε αρχικά από το Ίδρυμα Raspberry Pi (Raspberry Pi Foundation), έναν φιλανθρωπικό οργανισμό με έδρα το Ηνωμένο Βασίλειο. Η βασική αποστολή του ιδρύματος ήταν και παραμένει η προώθηση της πληροφορικής παιδείας και της πρόσβασης στην τεχνολογία, ιδιαίτερα σε αναπτυσσόμενες χώρες ή περιβάλλοντα χαμηλού προϋπολογισμού.



Σχημα 2.1: Το SBC του Raspberry Pi 5 [18.α]

Το πρώτο μοντέλο Raspberry Pi παρουσιάστηκε το 2012 και από τότε έχουν κυκλοφορήσει πολυάριθμες εκδόσεις και παραλλαγές, καθεμία εκ των οποίων προσέφερε σημαντικές βελτιώσεις ως προς τις επιδόσεις, τη συνδεσιμότητα, και τη διαχείριση ενέργειας και την επεκτασιμότητα. Τα δημοφιλέστερα μοντέλα, όπως το Raspberry Pi 4 Model B και το Raspberry Pi 5, ενσωματώνουν τετραπύρηνους επεξεργαστές αρχιτεκτονικής ARM, μεταβλητές ποσότητες μνήμης RAM (από 2 GB έως 8 GB), θύρες USB 2.0 και 3.0, HDMI έξοδο, κάρτα δικτύου Gigabit Ethernet, ενσωματωμένο Wi-Fi και Bluetooth, καθώς και θύρες GPIO για φυσική αλληλεπίδραση με εξωτερικές συσκευές και κυκλώματα. Το τελευταίο, καθότι και ο εγκέφαλος της παρούσας εργασίας παρουσιάστηκε επίσημα τον Σεπτέμβριο του 2023, σηματοδοτεί τη σημαντικότερη τεχνολογική αναβάθμιση στην ιστορία της πλατφόρμας, φέρνοντας μια σειρά από αρχιτεκτονικές καινοτομίες που το καθιστούν όχι μόνο τον πιο ισχυρό Raspberry Pi μέχρι σήμερα, αλλά και έναν ικανότατο μικροϋπολογιστή με δυνατότητες που πλησιάζουν πλέον αυτές ενός desktop συστήματος μικρής κλίμακας

Η πιο θεμελιώδης διαφορά σε σχέση με τους προκατόχους του είναι η χρήση ενός νέου επεξεργαστή: του Broadcom BCM2712, ο οποίος είναι τετραπύρηνος, βασισμένος στην αρχιτεκτονική ARM Cortex-A76, με συχνότητα λειτουργίας στα 2.4 GHz. Ο συγκεκριμένος πυρήνας, αν και λιγότερο ενεργειακά αποδοτικός από τους Cortex-A72 του Raspberry Pi 4, προσφέρει σημαντικά ανώτερη απόδοση ανά πυρήνα Μια σημαντική καινοτομία του Raspberry Pi 5 είναι η ενσωμάτωση του νέου Southbridge RP1, ενός επιπλέον chip σχεδιασμένου από το Raspberry Pi Foundation. Το RP1

αναλαμβάνει την ευθύνη για τις εξωτερικές διασυνδέσεις και φέρνει υποστήριξη για δύο θύρες USB 3.0 με πλήρες εύρος ζώνης (bandwidth) , διπλή έξοδο εικόνας μέσω micro-HDMI με υποστήριξη 4K στα 60Hz,, και βελτιωμένο δίαυλο SD για ταχύτερη πρόσβαση στην κάρτα microSD. Η υποστήριξη PCIe 2.0 x1 είναι ίσως το χαρακτηριστικό με τον πιο μακροπρόθεσμο αντίκτυπο, καθώς επιτρέπει πλέον την εγκατάσταση SSD δίσκων NVMe μέσω κατάλληλων μετατροπέων, κάτι που ανοίγει τον δρόμο για συστήματα υψηλής αποδοτικότητας, με χαμηλούς χρόνους εκκίνησης, γρήγορη απόκριση και μεγάλη αξιοπιστία στην αποθήκευση. Αυτό είναι εξαιρετικά χρήσιμο σε σενάρια όπου το Raspberry Pi χρησιμοποιείται ως always-on server, όπως στην παρούσα εργασία.

Η ιδιαίτερη σημασία του Raspberry Pi έγκειται στο γεγονός ότι, παρά το μικρό του μέγεθος και κόστος, λειτουργεί ως ένας πλήρως ικανός υπολογιστής, ικανός να εκτελέσει πληθώρα λειτουργιών όπως σερβερ, πύλη δικτύου (gateway) , πλατφόρμα αυτοματισμού, media center, ή ακόμα και βασικός σταθμός εργασίας. Αυτό το χαρακτηριστικό το καθιστά ιδανική επιλογή για πειραματισμούς, εκπαιδευτικά έργα, αλλά και για πρακτικές υλοποιήσεις σε επαγγελματικά ή οικιακά περιβάλλοντα. Η χρήση του Raspberry Pi σε έργα αυτοματισμού –όπως το παρόν σύστημα έξυπνου σπιτιού– βασίζεται τόσο στην επεξεργαστική του επάρκεια όσο και στη συμβατότητά του με δημοφιλή λογισμικά, μεταξύ των οποίων και ο Home Assistant. Η δυνατότητα εκτέλεσης εξειδικευμένων διανομών λειτουργικού συστήματος, όπως το Home Assistant OS, το Raspberry Pi OS (πρώην Raspbian) ή γενικότερα διανομές Linux (π.χ. Ubuntu), επιτρέπει στον χρήστη να διαμορφώσει το περιβάλλον του ακριβώς στις ανάγκες της εφαρμογής του. Η θύρα GPIO (General Purpose Input/Output) του Raspberry Pi αποτελεί ακόμη ένα καθοριστικό πλεονέκτημα. Μέσω αυτής, η πλακέτα μπορεί να επικοινωνεί απευθείας με ηλεκτρονικά κυκλώματα, αισθητήρες, ρελέ, κινητήρες και άλλες περιφερειακές συσκευές, επιτρέποντας την υλοποίηση πολύπλοκων φυσικών διαδράσεων χωρίς την ανάγκη εξωτερικών μικροελεγκτών. Η υποστήριξη για πρότυπα επικοινωνίας όπως I²C, SPI και UART προσφέρει επιπλέον δυνατότητες για ενσωμάτωση σε βιομηχανικές ή ερευνητικές εφαρμογές.Η ευρεία κοινότητα υποστήριξης, καθώς και ο τεράστιος όγκος τεκμηρίωσης, εκπαιδευτικού υλικού και έτοιμων έργων που διατίθενται δωρεάν, καθιστούν το Raspberry Pi εξαιρετικά προσιτό ακόμα και σε χρήστες χωρίς προηγούμενη εμπειρία στον προγραμματισμό ή στα ηλεκτρονικά κυκλώματα. Επιπλέον, η υποστήριξη από διεθνείς οργανισμούς και η αποδοχή του από τη βιομηχανία έχουν οδηγήσει στην ανάπτυξη ενός πλήρους οικοσυστήματος εξαρτημάτων, add-on πλακετών (HATs), καλωδίων και τροφοδοτικών, τα οποία καλύπτουν ένα ευρύ φάσμα εφαρμογών.

Αναφορικά με τη θερμική και ενεργειακή του συμπεριφορά, το Raspberry Pi χαρακτηρίζεται από εξαιρετική ενεργειακή αποδοτικότητα (< 30 W) , γεγονός που το καθιστά κατάλληλο για συνεχή λειτουργία σε εφαρμογές όπως η παρούσα. Σε κατάσταση αδράνειας (idle), το Raspberry Pi 5 καταναλώνει περίπου 2.8–3.5 W, ανάλογα με τη διανομή του λειτουργικού συστήματος, τις περιφερειακές συσκευές που είναι συνδεδεμένες (όπως USB dongles ή Zigbee sticks) και την ενεργοποίηση του Wi-Fi ή Bluetooth. Κατά τη διάρκεια έντονης χρήσης (π.χ. κατά την αναπαραγωγή πολυμέσων, εκτέλεση πολλαπλών υπηρεσιών ή έντονης διεργασίας μέσω Docker containers ή automations του Home Assistant), η κατανάλωση μπορεί να φτάσει ή και να ξεπεράσει τα 7–9 W. Σε εξαιρετικά απαιτητικές συνθήκες (πλήρες load και ταυτόχρονη χρήση των δύο USB 3.0 θυρών ή PCIe NVMe δίσκου), η μέγιστη καταγεγραμμένη κατανάλωση έχει προσεγγίσει τα 11–12 W. Το Raspberry Pi Foundation συνιστά για το Pi 5 την χρήση ενός τροφοδοτικού 27 W (5V / 5A) με υποστήριξη USB Power Delivery (PD). Αν και η συσκευή δεν καταναλώνει πάντα όλο το ρεύμα αυτό, το ισχυρότερο τροφοδοτικό είναι αναγκαίο ώστε να διασφαλιστεί σταθερότητα υπό φορτίο και να καλυφθούν περιφερειακές ανάγκες. Η διαχείριση θερμότητας σχετίζεται άμεσα με την κατανάλωση ενέργειας. Καθώς το Pi 5 παράγει αισθητά περισσότερη θερμότητα υπό φορτίο από τα προηγούμενα μοντέλα, απαιτείται ενεργό σύστημα ψύξης – συνήθως με ανεμιστήρα. Η χρήση ανεμιστήρα αυξάνει ελαφρώς

την συνολική κατανάλωση (περίπου +0.3–0.6 W), αλλά είναι απαραίτητη για την αποφυγή thermal throttling, το οποίο μπορεί να επηρεάσει την απόδοση σε συνεχή λειτουργία. Παρά ταύτα, η ενεργειακή του αποδοτικότητα παραμένει εξαιρετική σε σχέση με την απόδοση που προσφέρει. Για παράδειγμα, ένα τυπικό mini-PC θα απαιτούσε περισσότερα από 30 W για να επιτύχει παρόμοια αποτελέσματα με αυτά του Raspberry Pi 5.

Τέλος, η χρήση του Raspberry Pi ως βάση για ένα σύστημα έξυπνου σπιτιού προσφέρει ένα σημαντικό πλεονέκτημα: επιτρέπει την πλήρη ιδιοκτησία της υποδομής από τον τελικό χρήστη. Η λογική του αποκεντρωμένου ελέγχου και της ανεξαρτησίας από εμπορικά "κλειστά" οικοσυστήματα συνάδει απόλυτα με τη φιλοσοφία του Home Assistant και της ανοικτής τεχνολογίας, ενισχύοντας την ιδιωτικότητα, την ασφάλεια και τη μακροπρόθεσμη βιωσιμότητα του συστήματος.[4] [5] [28]

2.1: Home Assistant

Ο Home Assistant αποτελεί μία από τις πιο διαδεδομένες, ισχυρές και ταχέως εξελισσόμενες πλατφόρμες αυτοματισμού για οικιακή χρήση. Πρόκειται για ένα ανοικτού κώδικα λογισμικό (open-source home automation platform), το οποίο επιτρέπει τον έλεγχο και την αυτοματοποίηση μιας ευρείας γκάμας συσκευών και αισθητήρων που είναι συνδεδεμένες σε ένα έξυπνο σπίτι. Η βασική του αρχή στηρίζεται στη φιλοσοφία της ιδιωτικότητας, της ανεξαρτησίας από εταιρικά οικοσυστήματα και της πλήρους παραμετροποίησης από τον χρήστη. Η ανάπτυξη του Home Assistant ξεκίνησε το 2013 από τον Paulus Schoutsen, έναν Ολλανδό μηχανικό λογισμικού, ο οποίος επιδίωξε να δημιουργήσει μια πλατφόρμα ικανή να παρέχει ενοποιημένο έλεγχο για συσκευές έξυπνου σπιτιού, απαλλαγμένη από τις περιοριστικές πρακτικές των εμπορικών λύσεων της αγοράς. Η ανάπτυξή του υποστηρίζεται από την κοινότητα και τη μη κερδοσκοπική εταιρεία Nabu Casa Inc. , η οποία ιδρύθηκε το 2018 με σκοπό να διασφαλίσει τη βιωσιμότητα του έργου και να προσφέρει εμπορική υποστήριξη και πρόσθετες δυνατότητες χωρίς να επηρεάζεται η ανοιχτή φύση του.

Εικόνα 2.2: Το λογότυπο του Home Assistant [19.α]

Ο Home Assistant βασίζεται σε Python και μπορεί να εκτελεστεί τοπικά σε διάφορες συσκευές, όπως Raspberry Pi, mini PCs ή ακόμη και σε εικονικές μηχανές (virtual machines). Ουσιαστικά λειτουργεί ως ένας κεντρικός κόμβος ελέγχου (hub), συγκεντρώνοντας και ενωποιώντας τη λειτουργία έξυπνων συσκευών διαφορετικών κατασκευαστών, πρωτοκόλλων και τεχνολογιών όπως Zigbee, Z-Wave, Wi-Fi, Bluetooth και άλλες λοιπές τεχνολογίες, ενώ μέσω της υποστήριξης για YAML αρχεία επιτρέπει στον χρήστη να καθορίσει σύνθετους αυτοματισμούς και σενάρια λειτουργίας. Μια από τις θεμελιώδεις αρχές του Home Assistant είναι η τοπική λειτουργία χωρίς εξάρτηση από το διαδίκτυο. Οι περισσότερες λειτουργίες και αυτοματισμοί πραγματοποιούνται εξ ολοκλήρου εντός του τοπικού

δικτύου (LAN), γεγονός που ενισχύει σημαντικά την ιδιωτικότητα, την ασφάλεια και την αξιοπιστία. Παράλληλα, δίνεται η δυνατότητα απομακρυσμένης πρόσβασης μέσω λύσεων όπως το Home Assistant Cloud (Οπου το προσφέρει η ίδια η εταιρία) ή μέσω εναλλακτικών όπως VPN, reverse proxies και Cloudflare Tunnel, όπως ακριβώς υλοποιείται στην παρούσα εργασία. Η πλατφόρμα υποστηρίζει περισσότερες από 2500 ολοκληρωμένες ενσωματώσεις (integrations), καλύπτοντας πλήθος κατασκευαστών και έξυπνων συσκευών, από απλούς διακόπτες και αισθητήρες μέχρι πολύπλοκα συστήματα ψύξης και θέρμανσης, κάμερες ασφαλείας, συστήματα ψυχαγωγίας και ενεργειακής διαχείρισης . Η δυνατότητα επέκτασης με προσαρμοσμένα απο τον χρήστη εξαρτήματα καθιστά τον Home Assistant ιδιαίτερα ευέλικτο και κατάλληλο για απαιτητικές και εξειδικευμένες εγκαταστάσεις. Το περιβάλλον διαχείρισης του Home Assistant προσφέρει μια σύγχρονη και δυναμική διαδικτυακή διεπαφή (Web Interface), την οποία την ονομάζει ο κατασκευαστής του “Lovelace UI”, το οποίο είναι απόλυτα παραμετροποιήσιμο τόσο οπτικά όσο και λειτουργικά. Ο χρήστης μπορεί να δημιουργήσει ταμπλό (dashboards) που αντικατοπτρίζουν διαφορετικούς χώρους, σενάρια χρήσης ή ρόλους, ενώ είναι δυνατή η προσθήκη ειδικών καρτών (cards) για γραφήματα, ροές δεδομένων,και προσαρμοσμένα εκτελέσιμα σενάρια (Scripts) .

Σε επίπεδο αυτοματισμών, ο Home Assistant επιτρέπει τη δημιουργία σύνθετων σεναρίων με βάση τις λογικές συνθήκες (AND, OR, NOT, XOR), συμβάντα και χρονικά πλαίσια. Αυτοί οι αυτοματισμοί μπορούν να βασίζονται σε πλήθος μεταβλητών, όπως η παρουσία χρηστών, οι μετρήσεις από αισθητήρες. Η κοινότητα του Home Assistant είναι ιδιαιτέρως ενεργή και πολυπληθής, με συνεχή υποστήριξη και συνεισφορές στον πηγαίο κώδικα τουυ έργο, στην τεκμηρίωση, στα πρόσθετα του και στις βελτιώσεις ασφαλείας. Κάθε μήνα δημοσιεύονται νέες ενημερώσεις με βελτιώσεις, νέα χαρακτηριστικά και διορθώσεις σφαλμάτων, κάτι που καθιστά τον Home Assistant μια εξαιρετικά ζωντανή και επίκαιρη πλατφόρμα. Αναφορικά με την ασφάλεια, ο Home Assistant διαθέτει ενσωματωμένες λειτουργίες ελέγχου ταυτότητας, διαχείρισης χρηστών και καταγραφής συμβάντων (Logs). Η ασφαλής απομακρυσμένη πρόσβαση μπορεί να επιτευχθεί χωρίς ανάγκη ανοίγματος θυρών στο router, μέσω τεχνολογιών όπως το Cloudflare Tunnel, οι οποίες χρησιμοποιούνται στην παρούσα εργασία και διασφαλίζουν τη μέγιστη δυνατή προστασία έναντι επιθέσεων τύπου brute-force, port scanning ή man-in-the-middle.

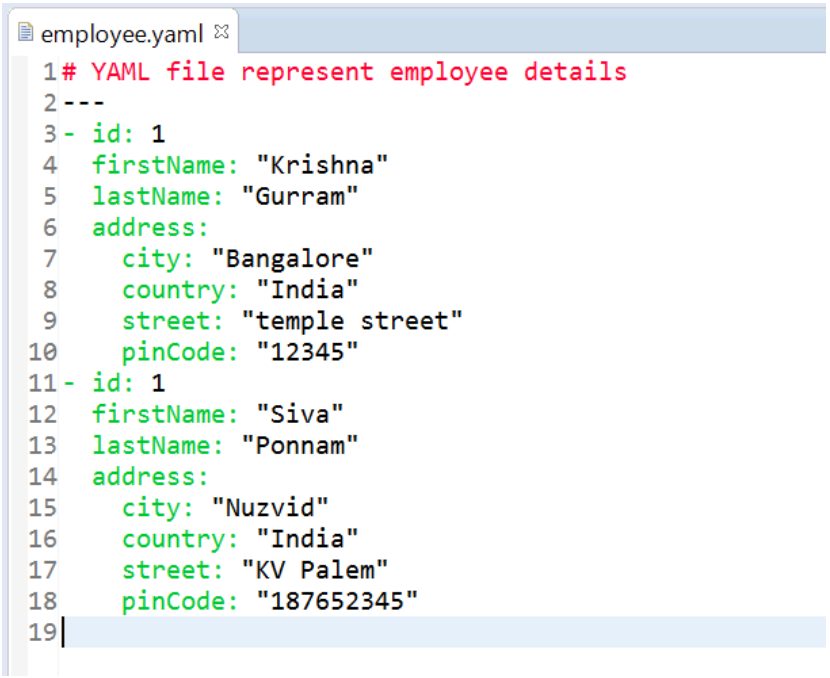
Οπως αναφέρθηκε και πιο πάνω,Ο Home Assistant, λόγω της αρχιτεκτονικής και της ευελιξίας του, μπορεί να εγκατασταθεί και να εκτελεστεί σε μια πληθώρα υπολογιστικών περιβαλλόντων, από μικροσκοπικές συσκευές χαμηλής κατανάλωσης ενέργειας έως ισχυρότερους οικιακούς ή επαγγελματικούς server. Η δυνατότητα λειτουργίας σε διαφορετικά υπολογιστικά συστήματα αποτελεί ένα από τα σημαντικότερα πλεονεκτήματα της πλατφόρμας και έχει συμβάλει καθοριστικά στη δημοτικότητά της. Κατ’ αρχάς, η πλέον διαδεδομένη πλατφόρμα για την εκτέλεση του Home Assistant είναι το Raspberry Pi, Το Raspberry Pi είναι μια μικρού μεγέθους μονοπλακετική υπολογιστική μονάδα, εξαιρετικά οικονομική και ενεργειακά αποδοτική, που προσφέρει ικανοποιητική επεξεργαστική ισχύ για τις ανάγκες ενός τυπικού οικιακού αυτοματισμού. Η επίσημη έκδοση Home Assistant OS μπορεί να εγκατασταθεί απευθείας σε κάρτα microSD, μονάδα αποθήκευσης USB ή SSD συνδεδεμένο στο Raspberry Pi, παρέχοντας ένα πλήρες λειτουργικό περιβάλλον ειδικά σχεδιασμένο για τη συγκεκριμένη εφαρμογή. Πέραν του Raspberry Pi, ο Home Assistant υποστηρίζει και άλλες αρχιτεκτονικές, όπως x86_64, ARMv7 και aarch64, επιτρέποντας την εγκατάστασή του σε υπολογιστές τύπου Intel NUC, σε εικονικές μηχανές (virtual machine) μέσω ειδικών πλατφορμών εποπτείας (Hypervisors) όπως το Proxmox ή το VirtualBox, καθώς και σε περιβάλλοντα Docker. Η χρήση εικονικών μηχανών και περιβάλλον κοντεινερ (containerized) παρέχει αυξημένη απομόνωση, επεκτασιμότητα και ευκολότερη διαχείριση για πιο σύνθετες ή απαιτητικές εγκαταστάσεις.

Για χρήστες που επιθυμούν μεγαλύτερο έλεγχο στο λειτουργικό σύστημα ή την παράλληλη εκτέλεση και άλλων εφαρμογών, υπάρχει η δυνατότητα εγκατάστασης του Home Assistant Supervised, ο οποίος εκτελείται σε διανομές Linux με πλήρη υποστήριξη επιπρόσθετων εφαρμογών (όπως θα μιλήσουμε και παρακάτω) , διατηρώντας ταυτόχρονα τη δυνατότητα του χρήστη να παρέμβει στο υποκείμενο λειτουργικό σύστημα.Μια άλλη διαδεδομένη επιλογή είναι η εγκατάσταση του Home Assistant σε Docker, όπου λειτουργεί ως container με ευκολία μεταφοράς, δημιουργίας αντιγράφων ασφαλείας και απομόνωσης. Αυτή η προσέγγιση προτιμάται συχνά από προχωρημένους χρήστες και διαχειριστές συστημάτων που έχουν ήδη διαμορφωμένες υποδομές βασισμένες σε Docker ή Kubernetes.Σε περιβάλλοντα με αυξημένες απαιτήσεις απόδοσης και σταθερότητας, ο Home Assistant μπορεί να εκτελεστεί σε οικιακούς server ή NAS (Network Attached Storage), προσφέροντας μεγαλύτερη αποθηκευτική χωρητικότητα, αυξημένη επεξεργαστική ισχύ και δυνατότητα ταυτόχρονης εκτέλεσης και άλλων υπηρεσιών, όπως media servers, δικτυακοί φάκελοι ή συστήματα εφεδρικής αποθήκευσης.

Αξίζει να σημειωθεί πως κάθε τρόπος εγκατάστασης έχει διαφορετικές δυνατότητες, περιορισμούς και απαιτήσεις. Η έκδοση Home Assistant OS παρέχει την πληρέστερη εμπειρία με ενσωματωμένα εργαλεία για διαχείριση συστήματος, ενημερώσεις και προσθήκες, ενώ οι εγκαταστάσεις τύπου Core ή Container απευθύνονται σε χρήστες με μεγαλύτερη τεχνική κατάρτιση που επιθυμούν προσαρμοσμένα ή υβριδικά συστήματα.[7] [19] [20]

2.2: YAML (YAML Ain’t Markup Language)

Η γλώσσα YAML (YAML Ain’t Markup Language) είναι μια ανθρώπινα αναγνώσιμη μορφή διαμόρφωσης δεδομένων, η οποία χρησιμοποιείται ευρέως στον τομέα της πληροφορικής για την αναπαράσταση δομημένων δεδομένων με τρόπο λιτό, ευανάγνωστο και εύκολα επεξεργάσιμο τόσο από ανθρώπους όσο και από μηχανές. Παρόλο που το όνομά της δηλώνει ότι "δεν είναι γλώσσα σήμανσης", στην πραγματικότητα αποτελεί μια εναλλακτική στη γλώσσα XML και JSON για πολλές εφαρμογές, κυρίως εκεί όπου απαιτείται απλότητα και σαφήνεια. Η σύνταξη της YAML βασίζεται σε εσοχές (indentation), χωρίς την ανάγκη παρενθέσεων, αγκιστρωτών ή κόμματος στο τέλος κάθε γραμμής, όπως συμβαίνει με το JSON ή το XML. Αυτή η επιλογή προσδίδει υψηλή αναγνωσιμότητα, αλλά ταυτόχρονα την καθιστά και ευάλωτη σε σφάλματα που προκύπτουν από λανθασμένη χρήση κενών ή tabs, τα οποία δεν επιτρέπονται. Στη YAML, οι βασικές δομές δεδομένων υλοποιούνται με πολύ απλό τρόπο: τα dictionaries (ή maps) δηλώνονται με μορφή key: value, ενώ οι λίστες δηλώνονται με παύλες (-) στην αρχή κάθε στοιχείου. Η γλώσσα αυτή υποστηρίζει επίσης προηγμένα χαρακτηριστικά όπως οι αγκυρώσεις (anchors) και οι αναφορές (aliases), που επιτρέπουν την επαναχρησιμοποίηση δομών εντός του ίδιου αρχείου, μειώνοντας τον πλεονασμό. Επιπλέον, παρέχει τη δυνατότητα για σχόλια με το σύμβολο #, κάτι ιδιαίτερα χρήσιμο κατά τον σχολιασμό ρυθμίσεων.



Εικόνα 2.3: Παράδειγμα κώδικα YAML [20.α]

Η σύνταξη της YAML έχει σχεδιαστεί ώστε να είναι απλή, καθαρή και ευανάγνωστη από τον άνθρωπο, χωρίς περιττά σύμβολα και σύνθετους κανόνες. Βασίζεται αποκλειστικά στην εσοχή με spaces (ποτέ με tab), η οποία χρησιμοποιείται για να δηλώσει την ιεραρχία και τις σχέσεις ανάμεσα στα δεδομένα. Τα βασικά στοιχεία της είναι οι λίστες, τα αντικείμενα (ή dictionaries) και οι απλές τιμές (scalars). Οι λίστες δηλώνονται με παύλα - μπροστά από κάθε στοιχείο, ενώ τα αντικείμενα ακολουθούν τη μορφή κλειδί: τιμή. Μπορούν να συνδυαστούν ελεύθερα ώστε να σχηματίζουν σύνθετες δομές δεδομένων. Η YAML υποστηρίζει επίσης και τα σχόλια με χρήση του χαρακτήρα #, ενώ προσφέρει και δυνατότητα εισαγωγής πολυγραμμικών κειμένων είτε διατηρώντας τη μορφοποίησή τους (με |) είτε ενώνοντάς τα σε μία γραμμή (με >). Υποστηρίζει διάφορους τύπους δεδομένων, όπως booleans, αριθμούς, null και ημερομηνίες, ενώ στις περιπτώσεις όπου υπάρχουν ειδικοί χαρακτήρες μέσα στο κείμενο, χρησιμοποιούνται εισαγωγικά. Επιπλέον, η YAML επιτρέπει την επαναχρησιμοποίηση δεδομένων μέσω anchors (&) και aliases (*), διευκολύνοντας έτσι την επαναλαμβανόμενη παραμετροποίηση. Η ευκολία της στη χρήση την καθιστά ιδανική για αρχεία ρυθμίσεων σε πλαίσια όπως το Home Assistant, ωστόσο απαιτείται προσοχή γιατί η ακατάλληλη εσοχή ή η χρήση tabs μπορεί να οδηγήσει σε σφάλματα κατά την ανάλυση των αρχείων. Η YAML έχει επικρατήσει ως η βασική μορφή παραμετροποίησης σε πολλά εργαλεία και πλατφόρμες σύγχρονης τεχνολογίας, όπως το Kubernetes, το Ansible, το Docker Compose, και βεβαίως το Home Assistant. Στην τελευταία περίπτωση, χρησιμοποιείται εκτενώς για τη ρύθμιση των αυτοματισμών, των οντοτήτων και των ολοκληρώσεων (integrations), διότι επιτρέπει στον χρήστη να γράψει σύνθετους κανόνες με μεγάλη ευκρίνεια και έλεγχο. Σε αντίθεση με άλλες γλώσσες παραμετροποίησης, η YAML δεν είναι προγραμματιστική γλώσσα με λογική ή συνθήκες ροής εκτέλεσης, αλλά χρησιμεύει αυστηρά για την περιγραφή δεδομένων και παραμέτρων. Παρόλα αυτά, η ευελιξία της στην αναπαράσταση ιεραρχημένων δομών την καθιστά ιδανική για συστήματα που χρειάζονται αρχεία παραμετροποίησης πολλών επιπέδων.

Ένα από τα πιο κρίσιμα χαρακτηριστικά της YAML είναι ότι δεν είναι μια γλώσσα προγραμματισμού με κλασική λογική ροή, αλλά μια γλώσσα περιγραφής δεδομένων (data serialization language). Αυτό σημαίνει πως δεν περιλαμβάνει εντολές ελέγχου ροής, loops ή συναρτήσεις, αλλά λειτουργεί αποκλειστικά ως μέσο αναπαράστασης δομημένων δεδομένων με τρόπο που να μπορεί να διαβαστεί και να ερμηνευτεί εύκολα τόσο από τον άνθρωπο όσο και από το σύστημα. Ιδιαίτερη αναφορά αξίζει να γίνει και στον τρόπο που διαχειρίζεται τις πολυγραμμικές συμβολοσειρές. Οι συμβολοσειρές αυτές μπορούν να κρατήσουν νέα γραμμή ή να την αντικαταστήσουν με κενό, κάτι που ελέγχεται μέσω των ειδικών χαρακτήρων | και >. Αυτή η δυνατότητα είναι κρίσιμη όταν χρειάζεται να ορίσουμε παραμέτρους που περιλαμβάνουν οδηγίες, scripts ή μεγάλα μπλοκ κειμένου. Αξίζει επίσης να αναφερθεί ότι ενώ η YAML προσφέρει μεγάλη αναγνωσιμότητα, η ίδια της η ευαισθησία στην εσοχή μπορεί να αποτελέσει πηγή λαθών, ειδικά σε μεγάλες διαμορφώσεις (configuration files) με πολλές φωλιασμένες δομές. Ο έλεγχος συντακτικού μέσω εργαλείων όπως YAML linters είναι απαραίτητος για την αποφυγή σφαλμάτων.

Τέλος, μια σημαντική πρακτική στη χρήση της YAML στο πλαίσιο του Home Assistant είναι ο διαχωρισμός των ρυθμίσεων σε διαφορετικά αρχεία και η χρήση του !include ή !include_dir_merge_named, που επιτρέπει την οργάνωση του συστήματος σε πιο ευανάγνωστα και διαχειρίσιμα τμήματα. Αυτό επιτρέπει καλύτερη επεκτασιμότητα, ευκολότερη συντήρηση και πιο καθαρή οργάνωση των αυτοματισμών, των σεναρίων και των οντοτήτων. Αυτός ο τρόπος γραφής είναι από τα βασικά πλεονεκτήματα της YAML σε συστήματα όπως το Home Assistant. [20]

2.3: Passive Infrared Sensors (PIR)

Οι αισθητήρες παθητικής υπέρυθρης ακτινοβολίας, ευρέως γνωστοί ως Passive Infrared Sensors (PIR), αποτελούν την πιο διαδεδομένη τεχνολογία ανίχνευσης κίνησης και χρησιμοποιούνται ευρέως σε συστήματα συναγερμών, αυτοματισμούς κατοικιών, συστήματα φωτισμού ασφαλείας και πολλές άλλες εφαρμογές. Η λειτουργία τους βασίζεται στην ικανότητά τους να ανιχνεύουν μεταβολές της υπέρυθρης (IR) ακτινοβολίας που εκπέμπεται φυσικά από τα θερμόαιμα σώματα, όπως ο άνθρωπος ή τα ζώα. Σε αντίθεση με τους ενεργούς αισθητήρες υπέρυθρης ακτινοβολίας που εκπέμπουν δέσμες και ανιχνεύουν ανακλάσεις, οι PIR αισθητήρες δεν εκπέμπουν καθόλου ακτινοβολία, αλλά παρακολουθούν τις μεταβολές της θερμικής ενέργειας στον χώρο τους, λειτουργώντας έτσι με παθητικό τρόπο.

Εικόνα 2.4: Ενας αισθητήρας παθητικής υπέρυθρης ακτινοβολίας

Η βασική τους κατασκευή περιλαμβάνει πυροηλεκτρικά στοιχεία, τα οποία μετατρέπουν τη θερμική ακτινοβολία σε ηλεκτρικό φορτίο όταν μεταβάλλεται η υπέρυθρη ακτινοβολία που προσπίπτει σε αυτά. Συνήθως χρησιμοποιούνται δύο τέτοια στοιχεία διατεταγμένα με τρόπο ώστε να ανιχνεύουν διαφορές θερμοκρασίας σε διαδοχικές ζώνες. Πάνω από αυτά τοποθετείται ένας φακός Fresnel ή μια σειρά μικροφακών που συγκεντρώνουν την υπέρυθρη ακτινοβολία από το περιβάλλον και τη διαχωρίζουν σε πολλαπλές ζώνες ανίχνευσης. Όταν μια θερμή πηγή, όπως το ανθρώπινο σώμα, κινείται από τη μία ζώνη στην άλλη, δημιουργείται μια ασύμμετρη μεταβολή στη θερμική ακτινοβολία, την οποία τα πυροηλεκτρικά στοιχεία μεταφράζουν σε ηλεκτρικό σήμα. Το σήμα αυτό επεξεργάζεται από ένα ηλεκτρονικό κύκλωμα ενίσχυσης και σύγκρισης, το οποίο τελικά ενεργοποιεί ή όχι την έξοδο του αισθητήρα. Η τεχνολογία αυτή είναι ευαίσθητη κυρίως σε μετακινήσεις θερμών σωμάτων και όχι σε σταθερά θερμά αντικείμενα, καθώς απαιτείται διαφορά στο θερμικό φορτίο για να προκληθεί αντίδραση. Για τον λόγο αυτό, οι αισθητήρες PIR είναι κατάλληλοι για εσωτερικούς χώρους χωρίς έντονες θερμικές μεταβολές ή ρεύματα αέρα που μπορεί να δημιουργήσουν ψευδείς ενδείξεις. Ορισμένοι αισθητήρες διαθέτουν ρυθμιζόμενη ευαισθησία, καθυστέρηση ενεργοποίησης και δυνατότητα παραμετροποίησης για ελαχιστοποίηση των ψευδώς θετικών σημάτων. Επιπλέον, λόγω της χαμηλής τους κατανάλωσης ενέργειας, είναι ιδανικοί για χρήση σε συστήματα που λειτουργούν με μπαταρία ή σε απομακρυσμένες εγκαταστάσεις.

Η αξιοπιστία, η απλότητα, το χαμηλό κόστος και η μεγάλη διάρκεια ζωής τους καθιστούν τους αισθητήρες PIR εξαιρετικά χρήσιμους σε εφαρμογές όπως αυτόματα φώτα, συναγερμοί, ανιχνευτές παρουσίας, καθώς και σε σύγχρονα έξυπνα σπίτια Ένα ιδιαίτερο χαρακτηριστικό αυτών των αισθητήρων είναι ο χρόνος επαναφοράς ή "cooldown" μετά από κάθε ενεργοποίηση, δηλαδή ένα χρονικό διάστημα κατά το οποίο ο αισθητήρας αγνοεί εκ νέου κίνηση, ακόμη κι αν αυτή υπάρχει. Αυτό δεν αποτελεί ένδειξη αδυναμίας, αλλά ενσωματωμένη τεχνολογία εξοικονόμησης ενέργειας, ειδικά σε συσκευές που τροφοδοτούνται με μπαταρία. Ο χρόνος αυτός μπορεί να ρυθμίζεται, ανάλογα με την κατασκευή και τις ανάγκες του εκάστοτε σεναρίου χρήσης. [29]

2.4: Αισθητήρες Παρουσίας

Οι αισθητήρες παρουσίας που βασίζονται σε τεχνολογία κυμάτων 5Ghz (γνωστοί και ως mmWave presence sensors) αποτελούν μια προηγμένη και ταχέως αναπτυσσόμενη μορφή ανίχνευσης παρουσίας και κίνησης, προσφέροντας ακρίβεια, λεπτομέρεια και ευαισθησία που ξεπερνά τις δυνατότητες των παραδοσιακών παθητικών υπερύθρων αισθητήρων (PIR). Αντί να βασίζονται σε θερμικές μεταβολές, οι αισθητήρες αυτοί χρησιμοποιούν μικροκυματική τεχνολογία, εκπέμποντας συνεχώς σήματα υψηλής συχνότητας στην περιοχή των 5.8GHz (ή και υψηλότερα, έως τα 60 GHz σε ορισμένες εκδόσεις) και αναλύοντας τις ανακλάσεις που επιστρέφουν από το περιβάλλον.

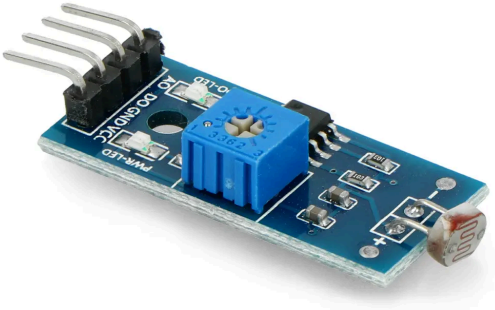
Σχήμα 2.5: Ενας αισθητήρας παρουσίας [21.a]

Η βασική αρχή λειτουργίας τους στηρίζεται σε τεχνικές ραντάρ τύπου Frequency-Modulated Continuous Wave (FMCW), οι οποίες επιτρέπουν την αναγνώριση ακόμα και της παραμικρής κίνησης – όπως η αναπνοή ενός καθιστού ανθρώπου – σε πραγματικό χρόνο. Μέσω της συνεχούς εκπομπής κυμάτων και της ακριβούς ανάλυσης της φάσης και της συχνότητας των επιστρεφόμενων σημάτων, ο αισθητήρας μπορεί να υπολογίσει με εντυπωσιακή ακρίβεια την απόσταση, την ταχύτητα και την κατεύθυνση ενός αντικειμένου, καθιστώντας τον ικανό να διακρίνει μεταξύ κίνησης, παρουσίας και αδράνειας. Σε αντίθεση με τους PIR αισθητήρες που περιορίζονται στην ανίχνευση κίνησης, οι αισθητήρες mmWave είναι σε θέση να ανιχνεύσουν την απλή παρουσία ενός ατόμου, ακόμα κι αν αυτό παραμένει ακίνητο, γεγονός που τους καθιστά ιδιαίτερα χρήσιμους σε εφαρμογές όπως η αυτόματη ενεργοποίηση φωτισμού, η εξαεριστική ρύθμιση δωματίου, η θερμική διαχείριση ή και η βελτιστοποίηση της ενεργειακής κατανάλωσης σε έξυπνα κτίρια. Ένα ουσιώδες χαρακτηριστικό αυτής της τεχνολογίας είναι η απαίτηση για συνεχή και σταθερή παροχή ρεύματος. Επειδή οι αισθητήρες mmWave βασίζονται σε ενεργή εκπομπή και λήψη ραδιοκυμάτων, η κατανάλωση ενέργειας είναι σημαντικά υψηλότερη από αυτή των παθητικών αισθητήρων, γεγονός που τους καθιστά ακατάλληλους για χρήση με μπαταρίες. Συνεπώς, είναι απαραίτητο να είναι συνδεδεμένοι μόνιμα στο ηλεκτρικό δίκτυο, προκειμένου να διατηρούν τη σταθερότητα και την ακρίβειά τους, αλλά και να υποστηρίζουν την απαραίτητη επεξεργαστική ισχύ που απαιτεί η αναλυτική επεξεργασία του σήματος.

Πέραν της υψηλής ευαισθησίας, οι αισθητήρες mmWave προσφέρουν και άλλα σημαντικά πλεονεκτήματα: λειτουργούν ανεξαρτήτως συνθηκών φωτισμού ή θερμοκρασίας, μπορούν να παρακολουθήσουν πολλαπλά αντικείμενα στον ίδιο χώρο και δεν επηρεάζονται από εμπόδια όπως κουρτίνες ή λεπτά δομικά στοιχεία, δεδομένου ότι τα ραδιοκύματα είναι ικανά να τα διαπερνούν. Ωστόσο, σε αντίθεση με αισθητήρες υπερύθρων ή υπερήχων, η ακρίβεια και η δυνατότητα λεπτομερούς ανάλυσης των αισθητήρων 5.8GHz τους καθιστούν πιο πολύπλοκους στη ρύθμιση και ελαφρώς πιο δαπανηρούς.[29]

2.5: Αισθητήρες Φωτεινότητας

Οι αισθητήρες φωτεινότητας, γνωστοί και ως αισθητήρες lux ή luminance sensors, αποτελούν βασικά ηλεκτρονικά εξαρτήματα στον χώρο των εφαρμογών αυτοματισμού και ειδικότερα στα έξυπνα σπίτια, με σκοπό την ακριβή μέτρηση της έντασης του φωτός στο περιβάλλον. Η μονάδα μέτρησης που χρησιμοποιούν είναι το lux, το οποίο εκφράζει τη φωτεινή ροή (lumen) ανά τετραγωνικό μέτρο και αντιστοιχεί στο πόσο φως προσπίπτει σε μία επιφάνεια, σε αντίθεση με την έννοια της φωτεινής πηγής. Οι αισθητήρες αυτοί βασίζονται κατά κύριο λόγο στη λειτουργία φωτοδιόδων ή φωτοαντισταστών, οι οποίοι παρουσιάζουν αλλαγή στην ηλεκτρική τους αντίσταση ή στην παραγόμενη τάση ανάλογα με την ποσότητα του προσπίπτοντος φωτός. Οι φωτοδίοδοι είναι συχνότερα χρησιμοποιούμενες σε σύγχρονους ψηφιακούς αισθητήρες, καθώς προσφέρουν μεγαλύτερη ακρίβεια, ταχύτερη απόκριση και καλύτερη ευαισθησία σε μεταβολές του φωτισμού.



Εικόνα 2.6: Ένας αισθητήρας φωτεινότητας [22.a]

Στην πράξη, οι αισθητήρες lux εντοπίζουν την παρουσία και την ένταση του φυσικού ή τεχνητού φωτισμού σε έναν χώρο και μετατρέπουν αυτές τις μετρήσεις σε αναγνώσιμες ψηφιακές τιμές, οι οποίες μπορούν να αξιοποιηθούν από ένα σύστημα αυτοματισμού, όπως το Home Assistant, για την εκτέλεση προγραμματισμένων ενεργειών. Εφαρμογές τέτοιες περιλαμβάνουν την αυτόματη ενεργοποίηση ή απενεργοποίηση του φωτισμού βάσει των πραγματικών επιπέδων φωτεινότητας, την προσαρμογή της φωτεινότητας λαμπτήρων LED σε εσωτερικούς χώρους, ή ακόμα και την ενεργοποίηση συστημάτων σκίασης σε συνδυασμό με αισθητήρες θερμοκρασίας. Οι αισθητήρες αυτοί μπορούν να λειτουργούν είτε αυτόνομα, είτε ενσωματωμένοι σε σύνθετες συσκευές όπως έξυπνα φωτιστικά ή πολυαισθητήρες που περιλαμβάνουν, επιπλέον, αισθητήρες θερμοκρασίας, υγρασίας ή κίνησης. Η συνδεσιμότητα τους με το σύστημα αυτοματισμού εξαρτάται από το εκάστοτε πρωτόκολλο επικοινωνίας που υποστηρίζουν, όπως Zigbee, Z-Wave, Wi-Fi ή Bluetooth Low Energy. Ιδιαίτερα τα Zigbee lux sensors, όπως ο Philips Hue Motion Sensor ή οι Aqara Light Sensors, είναι δημοφιλείς λόγω της αξιοπιστίας και της χαμηλής κατανάλωσης ενέργειας. Εξαιρετικής σημασίας για την ορθή λειτουργία ενός αισθητήρα φωτεινότητας είναι η τοποθέτησή του στο σωστό σημείο του δωματίου, ώστε να λαμβάνει ακριβώς το φως που αφορά τη χρήση του χώρου και όχι, για παράδειγμα, αντανάκλαση από τζάμια ή φώτα που αλλοιώνουν την πραγματική φωτεινή κατάσταση. Οι τιμές που παρέχουν μπορούν να κυμαίνονται από πολύ χαμηλά επίπεδα (κάτω του 1 lux, όπως σε σκοτεινό δωμάτιο) έως πολύ υψηλά (άνω των 100.000 lux, όπως σε άμεσο ηλιακό φως), και η ανάλυση των δεδομένων αυτών είναι ιδιαίτερα κρίσιμη για τη διαμόρφωση αποδοτικών σεναρίων αυτοματισμού. [29]

2.7: Αισθητήρες Θυρών

Οι αισθητήρες θυρών, γνωστοί και ως door sensors ή contact sensors, αποτελούν ένα από τα πιο διαδεδομένα στοιχεία στα συστήματα ασφαλείας και αυτοματισμού έξυπνων σπιτιών. Η βασική τους λειτουργία είναι να ανιχνεύουν την κατάσταση μιας πόρτας ή παραθύρου, δηλαδή εάν είναι ανοιχτή ή κλειστή, και να ενεργοποιούν σενάρια αυτοματισμού ή ειδοποιήσεις ασφαλείας. Πολλοί από αυτούς τους αισθητήρες βασίζονται στο φυσικό φαινόμενο Hall, γνωστό ως Hall Effect, για την ανίχνευση της σχετικής θέσης δύο επιμέρους εξαρτημάτων.

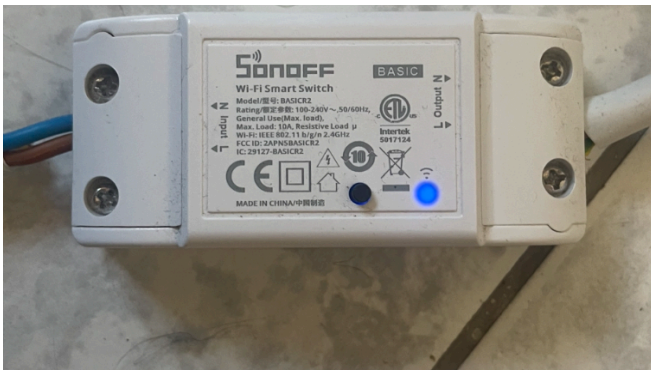
Εικόνα 2.7: Ένας αισθητήρας θύρας

Το Hall Effect ανακαλύφθηκε το 1879 από τον Edwin Hall και περιγράφει το φαινόμενο κατά το οποίο σε έναν αγωγό ή ημιαγωγό, όταν διαρρέεται από ρεύμα και ταυτόχρονα υποβάλλεται σε κάθετο μαγνητικό πεδίο, αναπτύσσεται μια τάση κάθετη τόσο στη ροή του ρεύματος όσο και στο μαγνητικό πεδίο. Αυτή η παραγόμενη τάση ονομάζεται τάση Hall και μπορεί να μετρηθεί για να εξαχθούν πληροφορίες σχετικά με την παρουσία ή την ένταση ενός μαγνητικού πεδίου. Σε μια τυπική εφαρμογή αισθητήρα πόρτας που χρησιμοποιεί Hall Effect, υπάρχουν δύο κύρια εξαρτήματα: ένας μαγνήτης και ένας αισθητήρας Hall. Ο αισθητήρας τοποθετείται συνήθως στο πλαίσιο της πόρτας ή του παραθύρου, ενώ ο μικρός μαγνήτης τοποθετείται στην κινούμενη πλευρά, δηλαδή στο φύλλο της πόρτας ή του παραθύρου. Όταν η πόρτα είναι κλειστή, ο μαγνήτης βρίσκεται σε εγγύτητα με τον αισθητήρα και το μαγνητικό πεδίο που ανιχνεύεται προκαλεί συγκεκριμένη αντίδραση στον αισθητήρα Hall, συνήθως με τη μορφή τάσης ή λογικής κατάστασης. Όταν η πόρτα ανοίξει, ο μαγνήτης απομακρύνεται, η μαγνητική επιρροή μειώνεται ή παύει, και το κύκλωμα αλλάζει κατάσταση, ενημερώνοντας το σύστημα ότι υπάρχει μεταβολή. Η χρήση του Hall Effect σε σχέση με άλλες μεθόδους, όπως τα παραδοσιακά reed switches (μαγνητικοί διακόπτες επαφής), προσφέρει ορισμένα πλεονεκτήματα. Οι αισθητήρες Hall είναι πιο ανθεκτικοί σε μηχανικές φθορές, δεν περιέχουν κινητά μέρη, και λειτουργούν με μεγαλύτερη ακρίβεια και αξιοπιστία σε περιβάλλοντα με κραδασμούς ή σκόνη. Επίσης, μπορούν να τοποθετηθούν με μεγαλύτερη ευελιξία και να προσφέρουν ψηφιακή έξοδο, κάτι που διευκολύνει την άμεση διασύνδεσή τους με μικροελεγκτές ή έξυπνα hubs.
Οι door sensors που βασίζονται σε Hall Effect χρησιμοποιούνται εκτενώς σε έξυπνα σπίτια για αυτοματισμούς όπως η ενεργοποίηση φωτισμού όταν ανοίγει μια πόρτα, η απενεργοποίηση του θερμοστάτη όταν ανιχνευθεί ότι μια μπαλκονόπορτα παραμένει ανοιχτή, ή για λόγους ασφαλείας, όπως η αποστολή ειδοποιήσεων σε περίπτωση παραβίασης. Μπορούν να λειτουργούν είτε μέσω ασύρματης τεχνολογίας, όπως Zigbee, Z-Wave ή Wi-Fi, είτε με καλωδιακή σύνδεση σε συστήματα συναγερμού. Οι περισσότερες συσκευές αυτού του είδους λειτουργούν με μικρή κατανάλωση

ρεύματος και μπορούν να τροφοδοτούνται με μπαταρία για πολλούς μήνες ή ακόμα και χρόνια. Ωστόσο, για συστήματα που απαιτούν άμεση και συνεχή επικοινωνία με τον controller, όπως επαγγελματικά ή βιομηχανικά, είναι συνήθης η μόνιμη τροφοδοσία.[29]

2.8:Ενδιάμεσοι Διακόπτες

Τα ενδιάμεσα smart switches αποτελούν μία από τις πιο ευέλικτες λύσεις στον χώρο του οικιακού αυτοματισμού, προσφέροντας τη δυνατότητα ελέγχου της ηλεκτρικής παροχής σε υπάρχουσες συσκευές χωρίς την ανάγκη αντικατάστασης όλης της ηλεκτρικής υποδομής. Πρόκειται για μικρές ηλεκτρονικές μονάδες που μπορούν να εγκατασταθούν είτε πίσω από έναν παραδοσιακό τοίχινο διακόπτη, είτε απευθείας σε μια πρίζα, είτε ακόμη και εν σειρά με πολύπριζα ή ηλεκτρικές γραμμές. Ο βασικός τους ρόλος είναι να λειτουργούν ως ηλεκτρονικά ρελέ, επιτρέποντας ή διακόπτοντας την παροχή ρεύματος προς τη συνδεδεμένη συσκευή, μέσω απομακρυσμένης εντολής ή αυτοματισμού.



Εικόνα 2.8: Ένας ενδιάμεσος διακόπτης

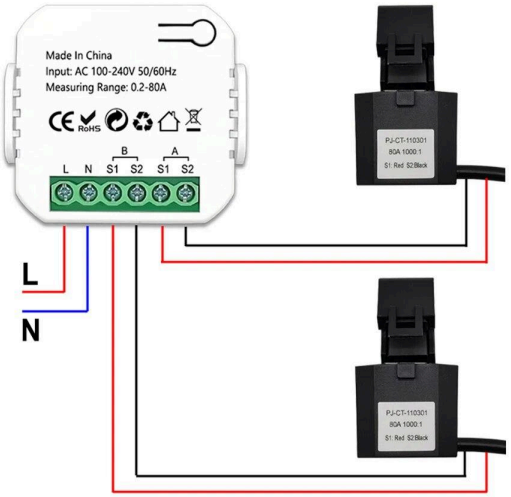
Οι εν λόγω συσκευές υποστηρίζουν συνήθως δύο βασικά πρότυπα επικοινωνίας: Wi-Fi και Zigbee. Η επιλογή της τεχνολογίας καθορίζεται τόσο από την αρχιτεκτονική του έξυπνου σπιτιού όσο και από τις ανάγκες σταθερότητας, ταχύτητας και ενεργειακής αποδοτικότητας. Οι Wi-Fi εκδόσεις είναι πιο ανεξάρτητες από την ύπαρξη κόμβου (hub) και συνδέονται απευθείας στο οικιακό δίκτυο, ενώ οι Zigbee εκδόσεις απαιτούν συνήθως έναν Zigbee coordinator για τη δικτύωσή τους, προσφέροντας όμως καλύτερη σταθερότητα, mesh λειτουργία και μειωμένη κατανάλωση ενέργειας. Ένα σημαντικό τεχνικό πλεονέκτημα ορισμένων μοντέλων smart switches είναι η δυνατότητα λειτουργίας τους χωρίς την παρουσία ουδέτερου αγωγού (neutral wire), κάτι που αποτελεί κρίσιμο παράγοντα σε παλαιότερες ηλεκτρικές εγκαταστάσεις, όπου το ουδέτερο σύρμα δεν είναι διαθέσιμο στον τοίχινο διακόπτη. Η λειτουργία αυτή υλοποιείται μέσω ειδικών κυκλωμάτων που αντλούν ελάχιστο ρεύμα από το κύκλωμα του φορτίου, επιτρέποντας τη διατήρηση της ηλεκτρονικής μονάδας σε λειτουργία χωρίς να απαιτείται πλήρης κύκλωμα τροφοδοσίας. Ωστόσο, η σταθερότητα αυτής της μεθόδου εξαρτάται από τη φύση του φορτίου (λαμπτήρες LED, πυρακτώσεως, ηλεκτρονικές συσκευές κ.λπ.) και ορισμένες φορές συνοδεύεται από την ανάγκη τοποθέτησης πυκνωτή στο κύκλωμα για την αποφυγή τρεμοπαίγματος ή λανθασμένης λειτουργίας. Τα smart switches συχνά υποστηρίζουν πλήρη ενσωμάτωση με πλατφόρμες αυτοματισμού όπως το Home Assistant, Google Home, Amazon Alexa και Apple HomeKit, προσφέροντας δυνατότητες χρονοπρογραμματισμού, συνδυασμών trigger-action (π.χ. “αν ανιχνευτεί κίνηση, άνοιξε το φως”) και εξ αποστάσεως ελέγχου μέσω εφαρμογών ή φωνητικών εντολών. Επιπλέον, αρκετά από αυτά προσφέρουν δυνατότητες μέτρησης κατανάλωσης ενέργειας (power metering), παρέχοντας στον χρήστη πληροφορίες σε πραγματικό χρόνο για τη χρήση της κάθε συσκευής.

Τα ενδιάμεσα smart switches, εκτός από τον βασικό τους ρόλο στην απομακρυσμένη ενεργοποίηση και απενεργοποίηση κυκλωμάτων, ενσωματώνουν συχνά λειτουργίες που ξεπερνούν τη χρήση ενός απλού ηλεκτρονικού ρελέ. Μία από τις πιο σημαντικές δυνατότητες τους είναι η υποστήριξη σεναρίων αυτοματισμού με βάση αισθητήρες ή άλλες συσκευές του συστήματος. Για παράδειγμα, ένα smart switch μπορεί να ενεργοποιηθεί αυτόματα όταν ένας αισθητήρας κίνησης εντοπίσει παρουσία ή όταν το επίπεδο φωτεινότητας σε έναν χώρο πέσει κάτω από ένα ορισμένο κατώφλι. Αυτές οι δυνατότητες υλοποιούνται μέσω κανόνων τύπου “if-this-then-that” (IFTTT) είτε μέσα από την εγγενή εφαρμογή της συσκευής είτε μέσω προχωρημένων πλατφορμών όπως το Home Assistant. Επιπλέον, τα περισσότερα smart switches υποστηρίζουν over-the-air (OTA) αναβαθμίσεις λογισμικού, κάτι που εξασφαλίζει τη μελλοντική επεκτασιμότητα, την επίλυση σφαλμάτων και την ενσωμάτωση νέων χαρακτηριστικών. Η ικανότητα αυτών των συσκευών να προσαρμόζονται σε διαφορετικά περιβάλλοντα – είτε πρόκειται για ρευματοδότες, είτε για φωτιστικά σώματα, είτε για κινητήρες ρολών – τις καθιστά εξαιρετικά ευέλικτες και οικονομικά συμφέρουσες, καθώς δεν απαιτούν ειδική υποδομή για κάθε διαφορετική εφαρμογή.

Ένα ακόμη σημαντικό τεχνικό χαρακτηριστικό αφορά το ποσοστό αντίδρασης και τον χρόνο καθυστέρησης (latency) στις εντολές. Σε περιβάλλοντα με Wi-Fi, το latency εξαρτάται από τη σταθερότητα του ασύρματου δικτύου και ενδέχεται να επηρεαστεί από συμφόρηση ή παρεμβολές. Αντιθέτως, τα Zigbee-based switches προσφέρουν γενικά πιο αξιόπιστη και χαμηλής καθυστέρησης απόκριση, ιδίως όταν χρησιμοποιούνται σε πλέγμα (mesh topology), όπου τα μηνύματα μπορούν να δρομολογηθούν εναλλακτικά μέσω ενδιάμεσων συσκευών. Σε τέτοια δίκτυα, όπως έχει ήδη αναφερθεί, μόνο οι συσκευές που είναι συνεχώς τροφοδοτούμενες (όπως τα smart switches) μπορούν να λειτουργούν ως δρομολογητές (routers), ενισχύοντας τη συνολική εμβέλεια και αξιοπιστία του δικτύου.
Η ασφάλεια των smart switches δεν είναι αμελητέα. Πολλά μοντέλα χρησιμοποιούν κρυπτογράφηση στις ασύρματες επικοινωνίες τους (π.χ. AES-128), ιδίως τα Zigbee μοντέλα, ενώ τα Wi-Fi switches συχνά βασίζονται στην ασφάλεια του οικιακού δικτύου για την προστασία των δεδομένων. Παρ’ όλα αυτά, η ύπαρξη ενημερωμένου firmware και η αποφυγή χρήσης cloud-only λύσεων χαμηλής αξιοπιστίας αποτελεί σημαντικό παράγοντα για τη διατήρηση της ασφάλειας και της ιδιωτικότητας. [29]

2.9: Μετρητές Τάσης, Κατανάλωσης και Ρεύματος

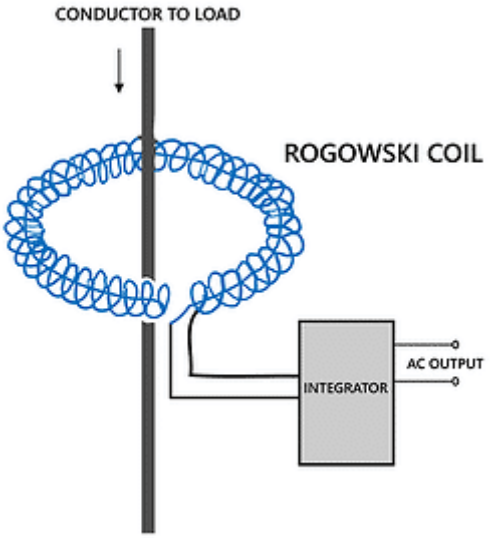
Οι μετρητές ρεύματος που βασίζονται σε πηνίο Rogowski αποτελούν μία ιδιαίτερα αξιόπιστη και ασφαλή λύση για την παρακολούθηση της ηλεκτρικής κατανάλωσης σε ένα σύστημα, είτε σε οικιακό είτε σε βιομηχανικό περιβάλλον. Το πηνίο Rogowski είναι ένας τύπος αισθητήρα ρεύματος χωρίς σιδηρομαγνητικό πυρήνα, συνήθως κατασκευασμένος ως εύκαμπτο σωληνοειδές πηνίο που τοποθετείται γύρω από έναν αγωγό μεταφοράς ρεύματος. Η βασική του λειτουργία στηρίζεται στον νόμο του Faraday, καθώς μετρά την τάση που επάγεται στο πηνίο λόγω της μεταβολής του μαγνητικού πεδίου από το εναλλασσόμενο ρεύμα του αγωγού. Στη συνέχεια, η τάση αυτή ολοκληρώνεται χρονικά μέσω ενός κυκλώματος ολοκλήρωσης για να εξαχθεί η τιμή του ρεύματος.Ένα σημαντικό πλεονέκτημα των Rogowski coils είναι ότι δεν απαιτούν άμεση επαφή με τον αγωγό ρεύματος, γεγονός που αυξάνει σημαντικά την ασφάλεια κατά την εγκατάσταση και λειτουργία. Επίσης, λόγω της απουσίας σιδηρομαγνητικού πυρήνα, εμφανίζουν εξαιρετικά γραμμική συμπεριφορά ακόμα και σε υψηλά ρεύματα, ενώ δεν κορεσμένα όπως οι συμβατικοί μετασχηματιστές ρεύματος (CTs). Αυτό τους καθιστά ιδανικούς για καταστάσεις μέτρησης ρεύματος με μεγάλες διακυμάνσεις ή παρουσία αρμονικών. Οι αισθητήρες τύπου Rogowski χρησιμοποιούνται ευρέως σε συστήματα παρακολούθησης κατανάλωσης ηλεκτρικής ενέργειας σε real time, σε smart metering εφαρμογές, σε μετρητές συνδεδεμένους με Home Assistant ή άλλες πλατφόρμες αυτοματισμού, καθώς και για την παρακολούθηση της ποιότητας ισχύος. Το γεγονός ότι είναι εύκαμπτοι και ελαφριοί διευκολύνει την εγκατάστασή τους ακόμα και σε πίνακες όπου δεν υπάρχει πολύς χώρος. Ωστόσο, μειονέκτημά τους αποτελεί το γεγονός ότι απαιτούν επιπλέον κύκλωμα ολοκλήρωσης (integration circuit) για να δώσουν άμεση ένδειξη ρεύματος, καθώς και ότι δεν είναι κατάλληλοι για μέτρηση συνεχούς ρεύματος (DC), αφού δεν παράγεται μεταβαλλόμενο μαγνητικό πεδίο σε αυτή την περίπτωση.



Εικόνα 2.9: Ένας μετρητής ρεύματος και τα πηνία Rogowski [23.α]

Το πηνίο Rogowski είναι ένας τύπος αισθητήρα ρεύματος που λειτουργεί με βάση την επαγωγική αρχή του Νόμου του Faraday, αλλά διαφέρει σημαντικά από τους κλασικούς μετασχηματιστές ρεύματος (Current Transformers - CTs) στον τρόπο σχεδίασης και λειτουργίας. Η βασική του αρχή στηρίζεται στην επαγωγή τάσης σε ένα αερόπυκνο πηνίο (χωρίς σιδηρομαγνητικό πυρήνα) το οποίο τοποθετείται γύρω από έναν αγωγό που διαρρέεται από εναλλασσόμενο ρεύμα. Η αλλαγή του μαγνητικού πεδίου που προκαλείται από το ρεύμα στον αγωγό επάγει μία ηλεκτρική τάση στο πηνίο,

η οποία είναι ανάλογη με τον ρυθμό μεταβολής του ρεύματος (di/dt). Αυτή η τάση στη συνέχεια περνά από ένα κύκλωμα ολοκλήρωσης ώστε να μετατραπεί σε σήμα που αντιπροσωπεύει τη στιγμιαία τιμή του ρεύματος. Αυτό που κάνει το πηνίο Rogowski ιδιαίτερο είναι η ευελιξία του είναι ότι πρόκειται για ένα λεπτό, εύκαμπτο καλώδιο σε μορφή βρόχου, το οποίο μπορεί να τυλιχτεί γύρω από τον αγωγό χωρίς να απαιτείται αποσύνδεση ή διακοπή του κυκλώματος. Αυτό το χαρακτηριστικό είναι εξαιρετικά χρήσιμο σε περιπτώσεις όπου απαιτείται να μετρηθεί το ρεύμα σε εγκαταστάσεις υπό τάση, όπως σε βιομηχανικούς πίνακες ή σε πυκνοκατοικημένα κουτιά ασφαλειών. Επιπλέον, η απουσία πυρήνα σημαίνει ότι δεν υπάρχει κορεσμός, ένα φαινόμενο που περιορίζει την ακρίβεια των μετασχηματιστών ρεύματος σε υψηλά ρεύματα ή σε καταστάσεις με πολλές αρμονικές.



Σχήμα 2.10: Διάγραμμα λειτουργίας πηνίου [24.α]

Ένα από τα πιο σημαντικά χαρακτηριστικά του πηνίου Rogowski είναι η πολύ καλή απόκριση του σε ταχείες μεταβολές του ρεύματος, καθώς και η ευαισθησία του στην ανίχνευση αρμονικών και παραμορφωμένων κυματομορφών. Αυτό το καθιστά κατάλληλο για προηγμένες εφαρμογές παρακολούθησης ποιότητας ισχύος και καταγραφής συμβάντων (π.χ. αιχμές τάσης ή μεταβατικά φαινόμενα). Επιπλέον, λόγω της ανοιχτής αρχιτεκτονικής του, έχει πολύ μικρή χωρητική και επαγωγική σύνδεση με το περιβάλλον, γεγονός που το καθιστά πιο ανθεκτικό σε ηλεκτρομαγνητικές παρεμβολές σε σχέση με άλλες τεχνολογίες. Ωστόσο, επειδή η τάση που παράγεται στο πηνίο είναι ανάλογη του di/dt και όχι του ίδιου του ρεύματος, απαιτείται πάντα ένα ακριβές και καλά σχεδιασμένο κύκλωμα ολοκλήρωσης για την απόδοση αξιόπιστων μετρήσεων. Αυτό προσθέτει μία πολυπλοκότητα στο συνολικό κύκλωμα μέτρησης, αν και πλέον υπάρχουν εμπορικά διαθέσιμες λύσεις (modules) που ενσωματώνουν τα πάντα, καθιστώντας την εγκατάσταση πολύ απλή για τον τελικό χρήστη.

Το πηνίο Rogowski δεν είναι κατάλληλο για μέτρηση συνεχούς ρεύματος (DC), καθώς η συνεχής τάση δεν δημιουργεί μεταβαλλόμενο μαγνητικό πεδίο και άρα δεν επάγεται τάση στο πηνίο. Ωστόσο, για εναλλασσόμενες εφαρμογές (AC), ειδικά εκεί όπου υπάρχουν μεγάλες εντάσεις ρεύματος ή δύσκολες συνθήκες εγκατάστασης, αποτελεί μία ιδανική λύση, που κερδίζει συνεχώς έδαφος στην αγορά των έξυπνων μετρητών ενέργειας, των συστημάτων αυτοματισμού, και της βιομηχανικής παρακολούθησης.[29]

2.10: Φωνητική εντολή μέσω Google Home

Η δυνατότητα φωνητικού ελέγχου αποτελεί τον πυρήνα της εμπειρίας χρήσης του Google Home, καθιστώντας τον φυσικό διάλογο το βασικό μέσο αλληλεπίδρασης ανάμεσα στον χρήστη και το έξυπνο οικιακό οικοσύστημα. Ο μηχανισμός αυτός βασίζεται στη λειτουργία του Google Assistant, ο οποίος είναι ενσωματωμένος στα φυσικά προϊόντα της Google, όπως τα Google Nest Audio, Nest Mini, Nest Hub και παλαιότερα Google Home, και χρησιμοποιεί προηγμένες τεχνικές επεξεργασίας φυσικής γλώσσας (NLP) και φωνητικής αναγνώρισης (ASR – Automatic Speech Recognition) για την κατανόηση και εκτέλεση εντολών.

Το hardware αυτών των συσκευών διαθέτει πολλαπλά μικρόφωνα υψηλής ευαισθησίας τα οποία είναι διατεταγμένα κυκλικά, ώστε να μπορούν να εντοπίσουν την κατεύθυνση από την οποία προέρχεται ο ήχος. Η τεχνική αυτή ονομάζεται beamforming και επιτρέπει στο σύστημα να απομονώσει τη φωνή του χρήστη ακόμη και σε θορυβώδη περιβάλλοντα ή όταν η συσκευή αναπαράγει μουσική. Τα μικρόφωνα παραμένουν συνεχώς ενεργά, σε μια κατάσταση χαμηλής κατανάλωσης, ακούγοντας αποκλειστικά για τη φράση αφύπνισης (“Hey Google” ή “OK Google”), η οποία όταν εντοπιστεί, ενεργοποιεί τη συσκευή για να ξεκινήσει την πλήρη ηχογράφηση και ανάλυση της εντολής. Αξιοσημείωτο είναι ότι οι φωνητικές εντολές δεν επεξεργάζονται εξ ολοκλήρου τοπικά. Αντιθέτως, αποστέλλονται στους servers της Google στο cloud, όπου εφαρμόζονται εξελιγμένα μοντέλα μηχανικής μάθησης και τεχνητής νοημοσύνης για την κατανόηση του φυσικού λόγου και την εξαγωγή προθέσεων (intents). Αυτό επιτρέπει στον Google Assistant να εκτελεί σύνθετες εντολές, να κατανοεί συμφραζόμενα και να μαθαίνει από τις αλληλεπιδράσεις για την παροχή πιο ακριβών και προσωποποιημένων απαντήσεων. Η φυσική διάταξη των συσκευών Google Home περιλαμβάνει επιπλέον κουμπιά απενεργοποίησης του μικροφώνου (mute button), για να προσφέρει έλεγχο στον χρήστη σχετικά με την ιδιωτικότητα. Σε αυτή την περίπτωση, τα μικρόφωνα απενεργοποιούνται πλήρως σε υλικό (hardware level) και δεν καταγράφεται κανένα ηχητικό σήμα, γεγονός που ενισχύει το αίσθημα ασφάλειας στον τελικό χρήστη.

Η αναγνώριση φωνής είναι επίσης εξατομικευμένη. Η Google παρέχει την τεχνολογία Voice Match, η οποία μπορεί να διακρίνει ανάμεσα σε διαφορετικές φωνές, επιτρέποντας σε κάθε μέλος του σπιτιού να έχει πρόσβαση σε προσωποποιημένα αποτελέσματα, όπως ημερολόγια, υπενθυμίσεις, λίστες αγορών ή προτιμήσεις πολυμέσων. Η φωνητική αυτή διαφοροποίηση πραγματοποιείται μέσω μιας διαδικασίας εκμάθησης της φωνής κατά την πρώτη ρύθμιση του προφίλ και εξελίσσεται με την πάροδο του χρόνου. Η φυσική έξοδος της συσκευής –είτε μέσα από ενσωματωμένα ηχεία, είτε με σύνδεση σε εξωτερικά– επιτρέπει την άμεση αναπαραγωγή απαντήσεων, μουσικής, ηχητικών ειδοποιήσεων και την υποστήριξη ολόκληρων smart home σεναρίων, όπως φωνητικές εντολές για άνοιγμα φώτων, κλείσιμο θυρών ή ενεργοποίηση του θερμοστάτη.[31]

2.11: Φωνητική εντολή μέσω Amazon Alexa

Η τεχνολογία φωνητικού ελέγχου μέσω της Alexa, της φωνητικής βοηθού της Amazon, αποτελεί έναν από τους βασικότερους πυλώνες της πλατφόρμας Amazon Echo και γενικότερα του έξυπνου οικοσυστήματος της εταιρείας. Η Alexa λανσαρίστηκε το 2014, ενσωματωμένη στο πρώτο Echo smart speaker, και έκτοτε εξελίχθηκε σε μία από τις πιο διαδεδομένες πλατφόρμες φωνητικής αλληλεπίδρασης, αξιοποιώντας τεχνολογίες αιχμής στον τομέα της φυσικής γλώσσας και της τεχνητής νοημοσύνης.

Το hardware των συσκευών Echo περιλαμβάνει πολλαπλά μικρόφωνα διατεταγμένα κυκλικά για περιμετρική κάλυψη του χώρου, υλοποιώντας τεχνολογία beamforming ώστε να εντοπίζουν τη φωνή του χρήστη από διαφορετικές γωνίες. Το σύστημα λειτουργεί σε κατάσταση παθητικής ακρόασης, αναζητώντας την φράση αφύπνισης (“Alexa”) η οποία, όταν ανιχνευθεί, ενεργοποιεί τη συσκευή για να ξεκινήσει την καταγραφή της εντολής. Η αρχική φάση της επεξεργασίας γίνεται τοπικά, ωστόσο η πλήρης ανάλυση και κατανόηση του περιεχομένου αποστέλλεται στο cloud της Amazon, όπου υπερσύγχρονα νευρωνικά δίκτυα αναλύουν τη φωνή, εξάγουν νόημα (intent recognition) και επιστρέφουν την κατάλληλη ενέργεια. Η Alexa υποστηρίζει ένα πλούσιο σύστημα δεξιοτήτων (skills), που επιτρέπουν την επέκταση της λειτουργικότητάς της με εφαρμογές τρίτων, οι οποίες μπορούν να ενεργοποιηθούν μέσω φωνής. Μέσα από αυτή την ευελιξία, η φωνητική βοηθός μπορεί να λειτουργεί ως κόμβος ελέγχου για έξυπνες συσκευές, να απαντά σε ερωτήσεις, να διαχειρίζεται ημερολόγια, λίστες, μουσική και πλήθος άλλων λειτουργιών, καθιστώντας την ένα πλήρως ενοποιημένο μέσο διαχείρισης του έξυπνου σπιτιού.
Η ασφάλεια και το απόρρητο των φωνητικών δεδομένων είναι επίσης σημαντικός τομέας στην αρχιτεκτονική της Alexa. Οι ηχογραφήσεις αποθηκεύονται στους servers της Amazon και είναι προσβάσιμες μέσω του λογαριασμού του χρήστη, ο οποίος έχει την επιλογή να τις διαγράψει ανά πάσα στιγμή. Οι συσκευές Echo διαθέτουν και φυσικό διακόπτη απενεργοποίησης των μικροφώνων (mute button), το οποίο απενεργοποιεί εντελώς την ακρόαση σε επίπεδο υλικού (hardware-level). Ένα ιδιαίτερα προηγμένο χαρακτηριστικό του φωνητικού συστήματος της Alexa είναι το voice profiling. Μέσω αυτής της τεχνολογίας, οι συσκευές μπορούν να διακρίνουν ανάμεσα σε διαφορετικούς χρήστες του ίδιου νοικοκυριού, επιτρέποντας προσωποποιημένες απαντήσεις, όπως για παράδειγμα προβολή ατομικών ημερολογίων, υπενθυμίσεων, ή προτιμήσεων μουσικής. Η εκπαίδευση του προφίλ γίνεται με απλή διαδικασία και εξελίσσεται δυναμικά όσο χρησιμοποιείται η συσκευή.

Η διάδραση με την Alexa μπορεί να είναι είτε φωνητική είτε μέσω της εφαρμογής Alexa App, προσφέροντας ένα ευέλικτο περιβάλλον διαχείρισης συσκευών και αυτοματισμών. Επιπλέον, οι συσκευές Echo υποστηρίζουν επικοινωνία μεταξύ τους (drop-in), broadcast λειτουργίες και integration με πρωτόκολλα όπως Zigbee (σε μοντέλα Echo με ενσωματωμένο hub), ενισχύοντας ακόμη περισσότερο τον ρόλο τους ως επίκεντρο του έξυπνου σπιτιού. [30]

2.12: DNS Server

Το DNS, ή αλλιώς Domain Name System, είναι ένα από τα θεμελιώδη συστατικά του σύγχρονου διαδικτύου και λειτουργεί ως ο "τηλεφωνικός κατάλογος" του. Η βασική του λειτουργία είναι να μεταφράζει τα φιλικά προς τον άνθρωπο ονόματα τομέων (όπως www.example.com) στις αντίστοιχες διευθύνσεις IP (όπως 93.184.216.34) που χρειάζονται οι υπολογιστές για να εντοπίζουν και να επικοινωνούν μεταξύ τους. Χωρίς το DNS, κάθε φορά που θα θέλαμε να επισκεφτούμε έναν ιστότοπο, θα έπρεπε να θυμόμαστε και να πληκτρολογούμε τη σχετική αριθμητική διεύθυνση, κάτι που θα ήταν άβολο και αντιπαραγωγικό. Η ύπαρξη ενός τοπικού DNS server στον χώρο μας (για

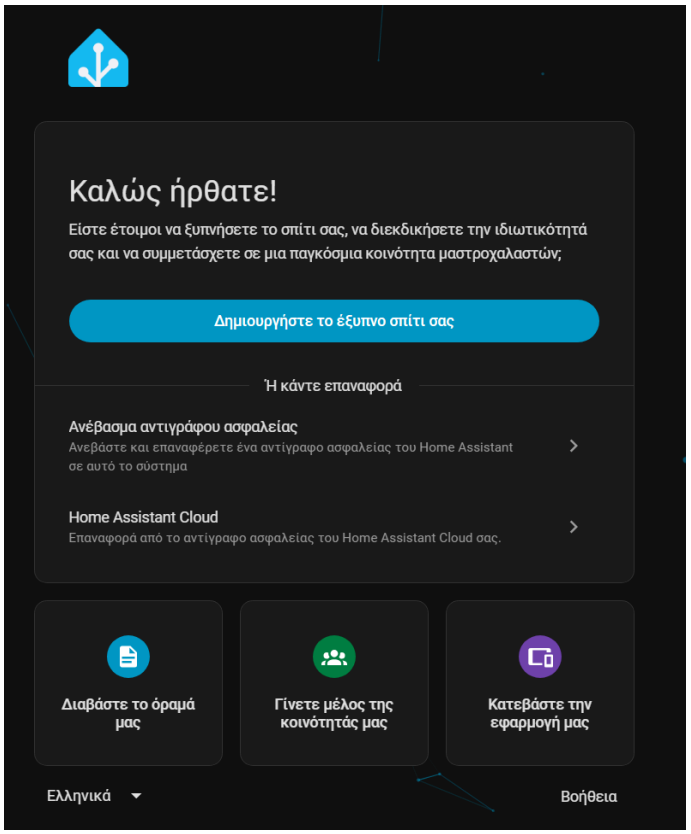
παράδειγμα σε ένα οικιακό ή επαγγελματικό δίκτυο) μπορεί να προσφέρει σημαντικά πλεονεκτήματα. Πρώτον, επιτρέπει τη δημιουργία εσωτερικών ονομάτων για τις συσκευές ή τις υπηρεσίες μας (όπως printer.local ή homeassistant.local), κάτι που διευκολύνει την πρόσβαση και τη διαχείριση τους χωρίς να χρειάζεται να θυμόμαστε εσωτερικές IP διευθύνσεις. Δεύτερον, μειώνει τον χρόνο απόκρισης των αιτήσεων DNS, καθώς οι τοπικές αναζητήσεις δεν χρειάζεται να φτάνουν μέχρι τους εξωτερικούς DNS servers μέσω του διαδικτύου. Ένα τοπικό DNS cache μπορεί να αποθηκεύει προσωρινά τις απαντήσεις για συχνά επισκεπτόμενους ιστότοπους ή υπηρεσίες, επιταχύνοντας την πλοήγηση και μειώνοντας την εξάρτηση από εξωτερικούς παράγοντες. Τρίτον, προσφέρει καλύτερο έλεγχο και ασφάλεια, αφού μπορούμε να φιλτράρουμε ή να ανακατευθύνουμε αιτήσεις, να αποκλείουμε διαφημιστικούς ή κακόβουλους τομείς (όπως γίνεται σε DNS-based ad blockers τύπου Pi-hole), ή να ελέγχουμε τις συνδέσεις που πραγματοποιούνται από τις έξυπνες συσκευές του σπιτιού μας.

Σε ένα περιβάλλον smart home, η χρήση ενός τοπικού DNS server αποκτά ακόμα μεγαλύτερη σημασία. Επιτρέπει στο σύστημα να λειτουργεί ανεξάρτητα από το διαδίκτυο, αφού οι συσκευές μπορούν να επικοινωνούν με βάση τοπικά domain names ακόμα κι αν η σύνδεση προς τα έξω διακοπεί. Ένας τοπικός DNS server δεν εξυπηρετεί μόνο την απόδοση και την ευχρηστία ενός δικτύου, αλλά αποτελεί και ένα κρίσιμο εργαλείο για την ενίσχυση της ασφάλειάς του. Μέσα από τον DNS μπορεί κανείς να ελέγξει ποιοι τομείς επιτρέπεται να επιλυθούν και ποιοι θα απορρίπτονται, λειτουργώντας ουσιαστικά ως ένα φίλτρο μεταξύ των χρηστών του δικτύου και του ευρύτερου διαδικτύου. Αυτό σημαίνει ότι μπορούμε να μπλοκάρουμε ανεπιθύμητες ή επικίνδυνες σελίδες, όπως ιστοσελίδες phishing, malware domains, ή spam hosts, αποτρέποντας έτσι τις συσκευές μας από το να έρθουν σε επαφή με κακόβουλο περιεχόμενο Η δυνατότητα αυτή είναι εξαιρετικά χρήσιμη σε περιβάλλοντα smart home, όπου πολλές συνδεδεμένες συσκευές δεν έχουν μηχανισμούς ασφαλείας υψηλού επιπέδου και μπορεί να επιχειρούν τακτικά συνδέσεις προς servers τρίτων κατασκευαστών, πολλές φορές χωρίς λόγο ή χωρίς τη συγκατάθεση του χρήστη. Μέσω ενός τοπικού DNS server μπορούμε όχι μόνο να περιορίσουμε τέτοιες συνδέσεις, αλλά και να καταγράψουμε πλήρως την DNS κίνηση του δικτύου, αποκτώντας ορατότητα σε ποια domains συνδέεται κάθε συσκευή.

Επιπλέον, η χρήση ενός DNS firewall ή η υλοποίηση κανόνων blacklists/whitelists, όπως γίνεται με λύσεις τύπου Pi-hole ή Unbound DNS με DNS blocking, μας επιτρέπει να ελέγξουμε το περιεχόμενο του διαδικτύου στο οποίο έχουν πρόσβαση οι χρήστες του δικτύου —π.χ. περιορίζοντας πρόσβαση σε social media, τυχερά παιχνίδια ή περιεχόμενο για ενηλίκους, κάτι χρήσιμο για οικογένειες ή εταιρικά περιβάλλοντα. Ο έλεγχος αυτός γίνεται σε επίπεδο DNS, πριν καν υπάρξει οποιαδήποτε σύνδεση HTTP/HTTPS με τον τελικό server, γεγονός που σημαίνει πως δεν χρειάζεται πολύπλοκη εγκατάσταση φίλτρων περιεχομένου ή proxies.Επιπλέον, ένας σωστά διαμορφωμένος τοπικός DNS server μπορεί να προστεθεί και στην αρχιτεκτονική ενός VPN server, προσφέροντας στους απομακρυσμένους χρήστες ασφαλείς, φιλτραρισμένες και ελεγχόμενες DNS υπηρεσίες ακόμα και εκτός του τοπικού δικτύου. Συνολικά, η ενσωμάτωση ενός DNS server με εστίαση στην ασφάλεια δίνει στον διαχειριστή του δικτύου τον έλεγχο, τη διαφάνεια και την δυνατότητα πρόληψης επιθέσεων ή διαρροής δεδομένων, σε ένα κρίσιμο σημείο —εκεί που αρχίζει η κάθε σύνδεση: στη μετάφραση του domain name.[1]

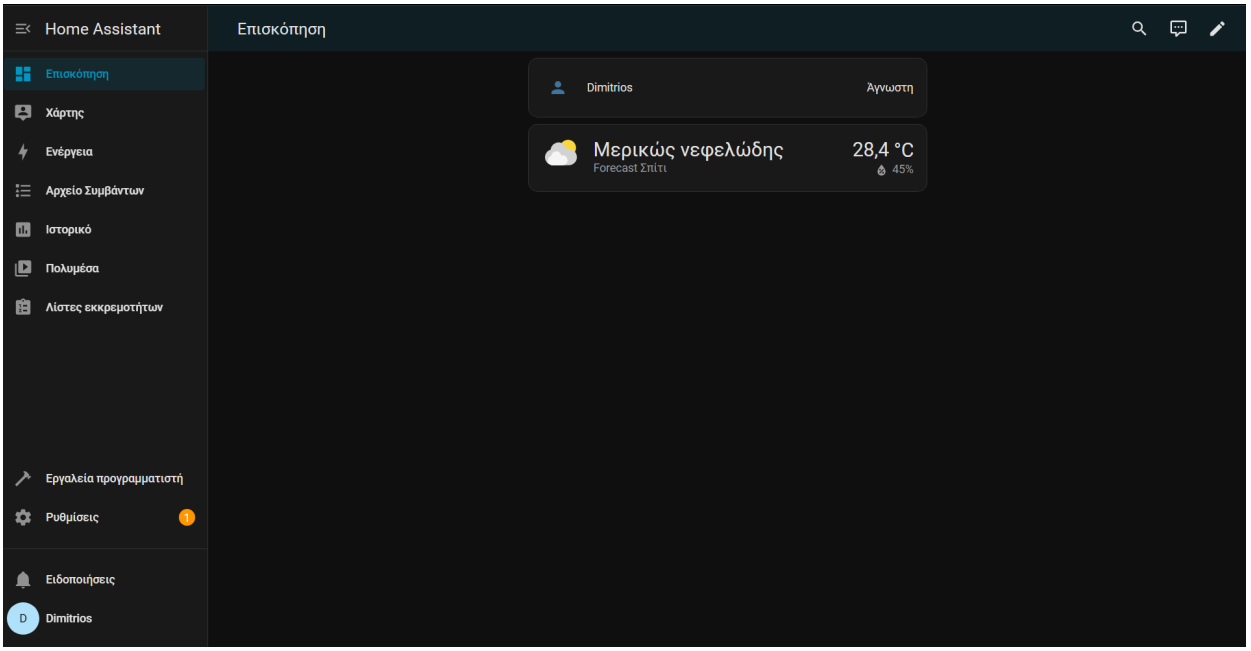
Κεφάλαιο 3ο: Εγκατάσταση και υλοποίηση ενος Smart Home χρησιμοποιώντας τον Home Assistant σε Raspberry Pi

Έπειτα, αφού ολοκληρωθεί επιτυχώς η εγκατάσταση του λειτουργικού συστήματος του Home Assistant επάνω στο Raspberry Pi και εμφανιστεί στην οθόνη η αντίστοιχη έξοδος εκκίνησης, το επόμενο βήμα αφορά την πρόσβαση στο γραφικό περιβάλλον διαχείρισης του συστήματος μέσω του δικτύου. Για να καταστεί αυτό εφικτό, απαιτείται να εντοπίσουμε τη διεύθυνση IP που έχει εκχωρηθεί αυτόματα στη συσκευή μας από τον διακομιστή DHCP του τοπικού δικτύου. Η διαδικασία αυτή είναι απαραίτητη, καθώς η IP διεύθυνση αποτελεί το μοναδικό αναγνωριστικό του Raspberry Pi στο δίκτυο, μέσω του οποίου μπορούμε να επικοινωνήσουμε μαζί του. Η πληροφορία αυτή μπορεί να αντληθεί απευθείας από το Command Line Interface (CLI) του Home Assistant, το οποίο παρέχει στον χρήστη όλες τις βασικές παραμέτρους που απαιτούνται για τη σύνδεση. Παρατηρώντας, λοιπόν, τη διεύθυνση IPv4 που εμφανίζεται, στην προκειμένη περίπτωση την **192.168.2.12**, και λαμβάνοντας υπόψη την αντίστοιχη θύρα επικοινωνίας, η οποία είναι η **8089**, μπορούμε να εισαγάγουμε τα στοιχεία αυτά σε έναν φυλλομετρητή διαδικτύου (browser) και να αποκτήσουμε πρόσβαση στο Web Interface της πλατφόρμας. Μέσα από το περιβάλλον αυτό ξεκινά η κύρια διαδικασία παραμετροποίησης, η οποία επιτρέπει στον χρήστη να προχωρήσει στη δημιουργία λογαριασμού, στη ρύθμιση των αρχικών παραμέτρων λειτουργίας και στην ενσωμάτωση των πρώτων συσκευών στο σύστημα αυτοματισμού. Με τον τρόπο αυτόν, η αρχική δικτυακή σύνδεση καθίσταται καθοριστικής σημασίας, καθώς αποτελεί το θεμέλιο για την περαιτέρω αξιοποίηση του Home Assistant και την ομαλή λειτουργία του σε ένα έξυπνο περιβάλλον κατοικίας.



Εικόνα 3.1: Οθόνη καλωσορίσματος στο home assistant

Το πρώτο στοιχείο που αντικρίζει ο χρήστης κατά την αρχική εκκίνηση του Home Assistant είναι το μήνυμα καλωσορίσματος, το οποίο σηματοδοτεί την έναρξη της διαδικασίας παραμετροποίησης του συστήματος. Σε αυτό το σημείο παρέχεται η δυνατότητα επαναφοράς ενός αντιγράφου ασφαλείας (backup) από κάποιο άλλο εγκατεστημένο σύστημα, είτε μέσω τοπικού αρχείου είτε αξιοποιώντας την υπηρεσία cloud της εταιρείας Nabu Casa Inc., η οποία έχει αναπτυχθεί ειδικά για να προσφέρει στους χρήστες ασφαλή και άμεση πρόσβαση στις ρυθμίσεις τους. Στη συνέχεια, με την επιλογή της διαδικασίας «Δημιουργία Έξυπνου Σπιτιού», ο χρήστης καθοδηγείται στο επόμενο βήμα, το οποίο περιλαμβάνει τον ορισμό του ονόματος χρήστη που θα λειτουργεί ως ο κεντρικός διαχειριστής (Master Administrator) του συστήματος, καθώς και την εισαγωγή της γεωγραφικής θέσης της κατοικίας. Η σωστή καταχώρηση των συντεταγμένων είναι ιδιαίτερα κρίσιμη, καθώς η ακριβής τοποθεσία θα αποτελέσει μελλοντικά τη βάση για την υλοποίηση διαφόρων αυτοματισμών, τόσο στον τομέα της ασφάλειας όσο και στην ενίσχυση της καθημερινής άνεσης και διευκόλυνσης της ζωής του χρήστη (Ease of Life). Ολοκληρώνοντας τα παραπάνω βήματα και αποδεχόμενοι τους όρους χρήσης, ο χρήστης οδηγείται στο τελικό στάδιο, όπου παρουσιάζεται το Lovelace UI, δηλαδή το βασικό γραφικό περιβάλλον χρήστη του Home Assistant, το οποίο αποτελεί το κεντρικό σημείο διαχείρισης και αλληλεπίδρασης με όλες τις συνδεδεμένες συσκευές και λειτουργίες του έξυπνου σπιτιού.

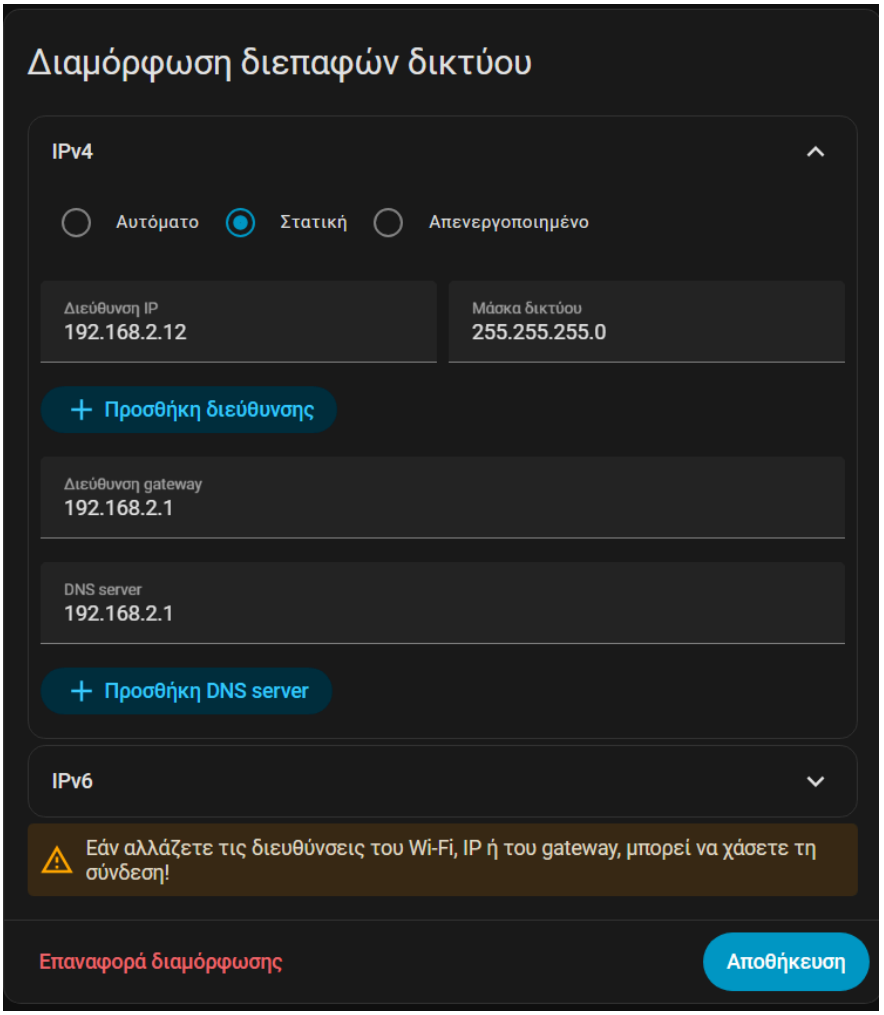


Εικόνα 3.2: Αρχικο ταμπλό πριν την παραμετροποίηση

Υπάρχουν ορισμένες κρίσιμες ενέργειες που είναι απαραίτητο να υλοποιηθούν σε αυτό το στάδιο, ώστε το σύστημα να μπορέσει να λειτουργήσει σωστά, με σταθερότητα και αξιοπιστία στο μέλλον. Πρώτο και πιο σημαντικό βήμα αποτελεί η απονομή μίας στατικής διεύθυνσης IP στον κεντρικό κόμβο του συστήματος, δηλαδή στον host. Με τον τρόπο αυτό εξασφαλίζεται ότι όλες οι τερματικές συσκευές, τα Virtual Private Networks, αλλά και τα διάφορα tunnels θα μπορούν να αναγνωρίζουν και να επικοινωνούν με συνέπεια με τον host, χωρίς να επηρεάζονται από πιθανές αλλαγές στη διευθυνσιοδότηση. Παράλληλα, είναι ιδιαίτερα χρήσιμο να αποδοθούν στατικές διευθύνσεις IP και στις υπόλοιπες συσκευές που πρόκειται να ενσωματωθούν στο περιβάλλον του έξυπνου σπιτιού, καθώς αυτό αποτρέπει την εμφάνιση του φαινομένου του DHCP flooding, δηλαδή της υπερβολικής κυκλοφορίας πακέτων που σχετίζονται με τη δυναμική εκχώρηση διευθύνσεων. Ένα τέτοιο φαινόμενο όχι μόνο επηρεάζει αρνητικά την απόδοση του δικτύου, αλλά μπορεί να προκαλέσει και

σύγχυση στην αναγνώριση των συσκευών. Τέλος, η χρήση στατικών διευθύνσεων δεν εξυπηρετεί μόνο τη σταθερότητα του συστήματος, αλλά και την εργασία του προγραμματιστή ή του διαχειριστή που το υλοποιεί, καθώς δημιουργεί μια πιο οργανωμένη εικόνα του δικτύου και διευκολύνει την ταξινόμηση, την κατηγοριοποίηση και τη λογική συσχέτιση κάθε συσκευής με τον ρόλο της. Με αυτόν τον τρόπο, διασφαλίζεται ότι η υποδομή του έξυπνου σπιτιού θα είναι καλύτερα διαχειρίσιμη, περισσότερο ασφαλής και πιο ανθεκτική σε πιθανά προβλήματα που ενδέχεται να προκύψουν.

Πηγαίνοντας, λοιπόν, στις ρυθμίσεις του συστήματός μας και συγκεκριμένα στην υποκατηγορία «Σύστημα», μπορούμε να επιλέξουμε την καρτέλα «Δίκτυο» και στη συνέχεια την επιλογή «Διαμόρφωση διεπαφών δικτύου». Εκεί, στη ρύθμιση που αφορά το IPv4, μας δίνεται η δυνατότητα να ορίσουμε τη στατική διεύθυνση IP που επιθυμούμε για το σύστημά μας, κάτι που είναι απαραίτητο για τη σταθερότητα του τοπικού μας δικτύου. Εκτός από την ίδια τη διεύθυνση, πρέπει να δηλώσουμε και τη μάσκα υποδικτύου (Subnet Mask), η οποία καθορίζει το μέγεθος του δικτύου και ποια IP ανήκουν σε αυτό, καθώς και τη διεύθυνση του δρομολογητή (Gateway), μέσω της οποίας επιτυγχάνεται η επικοινωνία με το διαδίκτυο και άλλα εξωτερικά δίκτυα. Εξίσου σημαντική είναι η σωστή ρύθμιση ενός έγκυρου DNS Server, αφού αυτός είναι υπεύθυνος για τη μετάφραση των ονομάτων τομέων (domain names) σε αριθμητικές IP διευθύνσεις, επιτρέποντας την εύκολη πρόσβαση σε υπηρεσίες και ιστοσελίδες. Σε αρχικό στάδιο, μπορούμε να χρησιμοποιήσουμε ως DNS τον ίδιο τον δρομολογητή μας, ώστε να λειτουργεί ως ενδιάμεσος στη διαχείριση των DNS αιτημάτων. Ωστόσο, σε πιο προχωρημένο επίπεδο, όταν εγκατασταθεί και διαμορφωθεί ένας τοπικός DNS Server στο εσωτερικό του συστήματος, θα πραγματοποιηθεί η αντίστοιχη αλλαγή. Αφου λοιπόν επιτυχώς κάνουμε την αλλαγή τότε πηγαίνουμε στην νέα διεύθυνση στον browser μας ώστε να ξανά αποκτήσουμε πρόσβαση.



Εικόνα 3.3: Επιλογή στατικής διεύθυνσης

3.1: Υλοποίηση VPN , DNS Server, Tunnel και μέτρων ασφαλείας

Αφού, λοιπόν, το σύστημά μας βρίσκεται πλέον σε πλήρη λειτουργία, το επόμενο βήμα είναι να προχωρήσουμε σε μια σειρά ενεργειών με στόχο τη θωράκισή του απέναντι σε εξωτερικές επιθέσεις, αλλά και την αποτροπή τυχόν απόπειρας μη εξουσιοδοτημένης πρόσβασης από άγνωστους χρήστες. Η ασφάλεια αποτελεί κρίσιμο ζήτημα, καθώς το σύστημα ενός έξυπνου σπιτιού περιλαμβάνει προσωπικά δεδομένα, δικτυακούς πόρους και ευαίσθητες πληροφορίες, οι οποίες σε περίπτωση παραβίασης θα μπορούσαν να θέσουν σε κίνδυνο τόσο την ιδιωτικότητα όσο και τη λειτουργικότητα του χώρου. Παράλληλα, απαιτείται η διαμόρφωση του συστήματος με τρόπο που να είναι προσβάσιμο από το διαδίκτυο, προκειμένου να μπορούμε να το ελέγχουμε απομακρυσμένα από οποιοδήποτε σημείο. Ωστόσο, η δημοσιοποίησή του στο διαδίκτυο πρέπει να συνοδεύεται πάντοτε από τις κατάλληλες δικλείδες ασφαλείας, Με αυτόν τον τρόπο, εξασφαλίζεται ότι η πρόσβαση στο σύστημα πραγματοποιείται αποκλειστικά από εξουσιοδοτημένους χρήστες, ενώ ταυτόχρονα επιτυγχάνεται η απαραίτητη ισορροπία ανάμεσα στη διαθεσιμότητα και την ασφάλεια.

Με γνώμονα τη λογική της ασφάλειας και ακολουθώντας μια κλιμακωτή προσέγγιση, ξεκινώντας δηλαδή από το τοπικό δίκτυο και επεκτεινόμενοι σταδιακά προς το εξωτερικό περιβάλλον, το πρώτο

βήμα που καλούμαστε να υλοποιήσουμε είναι η προσθήκη ενός μηχανισμού αναγνώρισης του χρήστη μέσω One Time Password (OTP). Πρόκειται για μια εξαιρετικά σημαντική διαδικασία, καθώς εισάγει μια επιπλέον βαθμίδα ασφάλειας με τη μορφή της πολλαπλής μεθόδου ταυτοποίησης (Multi-Factor Authentication - MFA), καθιστώντας την πρόσβαση στο σύστημα δυσκολότερη για οποιονδήποτε μη εξουσιοδοτημένο χρήστη. Σε αυτό το στάδιο, οφείλουμε να επιλέξουμε την κατάλληλη εφαρμογή για τη δημιουργία και τη διαχείριση αυτών των προσωρινών κωδικών. Καθώς υπάρχουν διαθέσιμες πολλές λύσεις στα ηλεκτρονικά καταστήματα εφαρμογών (App Store και Google Play), η δική μας επιλογή επικεντρώνεται στο Google Authenticator, μια από τις πιο διαδεδομένες και αξιόπιστες εφαρμογές του είδους. Η συγκεκριμένη εφαρμογή θα αναλάβει τη δημιουργία των προαναφερθέντων μοναδικών κωδικών πρόσβασης, οι οποίοι ανανεώνονται συνεχώς, ενισχύοντας περαιτέρω το επίπεδο ασφάλειας.

Έπειτα από την επιλογή του μηχανισμού ταυτοποίησης, το επόμενο βήμα είναι η τροποποίηση του αρχείου configuration.yaml του Home Assistant, το οποίο αποτελεί το κεντρικό σημείο διαχείρισης και αρχικοποίησης του συστήματος. Σε αυτό το αρχείο θα πρέπει να καταχωρηθούν οι παρακάτω γραμμές κώδικα που ενεργοποιούν τη λειτουργία του OTP, επιτρέποντας έτσι την ενσωμάτωση της νέας αυτής μεθόδου ταυτοποίησης και διασφαλίζοντας ότι κάθε απόπειρα σύνδεσης θα περνάει από αυτόν τον κρίσιμο μηχανισμό ελέγχου

```
# 2fa Line
  auth_mfa_modules:
    - type: totp
```

Εικόνα 3.4: Εντολές που πρέπει να προστεθούν στο configuration.yaml

Μετά την επανεκκίνηση του Home Assistant, στο προφίλ μας και συγκεκριμένα στην καρτέλα «Ασφάλεια», εμφανίζεται πλέον μια νέα επιλογή με την ονομασία «Μονάδες ελέγχου ταυτότητας πολλαπλών παραγόντων». Στην ενότητα αυτή, εάν επιλέξουμε το OTP Password και πατήσουμε «Ενεργοποίηση», το σύστημα μας εμφανίζει έναν μοναδικό QR Code, τον οποίο θα πρέπει να σαρώσουμε με την εφαρμογή Google Authenticator. Μετά τη σάρωση, η εφαρμογή δημιουργεί έναν δυναμικό κωδικό πρόσβασης, ο οποίος ανανεώνεται αυτόματα κάθε 30 δευτερόλεπτα. Ο κωδικός αυτός θα πρέπει να εισάγεται ως δεύτερο βήμα στη διαδικασία σύνδεσης με το σύστημα, εξασφαλίζοντας ότι μόνο ο κάτοχος της εφαρμογής μπορεί να ολοκληρώσει την ταυτοποίηση και να αποκτήσει πρόσβαση στο περιβάλλον του Home Assistant.
Μετέπειτα, το επόμενο βήμα για την ενίσχυση της ασφάλειας του έξυπνου σπιτιού μας είναι η προσθήκη μιας δικλείδας ασφαλείας, σύμφωνα με την οποία κάθε διεύθυνση IP που θα εισάγει λανθασμένο κωδικό πρόσβασης δύο συνεχόμενες φορές θα αποκλείεται αυτόματα από το σύστημα. Η πρακτική αυτή μας προστατεύει αποτελεσματικά από επιθέσεις τύπου Brute Force. Οι επιθέσεις Brute Force αποτελούν μία από τις πιο απλές, αλλά ταυτόχρονα και πιο διαδεδομένες μεθόδους παραβίασης κωδικών πρόσβασης. Η βασική τους αρχή έγκειται στο ότι ο επιτιθέμενος επιχειρεί συστηματικά να δοκιμάσει όλες τις πιθανές συνδυαστικές εκδοχές χαρακτήρων έως ότου εντοπίσει τον σωστό κωδικό. Πρόκειται, δηλαδή, για μια διαδικασία εξαντλητικής αναζήτησης, η οποία μπορεί να στοχεύει είτε απλούς κωδικούς, όπως αριθμητικά PIN, είτε πιο σύνθετα συνθηματικά που περιλαμβάνουν γράμματα, αριθμούς και ειδικούς χαρακτήρες. Η λειτουργία τέτοιων επιθέσεων βασίζεται σε αυτοματοποιημένα εργαλεία και λογισμικά, τα οποία είναι σε θέση να δοκιμάζουν εκατοντάδες ή και χιλιάδες συνδυασμούς ανά δευτερόλεπτο. Σε πιο εξελιγμένες μορφές, συναντούμε τις λεγόμενες επιθέσεις λεξικού (dictionary attacks), όπου χρησιμοποιούνται λίστες με γνωστούς ή συχνούς κωδικούς πρόσβασης, μειώνοντας έτσι τον χρόνο εύρεσης του σωστού. Επιπλέον, υπάρχουν οι

υβριδικές επιθέσεις (hybrid attacks), οι οποίες συνδυάζουν την τεχνική του λεξικού με αυτοματοποιημένες τροποποιήσεις, όπως για παράδειγμα η προσθήκη αριθμών στο τέλος λέξεων. Το κύριο μειονέκτημα για τον επιτιθέμενο είναι ότι αυτού του είδους οι επιθέσεις απαιτούν σημαντικό χρόνο και υπολογιστική ισχύ, ιδίως όταν οι κωδικοί είναι μεγάλοι και περίπλοκοι. Ωστόσο, η φύση τους στηρίζεται στο γεγονός ότι η προσπάθεια επαναλαμβάνεται συνεχώς, έως ότου επιτευχθεί η παραβίαση του σωστού κωδικού.Πηγαίνοντας εκ νέου στο αρχείο configuration.yaml, θα πρέπει να προχωρήσουμε στην προσθήκη της παρακάτω γραμμής κώδικα.

```
30  ip_ban_enabled: true
31  login_attempts_threshold: 2
```

Εικόνα 3.5: Εντολές για τον αποκλεισμό των IP

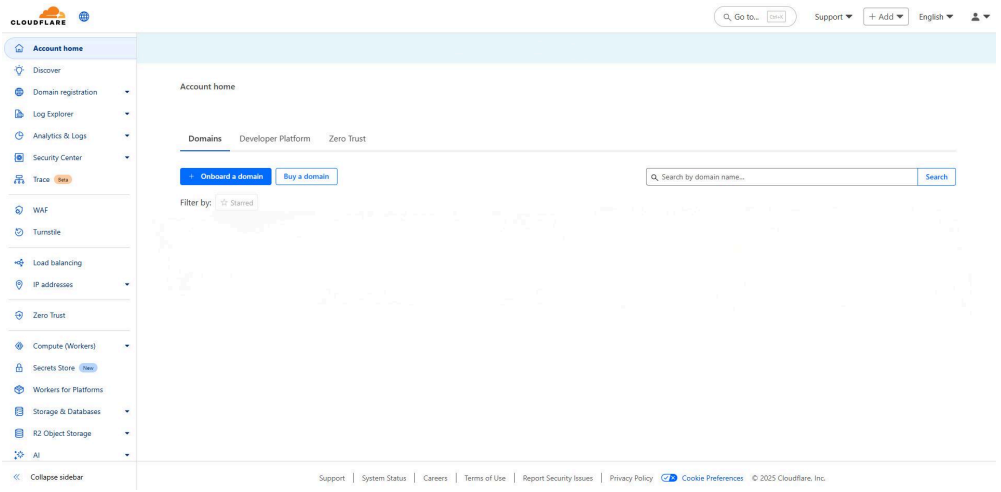
Η παράμετρος “login_attempts_threshold” αντιπροσωπεύει τον αριθμό των αποτυχημένων προσπαθειών εισόδου που επιτρέπεται να πραγματοποιήσει ένας χρήστης από μια συγκεκριμένη διεύθυνση IP, πριν το σύστημα προβεί σε αυτόματο αποκλεισμό της. Ο καθορισμός του συγκεκριμένου ορίου πρέπει να γίνεται με προσοχή, ώστε να εξισορροπείται η προστασία του συστήματος με την ευχρηστία για τον τελικό χρήστη, αποφεύγοντας άσκοπους αποκλεισμούς σε περιπτώσεις τυχαίων σφαλμάτων κατά την πληκτρολόγηση. Κάθε διεύθυνση IP που αποκλείεται από το σύστημα καταγράφεται αυτόματα στο αρχείο “ip_bans.yaml” , συνοδευόμενη από την ημερομηνία και την ακριβή ώρα κατά την οποία επιβλήθηκε ο αποκλεισμός. Η καταγραφή αυτή συμβάλλει στη διατήρηση αρχείου συμβάντων ασφαλείας, ώστε ο διαχειριστής να έχει πλήρη εικόνα των προσπαθειών μη εξουσιοδοτημένης πρόσβασης. Σε περίπτωση που κριθεί απαραίτητο να επιτραπεί εκ νέου η πρόσβαση σε μία συγκεκριμένη διεύθυνση IP, η διαδικασία είναι ιδιαίτερα απλή: αρκεί η διαγραφή της αντίστοιχης εγγραφής από το εν λόγω αρχείο. Με αυτόν τον τρόπο, η διεύθυνση IP αποδεσμεύεται από τον αποκλεισμό και μπορεί να αποκτήσει ξανά πρόσβαση στο σύστημα.

Αφού ολοκληρώθηκε η υλοποίηση του πρώτου επιπέδου ασφαλείας, το επόμενο βήμα είναι η ενεργοποίηση της πρόσβασης στο σύστημα μέσω του δημόσιου διαδικτύου, προσθέτοντας παράλληλα και ένα δεύτερο επίπεδο προστασίας. Υπάρχουν πολλαπλοί τρόποι για να επιτευχθεί η απομακρυσμένη πρόσβαση στο Home Assistant, ωστόσο δεν είναι όλοι ασφαλείς ή πρακτικοί. Για παράδειγμα, η μέθοδος του port forwarding χρησιμοποιείται συχνά από ανυποψίαστους χρήστες, αλλά ενέχει σοβαρούς κινδύνους, καθώς εκθέτει το σύστημα απευθείας στο διαδίκτυο χωρίς ουσιαστική προστασία. Από την άλλη πλευρά, η χρήση VPN προσφέρει ισχυρό επίπεδο ασφαλείας, αλλά μπορεί να θεωρηθεί μη πρακτική, καθώς προϋποθέτει τη συνεχή ενεργοποίηση του VPN από κάθε συσκευή που επιχειρεί πρόσβαση, γεγονός που δυσκολεύει την καθημερινή χρήση. Για τον λόγο αυτό, επιλέγεται η λύση της δημιουργίας tunnel, και πιο συγκεκριμένα μέσω της υπηρεσίας Cloudflare Tunnel, η οποία προσφέρει ένα ιδιαίτερα ισχυρό πλέγμα ασφαλείας. Η Cloudflare παρέχει, μεταξύ άλλων, δυνατότητες όπως το Web Application Firewall (WAF), που αποτελεί κρίσιμο παράγοντα για την αποτροπή κακόβουλων προσπαθειών πρόσβασης και για την ενίσχυση της συνολικής προστασίας του συστήματος. Η μόνη προϋπόθεση για την αξιοποίηση αυτής της λύσης είναι η ύπαρξη ενός κατοχυρωμένου domain, στο οποίο πρέπει να έχει οριστεί η Cloudflare ως πάροχος DNS. Με αυτόν τον τρόπο, το σύστημα παραμένει ασφαλές, διατηρώντας ταυτόχρονα την απαραίτητη ευελιξία και ευχρηστία στην απομακρυσμένη πρόσβαση.

Ξεκινώντας, το πρώτο βήμα είναι η δημιουργία ενός δωρεάν λογαριασμού στην πλατφόρμα της Cloudflare. Αφού ολοκληρωθεί η εγγραφή και η επαλήθευση του λογαριασμού, ο χρήστης μεταφέρεται στο κεντρικό διαχειριστικό περιβάλλον, από όπου μπορεί να πραγματοποιήσει όλες τις

απαραίτητες ρυθμίσεις. Στο σημείο αυτό, απαιτείται η διαδικασία ενσωμάτωσης (enrollment) του domain στην Cloudflare. Επιλέγοντας την εντολή “Onboard a site”, εμφανίζεται η δυνατότητα εισαγωγής του ονόματος του domain που επιθυμούμε να χρησιμοποιήσουμε.Αφού προηγουμένως έχει αποκτηθεί ένα domain name από πάροχο της επιλογής μας, το επόμενο βήμα είναι η ενημέρωση των εξυπηρετητών DNS (Name Servers) ώστε να αντιστοιχούν σε αυτούς που παρέχει η Cloudflare. Η διαδικασία αυτή πραγματοποιείται μέσα από το διαχειριστικό περιβάλλον του παρόχου του domain, όπου αντικαθίστανται οι υπάρχοντες DNS servers με αυτούς της Cloudflare, όπως υποδεικνύεται στο σχετικό βήμα.

Αξίζει να σημειωθεί ότι η ενημέρωση των nameservers δεν γίνεται άμεσα· απαιτείται συνήθως ένα χρονικό διάστημα, το οποίο διαφέρει ανάλογα με τον πάροχο και τη συχνότητα με την οποία ανανεώνει τα αρχεία DNS. Μόλις ολοκληρωθεί η διαδικασία, η Cloudflare ενημερώνει τον χρήστη ότι η μετάβαση πραγματοποιήθηκε επιτυχώς, οπότε και μπορεί να συνεχιστεί απρόσκοπτα η υπόλοιπη διαμόρφωση του συστήματος.



Εικόνα 3.6: Διαχειριστική σελίδα της cloudflare

Μόλις ολοκληρωθεί η διαδικασία ενημέρωσης των nameservers και αυτό επιβεβαιωθεί μέσα από το dashboard της Cloudflare, μπορούμε να προχωρήσουμε στα επόμενα βήματα ρύθμισης. Το επόμενο στάδιο αφορά τη μετάβαση στην καρτέλα Zero Trust, η οποία παρέχει προηγμένα εργαλεία ασφάλειας και διαχείρισης της πρόσβασης. Από εκεί, επιλέγουμε την ενότητα Networks και στη συνέχεια την υποκατηγορία Tunnels, όπου και θα δημιουργηθεί το απαραίτητο tunnel που θα συνδεθεί με το Home Assistant. Ωστόσο, πριν ξεκινήσει η διαδικασία δημιουργίας του tunnel μέσα από το περιβάλλον της Cloudflare, είναι απαραίτητο να προετοιμαστεί το Home Assistant ώστε να μπορεί να το δεχθεί και να λειτουργήσει ομαλά η επικοινωνία. Για τον σκοπό αυτό απαιτείται η εγκατάσταση του Cloudflare Tunnel client, ο οποίος ονομάζεται cloudflared. Ο client αυτός είναι υπεύθυνος για τη διασύνδεση του τοπικού συστήματος με την πλατφόρμα της Cloudflare και επιτρέπει τη δημιουργία ενός ασφαλούς καναλιού επικοινωνίας χωρίς να χρειάζεται η χρήση μεθόδων όπως το port forwarding.Η εγκατάσταση του cloudflared αποτελεί κρίσιμο βήμα, καθώς ουσιαστικά δρα ως ο «μεσάζων» που εξασφαλίζει την ασφαλή δρομολόγηση της κίνησης από το διαδίκτυο προς τον Home Assistant, εφαρμόζοντας ταυτόχρονα όλα τα επίπεδα προστασίας που προσφέρει η Cloudflare μέσω της Zero Trust αρχιτεκτονικής της.

Πηγαίνοντας, λοιπόν, στις ρυθμίσεις του συστήματός μας από το κεντρικό μενού του Home Assistant και επιλέγοντας την καρτέλα «Πρόσθετα», μας δίνεται η δυνατότητα να εγκαταστήσουμε εφαρμογές

οι οποίες εκτελούνται παράλληλα με τον Home Assistant, προσφέροντας επιπλέον λειτουργίες και επεκτάσεις. Μία από αυτές είναι και το cloudflared, το οποίο είναι απαραίτητο για την υλοποίηση του Cloudflare Tunnel.Η συγκεκριμένη εφαρμογή, ωστόσο, δεν περιλαμβάνεται εξ ορισμού στο επίσημο κατάστημα προσθέτων του Home Assistant, αλλά απαιτείται η προσθήκη του αντίστοιχου repository που φιλοξενείται στο GitHub. Για να το επιτύχουμε αυτό, μεταβαίνουμε στο υπομενού Πρόσθετα, και στη συνέχεια, κάτω δεξιά, επιλέγουμε το Κατάστημα προσθέτων. Από εκεί, στην επάνω δεξιά γωνία, υπάρχει η επιλογή «Προσθήκη αποθετηρίου» (Add Repository), όπου και εισάγουμε το σύνδεσμο (URL) του repository που αντιστοιχεί στο cloudflared.

Αφού ολοκληρώσουμε αυτήν την ενέργεια, απαιτείται μία επανεκκίνηση του Home Assistant ώστε να ενημερωθεί το κατάστημα και να καταστεί διαθέσιμο το νέο πρόσθετο. Στη συνέχεια, το cloudflared εμφανίζεται πλέον στη λίστα προσθέτων και μπορούμε να το εγκαταστήσουμε και να το ενεργοποιήσουμε.Το τελευταίο βήμα είναι η παραμετροποίησή του, η οποία είναι απαραίτητη ώστε να διασφαλιστεί η ορθή επικοινωνία με την πλατφόρμα της Cloudflare και, κατά συνέπεια, η ασφαλής πρόσβαση στο σύστημά μας μέσω του δημόσιου δικτύου.

Τελειώνοντας με την εγκατάσταση του πρόσθετου, μεταβαίνουμε εκ νέου στο Κατάστημα Προσθέτων του Home Assistant, όπου πλέον εμφανίζεται διαθέσιμη η επιλογή cloudflared. Το επιλέγουμε από τη λίστα και προχωρούμε στην εγκατάστασή του. Αφού ολοκληρωθεί η διαδικασία, εκκινούμε την εφαρμογή και κατευθυνόμαστε στην καρτέλα «Παραμετροποίηση» (Configuration).Στο πεδίο «Ονοματοχώρου» (hostname) εισάγουμε το όνομα του domain που έχουμε προμηθευτεί και στο οποίο έχουμε ήδη πραγματοποιήσει την εγγραφή (enroll) στην πλατφόρμα της Cloudflare. Με αυτόν τον τρόπο διασφαλίζεται η σύνδεση του συστήματός μας με το αντίστοιχο domain.Στη συνέχεια, μεταβαίνουμε στην καρτέλα «Αρχείο Καταγραφής» (Log File), όπου εμφανίζεται ένα μοναδικό σύνδεσμος (URL). Τοποθετώντας τον στον browser μας, οδηγούμαστε στη διαδικασία ταυτοποίησης λογαριασμού μέσω Cloudflare. Η συγκεκριμένη ενέργεια είναι απαραίτητη, καθώς συνδέει το tunnel με τον λογαριασμό μας και ενεργοποιεί επίσημα τη λειτουργία του.

Από τη στιγμή που ολοκληρωθεί η ταυτοποίηση, το tunnel έχει πλέον δημιουργηθεί. Είναι, όμως, κρίσιμο βήμα να προχωρήσουμε και σε πρόσθετη παραμετροποίηση μέσω του αρχείου configuration.yaml, προσθέτοντας τις παρακάτω γραμμές κώδικα, ώστε να μπορέσει το Home Assistant να λειτουργήσει ομαλά και να είναι προσβάσιμο με ασφάλεια μέσω του Cloudflare Tunnel.

```
37 http:
38   use_x_forwarded_for: true
39   trusted_proxies:
40     - 172.30.33.0/24
```

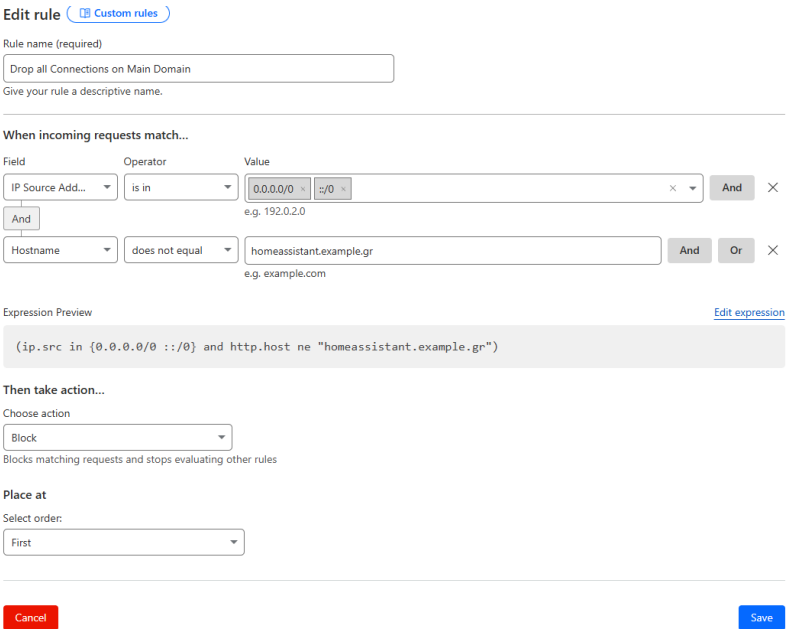
Εικόνα 3.7: Απαραίτητες εντολές για την λειτουργία του tunnel

Η αλλαγή που πραγματοποιείται στο αρχείο configuration.yaml είναι απαραίτητη, καθώς από προεπιλογή ο Home Assistant απορρίπτει όλες τις προσπάθειες σύνδεσης που διενεργούνται μέσω proxy. Με τη συγκεκριμένη ρύθμιση επιτρέπεται η αναγνώριση του προκαθορισμένου υποδικτύου που χρησιμοποιεί το Cloudflared, το οποίο θεωρείται αξιόπιστο, με αποτέλεσμα να μην μπλοκάρονται νόμιμες προσπάθειες σύνδεσης και ταυτόχρονα να διατηρείται η απαιτούμενη ασφάλεια του συστήματος. Αφού ολοκληρωθεί η διαδικασία αυτή, ο χρήστης πρέπει να μεταβεί εκ νέου στο Zero Trust dashboard της Cloudflare και συγκεκριμένα στην καρτέλα Tunnels, όπου θα διαπιστώσει ότι το tunnel που δημιουργήθηκε εμφανίζεται πλέον ενεργό και υγιές. Στη συνέχεια, επιλέγεται το

συγκεκριμένο tunnel και από το μενού Public Hostnames προστίθεται ένα νέο hostname. Σε αυτό το σημείο, είναι αναγκαίο να δηλωθεί το subdomain που θα προηγείται του domain (πχ. homeassistant.example.gr), ώστε να καθοδηγεί σωστά τις αιτήσεις προς τον Home Assistant, καθώς και η τοπική διεύθυνση IP του Home Assistant με την αντίστοιχη θύρα. Ιδιαίτερη προσοχή πρέπει να δοθεί στη χρήση του πρωτοκόλλου HTTP και όχι HTTPS, δεδομένου ότι η Cloudflare αναλαμβάνει την κρυπτογράφηση της επικοινωνίας μέσω TLS/SSL και μετατρέπει αυτόματα τη σύνδεση σε HTTPS για πρόσβαση από το δημόσιο διαδίκτυο, εξασφαλίζοντας πλήρη ασφάλεια χωρίς την ανάγκη πρόσθετης εγκατάστασης πιστοποιητικών στον ίδιο τον Home Assistant.

Από τη στιγμή που το σύστημα Home Assistant είναι πλέον προσβάσιμο μέσω του δημόσιου διαδικτύου, καθίσταται απολύτως απαραίτητο να θωρακιστεί απέναντι σε άγνωστες απειλές, αυτοματοποιημένα scripts και επιθετικά bots τα οποία πιθανότατα θα επιχειρήσουν να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση. Η απλή ύπαρξη ενός ενεργού tunnel μέσω Cloudflare δεν αρκεί από μόνη της, καθώς η δημόσια έκθεση της υπηρεσίας αυξάνει σημαντικά τον κίνδυνο κακόβουλων ενεργειών. Για τον λόγο αυτό αξιοποιείται το Web Access Firewall (WAF) που προσφέρει η ίδια η Cloudflare, το οποίο λειτουργεί ως πρόσθετο επίπεδο προστασίας φιλτράροντας την εισερχόμενη κίνηση. Μέσω του WAF μπορούμε να εφαρμόσουμε κανόνες ασφαλείας, να αποκλείσουμε ύποπτες ή κακόβουλες διευθύνσεις IP, να περιορίσουμε αυτοματοποιημένα αιτήματα που προέρχονται από bots, καθώς και να εντοπίσουμε και να αποτρέψουμε γνωστά μοτίβα επιθέσεων όπως SQL injection ή cross-site scripting. Με τον τρόπο αυτό δημιουργείται μια ισχυρή γραμμή άμυνας που λειτουργεί προληπτικά και μειώνει στο ελάχιστο την πιθανότητα παραβίασης, εξασφαλίζοντας ότι η απομακρυσμένη πρόσβαση στον Home Assistant παραμένει ασφαλής και σταθερή.

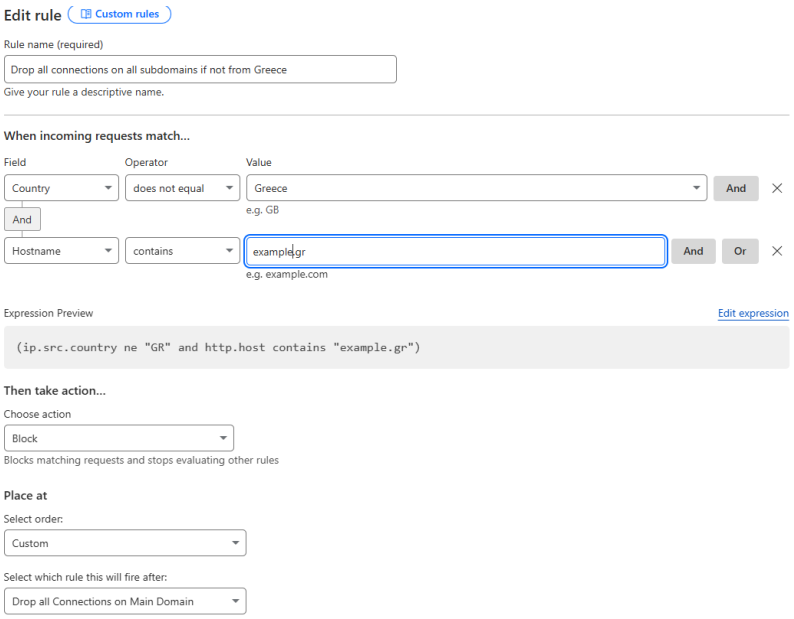
Επιστρέφοντας στο κεντρικό πάνελ διαχείρισης της Cloudflare και επιλέγοντας το domain που έχουμε δηλώσει, μπορούμε από το αριστερό μενού να μεταβούμε στην επιλογή “Security” και στη συνέχεια στην υποκατηγορία “WAF”, όπου μας δίνεται η δυνατότητα να καθορίσουμε τα κατάλληλα rules για την προστασία του συστήματός μας. Στο στάδιο αυτό θα δημιουργήσουμε δύο κανόνες, ώστε να επιτύχουμε μία ισορροπία ανάμεσα στην ασφάλεια και την πρακτικότητα, καθώς η υπερβολική έμφαση στο ένα κομμάτι μπορεί να αποδυναμώσει το άλλο. Ο πρώτος κανόνας αφορά την απαγόρευση πρόσβασης σε οποιονδήποτε επιχειρήσει να εισέλθει μέσω του βασικού domain. Ο λόγος που δεν χρησιμοποιούμε το αρχικό domain (π.χ. *domain.gr*) και φροντίζουμε να το ασφαλίσουμε είναι επειδή το συγκεκριμένο δηλώνεται σε όλα τα root servers και, κατά συνέπεια, αποτελεί τον πρωταρχικό στόχο για αυτοματοποιημένα bots που σαρώνουν μαζικά τα domains. Επιλέγοντας να δρομολογούμε την πρόσβαση στον Home Assistant μέσα από ένα ειδικό subdomain (π.χ. *homeassistant.example.gr*), αποτρέπουμε ένα μεγάλο ποσοστό κακόβουλου traffic το οποίο στοχεύει αδιακρίτως στο κύριο domain. Για τη δημιουργία του πρώτου κανόνα, επιλέγουμε “Create a Rule” και συντάσσουμε τον εξής όρο: εάν η διεύθυνση IP προέλευσης αντιστοιχεί σε ολόκληρο το διαδίκτυο (0.0.0.0/0) και ο ονοματοχώρος που επιχειρείται να προσπελαστεί δεν είναι το *homeassistant.example.gr*, τότε το σύστημα θα πρέπει να απορρίπτει (drop) κάθε σύνδεση. Είναι σημαντικό να σημειωθεί ότι τα firewall rules εκτελούνται με βάση την ιεραρχία που τους αποδίδεται, γεγονός που καθιστά κρίσιμη τη σωστή σειρά τοποθέτησης των εντολών για την αποφυγή ανεπιθύμητων αποτελεσμάτων.Για αυτό και αυτη η εντολή πρέπει να βρίσκεται στην πρώτη θέση.



Εικόνα 3.8: Παράδειγμα κανόνα για το WAF της Cloudflare

Το επόμενο βήμα είναι η δημιουργία του δεύτερου κανόνα ασφαλείας. Στην περίπτωση αυτή, στόχος μας είναι να απαγορεύσουμε την πρόσβαση προς όλα τα subdomains από οποιαδήποτε χώρα εκτός της Ελλάδας. Ο λόγος είναι ότι η πλειονότητα των αυτοματοποιημένων επιθέσεων (bots) προέρχεται από το εξωτερικό, επομένως με τον αποκλεισμό αυτόν περιορίζουμε δραστικά τον όγκο των πιθανών κακόβουλων αιτημάτων. Παράλληλα, ακόμη και αν χρειαστεί εμείς να αποκτήσουμε πρόσβαση στο Home Assistant ενώ βρισκόμαστε στο εξωτερικό, θα μπορέσουμε να το πραγματοποιήσουμε μέσω του VPN που θα υλοποιηθεί σε επόμενο στάδιο, εξασφαλίζοντας έτσι την ομαλή λειτουργικότητα του συστήματος.

Για τη δημιουργία αυτού του κανόνα, επιλέγουμε ξανά “Create a Rule” και διαμορφώνουμε τη λογική ως εξής: εάν η χώρα προέλευσης του αιτήματος δεν είναι η Ελλάδα, και στο αίτημα περιλαμβάνεται ο όρος example.gr, τότε το σύστημα πρέπει να απορρίπτει (drop) το συγκεκριμένο αίτημα. Με αυτόν τον τρόπο, επιτυγχάνουμε μία επιπλέον θωράκιση του περιβάλλοντος, αποκλείοντας μη εξουσιοδοτημένη πρόσβαση από το εξωτερικό και μειώνοντας σημαντικά τις πιθανότητες στοχοποίησης από αυτοματοποιημένα εργαλεία επιθέσεων.



Εικόνα 3.9: Παράδειγμα κανόνα για το WAF της Cloudflare

Στο επόμενο στάδιο εγκαθίσταται και ρυθμίζεται ένα εικονικό ιδιωτικό δίκτυο (VPN), ώστε να διασφαλιστεί ότι ο χρήστης μπορεί να έχει ασφαλή πρόσβαση στον Home Assistant από οποιοδήποτε σημείο και αν βρίσκεται, ακόμα και εκτός Ελλάδος. Η λύση που επιλέγεται είναι το Tailscale, μία σύγχρονη υλοποίηση VPN βασισμένη στο πρωτόκολλο WireGuard, η οποία έχει ως βασικό της πλεονέκτημα την απλοποίηση της απομακρυσμένης συνδεσιμότητας. Μέσω του Tailscale, ο Home Assistant καθίσταται προσβάσιμος αποκλειστικά από τις συσκευές που έχουν εξουσιοδοτηθεί, ενώ η επικοινωνία παραμένει πλήρως κρυπτογραφημένη από άκρο σε άκρο. Σε αντίθεση με τις παραδοσιακές λύσεις VPN που απαιτούν πολύπλοκες ρυθμίσεις, στατικές IP διευθύνσεις και κανόνες firewall, το Tailscale αυτοματοποιεί τη διαδικασία, αναθέτοντας σε κάθε συσκευή μια εσωτερική διεύθυνση IP στον χώρο 100.x.x.x και δημιουργώντας ένα mesh δίκτυο, στο οποίο κάθε κόμβος μπορεί να επικοινωνεί απευθείας με τον Home Assistant. Σε περιπτώσεις όπου η απευθείας σύνδεση εμποδίζεται από περιορισμούς δικτύου, η επικοινωνία πραγματοποιείται μέσω των DERP servers, που λειτουργούν αποκλειστικά ως ασφαλείς αναμεταδότες χωρίς δυνατότητα αποκρυπτογράφησης.

Ιδιαίτερα σημαντική για τη χρήση του Home Assistant από το εξωτερικό είναι η δυνατότητα αξιοποίησης Exit Nodes, μέσω των οποίων ολόκληρη η κίνηση μιας συσκευής μπορεί να δρομολογηθεί μέσα από το οικιακό δίκτυο, εμφανίζοντας τον χρήστη με την ελληνική διεύθυνση IP και εξασφαλίζοντας πρόσβαση στο περιβάλλον αυτοματισμού με τρόπο απολύτως διαφανή και ασφαλή. Παράλληλα, μέσω Subnet Routers είναι δυνατή η απομακρυσμένη πρόσβαση όχι μόνο στον ίδιο τον Home Assistant, αλλά και σε οποιαδήποτε άλλη συσκευή του τοπικού δικτύου (π.χ. 192.168.1.0/24), ενώ τα Access Control Lists (ACLs) επιτρέπουν την αυστηρή διαχείριση των δικαιωμάτων πρόσβασης. Το χαρακτηριστικό MagicDNS απλοποιεί ακόμη περισσότερο τη διαδικασία, καθώς εξαλείφει την ανάγκη απομνημόνευσης IP διευθύνσεων, δίνοντας τη δυνατότητα σύνδεσης στον Home Assistant με φιλική ονομασία. Η εγκατάσταση πραγματοποιείται μέσω των πρόσθετων της κοινότητας του Home Assistant (Home Assistant Community Add-ons), όπου μετά την εγκατάσταση και ενεργοποίηση αρκεί η σύνδεση με τον Google λογαριασμό του χρήστη για να καταστεί το VPN άμεσα λειτουργικό. Τέλος, με την εγκατάσταση της εφαρμογής Tailscale σε οποιοδήποτε τερματικό, ο χρήστης αποκτά ολοκληρωμένη, ασφαλή και αξιόπιστη απομακρυσμένη

πρόσβαση στον Home Assistant, διασφαλίζοντας την απρόσκοπτη χρήση του συστήματος σε κάθε περίσταση.

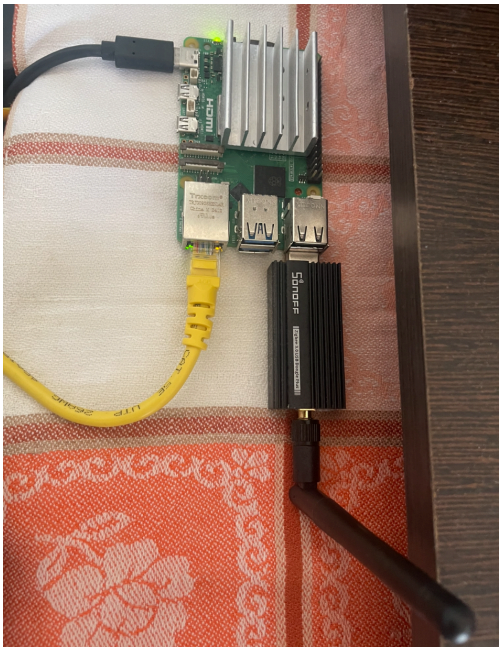
Στο πλαίσιο της συνολικής θωράκισης του συστήματος, ιδιαίτερη βαρύτητα έχει η χρήση ενός DNS server, ο οποίος αναλαμβάνει την προστασία σε επίπεδο εφαρμογής (OSI Layer 7). Μέσω αυτού καθίσταται δυνατός ο φιλτράρισμα της διαδικτυακής κίνησης, με αποτέλεσμα να αποκόπτονται ανεπιθύμητες διαφημίσεις, κακόβουλοι ιστότοποι αλλά και περιεχόμενο που κρίνεται ακατάλληλο ή επικίνδυνο. Στην παρούσα υλοποίηση επιλέγεται ο AdGuard Home, ένα εργαλείο που λειτουργεί ως DNS resolver με δυνατότητες φιλτραρίσματος, το οποίο υποστηρίζεται πλήρως και διατίθεται ως πρόσθετο στο κατάστημα του Home Assistant. Η διαδικασία εγκατάστασης είναι ανάλογη με αυτή που ακολουθήθηκε στα προηγούμενα στάδια: μέσα από το κατάστημα πρόσθετων του Home Assistant επιλέγεται το AdGuard Home και εγκαθίσταται. Με την ολοκλήρωση της εγκατάστασης, στο αριστερό μενού του περιβάλλοντος εμφανίζεται πλέον η αντίστοιχη επιλογή. Ανοίγοντας την εφαρμογή, ο χρήστης οδηγείται στο διαχειριστικό της πάνελ, όπου παρέχονται όλες οι απαραίτητες ρυθμίσεις για την παραμετροποίηση του συστήματος. Από εκεί καθίσταται εφικτός ο καθορισμός λιστών φιλτραρίσματος, η δημιουργία εξαιρέσεων και η παρακολούθηση της δραστηριότητας του δικτύου, ώστε ο Home Assistant και οι συσκευές του τοπικού δικτύου να είναι προστατευμένα από απειλές και ανεπιθύμητο περιεχόμενο σε πραγματικό χρόνο.

Στο επόμενο στάδιο της παραμετροποίησης, ιδιαίτερη σημασία έχει η εγκατάσταση των λιστών φιλτραρίσματος, οι οποίες καθορίζουν ποια domains θα αποκλείονται αυτόματα κατά την επίλυση DNS. Για τον σκοπό αυτό, μεταβαίνουμε στην καρτέλα Settings και στη συνέχεια στην υποενότητα DNS Blocklists. Εκεί μπορούμε να προσθέσουμε τις λίστες που επιθυμούμε, ανάλογα με το επίπεδο προστασίας που θέλουμε να επιτύχουμε. Αν και το AdGuard παρέχει ορισμένες προεγκατεστημένες επιλογές, στη συγκεκριμένη υλοποίηση προτιμάται η χρήση των λιστών του developer OISD, οι οποίες θεωρούνται ιδιαίτερα αξιόπιστες και αποδεδειγμένα έχουν την υποστήριξη και την έγκριση της κοινότητας. Με την ενσωμάτωση των συγκεκριμένων blocklists διασφαλίζεται πιο αποτελεσματικός αποκλεισμός διαφημίσεων και κακόβουλου περιεχομένου, ενισχύοντας ακόμη περισσότερο την ασφάλεια του συστήματος και την ποιότητα της διαδικτυακής εμπειρίας. Τέλος, για να μπορέσει το AdGuard να αναλάβει πλήρως τον ρόλο του DNS server, είναι απαραίτητο να ενημερώσουμε όλες τις συσκευές του τοπικού μας δικτύου ώστε να χρησιμοποιούν τον Home Assistant ως πηγή επίλυσης ονομάτων. Η πιο ενδεδειγμένη μέθοδος είναι να μεταβούμε στις ρυθμίσεις DHCP του δρομολογητή μας και να ορίσουμε ως διεύθυνση DNS την IP του Home Assistant. Με αυτόν τον τρόπο, κάθε νέα συσκευή που θα συνδέεται στο δίκτυο θα λαμβάνει αυτόματα τη σωστή διεύθυνση DNS, χωρίς να απαιτείται επιπλέον παρέμβαση. Σε περιπτώσεις όπου κάποια συσκευή διαθέτει στατική διεύθυνση IP, η ρύθμιση γίνεται χειροκίνητα, εισάγοντας απευθείας την IP του Home Assistant στο πεδίο DNS. Έτσι, διασφαλίζεται ότι όλη η δικτυακή κίνηση διέρχεται μέσα από το AdGuard, αποκομίζοντας τα οφέλη του φιλτραρίσματος και της προστασίας που αυτό παρέχει.

3.2: Παραμετροποίηση εξοπλισμού και ενεργοποίηση τελικού συστήματος.

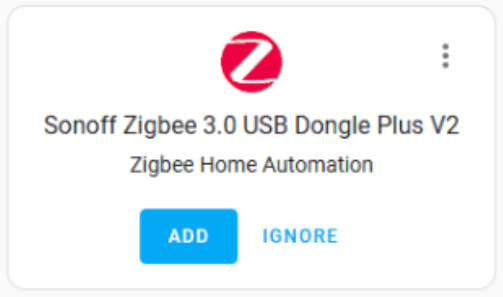
Αφού ολοκληρώσαμε τη διαδικασία θωράκισης και διασφαλίσαμε την απομακρυσμένη πρόσβαση στο σύστημά μας μέσω του διαδικτύου, ήρθε πλέον η στιγμή να περάσουμε στο στάδιο της τελικής παραμετροποίησης. Σε αυτό το στάδιο θα πρέπει να εγγράψουμε τις τερματικές συσκευές που θα συνδεθούν στον Home Assistant, είτε αυτές βασίζονται στο πρότυπο Zigbee είτε σε τεχνολογία Wi-Fi,

ώστε να γίνουν ορατές και διαχειρίσιμες μέσα από το κεντρικό μας σύστημα. Ξεκινώντας από το οικοσύστημα του Zigbee, θα χρησιμοποιήσουμε ως συντονιστή (coordinator) το gateway της Sonoff, και πιο συγκεκριμένα το "Zigbee 3.0 USB Dongle Plus". Ο συγκεκριμένος αντάπτορας θα αποτελέσει τον βασικό κόμβο επικοινωνίας μεταξύ του Home Assistant και όλων των Zigbee συσκευών μας, δημιουργώντας τοπικά το ιδιωτικό δίκτυο που απαιτείται για τη λειτουργία τους.



Εικόνα 3.9: Ο συντονιστής για το δίκτυο Zigbee πανω στο σύστημα μας

Μόλις συνδέσουμε το Zigbee 3.0 USB Dongle Plus στο σύστημά μας (Raspberry Pi), ο Home Assistant το αναγνωρίζει αυτόματα και μας δίνει τη δυνατότητα να το παραμετροποιήσουμε. Στις ρυθμίσεις, και πιο συγκεκριμένα στην καρτέλα των συσκευών, εμφανίζεται η επιλογή "Zigbee Home Automation (ZHA)", η οποία αποτελεί τον μεσάζοντα (broker) ανάμεσα στον coordinator και τον Home Assistant. Μέσω αυτής της διεπαφής διασφαλίζεται η ομαλή επικοινωνία του dongle με το κεντρικό μας σύστημα, ενώ ταυτόχρονα μας επιτρέπεται να προσθέτουμε, να διαχειριζόμαστε και να παρακολουθούμε όλες τις Zigbee συσκευές που θα εγγραφούν στο δίκτυο.



Εικόνα 3.10: Επιλογή προσθήκης συσκευής στο home assistant

Πατώντας την επιλογή "Προσθήκη" (Add) ξεκινά η διαδικασία ενεργοποίησης του coordinator και, κατ' επέκταση, ολόκληρου του Zigbee δικτύου. Ακολουθώντας τις οδηγίες που εμφανίζονται στην οθόνη, φτάνουμε στο σημείο όπου το ZHA (Zigbee Home Automation) μας ζητά να καθορίσουμε τις παραμέτρους λειτουργίας του δικτύου. Σε αυτό το στάδιο επιλέγουμε την επιλογή "Δημιουργία νέου

δικτύου", με αποτέλεσμα να ολοκληρώνεται η αρχική παραμετροποίηση και να δημιουργείται το Zigbee mesh δίκτυο μας. Το επόμενο βήμα είναι να προχωρήσουμε στην προσθήκη των τερματικών συσκευών μας, όπως αισθητήρες, διακόπτες και έξυπνοι λαμπτήρες, ώστε να εγγραφούν στο σύστημα και να αρχίσουν να επικοινωνούν με τον Home Assistant.

Για τις ανάγκες του παραδείγματος στην παρούσα εργασία θα προχωρήσουμε στην προσθήκη τριών ενδεικτικών συσκευών: ενός αισθητήρα κίνησης (PIR) της Sonoff, ενός αισθητήρα πόρτας (Hall) επίσης της Sonoff και ενός μετρητή κατανάλωσης ρεύματος. Αρχικά, είναι απαραίτητο οι συσκευές αυτές να τεθούν σε λειτουργία και στη συνέχεια να εισέλθουν σε διαδικασία ανακάλυψης (discovery mode) από τον coordinator. Στην περίπτωση των δύο αισθητήρων, οι οποίοι τροφοδοτούνται με μπαταρία, το πρώτο βήμα είναι να αφαιρεθεί η πλαστική ασφάλεια που παρεμβάλλεται μεταξύ της μπαταρίας και της επαφής, ώστε να ενεργοποιηθεί το κύκλωμα. Αντιθέτως, για τον μετρητή κατανάλωσης ρεύματος απαιτείται η ένταξή του στο ηλεκτρικό δίκτυο του σπιτιού, ακολουθώντας την τυπική διαδικασία σύνδεσης που απεικονίζεται στο παρακάτω σχεδιάγραμμα:

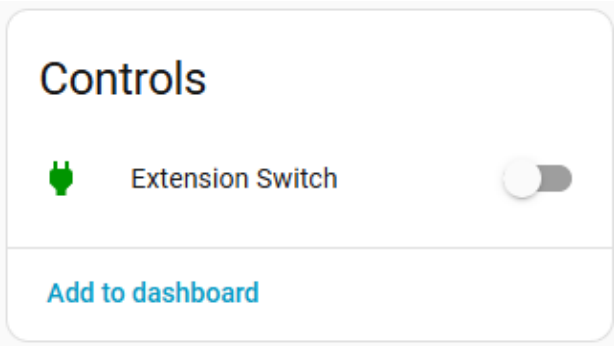
Αφού ολοκληρωθεί η διαδικασία ενεργοποίησης των συσκευών, το επόμενο βήμα είναι η εισαγωγή τους σε λειτουργία ευρεσιμότητας (*pairing mode*). Αυτό επιτυγχάνεται με το παρατεταμένο πάτημα του πλήκτρου που διαθέτει κάθε συσκευή, μέχρι να εμφανιστεί η αντίστοιχη φωτεινή ένδειξη, η οποία και επιβεβαιώνει ότι η συσκευή είναι πλέον έτοιμη για σύνδεση. Στη συνέχεια, μέσω του μενού «Ρυθμίσεις» στο Zigbee Home Assistant, επιλέγουμε την ενότητα «Προσθήκη συσκευών». Το σύστημα ξεκινά τη διαδικασία αναζήτησης νέων συσκευών, και σταδιακά καθεμία από αυτές αναγνωρίζεται και εντάσσεται αυτόματα στο δίκτυο Zigbee, καθιστώντας την άμεσα διαθέσιμη προς χρήση μέσα από την πλατφόρμα του Home Assistant.

Πριν περάσουμε στην παραμετροποίηση της διεπαφής Lovelace, είναι απαραίτητο να εντάξουμε και ορισμένες συσκευές τύπου Wi-Fi, οι οποίες θα εμπλουτίσουν περαιτέρω τη λειτουργικότητα του συστήματος. Στο παράδειγμά μας θα προστεθεί ένας διακόπτης της εταιρείας Sonoff, καθώς και ένας εκπομπός υπερύθρων (IR Blaster) της Broadlink, ο οποίος δίνει τη δυνατότητα ελέγχου παραδοσιακών συσκευών που λειτουργούν με τηλεχειριστήριο, όπως παλαιότερα κλιματιστικά.

Η διαδικασία ενσωμάτωσης των Wi-Fi συσκευών διαφοροποιείται ελαφρώς σε σχέση με εκείνη των Zigbee. Αρχικά απαιτείται η παραμετροποίησή τους μέσω της επίσημης εφαρμογής του εκάστοτε κατασκευαστή, ώστε να συνδεθούν σωστά στο τοπικό μας δίκτυο. Στη συνέχεια, μεταβαίνουμε στις ρυθμίσεις του Home Assistant και συγκεκριμένα στην ενότητα των συσκευών, όπου προσθέτουμε τα σχετικά πρόσθετα (integrations) για τις δύο αυτές πλατφόρμες. Ακολουθώντας τα βήματα που υποδεικνύει το σύστημα, οι εφαρμογές συνδέονται με επιτυχία στο Home Assistant, με αποτέλεσμα οι συσκευές να ενταχθούν στο κεντρικό οικοσύστημα και να είναι πλέον διαθέσιμες προς έλεγχο και αυτοματισμό.

Εικόνα 3.11: Παράδειγμα επιτυχημένης ένταξης συσκευής στο home assistant

Κατά την ολοκλήρωση της διαδικασίας προσθήκης των Wi-Fi συσκευών, ο Home Assistant μας δίνει τη δυνατότητα να επιλέξουμε αν θα ενεργοποιήσουμε ή όχι τη συγκεκριμένη ενσωμάτωση. Αυτος ο διακόπτης είναι και αυτός που θα εντάξουμε στην διεπαφή lovelace.



Εικόνα 3.12: Παράδειγμα κάρτας για το κεντρικό ταμπλό

Στην τελική φάση ένταξης του εξοπλισμού στο σύστημα Home Assistant, πραγματοποιείται η ενσωμάτωση του μετρητή ηλεκτρικής ενέργειας καθώς και του υπέρυθρου εκπομπού (IR Blaster). Αρχικά, για την περίπτωση του μετρητή ρεύματος, απαιτείται η φυσική εγκατάστασή του στον ηλεκτρολογικό πίνακα της οικίας. Η συσκευή διαθέτει έξι υποδοχές: τις ακροδέκτες της φάσης (L), του ουδετέρου (N), καθώς και τέσσερις ακροδέκτες για τα δύο πηνία τύπου Rogowski (1–, 1+, 2–, 2+). Είναι σημαντικό να σημειωθεί ότι για κάθε φάση που υπάρχει στο ηλεκτρικό δίκτυο, απαιτείται και ένα αντίστοιχο πηνίο. Έτσι, σε μονοφασική εγκατάσταση απαιτείται μόνο ένα πηνίο, ενώ σε τριφασική εγκατάσταση χρειάζονται τρία. Η διαδικασία σύνδεσης περιλαμβάνει την τοποθέτηση των καλωδίων φάσης και ουδετέρου στις αντίστοιχες υποδοχές, ώστε ο μετρητής να τροφοδοτείται με ρεύμα από το δίκτυο, ενώ το πηνίο συνδέεται στους ακροδέκτες 1– και 1+.
Στη συνέχεια, τοποθετείται περιμετρικά της φάσης του σπιτιού, αμέσως μετά τον γενικό ασφαλειοδιακόπτη. Ιδιαίτερη προσοχή απαιτείται στην κατεύθυνση τοποθέτησης του πηνίου, καθώς φέρει ένδειξη ροής, η οποία πρέπει να τοποθετηθεί σύμφωνα με τη φορά του ηλεκτρικού ρεύματος, προκειμένου οι μετρήσεις να είναι ακριβείς.

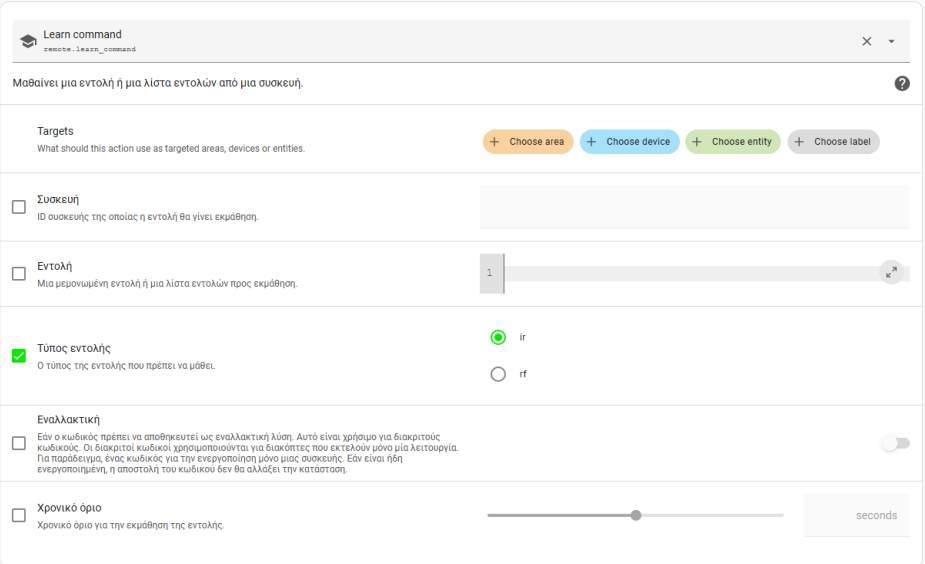
Εικόνα 3.13: Ένας μετρητής ρεύματος [23.α]

Δεδομένου ότι ο διακόπτης που χρησιμοποιείται βασίζεται στην τεχνολογία Zigbee, με την τροφοδοσία του ενεργοποιείται αυτόματα η δυνατότητα εισαγωγής του στο δίκτυο. Στην αριστερή πλευρά της συσκευής βρίσκεται το πλήκτρο ενεργοποίησης της διαδικασίας ανακάλυψης (discovery

mode). Με την παρατεταμένη πίεση του πλήκτρου, η συσκευή εισέρχεται στη λειτουργία ανακάλυψης, γεγονός που υποδεικνύεται από την αντίστοιχη φωτεινή ένδειξη. Στη συνέχεια, μέσω της πλατφόρμας ZHA (Zigbee Home Automation) στο Home Assistant, είναι δυνατή η ανίχνευση και η καταχώρηση του διακόπτη στο σύστημα, ολοκληρώνοντας έτσι τη διαδικασία ενσωμάτωσής του στο οικιακό δίκτυο αυτοματισμού. Ολοκληρώνοντας την εγκατάσταση, προχωρούμε στην ενσωμάτωση του εκπομπού υπερύθρων (IR Blaster), ο οποίος λόγω της φύσης του ως συσκευή Wi-Fi ακολουθεί διαφορετική διαδικασία προσθήκης στο Home Assistant σε σχέση με τις Zigbee συσκευές. Συγκεκριμένα, μεταβαίνουμε στις ρυθμίσεις του συστήματος και στην καρτέλα «Συσκευές», όπου επιλέγουμε την προσθήκη νέας ενότητας. Από τη λίστα των διαθέσιμων ενοτήτων αναζητούμε την εφαρμογή που αντιστοιχεί στον κατασκευαστή της συσκευής μας· στην παρούσα περίπτωση πρόκειται για την Broadlink. Κατά τη διαδικασία παραμετροποίησης, το σύστημα ζητά την εισαγωγή της διεύθυνσης IP του εκπομπού, την οποία μπορούμε να εντοπίσουμε μέσω των ρυθμίσεων του δρομολογητή μας, αντιστοιχίζοντας τη MAC address της συσκευής. Μόλις ολοκληρωθεί η ρύθμιση αυτή, ο εκπομπός είναι έτοιμος να καταγράψει και να αποθηκεύσει τις εντολές οποιουδήποτε τηλεχειριστηρίου υπερύθρων, καθιστώντας εφικτό τον απομακρυσμένο έλεγχο «μη έξυπνων» συσκευών, όπως κλιματιστικών παλαιότερης τεχνολογίας ή άλλων οικιακών συσκευών που βασίζονται σε συμβατική υπέρυθρη επικοινωνία.

Η διαδικασία εκμάθησης των εντολών υπερύθρων από τον εκπομπό πραγματοποιείται με συγκεκριμένα βήματα, τα οποία διασφαλίζουν ότι κάθε λειτουργία που επιθυμούμε να ενσωματώσουμε στο Home Assistant θα καταγραφεί σωστά. Συγκεκριμένα, για κάθε εντολή του τηλεχειριστηρίου που θέλουμε να αναπαραχθεί από το σύστημα, απαιτείται να τη μεταφέρουμε στον IR Blaster μέσω της διαδικασίας εκμάθησης. Για τον σκοπό αυτό, μεταβαίνουμε στο αριστερό μενού του Home Assistant και επιλέγουμε την ενότητα «Εργαλεία Προγραμματιστή».

Στη συνέχεια, στην καρτέλα «Actions» έχουμε τη δυνατότητα να καλέσουμε έτοιμες συναρτήσεις, οι οποίες έχουν σχεδιαστεί για την εκτέλεση τέτοιου είδους λειτουργιών. Η συνάρτηση που χρησιμοποιείται για την εκμάθηση εντολών είναι η *remote.learn_command*, η οποία επιτρέπει στο σύστημα να καταγράψει και να αποθηκεύσει το σήμα της υπέρυθρης εντολής που στέλνει το τηλεχειριστήριο, ώστε να μπορεί να αναπαραχθεί οποιαδήποτε στιγμή στο μέλλον.

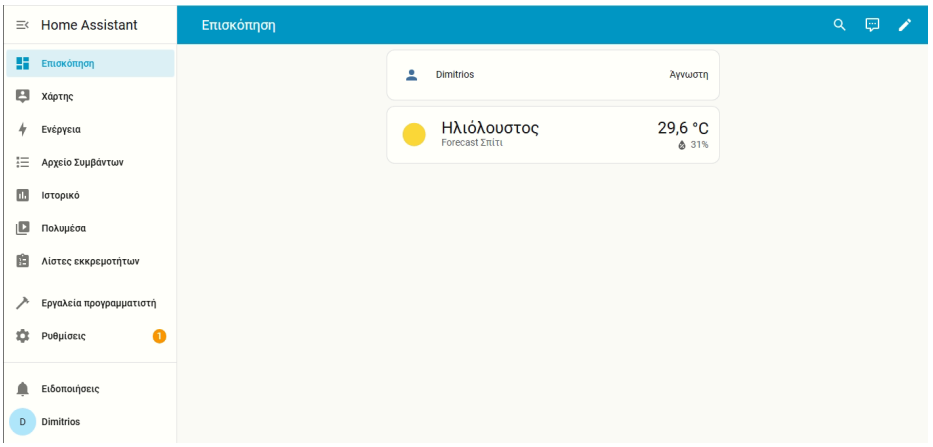


Εικόνα 3.14: Σελίδα προγραμματισμού συσκευής υπερύθρων

Στο επόμενο βήμα της διαδικασίας εκμάθησης επιλέγεται ο στόχος (*target*) της εντολής. Συγκεκριμένα, μέσω της επιλογής «Επιλογή Οντότητας» καθορίζεται ο εκπομπός που έχει ήδη ενταχθεί στο Home Assistant στο προηγούμενο στάδιο. Στη συνέχεια, ενεργοποιείται η επιλογή «Συσκευή», στην οποία εισάγεται το όνομα της συσκευής που πρόκειται να ελεγχθεί (για παράδειγμα *Air_Condition*). Ακολούθως, ενεργοποιείται και η επιλογή «Εντολή», όπου ορίζεται η ονομασία της εντολής που θα εκτελείται, όπως για παράδειγμα *PowerOff*. Στο σημείο που απαιτείται η επιλογή τύπου εντολής, καθορίζεται η χρήση υπερύθρων (*InfraRed*), δεδομένου ότι το ζητούμενο είναι η αναπαραγωγή εντολών μέσω υπέρυθρης τεχνολογίας. Ωστόσο, υπάρχει και η δυνατότητα επιλογής τύπου *Radio Frequency (RF)*, ώστε να εισαχθούν εντολές από τηλεχειριστήρια τα οποία βασίζονται σε ραδιοσυχνότητες.

Με την ολοκλήρωση της ρύθμισης των παραπάνω πεδίων, ο χρήστης καλείται να πατήσει την επιλογή «Κάλεσμα Εντολής» που βρίσκεται στο κάτω δεξί μέρος της διεπαφής. Ο εκπομπός παρέχει τότε οπτική ένδειξη, η οποία λειτουργεί ως ειδοποίηση ότι είναι έτοιμος να καταγράψει την εκάστοτε εντολή. Στο σημείο αυτό, το τηλεχειριστήριο της συσκευής στοχεύει προς τον εκπομπό και πατιέται το επιθυμητό πλήκτρο, ώστε το σήμα να καταγραφεί και να αποθηκευτεί στο σύστημα.Η παραπάνω διαδικασία εκμάθησης πρέπει να επαναληφθεί για κάθε επιθυμητή εντολή του τηλεχειριστηρίου που επιθυμούμε να ενσωματώσουμε στο σύστημα.

3.3: Παραμετροποίηση της αρχικης σελιδας (Lovelace)

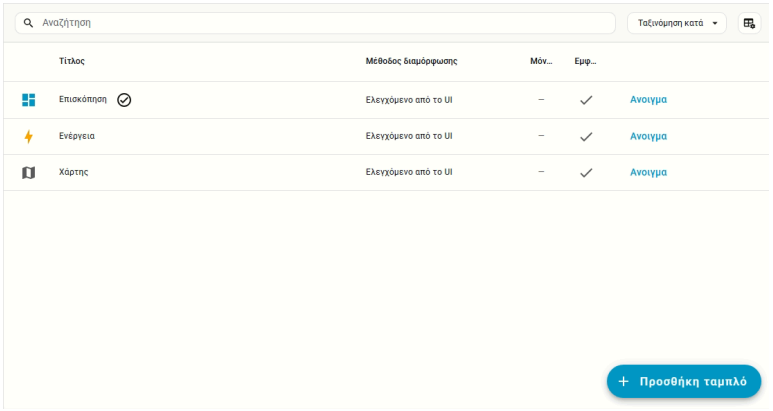


Εικόνα 3.15: Κεντρικό ταμπλό

Όπως παρατηρούμε, η αρχική σελίδα του Home Assistant (Lovelace UI) εμφανίζεται κενή, καθώς δεν έχει ακόμη διαμορφωθεί. Στο σημείο αυτό καλούμαστε να οργανώσουμε και να εντάξουμε όλες τις συσκευές που έχουμε προσθέσει, με τρόπο που να ανταποκρίνεται στις προσωπικές μας ανάγκες και προτιμήσεις. Η φιλοσοφία του Lovelace δίνει στον χρήστη τη δυνατότητα πλήρους παραμετροποίησης, τόσο σε επίπεδο διάταξης όσο και σε επίπεδο παρουσίασης δεδομένων, επιτρέποντας έτσι τη δημιουργία ενός πίνακα ελέγχου απόλυτα προσαρμοσμένου στο εκάστοτε σενάριο χρήσης.

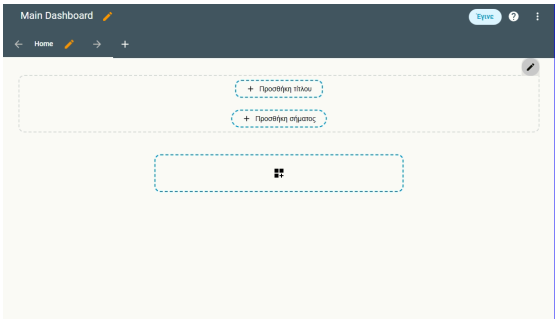
Στην παρούσα εργασία θα δημιουργήσουμε μία κεντρική σελίδα, στην οποία θα απεικονίζονται οι βασικές πληροφορίες που μας ενδιαφέρουν για την καθημερινή παρακολούθηση και διαχείριση του συστήματος. Συγκεκριμένα, θα τοποθετήσουμε τους διακόπτες που ελέγχουν τις συσκευές μας, θα

εμφανίσουμε τα δεδομένα κατανάλωσης ρεύματος, θα προσθέσουμε ένα πλαίσιο με τις τρέχουσες καιρικές συνθήκες και τέλος θα ενσωματώσουμε τις ενδείξεις των αισθητήρων μας, όπως του ανιχνευτή κίνησης και της παγίδας πόρτας. Με αυτόν τον τρόπο διαμορφώνεται ένα ολοκληρωμένο και λειτουργικό περιβάλλον, το οποίο παρέχει στον χρήστη άμεση και εύκολη εικόνα της κατάστασης του έξυπνου σπιτιού του.Πηγαίνοντας στις ρυθμίσεις και επιλέγοντας την κατηγορία «Ταμπλό», μας δίνεται η δυνατότητα να προσθέσουμε ένα νέο ταμπλό. Το συγκεκριμένο βήμα είναι απαραίτητο, καθώς το αρχικό ταμπλό με την ονομασία «Επισκόπηση» δεν είναι πλήρως παραμετροποιήσιμο και δεν προσφέρει την ευελιξία που απαιτείται για μια ολοκληρωμένη και προσωπικά διαμορφωμένη παρουσίαση. Για τον λόγο αυτό δημιουργούμε ένα νέο ταμπλό, το οποίο ονομάζουμε «Main Dashboard», ώστε να αποτελέσει την κεντρική σελίδα ελέγχου και απεικόνισης όλων των συσκευών και αυτοματισμών του συστήματός μας.



Εικόνα 3.16: Διαθέσιμες επιλογές ταμπλό

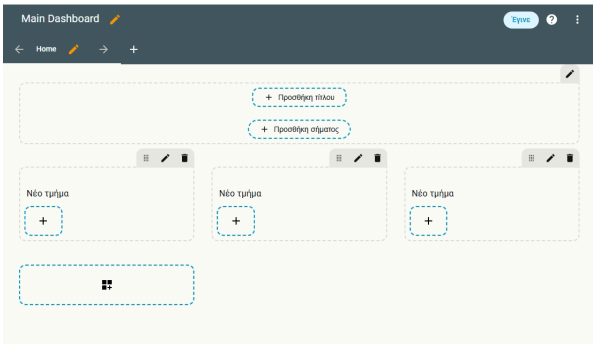
Έτσι λοιπόν, επιλέγουμε την εντολή «Προσθήκη ταμπλό» και δημιουργούμε ένα καινούριο, ξεκινώντας από το μηδέν, το οποίο ονομάζουμε *Main Dashboard*. Μόλις ολοκληρωθεί η δημιουργία, παρατηρούμε ότι στο αριστερό μενού του Home Assistant εμφανίζεται πλέον το νέο μας ταμπλό, το οποίο σε αυτή τη φάση είναι εντελώς κενό. Επιλέγοντάς το, μεταφερόμαστε στη νέα σελίδα, όπου έχουμε τη δυνατότητα να αρχίσουμε τη διαμόρφωση του περιβάλλοντος. Πατώντας το εικονίδιο του μολυβιού που βρίσκεται πάνω δεξιά, ενεργοποιείται η λειτουργία επεξεργασίας, μέσα από την οποία μπορούμε να προσθέσουμε κάρτες (cards), να οργανώσουμε τις συσκευές μας και να προσαρμόσουμε την εμφάνιση του ταμπλό σύμφωνα με τις ανάγκες μας.



Εικόνα 3.17: Διαδικασία παραμετροποίησης ταμπλό

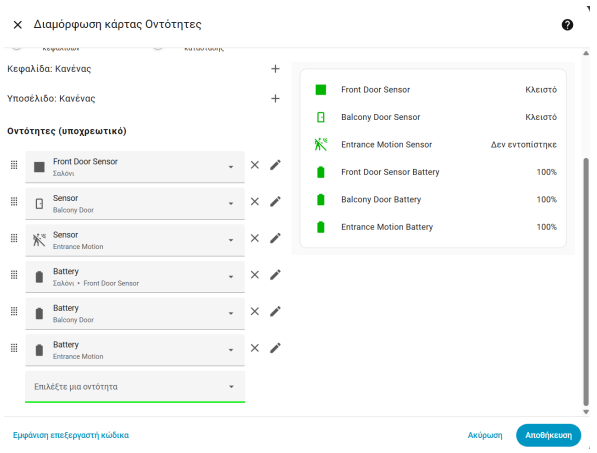
Στην παρούσα υλοποίηση επιλέγουμε να μην προσθέσουμε κεφαλίδα στο ταμπλό μας, καθώς η ύπαρξή της θα κατέλαβε πολύτιμο χώρο από την οθόνη και θα περιόριζε την ορατότητα σημαντικών πληροφοριών. Αντί αυτού, προχωρούμε στη δημιουργία ξεχωριστών τμημάτων μέσα στο Main

Dashboard, ώστε η παρουσίαση των δεδομένων να είναι όσο το δυνατόν πιο ευκρινής και οργανωμένη. Πατώντας στην επιλογή δημιουργίας νέων τμημάτων, προσθέτουμε τρία βασικά τμήματα: το πρώτο αφιερωμένο στους αισθητήρες κίνησης και επαφής (παγίδες), το δεύτερο για την παρακολούθηση των καταναλώσεων ενέργειας, και το τρίτο για τον έλεγχο των διακοπτών.



Εικόνα 3.18: Οργάνωση του ταμπλό

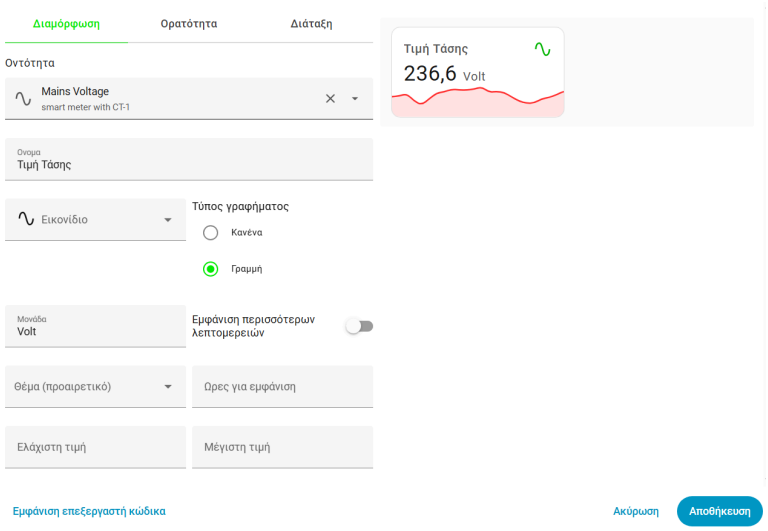
Σε κάθε ένα από τα τμήματα που δημιουργήθηκαν, είναι απαραίτητο να οριστεί ένα όνομα και να προστεθούν οι κατάλληλες κάρτες για την απεικόνιση των δεδομένων. Ξεκινώντας από το τμήμα που αφορά την εποπτεία της κατάστασης των αισθητήρων, επιλέγουμε το «Νέο τμήμα» και προχωρούμε στη μετονομασία του σύμφωνα με τις ανάγκες μας. Στη συνέχεια, πατώντας το σύμβολο **"+"**, μας παρέχεται η δυνατότητα προσθήκης καρτών, από τις οποίες επιλέγουμε την κάρτα «Οντότητες». Στο πεδίο των οντοτήτων καθορίζουμε ποιες θα εμφανίζονται στην κάρτα αυτή. Στην παρούσα εργασία επιλέγονται οι εξής: *front door sensor, balcony door sensor* και *entrance motion sensor*.Μετά την εισαγωγή τους, στην αριστερή πλευρά της οθόνης εμφανίζεται προεπισκόπηση της κάρτας, όπου μπορούμε να διαπιστώσουμε την τελική μορφή που θα έχει στην αρχική σελίδα. Επιπλέον, προσφέρεται η δυνατότητα να προστεθεί στην ίδια κάρτα και το ποσοστό φόρτισης των μπαταριών κάθε αισθητήρα, γεγονός που διευκολύνει την παρακολούθηση της αυτονομίας τους. Αυτό επιτυγχάνεται με την εισαγωγή τριών επιπλέον οντοτήτων, οι οποίες αντιστοιχούν στο επίπεδο μπαταρίας για τον κάθε αισθητήρα αντίστοιχα. Με τον τρόπο αυτό δημιουργείται μια ολοκληρωμένη εικόνα της κατάστασης και της λειτουργικότητας των συσκευών, σε μία ενιαία κάρτα του πίνακα ελέγχου.



Εικόνα 3.19: Παραμετροποίηση της κάρτας των αισθητήρων

Στο δεύτερο τμήμα του πίνακα ελέγχου, ενσωματώνονται τα γραφήματα που αφορούν τις μετρήσεις του μετρητή ηλεκτρικής ενέργειας, και συγκεκριμένα την τάση, την ένταση και την κατανάλωση. Η διαδικασία προσθήκης είναι παρόμοια με αυτήν που ακολουθήθηκε για τους αισθητήρες, με τη διαφορά ότι, αντί για την επιλογή της κάρτας «Οντότητες», επιλέγεται η κάρτα «Αισθητήρας».

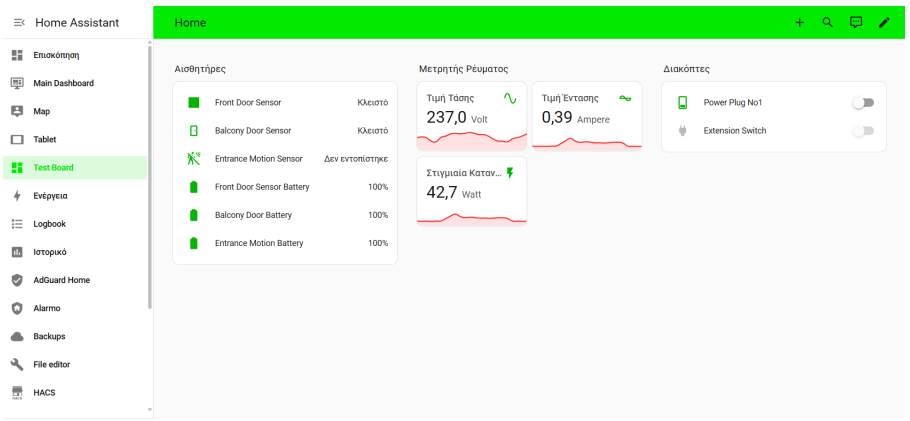
Αφού δημιουργηθεί η κάρτα, στο πεδίο της οντότητας επιλέγεται η μέτρηση της τάσης από τον μετρητή, δίνοντάς της ένα κατάλληλο όνομα για να εμφανίζεται στην κάρτα, καθώς και τη σωστή μονάδα μέτρησης, που στην περίπτωση αυτή είναι τα Volt (V). Η ίδια διαδικασία επαναλαμβάνεται για την ένταση του ρεύματος, με μονάδα μέτρησης τα Ampere (A), καθώς και για την κατανάλωση ενέργειας, με την αντίστοιχη μονάδα μέτρησης σε kilowatt-hours (kWh).Με αυτόν τον τρόπο, το τμήμα του πίνακα ελέγχου αποκτά δυναμική μορφή, προσφέροντας μια άμεση και ευδιάκριτη απεικόνιση των κρίσιμων ηλεκτρικών παραμέτρων του συστήματος. Τα γραφήματα αυτά παρέχουν στον χρήστη τη δυνατότητα παρακολούθησης σε πραγματικό χρόνο, αλλά και την ευχέρεια να εντοπίζει τυχόν ανωμαλίες ή αυξημένες καταναλώσεις που μπορεί να απαιτούν περαιτέρω διερεύνηση.



Εικόνα 3.20: Παραμετροποίηση της κάρτας του μετρητή ρεύματος

Στο τελευταίο τμήμα της διαμόρφωσης του πίνακα ελέγχου πραγματοποιείται η ενσωμάτωση των διακοπτών. Η διαδικασία υλοποιείται με τον ίδιο τρόπο όπως και στα προηγούμενα στάδια, μέσω της επιλογής του συμβόλου «+» για την προσθήκη νέας κάρτας και της επιλογής «Οντότητες». Στο συγκεκριμένο σημείο, αντί για αισθητήρες, εισάγονται οι αντίστοιχες οντότητες που αντιπροσωπεύουν τους διακόπτες του συστήματος.Για την παρούσα υλοποίηση προστέθηκαν οι οντότητες Extension Switch και Power Plug No1, οι οποίες επιτρέπουν την άμεση ενεργοποίηση ή απενεργοποίηση των συνδεδεμένων ηλεκτρικών συσκεύων. Με τον τρόπο αυτό ολοκληρώνεται η δημιουργία του τρίτου τμήματος, το οποίο λειτουργεί ως κεντρικό σημείο ελέγχου για τις βασικές συσκευές του συστήματος.

Κατόπιν της ολοκλήρωσης και αυτού του βήματος, η αρχική οθόνη (Main Dashboard) αποκτά πλήρη μορφή, περιλαμβάνοντας τις καταστάσεις των αισθητήρων, τα γραφήματα κατανάλωσης ενέργειας και τους διακόπτες. Το αποτέλεσμα είναι ένα ενιαίο και λειτουργικό περιβάλλον εποπτείας και ελέγχου, το οποίο παρέχει στον χρήστη την απαραίτητη πληροφόρηση αλλά και τα εργαλεία άμεσης παρέμβασης για τη διαχείριση του έξυπνου σπιτιού.



Εικόνα 3.21: Παράδειγμα ολοκληρωμένου ταμπλό

3.4: Εφαρμογή για το κινητό και geotracking

Αφού ολοκληρωθεί η διαμόρφωση της αρχικής σελίδας σύμφωνα με τις απαιτήσεις του χρήστη, το επόμενο βήμα αφορά τη σύνδεση της εφαρμογής Home Assistant σε κινητές συσκευές. Η χρήση της εφαρμογής είναι ιδιαίτερα σημαντική, καθώς πέρα από την παροχή απομακρυσμένης πρόσβασης, ενεργοποιεί και τη δυνατότητα παρακολούθησης της τοποθεσίας του χρήστη (location tracking). Η λειτουργία αυτή επιτρέπει τη δημιουργία αυτοματισμών που βασίζονται στη γεωγραφική θέση, όπως για παράδειγμα τον έλεγχο συσκευών ή την ενεργοποίηση σεναρίων όταν ο χρήστης βρίσκεται εντός ενός προκαθορισμένου νοητού κύκλου (geofence), ο οποίος ορίζεται μέσα από τις ρυθμίσεις του συστήματος. Η εφαρμογή διατίθεται επίσημα τόσο στο App Store (iOS) όσο και στο Google Play Store (Android), και η εγκατάστασή της είναι απλή και γρήγορη. Μετά την εγκατάσταση, ο χρήστης καλείται να πραγματοποιήσει είσοδο με τα στοιχεία του Home Assistant ώστε να ολοκληρωθεί η σύνδεση με το σύστημα του έξυπνου σπιτιού. Με αυτόν τον τρόπο, το κινητό τηλέφωνο εντάσσεται στο οικοσύστημα ως μία ακόμη συσκευή, παρέχοντας επιπλέον δυνατότητες αυτοματοποίησης και αυξάνοντας τον βαθμό εξατομίκευσης και ασφάλειας του συστήματος.

Μόλις η εφαρμογή του Home Assistant εγκατασταθεί στη συσκευή μας, την ανοίγουμε και ακολουθούμε τα απαραίτητα βήματα προκειμένου να επιτευχθεί η σύνδεση με το σύστημα. Σε πρώτο στάδιο, η εφαρμογή επιχειρεί να ανιχνεύσει την παρουσία του Home Assistant σε τοπικό επίπεδο, δηλαδή εντός του τοπικού δικτύου (LAN). Ωστόσο, στην παρούσα υλοποίηση δεν επιλέγεται αυτή η μέθοδος, καθώς ο στόχος είναι η απομακρυσμένη και ασφαλής πρόσβαση μέσω διαδικτύου, ανεξάρτητα από το αν η συσκευή βρίσκεται συνδεδεμένη στο οικιακό δίκτυο. Για τον σκοπό αυτό έχει ήδη υλοποιηθεί η ενσωμάτωση του Cloudflare Tunnel, Συνεπώς, επιλέγεται η χειροκίνητη εισαγωγή της διεύθυνσης του συστήματος. Στο σχετικό πεδίο πληκτρολογούμε το domain name που έχει παραμετροποιηθεί μέσω της υπηρεσίας Cloudflare, φροντίζοντας να δηλώσουμε ορθά το πρωτόκολλο επικοινωνίας (http ή https), καθώς χωρίς αυτό η σύνδεση δεν μπορεί να ολοκληρωθεί. Μετά την καταχώρηση της διεύθυνσης, η εφαρμογή μας μεταφέρει στη σελίδα εισόδου, όπου πραγματοποιείται η αυθεντικοποίηση με τα ίδια διαπιστευτήρια που χρησιμοποιούνται και στη διαδικτυακή έκδοση. Αμέσως μετά την επιτυχή σύνδεση, εμφανίζεται το ταμπλό που έχει ήδη διαμορφωθεί, δίνοντας στο χρήστη τη δυνατότητα να αλληλεπιδρά με το σύστημα από το κινητό του τηλέφωνο με τον ίδιο τρόπο όπως από τον υπολογιστή.

3.5: Δημιουργία αυτοματισμών

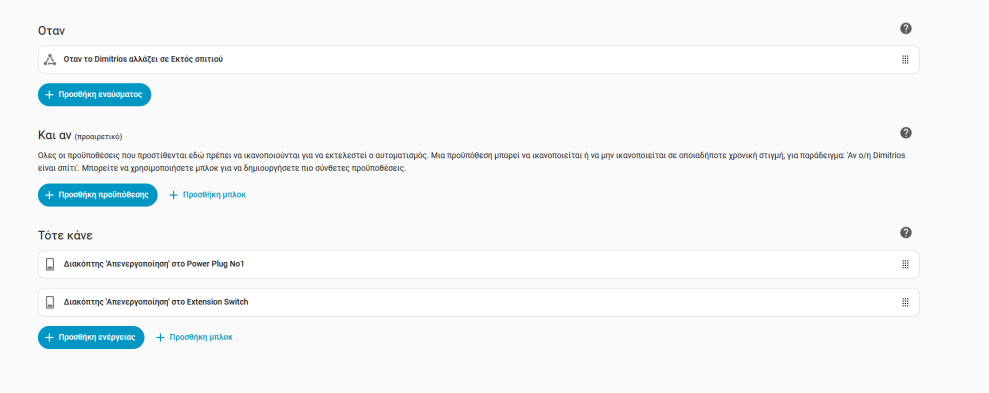
Η ενσωμάτωση της εφαρμογής του Home Assistant στην κινητή συσκευή δεν παρέχει μόνο την πρόσβαση στο γραφικό περιβάλλον και τη δυνατότητα ελέγχου των συσκευών, αλλά ενεργοποιεί και μια πρόσθετη λειτουργία: αυτή του geotracker. Μέσω του ενσωματωμένου GPS της συσκευής, το Home Assistant μπορεί να παρακολουθεί τη γεωγραφική θέση του χρήστη και να την εντάσσει σε αυτοματισμούς.

Με αυτόν τον τρόπο καθίσταται εφικτή η ενεργοποίηση ή απενεργοποίηση συσκευών και καταστάσεων, ανάλογα με την παρουσία ή απουσία του χρήστη σε έναν προκαθορισμένο γεωγραφικό χώρο. Ο μηχανισμός αυτός βασίζεται στη δημιουργία ενός νοητού κύκλου (geofence), ο οποίος ορίζεται μέσα από τις ρυθμίσεις του Home Assistant. Ο χρήστης μπορεί να καθορίσει την ακτίνα και το κέντρο αυτού του κύκλου, συνήθως στην τοποθεσία της κατοικίας ή του χώρου εργασίας. Στη συνέχεια, το σύστημα παρακολουθεί την είσοδο ή έξοδο από τον κύκλο αυτό και παράγει τα αντίστοιχα συμβάντα που μπορούν να χρησιμοποιηθούν ως συνθήκες σε αυτοματισμούς.

Στην παρούσα εργασία υλοποιούνται τρία διαφορετικά σενάρια αυτοματισμών, τα οποία αξιοποιούν την πληροφορία γεωεντοπισμού της κινητής συσκευής αλλά και τους αισθητήρες που έχουν ενταχθεί στο σύστημα. Στο πρώτο σενάριο, κάθε φορά που ο χρήστης απομακρύνεται από τον προκαθορισμένο νοητό κύκλο γύρω από την κατοικία του, ενεργοποιείται ένας μηχανισμός ο οποίος απενεργοποιεί αυτόματα όλους τους έξυπνους διακόπτες. Με τον τρόπο αυτό εξασφαλίζεται ότι συσκευές όπως φωτιστικά, πολύπριζα ή άλλες ηλεκτρικές εγκαταστάσεις δεν παραμένουν ανοιχτές χωρίς λόγο, γεγονός που συμβάλλει τόσο στη μείωση της κατανάλωσης ενέργειας όσο και στην ασφάλεια του χώρου. Στο δεύτερο σενάριο, αξιοποιείται ο μετρητής κατανάλωσης ρεύματος ώστε, όταν ο χρήστης αποχωρεί από το σπίτι, να πραγματοποιείται έλεγχος της τρέχουσας κατανάλωσης. Σε περίπτωση που αυτή ξεπερνά ένα προκαθορισμένο όριο, αποστέλλεται ειδοποίηση στην κινητή συσκευή του χρήστη, υποδεικνύοντας ότι πιθανόν έχει παραμείνει ενεργή κάποια συσκευή μεγάλης κατανάλωσης, όπως ο θερμοσίφωνας ή το κλιματιστικό. Έτσι, ο χρήστης μπορεί να παρέμβει απομακρυσμένα και να απενεργοποιήσει τη συσκευή μέσω του Home Assistant. Τέλος, στο τρίτο σενάριο, αξιοποιείται ο αισθητήρας επαφής που έχει τοποθετηθεί στην εξώπορτα. Εάν η πόρτα παραμείνει ανοικτή για χρονικό διάστημα μεγαλύτερο των πέντε λεπτών, το σύστημα αποστέλλει ειδοποίηση προκειμένου να ενημερώσει τον χρήστη για την κατάσταση αυτή. Η λειτουργία αυτή ενισχύει σημαντικά την ασφάλεια της οικίας, καθώς μειώνει τον κίνδυνο παραβίασης, ενώ ταυτόχρονα συμβάλλει στην αποφυγή απώλειας ενέργειας από την ανεπιθύμητη παραμονή της πόρτας ανοικτής.

Για τη δημιουργία ενός αυτοματισμού μέσα από το Home Assistant ακολουθούμε μία διαδικασία που βασίζεται στο γραφικό περιβάλλον χρήστη, γεγονός που καθιστά τον ορισμό των συνθηκών και των ενεργειών ιδιαίτερα κατανοητό και εύχρηστο. Συγκεκριμένα, μεταβαίνουμε στις ρυθμίσεις και στην καρτέλα των αυτοματισμών, όπου κάτω δεξιά επιλέγουμε τη δημιουργία νέου αυτοματισμού. Στη συνέχεια, μας εμφανίζεται η σελίδα διαμόρφωσης, όπου μέσα από το Graphical User Interface μπορούμε να συντάξουμε βήμα προς βήμα τον αυτοματισμό. Για την πρώτη περίπτωση, που αφορά το σενάριο απενεργοποίησης των διακοπτών όταν ο χρήστης απομακρύνεται από το σπίτι, ξεκινάμε με την παράμετρο “Όταν”. Εκεί ορίζουμε ως συνθήκη το geotracker της κινητής συσκευής, το οποίο πρέπει να ανιχνεύσει ότι η συσκευή έχει βγει εκτός της προκαθορισμένης ζώνης που αντιστοιχεί στην οικία.

Αμέσως μετά, προχωράμε στην ενότητα “Τότε”, όπου προσθέτουμε την ενέργεια που πρέπει να εκτελεστεί: την απενεργοποίηση του διακόπτη με την ονομασία “extention_switch” καθώς και του “power_plug”. Με αυτό τον τρόπο, κάθε φορά που ο χρήστης εγκαταλείπει τη ζώνη του σπιτιού, το σύστημα φροντίζει αυτόματα να κλείσει τις συγκεκριμένες συσκευές, εξασφαλίζοντας εξοικονόμηση ενέργειας και αυξημένο επίπεδο ασφάλειας. Στο γραφικό περιβάλλον, όλα τα παραπάνω αποτυπώνονται με σαφήνεια, καθώς ορίζεται πρώτα η συνθήκη αποχώρησης από την περιοχή και στη συνέχεια η ενέργεια της απενεργοποίησης των δύο διακοπτών, διαμορφώνοντας έναν πλήρη και απολύτως λειτουργικό αυτοματισμό.



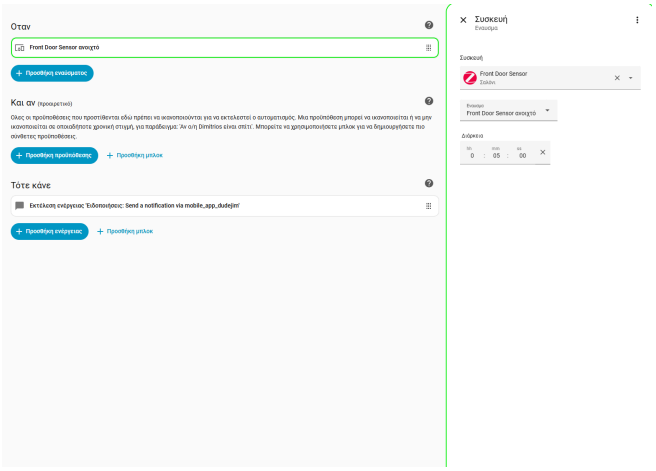
Εικόνα 3.22: Παραμετροποίηση του αυτοματισμού σε γραφικό περιβάλλον

Στη δεύτερη περίπτωση, που αφορά τη χρήση του μετρητή ρεύματος, η λογική του αυτοματισμού επικεντρώνεται στην παρακολούθηση της κατανάλωσης με στόχο την ειδοποίηση του χρήστη σε περίπτωση που παραμένει ενεργοβόρα συσκευή ανοικτή ενώ εκείνος λείπει από το σπίτι. Αρχικά, στη συνθήκη “Όταν” επιλέγουμε ως οντότητα τον μετρητή ρεύματος, ώστε ο αυτοματισμός να βασίζεται στις μετρήσεις του. Στην επόμενη επιλογή, “Τιμή κάτω από”, ορίζουμε ως κατώφλι τα 1.7 Ampere, ώστε να ανιχνεύεται αν υπάρχει συσκευή που συνεχίζει να καταναλώνει υψηλό ρεύμα. Ωστόσο, επειδή πολλές οικιακές συσκευές, όπως για παράδειγμα τα ψυγεία, μπορούν να τραβήξουν στιγμιαία μεγαλύτερο ρεύμα κατά την εκκίνηση του μοτέρ τους, είναι απαραίτητο να εισάγουμε και έναν χρονικό περιορισμό. Συγκεκριμένα, η συνθήκη πρέπει να ισχύει συνεχόμενα για τουλάχιστον πέντε λεπτά, ώστε να αποφεύγονται τα λεγόμενα “false positives”. Στη συνέχεια, στην ενότητα “Και αν” προσθέτουμε την παράμετρο που αφορά το geotracker της κινητής συσκευής, θέτοντας ως προϋπόθεση ότι το τηλέφωνο δεν πρέπει να βρίσκεται στη ζώνη του σπιτιού. Με αυτό τον τρόπο, ο αυτοματισμός θα λειτουργεί μόνο όταν ο χρήστης είναι εκτός οικίας. Τέλος, στην ενότητα “Τότε” καθορίζουμε την ενέργεια που θα εκτελείται, η οποία είναι η αποστολή ειδοποίησης στο κινητό τηλέφωνο μέσω της εφαρμογής του Home Assistant. Έτσι, σε περίπτωση που κάποια συσκευή με υψηλή κατανάλωση παραμείνει ενεργή ενώ το σπίτι είναι άδειο, ο χρήστης θα ενημερώνεται άμεσα. Σε μορφή YAML, η δομή αυτού του αυτοματισμού αποτυπώνεται ως εξής:

```yaml
alias: "Ease Of Life: Abnormal Current Draw When Away"
description: ""
triggers:
  - trigger: numeric_state
    entity_id:
      - sensor.mains_current
    for:
      hours: 0
      minutes: 5
      seconds: 0
    above: 1.7
conditions:
  - condition: state
    entity_id: person.dimitrios
    state: not_home
actions:
  - action: notify.mobile_app_dudejim
    metadata: {}
    data:
      message: >-
        The current draw is measured to be abnormal. You need to check the
        online devices!
      title: Abnormal Current Draw
      data:
        push:
          sound:
            name: default
            critical: 1
            volume: 1
mode: single
```

Εικόνα 3.23: Παραμετροποίηση του αυτοματισμού σε κώδικα YAML

Στην τρίτη περίπτωση ο αυτοματισμός έχει ως σκοπό την ενίσχυση της ασφάλειας της οικίας, μέσω της έγκαιρης ειδοποίησης σε περίπτωση που η εξώπορτα παραμείνει ανοικτή για μεγάλο χρονικό διάστημα. Η λογική είναι απλή αλλά εξαιρετικά χρήσιμη: Στη συνθήκη “Όταν” επιλέγεται ο αισθητήρας της εξώπορτας και τίθεται η παράμετρος ώστε να παραμείνει στην κατάσταση “ανοικτό” για χρονικό διάστημα μεγαλύτερο των πέντε λεπτών. Αυτό επιτρέπει να αγνοηθούν οι περιπτώσεις όπου η πόρτα ανοίγει στιγμιαία για είσοδο ή έξοδο, και να δοθεί έμφαση μόνο στις καταστάσεις πραγματικής αμέλειας. Στη συνέχεια, στην ενότητα “Τότε” ορίζεται η ενέργεια της αποστολής ειδοποίησης στο κινητό τηλέφωνο του χρήστη μέσω της εφαρμογής του Home Assistant, η οποία λειτουργεί ως υπενθύμιση ότι η πόρτα παραμένει ανοιχτή. Με αυτόν τον τρόπο αποτρέπεται ο κίνδυνος να μείνει η οικία εκτεθειμένη σε ανεπιθύμητες καταστάσεις.



Εικόνα 3.24: Παραμετροποίηση του αυτοματισμού σε γραφικό περιβάλλον

Κεφάλαιο 4ο: Συμπέρασμα

Το συμπέρασμα αυτής της πτυχιακής εργασίας συνοψίζει τη μελέτη, τον σχεδιασμό και την υλοποίηση ενός έξυπνου σπιτιού με τη χρήση του Raspberry Pi και του Home Assistant, με στόχο τη δημιουργία ενός ολοκληρωμένου συστήματος απομακρυσμένου ελέγχου και αυτοματισμών. Η τεχνολογία του Home Assistant αναδείχθηκε ως η πλέον ευέλικτη και ολοκληρωμένη πλατφόρμα για την ενοποίηση διαφορετικών συσκευών και πρωτοκόλλων, προσφέροντας δυνατότητες που δεν συναντώνται συνδυαστικά σε αντίστοιχα εμπορικά συστήματα. Ιδιαίτερη βαρύτητα δόθηκε στο κομμάτι της ασφάλειας, τόσο σε τοπικό επίπεδο μέσω μηχανισμών όπως τα one-time passwords και ο αποκλεισμός κακόβουλων IP διευθύνσεων, όσο και σε επίπεδο δημόσιας πρόσβασης μέσω της Cloudflare, η οποία λειτουργεί ως αξιόπιστος μεσάζοντας χωρίς την ανάγκη port forwarding ή εξάρτησης από ιδιόκτητα cloud τρίτων κατασκευαστών. Με τον τρόπο αυτό επιτυγχάνεται μέγιστη προστασία της ιδιωτικότητας και εξασφαλίζεται η απρόσκοπτη και ασφαλής πρόσβαση στο σύστημα από οπουδήποτε. Σε σύγκριση με παραδοσιακές λύσεις, η προτεινόμενη υλοποίηση υπερτερεί στον τομέα της ασφάλειας, της επεκτασιμότητας και της προσαρμοστικότητας, αποδεικνύοντας ότι μια ανοιχτή και παραμετροποιήσιμη πλατφόρμα όπως το Home Assistant, σε συνδυασμό με κατάλληλους μηχανισμούς ασφαλείας, μπορεί να αποτελέσει τη βάση για ένα πλήρως λειτουργικό και σύγχρονο έξυπνο σπίτι. Ενα ακόμη εξαιρετικά αξιέπαινο χαρακτηριστικό της υλοποίησης είναι το γεγονός ότι το σύστημα που αναπτύχθηκε δεν περιορίζεται στο υλικό (hardware) κάποιου συγκεκριμένου παρόχου. Σε αντίθεση με εμπορικά συστήματα, όπως οι συναγερμοί εταιρειών που βασίζονται σε κλειστές αρχιτεκτονικές και απαιτούν ανταλλακτικά αποκλειστικά από τον ίδιο κατασκευαστή, η προτεινόμενη λύση αξιοποιεί το πλεονέκτημα της συμβατότητας με πλήθος διαφορετικών τερματικών συσκευών. Από ανιχνευτές κίνησης και αισθητήρες έως διακόπτες και ενεργειακούς μετρητές, το σύστημα μπορεί να συνεργαστεί με προϊόντα διαφορετικών εταιρειών χωρίς περιορισμούς. Αυτό εξασφαλίζει όχι μόνο μεγαλύτερη ευελιξία στην επιλογή εξοπλισμού αλλά και χαμηλότερο κόστος συντήρησης και αναβάθμισης, καθιστώντας το σύστημα πιο βιώσιμο και μελλοντικά επεκτάσιμο.

Παρά τα πλεονεκτήματα της προτεινόμενης λύσης, δεν θα πρέπει να παραλείψουμε και τον περιοριστικό παράγοντα του βασικού συστήματος στο οποίο υλοποιήθηκε, δηλαδή το Raspberry Pi. Αν και αποτελεί μία εξαιρετικά οικονομική και ενεργειακά αποδοτική πλατφόρμα, το γεγονός ότι δεν έχει σχεδιαστεί εξαρχής για έντονη χρήση containerization δημιουργεί συγκεκριμένα μειονεκτήματα. Για παράδειγμα, όπως φάνηκε με την υλοποίηση του DNS server μέσω του AdGuard, κάθε container που εκτελείται παράλληλα με τον Home Assistant καταναλώνει πρόσθετους πόρους, οι οποίοι είναι περιορισμένοι στο Raspberry Pi. Σε περιπτώσεις όπου προβλέπεται μεγαλύτερη κλίμακα αυτοματισμών και αυξημένες ανάγκες σε επιδόσεις, μια πιο κατάλληλη λύση θα ήταν η φιλοξενία του Home Assistant σε συστήματα αρχιτεκτονικής ARM_64 ή ακόμα και σε έναν συμβατικό υπολογιστή γραφείου, που μπορεί να παρέχει περισσότερη υπολογιστική ισχύ και μεγαλύτερη σταθερότητα.

Αξιοσημείωτο είναι επίσης το γεγονός ότι, ενώ η επιλογή ενός open source λειτουργικού προσφέρει ορισμένα στιβαρά πλεονεκτήματα, συνοδεύεται και από συγκεκριμένες προκλήσεις. Από τη μία πλευρά, τέτοιου είδους λειτουργικά συστήματα και εφαρμογές υποστηρίζονται ενεργά από την κοινότητά τους, γεγονός που συνεπάγεται ότι η ανάπτυξη και η υποστήριξή τους δεν διακόπτονται σχεδόν ποτέ, ενώ οι λειτουργίες τους σχεδιάζονται με στόχο να ανταποκρίνονται στις πραγματικές ανάγκες των χρηστών. Από την άλλη πλευρά, το γεγονός ότι ο πηγαίος κώδικας είναι δημόσια διαθέσιμος σημαίνει ότι ενδέχεται να εντοπίζονται πιο εύκολα κενά ασφαλείας σε σύγκριση με κλειστά συστήματα. Για τον λόγο αυτό, η ασφάλεια επαφίεται σε μεγάλο βαθμό στον ίδιο τον

χρήστη, ο οποίος καλείται να λάβει τα απαραίτητα μέτρα, όπως έγινε και στην παρούσα υλοποίηση με τη χρήση μηχανισμών πρόσθετης προστασίας, σαν και αυτά που χρησιμοποιήσαμε παραπάνω.

Βιβλιογραφία

[1] Δικτύωση Υπολογιστών, 7η Έκδοση, James F. Kurose, Keith W. Ross.

[2] Wi-Fi 7 In Depth: Your guide to mastering Wi-Fi 7, the 802.11be protocol, and their deployment, Jerome Henry, Binita Gupta, Brian Hart, Malcolm Smith

[3] Your Introduction to Planning and Deploying CGNAT, NFware Team, NFware, 2024

[4] Raspberry Pi Foundation (2023). Getting Started with Raspberry Pi. Raspberry Pi Press.

[5] Richardson, M. & Wallace, S. (2012). Getting Started with Raspberry Pi. O'Reilly Media.

[6] Karagiannis, V., Chatzimisios, P., Vazquez-Gallego, F. & Alonso-Zarate, J. (2015). "A survey on application layer protocols for the Internet of Things". Transaction on IoT, 17(3),

[7] Home Assistant (2025). Home Assistant Documentation.

[8] ZHA (Zigbee Home Automation) (2024). ZHA Integration Documentation.

[9] Fouladi, B. & Ghanoun, S. (2013). "Security evaluation of ZigBee networks". Black Hat USA Conference.

[10] Cloudflare (2025). Cloudflare Tunnel Documentation.

[11] Stallings, W. (2020). Foundations of Modern Networking: SDN, NFV, QoE, IoT, and Cloud. Addison-Wesley.

[12] Hu, F., Hao, Q. & Bao, K. (2012). "A survey on software-defined network and OpenFlow: From concept to research to practice". IEEE Communications Surveys & Tutorials, 14(4),

[13] Rekhter, Y., Moskowitz, B., Karrenberg, D., Groot, G. & Lear, E. (1996). Address Allocation for Private Internets (RFC 1918). IETF.

[14] Srisuresh, P. & Egevang, K. (2001). Traditional IP Network Address Translator (NAT). RFC 3022. IETF.

[15] Comer, D. (2019). Internetworking with TCP/IP. 7th edn. Pearson.

[16] Lee, J., Bagheri, B. & Kao, H. (2015). "A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems". Manufacturing Letters, 3, pp. 18–23.

[17] Han, J., Choi, C. & Park, I. (2014). "Smart home energy management system using IEEE 802.15.4 and ZigBee". IEEE Transactions on Consumer Electronics, 60(2), pp. 198–202.

[18] Alaa, M., Zaidan, A., Zaidan, B., Talal, M. & Kiah, M. (2017). "A review of smart home applications based on Internet of Things". Journal of Network and Computer Applications, 97,

[19] Nabu Casa Inc. (2020). *Home Assistant Cloud*. https://www.nabucasa.com/

[20] Lahti, M. (2022). *Smart Home Automation with Home Assistant: A step-by-step guide to creating smart home automation solutions using Home Assistant*. Packt Publishing.

[21] ZigBee® Network Protocols and Applications, Chandrasekaran Vasudevan, CRC Press, 2016

[22] Infrared: Wireless Infrared Communications, John R. Barry, Springer, 2025

[23] RF: RF and Microwave Engineering: Fundamentals of Wireless Communications, Frank Gustrau, Wiley, 2023

[24] Bluetooth: Introducing Bluetooth® LE Audio 2nd Edition, Nick Hunn, Bluetooth SIG, 2025

[25] VPNs Illustrated: Tunnels, VPNs, and IPsec, Jon Snader ,Addison-Wesley ,2014

[26] Network Security, Firewalls, and VPNs, 3rd Edition, William Stallings, Pearson, 2020

[27] Linux Containers and Virtualization: A Kernel Perspective, Shashank Mohan Jain, Apress, October 14, 2020

[28] The Official Raspberry Pi Handbook 2024, Raspberry Pi Press, 2024

[29] Modern Sensors Handbook, Pavel Ripka, Alois Tipek, Wiley ,2022

[30] https://en.wikipedia.org/wiki/Amazon_Alexa

[31] https://en.wikipedia.org/wiki/Google_Home

Εικόνες:

[1.α] https://www.swissns.ch/site/2017/06/the-various-types-of-network-topologies/
[2.α] https://www.oxitsolutions.co.uk/blog/ieee-wifi-standards-cheat-sheet
[3.α] https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/
[4α] https://www.geeksforgeeks.org/computer-networks/introduction-and-ipv4-datagram-header/
[5.α] https://networkproguide.com/common-ports-cheat-sheet/
[6.α] https://www.pynetlabs.com/vlan-vs-subnet-whats-the-difference/
[7.α] https://ipcisco.com/lesson/dhcp-dynamic-host-configuration-protocol/
[8.α] https://en.wikipedia.org/wiki/Network_address_translation
[9.α]
https://www.mathworks.com/help/comm/ug/zigbee-frame-generation-and-decoding-for-general-commands.html
[10.α] https://www.minew.com/history-of-bluetooth/
[11.α] https://www.geeksforgeeks.org/computer-networks/bluetooth-frame-structure/

[12.α] https://www.appviewx.com/blogs/why-is-tls-1-3-better-and-safer-than-tls-1-2/
[13.α] https://www.linkedin.com/pulse/designing-network-topology-architecture-akinkunmi-pillot
[14.α] https://www.researchgate.net/figure/The-format-of-Firewall-rule_fig5_320685890
[15.α] https://www.docker.com/resources/what-container/
[16.α] https://cloudzy.com/blog/virtual-machine-vm-what-why-when/
[17.α] https://www.bmc.com/blogs/containers-vs-virtual-machines/
[18.α]https://kitronik.co.uk/blogs/resources/the-differences-between-raspberry-pi-4-model-b-raspberry-pi-5?srsltid=AfmBOoru84YS7TjYwoa1q95Xgtoz4XhYtomd5-GHArqbpJHa7fQrromE
[19.α] https://www.home-assistant.io
[20.α] https://self-learning-java-tutorial.blogspot.com/2018/06/yaml-represent-list-members.html
[21.α] https://sonoff.tech
[22.α] https://www.electronics-lab.com
[23.α] https://www.gw-style.com/product-p-623057.html
[24.α]
https://www.dentinstruments.com/blog/optimizing-performance-from-rogowski-coil-current-transformers/