



ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

**ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ**

**ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΜΗΧΑΝΙΚΗΣ ΥΠΟΛΟΓΙΣΤΩΝ, ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΔΙΚΤΥΩΝ**

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

**Έξυπνες Τεχνικές για την Εύρεση Σημείων Πρόσβασης σε
Δίκτυα 5^{ης} Γενιάς**

ΜΙΧΑΗΛ Ε. ΚΟΨΙΑΥΤΗΣ

Επιβλέπων: Λάζαρος Μεράκος, Καθηγητής

ΑΘΗΝΑ

ΙΟΥΛΙΟΣ 2020

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Έξυπνες Τεχνικές για την Εύρεση Σημείων Πρόσβασης σε Δίκτυα 5^{ης} Γενιάς

Μιχαήλ Ε. Κοψιαύτης
A.M.: EN2180006

ΕΠΙΒΛΕΠΩΝ: Λάζαρος Μεράκος, Καθηγητής

ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ: Ευστάθιος Χατζηευθυμιιάδης, Καθηγητής
Νίκος Πασσάς, ΕΔΙΠ

Ιούλιος 2020

ΠΕΡΙΛΗΨΗ

Σε ένα περιβάλλον πολλαπλών τεχνολογιών και επιπέδων δικτύωσης, τα κινητά τεμαχικά με δυνατότητες δικτύωσης με πολλές τεχνολογίες καλούνται να εντοπίζουν με μικρό κόστος και άμεσα τις επιλογές δικτύωσης τους (σε όρους σημείων πρόσβασης) και να επιλέγουν το καταλληλότερο σημείο πρόσβασης βάσει της υπηρεσίας που θέλουν να εξυπηρετήσουν. Στα πλαίσια της εργασίας αυτής, εξετάζουμε τις τεχνικές εύρεσης κυψέλης που υποστηρίζονται από υπάρχοντα πρότυπα δικτύωσης (3GPP LTE, LTE-Advanced, LTE Rel.15 and Beyond (5G), IEEE Wifi). Επίσης, μελετάμε τεχνικές βελτιστοποίησης για την μείωση του χρόνου που απαιτείται για την εύρεση κάποιου σημείου πρόσβασης και την εξοικονόμηση πόρων (πχ μείωση καθυστέρησης, βελτίωση ενεργειακής αποδοτικότητας) κατά την φάση εύρεσης κυψέλης.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Signal Communications and Processing

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: 3GPP, Wi-Fi, MIMO, OFDMA, SSID, Virtual Access Point, Authentication

ABSTRACT

In a multi-technology and multi-layer networking environment, multi-technology mobile terminals are required to identify their networking options at low cost and immediately (in terms of access points) and to select the most suitable access point based on the service they want to serve. In this work, we review the techniques used for finding cell locations, which are supported by existing networking standards (3GPP LTE, LTE-Advanced, LTE Rel.15 and Beyond (5G), IEEE Wi-Fi). We also study optimization techniques to reduce the time required to find an access point and to save resources (e.g. delay reduction, energy efficiency improvement) during the cell search phase.

SUBJECT AREA: Signal Communications and Processing

KEYWORDS: 3GPP, Wi-Fi, MIMO, OFDMA, SSID, Virtual Access Point, Authentication

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω θερμά τον κ. Διονύση Ξενάκη για τη σημαντική συμβολή του, για την εμπιστοσύνη που μου έδειξε εξ' αρχής, αναθέτοντάς μου το συγκεκριμένο θέμα, την επιστημονική του καθοδήγηση, τις υποδείξεις του και την υπομονή του κατά την ολοκλήρωση αυτής της Διπλωματικής εργασίας.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΡΟΛΟΓΟΣ	13
1. ΠΡΟΒΛΕΨΕΙΣ ΑΥΞΗΣΗΣ ΚΙΝΗΣΗΣ	15
1.1 Παγκόσμια υιοθέτηση του Internet και συσκευές.....	15
1.2 Αύξηση κινητικότητας και ταχύτητες κινητών επικοινωνιών	16
1.3 Παγκόσμια απόδοση δικτύου και τάσεις	18
1.3.1 Χρήστες, συσκευές και συνδέσεις.....	19
1.3.2 Αύξηση κινητικότητας παγκοσμίως.....	19
1.4 Δεδομένα ανά περιοχή	21
1.5 Δεδομένα κινητικότητας για την Ελλάδα	22
1.6 Καθορισμός εξέλιξης κυψελωτών δικτύων	23
1.6.1 Απόδοση δικτύου και εμπειρία χρήστη.....	25
1.7 Ανάγκη για την ανάπτυξη νέων συστημάτων κινητών επικοινωνιών	26
2. IEEE 802.11AX ΚΑΙ ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΣΥΣΤΗΜΑΤΟΣ WIFI	28
2.1 IEEE 802.11ax (Wi-Fi 6)	28
2.2 Τι είναι και τι περιλαμβάνει το νέο πρότυπο 802.11ax	30
2.2.1 Βασικά οφέλη του IEEE 802.11ax.....	30
2.2.2 Δυνατότητες του IEEE 802.11ax	31
2.2.3 Αύξηση ταχύτητας δεδομένων στο 802.11ax	32
2.3 Επιλογή σημείου πρόσβασης στο 802.11ax.....	33
2.4 Επισκόπηση τεχνολογικών δυνατοτήτων του IEEE 802.11ax	35
2.4.1 OFDMA - Orthogonal Frequency Division Multiple Access	35
2.4.2 Μετάδοση μορφής δέσμης (Transmit beamforming)	37
2.4.3 Target Wake Time.....	38
2.4.4 Χωρική επαναχρησιμοποίηση και λειτουργία Overlapping BSS (OBSS)	39
2.4.5 BSS Coloring	40
2.5 Αρχιτεκτονική εταιρικού ασύρματου δικτύου.....	42

2.6	Αρχιτεκτονική εταιρικού ασύρματου Cloud Based Controller	45
2.7	Έλεγχος πρόσβασης σε ένα ασύρματο δίκτυο.....	48
2.7.1	Radius Authentication	50
2.7.2	Local Authentication.....	52
2.7.3	Multifactor Authentication	52
2.8	Σύγκριση προτύπου 802.11ac και 802.11ax.....	52
2.9	Περίληψη	54
3.	ΠΕΡΙΦΡΑΦΗ LTE RELEASE 15 (5G) ΚΑΙ ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΣΥΣΤΗΜΑΤΟΣ	56
3.1	3GPP LTE RELEASE 15 (5G)	56
3.2	Προϋποθέσεις (Standards) ενός 5G Συστήματος	57
3.3	Επισκόπηση νέων τεχνολογιών συστήματος.....	60
3.3.1	Enhanced Mobile Broadband (eMBB).....	61
3.3.2	Ultra-Reliable and Low Latency Communications (URLCC).....	61
3.3.3	Massive Machine-Type Communications (mMTC)	62
3.3.4	Φάσμα και Συχνότητα	62
3.3.5	MEC	63
3.3.6	Beamforming.....	63
3.4	3GPP Phases	64
3.4.1	5G Φάση Πρώτη (Release 15)	64
3.4.2	5G Φάση Δεύτερη (Release 16).....	64
3.5	Ορολογία του 3GPP Release 15 (5G).....	65
3.6	Διαφορές από την 4G Αρχιτεκτονική.....	66
3.7	Οντότητες και διεπαφές δικτύου κορμού 5G	66
3.7.1	AMF - Access and Mobility Function.....	67
3.7.2	AUSF - Authentication Server Function.....	68
3.7.3	UDM - Unified Data Management.....	68
3.7.4	PCF - Policy Control Function	68
3.7.5	SMF - Session Management Function.....	68
3.7.6	UPF - User Plane Function.....	68
3.8	Σενάρια ανάπτυξης/ Επιλογές αρχιτεκτονικής 5G.....	69
3.8.1	Non-Standalone 5G	71

3.8.2	Standalone 5G	72
3.9	Διαδικασία αρχικής πρόσβασης του UE – Διαδικασία Εύρεσης Κυψέλης	76
3.9.1	Συγχρονισμός κατερχόμενης ζεύξης.....	78
3.9.2	Πληροφορίες συστήματος μετάδοσης	79
3.9.3	Συγχρονισμός ανερχόμενης ζεύξης	79
3.10	Έλεγχος πρόσβασης σε ένα 5G Network	79
3.10.1	Subscription Permanent Identifier (SUPI)	81
3.10.2	Subscription Concealed Identifier (SUCI)	82
3.10.3	Σημείο τερματισμού του επιπέδου του χρήστη (User Plane)	83
3.10.4	Έλεγχος ταυτότητας και εξουσιοδότηση	83
3.10.5	5G SIM	84
3.11	Σύγκριση 4G και 5G	84
3.12	Περίληψη	87
4.	ΕΙΚΟΝΙΚΟΠΟΙΗΣΗ ΔΙΚΤΥΟΥ ΚΑΙ ΔΗΜΙΟΥΡΓΙΑ OTT ΥΠΗΡΕΣΙΑΣ	87
4.1	Virtual Access Points	87
4.2	Πλήθος SSID που μπορεί να εκπέμψει ένα access point.....	88
4.2.1	Σελίδα RF φάσματος σε Cisco Meraki ασύρματο controller	88
4.3	Εικονικοποίηση δικτύου σε Cisco WLAN Management Controller.....	89
4.5	Διαδικασία δημιουργίας Over the Top σε Cisco εξοπλισμό.....	95
	ΠΙΝΑΚΑΣ ΟΡΟΛΟΓΙΑΣ	102
	ΑΝΑΦΟΡΕΣ	103

ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

ΕΙΚΟΝΑ 1, SUBSCRIPTION PENETRATION Q3 2019 (ΠΟΣΟΣΤΟ ΤΟΥ ΠΛΗΘΥΣΜΟΥ), ERICSSON MOBILITY REPORT 2019.....	16
ΕΙΚΟΝΑ 2, ΠΑΓΚΟΣΜΙΑ ΚΙΝΗΣΗ ΔΕΔΟΜΕΝΩΝ ΚΙΝΗΤΗΣ ΤΗΛΕΦΩΝΙΑΣ ΚΑΙ ΕΤΗΣΙΑ ΑΥΞΗΣΗ (ΕΒ ΑΝΑ ΜΗΝΑ), MOBILE TRAFFIC ONLY. ERICSSON MOBILITY REPORT 2019	17
ΕΙΚΟΝΑ 3, ΚΑΤΑΝΑΛΩΣΗ ΑΠΟ ΚΙΝΗΤΑ ΑΝΑ ΚΑΤΗΓΟΡΙΑ ΕΦΑΡΜΟΓΗΣ ΑΝΑ ΜΗΝΑ (ΠΟΣΟΣΤΟ), ERICSSON MOBILITY REPORT 2019.....	18
ΕΙΚΟΝΑ 4, ΠΑΓΚΟΣΜΙΑ ΑΝΑΠΤΥΞΗ ΔΙΑΔΙΚΤΥΟΥ, SOURCE: CISCO ANNUAL INTERNET REPORT, 2018-2023	19
ΕΙΚΟΝΑ 5, ΠΑΓΚΟΣΜΙΑ ΑΥΞΗΣΗ ΣΥΝΔΡΟΜΗΤΩΝ ΚΙΝΗΤΗΣ ΤΗΛΕΦΩΝΙΑΣ, SOURCE: CISCO ANNUAL INTERNET REPORT, 2018–2023	20
ΕΙΚΟΝΑ 6, ΠΑΓΚΟΣΜΙΑ ΑΝΑΠΤΥΞΗ ΚΙΝΗΤΩΝ ΣΥΣΚΕΥΩΝ ΚΑΙ ΣΥΝΔΕΣΕΩΝ, SOURCE: CISCO ANNUAL INTERNET REPORT, 2018–2023	21
ΕΙΚΟΝΑ 7, ΔΕΔΟΜΕΝΑ ΧΡΗΣΗΣ ΣΤΗΝ ΕΛΛΑΔΑ, SOURCE HOOTSUITE	22
ΕΙΚΟΝΑ 8, ΧΡΗΣΗ ΚΙΝΗΤΩΝ ΣΥΣΚΕΥΩΝ ΣΤΗΝ ΕΛΛΑΔΑ, SOURCE HOOTSUITE	22
ΕΙΚΟΝΑ 9, ΧΡΗΣΗ ΔΙΑΔΙΚΤΥΟΥ ΜΕΣΩ ΚΙΝΗΤΩΝ ΣΥΣΚΕΥΩΝ, SOURCE HOOTSUITE	23
ΕΙΚΟΝΑ 10, ΚΙΝΗΤΕΣ ΣΥΝΔΕΣΕΙΣ ΑΝΑ ΤΥΠΟ, SOURCE HOOTSUITE	23
ΕΙΚΟΝΑ 11, ΠΑΓΚΟΣΜΙΑ ΑΝΑΠΤΥΞΗ ΚΙΝΗΤΩΝ ΣΥΣΚΕΥΩΝ ΚΑΙ ΣΥΝΔΕΣΕΩΝ, SOURCE: CISCO ANNUAL INTERNET REPORT, 2018–2023	24
ΕΙΚΟΝΑ 12, ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ ΚΑΙ ΕΞΕΛΙΞΗ ΤΩΝ ΕΝΣΥΡΜΑΤΩΝ ΚΑΙ ΑΣΥΡΜΑΤΩΝ ΤΕΧΝΟΛΟΓΙΩΝ, SOURCE: CISCO ANNUAL INTERNET REPORT, 2018–2023.....	25
ΕΙΚΟΝΑ 13, IMT 2020 ΒΑΣΙΚΕΣ ΚΑΤΕΥΘΥΝΣΕΙΣ ΑΝΑΠΤΥΞΗΣ ΤΟΥ 5G	27
ΕΙΚΟΝΑ 14, SOURCE ARUBA NETWORKS	30
ΕΙΚΟΝΑ 15 CISCO, ΥΠΟΛΟΓΙΖΟΝΤΑΣ ΤΗΝ ΤΑΧΥΤΗΤΑ ΤΟΥ 802.11AC ΚΑΙ ΤΟΥ 802.11AX.....	32
ΕΙΚΟΝΑ 16 TRIGGER FRAME	34
ΕΙΚΟΝΑ 17 TRIGGER FRAME	34
ΕΙΚΟΝΑ 18 Το OFDMA ΣΤΟ Wi-Fi 6 ΕΠΙΤΡΕΠΕΙ ΣΕ ΠΟΛΛΟΥΣ ΧΡΗΣΤΕΣ ΜΕ ΔΙΑΦΟΡΕΤΙΚΑ ΠΡΟΦΙΛ ΚΥΚΛΟΦΟΡΙΑΣ ΝΑ ΜΕΤΑΔΙΔΟΥΝ ΤΑΥΤΟΧΡΟΝΑ ΜΕΣΩ ΤΟΥ ΙΔΙΟΥ ΚΑΝΑΛΙΟΥ.....	35
ΕΙΚΟΝΑ 19 OFDM vs OFDMA BLOCK	36
ΕΙΚΟΝΑ 20 MULTI-USER MULTIPLE INPUT, MULTIPLE OUTPUT.....	37
ΕΙΚΟΝΑ 21 ΛΕΙΤΟΥΡΓΙΑ ΤΟΥ TARGET WAKEUP TIME (TWT).....	38
ΕΙΚΟΝΑ 22 ΛΕΙΤΟΥΡΓΙΑ BSS COLORING	40
ΕΙΚΟΝΑ 23 ΛΕΙΤΟΥΡΓΙΑ BSS COLORING, ΕΥΡΕΣΗ ΣΥΓΚΡΟΥΣΗΣ	41
ΕΙΚΟΝΑ 24 SOURCE ARUBA NETWORKS	41
ΕΙΚΟΝΑ 25 ΛΟΓΙΚΗ ΔΙΑΣΥΝΔΕΣΗ ΕΝΟΣ ACCESS POINT	43
ΕΙΚΟΝΑ 26 ΙΕΡΑΡΧΙΑ ΕΝΟΣ ΔΙΚΤΥΟΥ	43
ΕΙΚΟΝΑ 27 ΣΥΝΔΕΣΗ ΧΡΗΣΤΗ ΣΤΟ ACCESS LAYER.....	44
ΕΙΚΟΝΑ 28 ΑΡΧΙΤΕΚΤΟΝΙΚΗ CLOUD CONTROLLER.....	47
ΕΙΚΟΝΑ 29 ΣΧΕΔΙΑΣΜΟΣ ΤΟΥ WLANMAN ΥΠΟΣΥΣΤΗΜΑΤΟΣ ΣΤΟΝ ONOS CONTROLLER.....	47
ΕΙΚΟΝΑ 30 THE TOPOLOGY INDICATING THE AAA MECHANISMS USING THE EAP AUTHENTICATION PROTOCOL.....	49
ΕΙΚΟΝΑ 31 ΑΛΛΗΛΟΥΧΙΑ ΕΠΙΚΟΙΝΩΝΙΩΝ ΜΕΤΑΞΥ RADIUS SERVER ΚΑΙ CLIENT	51
ΕΙΚΟΝΑ 32 1024-QAM vs 256-QAM	53
ΕΙΚΟΝΑ 33 802.11ac vs 802.11ax ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ.....	54
ΕΙΚΟΝΑ 34 ΠΛΕΟΝΕΚΤΗΜΑΤΑ ΤΟΥ 802.11AX.....	55
ΕΙΚΟΝΑ 35 5G RAN ΚΑΙ CORE ΔΙΚΤΥΟ	57
ΕΙΚΟΝΑ 36 IMT-2020 STANDARD.....	58
ΕΙΚΟΝΑ 37 IMT- 2020 ΕΛΑΧΙΣΤΕΣ ΑΠΑΙΤΗΣΕΙΣ	58
ΕΙΚΟΝΑ 38 ΑΠΑΙΤΗΣΕΙΣ ΠΟΥ ΚΑΘΟΔΗΓΟΥΝ ΤΗΝ ΑΡΧΙΤΕΚΤΟΝΙΚΗ 5G	59
ΕΙΚΟΝΑ 39 IMT 2020 ΒΑΣΙΚΕΣ ΚΑΤΕΥΘΥΝΣΕΙΣ ΑΝΑΠΤΥΞΗΣ ΤΟΥ 5G.....	61

ΕΙΚΟΝΑ 40 ΛΟΓΙΚΗ ΔΙΑΣΥΝΔΕΣΗ 5G RAN ΜΕ 5G CORE ΔΙΚΤΥΟ	62
ΕΙΚΟΝΑ 41 BEAMFORMING	63
ΕΙΚΟΝΑ 42 ΣΥΣΤΑΤΙΚΑ ΜΕΡΗ - ΛΕΙΤΟΥΡΓΙΕΣ ΤΟΥ 5G CORE	67
ΕΙΚΟΝΑ 43 END-TO-END 5G ΑΡΧΙΤΕΚΤΟΝΙΚΗ	69
ΕΙΚΟΝΑ 44 5G ΕΠΙΠΕΔΑ ΠΡΟΣΒΑΣΗ, ΠΡΟΩΘΗΣΗΣ ΚΑΙ ΕΛΕΓΧΟΥ	70
ΕΙΚΟΝΑ 45 NON-STANDALONE & STANDALONE ΑΡΧΙΤΕΚΤΟΝΙΚΗ.....	71
ΕΙΚΟΝΑ 46 NON-STANDALONE & STANDALONE ΑΡΧΙΤΕΚΤΟΝΙΚΗ.....	74
ΕΙΚΟΝΑ 47 3GPP RELEASE 18 TIMEPLAN.....	75
ΕΙΚΟΝΑ 48 3GPP 5G TIMELINE	76
ΕΙΚΟΝΑ 49 GROUP-BASED ΑΡΧΙΚΑ ΚΕΡΔΗ ΠΡΟΣΒΑΣΗΣ ΣΕ ΣΧΕΣΗ ΜΕ ΤΗ ΜΕΣΗ ΜΕΙΩΣΗ ΤΟΥ ΡΥΘΜΟΥ ΣΥΓΚΡΟΥΣΗΣ.....	77
ΕΙΚΟΝΑ 50 ΑΡΧΙΚΗ ΠΡΟΣΒΑΣΗ ΜΕ ΥΠΟΒΟΗΘΟΥΜΕΝΗ ΣΥΧΝΟΤΗΤΑ ΣΕ ΕΤΕΡΟΓΕΝΕΣ ΔΙΚΤΥΟ	78
ΕΙΚΟΝΑ 51 4G vs 5G ΡΟΗ ΚΥΚΛΟΦΟΡΙΑΣ ΑΡΧΙΤΕΚΤΟΝΙΚΗΣ ΑΣΦΑΛΕΙΑΣ	81
ΕΙΚΟΝΑ 52 SUPR FRAME	82
ΕΙΚΟΝΑ 53 SUCI FRAME	82
ΕΙΚΟΝΑ 54 SUBSCRIBER IDENTIFICATION MECHANISM	82
ΕΙΚΟΝΑ 55 ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΑΣΦΑΛΕΙΑΣ 5G ΚΑΙ ΑΠΕΙΚΟΝΙΣΗ ΔΙΕΠΑΦΩΝ	83
ΕΙΚΟΝΑ 56 ΣΥΓΚΡΙΣΗ ΔΥΝΑΤΟΤΗΤΩΝ 4G ΚΑΙ 5G.....	85
ΕΙΚΟΝΑ 57 ΣΥΓΚΡΙΣΗ ΔΥΝΑΤΟΤΗΤΩΝ ΑΠΟΔΟΤΙΚΟΤΗΤΑΣ ΚΑΙ ΜΕΓΙΣΤΟΥ ΡΥΘΜΟΥ ΜΕΤΑΔΟΣΗΣ ΜΕΤΑΞΥ 4G ΚΑΙ 5G	85
ΕΙΚΟΝΑ 58 ΣΥΓΚΡΙΣΗ ΧΡΟΝΟΥ ΚΑΘΥΣΤΕΡΗΣΗΣ ΜΕΤΑΞΥ 4G ΚΑΙ 5G.....	85
ΕΙΚΟΝΑ 59 ΣΥΓΚΡΙΣΗ ΚΙΝΗΤΙΚΟΤΗΤΑΣ ΚΑΙ ΑΛΛΑΓΗΣ ΚΥΨΕΛΗΣ ΜΕΤΑΞΥ 4G ΚΑΙ 5G.....	86
ΕΙΚΟΝΑ 60 ΣΕΛΙΔΑ ΑΠΕΙΚΟΝΙΣΗΣ ΠΑΡΕΜΒΟΛΩΝ ΣΤΟΝ WIRELESS CONTROLLER CISCO MERAKI, SOURCE: CHANNEL PLANNING BEST PRACTICES, CISCO MERAKI.....	89
ΕΙΚΟΝΑ 61 ΔΙΑΜΟΡΦΩΣΗ SSID (1).....	91
ΕΙΚΟΝΑ 62 ΔΙΑΜΟΡΦΩΣΗ SSID (2).....	92
ΕΙΚΟΝΑ 63 ΔΙΑΜΟΡΦΩΣΗ SSID (3).....	93
ΕΙΚΟΝΑ 64 ΔΙΑΜΟΡΦΩΣΗ SSID (4).....	94
ΕΙΚΟΝΑ 65 ΔΙΑΜΟΡΦΩΣΗ SSID (5).....	94
ΕΙΚΟΝΑ 66 ΑΡΧΙΤΕΚΤΟΝΙΚΗ CAPTIVE PORTAL ΚΑΙ SOCIAL ID	95
ΕΙΚΟΝΑ 67 ΡΥΘΜΙΣΗ ΤΟΥ ΑΣΥΡΜΑΤΟΥ CONTROLLER ΓΙΑ ΑΝΑΚΑΤΕΥΘΥΝΣΗ ΤΟΥ ΧΡΗΣΤΗ ΣΤΗΝ ΣΕΛΙΔΑ ΤΟΥ CAPTIVE PORTAL (1)	96
ΕΙΚΟΝΑ 68 ΡΥΘΜΙΣΗ ΤΟΥ ΑΣΥΡΜΑΤΟΥ CONTROLLER ΓΙΑ ΑΝΑΚΑΤΕΥΘΥΝΣΗ ΤΟΥ ΧΡΗΣΤΗ ΣΤΗΝ ΣΕΛΙΔΑ ΤΟΥ CAPTIVE PORTAL (2)	97
ΕΙΚΟΝΑ 69 ΡΥΘΜΙΣΗ ΤΟΥ ΑΣΥΡΜΑΤΟΥ CONTROLLER ΓΙΑ ΑΝΑΚΑΤΕΥΘΥΝΣΗ ΤΟΥ ΧΡΗΣΤΗ ΣΤΗΝ ΣΕΛΙΔΑ ΤΟΥ CAPTIVE PORTAL (3)	98
ΕΙΚΟΝΑ 70 ΡΥΘΜΙΣΗ ΤΟΥ ΑΣΥΡΜΑΤΟΥ CONTROLLER ΓΙΑ ΑΝΑΚΑΤΕΥΘΥΝΣΗ ΤΟΥ ΧΡΗΣΤΗ ΣΤΗΝ ΣΕΛΙΔΑ ΤΟΥ CAPTIVE PORTAL (4)	98

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΠΙΝΑΚΑΣ 1 802.11AC VS 802.11AX	53
ΠΙΝΑΚΑΣ 2 ΣΥΓΚΡΙΣΗ ΤΕΧΝΙΚΩΝ ΠΡΟΔΙΑΓΡΑΦΩΝ ΜΕΤΑΞΥ LTE ΚΑΙ NR	86
ΠΙΝΑΚΑΣ 3 ΑΝΤΙΣΤΟΙΧΙΣΗ ΟΝΟΜΑΤΟΔΟΣΙΑΣ ΣΤΟΙΧΕΙΩΝ ΜΕΤΑΞΥ 4G ΚΑΙ 5G	86

ΠΡΟΛΟΓΟΣ

Η Διπλωματική εργασία διενεργήθηκε στο πλαίσιο ολοκλήρωσης του Μεταπτυχιακού Προγράμματος Σπουδών Μηχανικής Υπολογιστών, Τηλεπικοινωνιών και Δικτύων του Εθνικού και Καποδιστριακού Πανεπιστημίου Αθηνών.

ΕΙΣΑΓΩΓΗ

Η ανάπτυξη των κινητών και ασύρματων δικτύων πέμπτης γενιάς (5G) έχει προχωρήσει με ταχείς ρυθμούς. Το Wi-Fi εξελίσσεται, οδηγείται από περισσότερες συσκευές, περισσότερες συνδέσεις και εφαρμογές με μεγαλύτερη ευρυζωνικότητα. Στο άμεσο μέλλον τα δίκτυα θα χρειάζονται περισσότερη ασύρματη χωρητικότητα και αξιοπιστία. Εκεί μπαίνει η έκτη γενιά Wi-Fi, το IEEE 802.11ax, γνωστό και ως Wi-Fi 6, και το 3GPP LTE Release 15 (5G), τα οποία επιτρέπουν σε επιχειρήσεις και παρόχους υπηρεσιών να υποστηρίζουν νέες και αναδυόμενες εφαρμογές, παρέχοντας ταυτόχρονα υψηλότερη ποιότητα υπηρεσιών. Το IEEE 802.11ax δίνει τη δυνατότητα στα access points να υποστηρίζουν περισσότερους χρήστες και σε πιο πυκνά περιβάλλοντα δικτύωσης, πιο πυκνή κάλυψη και μικρότερη απόσταση τοποθέτησης μεταξύ των access points, έχοντας σαν αποτέλεσμα την παροχή μίας καλύτερης εμπειρίας για τους χρήστες των ασύρματων δικτύων. Εξασφαλίζει επίσης, πιο προβλέψιμη απόδοση για προηγμένες εφαρμογές, όπως 4K video, Ultra HD και Internet of Things (IoT). Τα 5G δίκτυα αναμένεται να ανταποκριθούν στις απαιτήσεις μιας κινητής και πλήρως συνδεδεμένης κοινωνίας. Ο πολλαπλασιασμός των συνδεδεμένων αντικειμένων και συσκευών θα ανοίξει τον δρόμο σε ένα ευρύ φάσμα νέων υπηρεσιών και σε συναφή επιχειρηματικά μοντέλα που θα επιτρέψουν την αυτοματοποίηση σε διάφορους τομείς της βιομηχανίας και στις κάθετες αγορές (πχ την ενέργεια, την ηλεκτρονική υγεία, την έξυπνη πόλη, τα συνδεδεμένα αυτοκίνητα, τη βιομηχανική παραγωγή κ.λπ.). Εκτός από τις πιο διαδεδομένες ανθρώπινες κεντρικές εφαρμογές, όπως η αύξηση της εικονικής και επαυξημένης πραγματικότητας, 4k video, κλπ., τα δίκτυα 5G θα υποστηρίξουν τις επικοινωνιακές ανάγκες των εφαρμογών τύπου μηχανή-σε-μηχανή και μηχανή-σε-ανθρώπινο είδος για να καταστήσουν τη ζωή μας πιο ασφαλή και πιο βολική.

1. ΠΡΟΒΛΕΨΕΙΣ ΑΥΞΗΣΗΣ ΚΙΝΗΣΗΣ

Καθώς όλο και περισσότερες συσκευές, από ένα ρολόι χειρός, ένα ψυγείο έως και ένα αυτοκίνητο, αποκτούν την δυνατότητα να συνδεθούν στο διαδίκτυο οι δυνατότητες και η χωρητικότητα των υφιστάμενων δικτύων αρχίζουν και μειώνονται. Καθώς η παγκόσμια δικτυακή κίνηση αυξάνει συνεχώς τα δίκτυα επικοινωνιών φτάνουν στα όριά τους. Επίσης με την εισαγωγή των IoT συσκευών και των συνδεδεμένων οχημάτων αλλάζει και ο τρόπος με τον οποίο γίνεται η αίτηση πρόσβασης σε ένα δίκτυο επικοινωνιών. Παρακάτω θα συζητηθεί η αύξηση του όγκου των δεδομένων κυρίως στα ασύρματα δίκτυα και με ποιόν τρόπο αυτή η αύξηση επιφέρει μία ανάγκη για εισαγωγή νέων συστημάτων και τεχνολογιών στα δίκτυα επικοινωνιών.

1.1 Παγκόσμια υιοθέτηση του Internet και συσκευές

Αναφορικά, με την αλματώδη αύξηση του όγκου των δεδομένων, εκτιμάται ότι οι χρήστες του Διαδικτύου έως το 2023 θα φτάνουν σχεδόν τα δύο τρίτα του παγκόσμιου πληθυσμού. Πιο συγκεκριμένα, υπολογίζεται ότι θα υπάρχουν συνολικά 5,3 δισεκατομμύρια χρήστες του Διαδικτύου (66 % του παγκόσμιου πληθυσμού) έως το 2023, από 3,9 δισεκατομμύρια (51 % του παγκόσμιου πληθυσμού) που ήταν το 2019.

- **Συσκευές και συνδέσεις**

Ο αριθμός των συσκευών που συνδέονται στα δίκτυα IP αναμένεται πως θα είναι τριπλάσιος από τον παγκόσμιο πληθυσμό έως το 2023. Θα υπάρχουν 3,6 δικτυακές συσκευές κατά κεφαλή έως το 2023, από 2,4 δικτυακές συσκευές κατά κεφαλή που είχαν καταγραφεί το 2018. Θα υπάρξουν 29,3 δισεκατομμύρια δικτυακές συσκευές έως το 2023, συγκριτικά με τις 18,4 δισεκατομμύρια το 2018. [1]

- **Οι συνδέσεις M2M θα είναι οι μισές από τις παγκόσμιες συνδεδεμένες συσκευές και συνδέσεις έως το 2023**

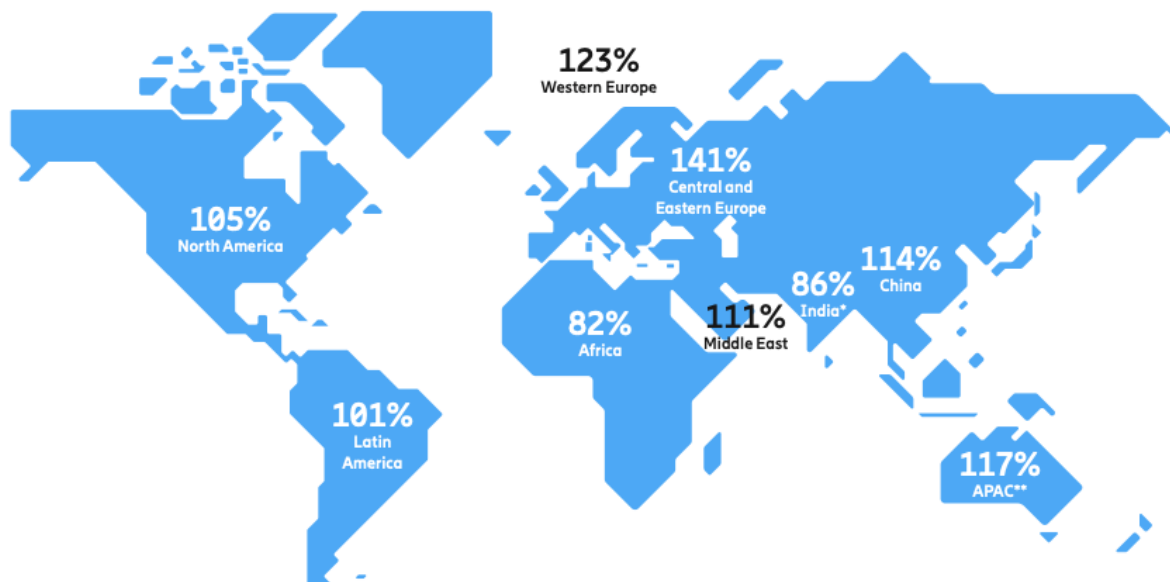
Το ποσοστό των συνδέσεων Machine-to-Machine (M2M) υπολογίζεται ότι θα αυξηθεί από 33% βάσει των δεδομένων του 2018 σε 50% έως το 2023. Επίσης, αναμένεται πως θα υπάρξουν 14,7 δισεκατομμύρια συνδέσεις M2M έως το 2023. [1]

- **Internet of Things (IoT)**

Στην κατηγορία συνδέσεων M2M (η οποία αναφέρεται επίσης ως IoT), οι συνδεδεμένες οικιακές εφαρμογές υπολογίζεται ότι θα έχουν το μεγαλύτερο μερίδιο κατανάλωσης δεδομένων και το συνδεδεμένο αυτοκίνητο θα είναι ο ταχύτερα αναπτυσσόμενος τύπος εφαρμογής. Οι συνδεδεμένες οικιακές εφαρμογές θα έχουν σχεδόν το ήμισυ ή το 48% του μεριδίου M2M έως το 2023 και οι εφαρμογές συνδεδεμένων αυτοκινήτων θα αυξηθούν ταχύτερα, στο 30% του Σύνθετου Ετήσιου Ρυθμού Ανάπτυξης, Compound Annual Growth (CAGR), κατά την περίοδο πρόβλεψης (2018 - 2023). [1]

1.2 Αύξηση κινητικότητας και ταχύτητες κινητών επικοινωνιών

Σε παγκόσμιο επίπεδο, η μέση ταχύτητα σύνδεσης δικτύου κινητής τηλεφωνίας το 2018 ήταν 13,2 Mbps. Η μέση ταχύτητα υπολογίζεται πως θα υπερδιπλασιαστεί και αναμένεται να είναι 43,9 Mbps έως το 2023. Ο συνολικός αριθμός συνδρομών για κινητά ήταν περίπου 8 δισεκατομμύρια το τρίτο τρίμηνο του 2019, με 61 εκατομμύρια συνδρομές να προστίθενται κατά τη διάρκεια του τριμήνου.



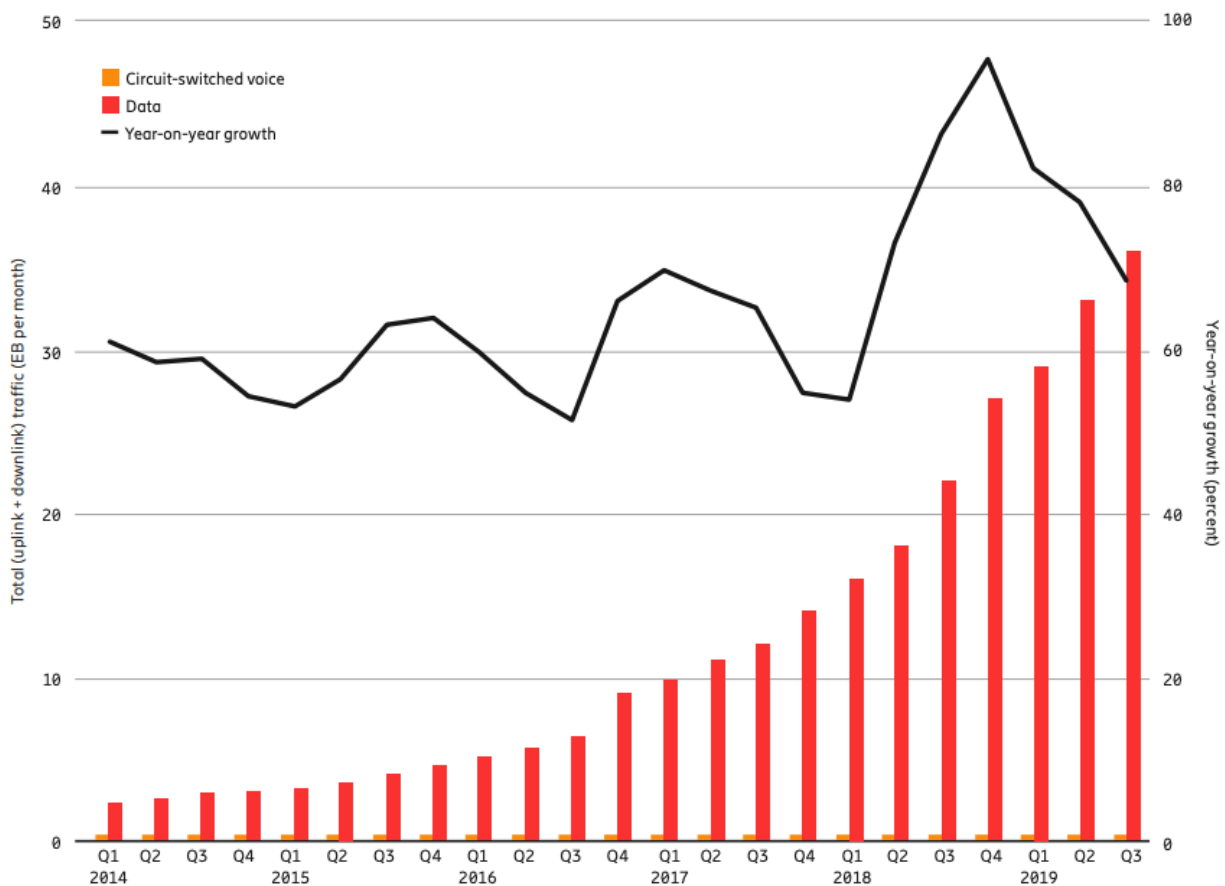
Εικόνα 1, Subscription penetration Q3 2019 (ποσοστό του πληθυσμού), Ericsson Mobility Report 2019

Πάνω από το 70% του παγκόσμιου πληθυσμού θα έχει συνδεσιμότητα μέσω κινητού έως το 2023. Ο συνολικός αριθμός των παγκόσμιων συνδρομητών κινητής τηλεφωνίας αναμένεται πως θα αυξηθεί από 5,1 δισεκατομμύρια (66% του πληθυσμού) το 2018 σε 5,7 δισεκατομμύρια (71% του πληθυσμού) έως το 2023. Οι 5G συσκευές και συνδέσεις θα είναι πάνω από το 10% των παγκόσμιων κινητών συσκευών και συνδέσεων έως το 2023. Μέχρι το 2023, οι παγκόσμιες φορητές συσκευές υπολογίζεται πως θα αυξηθούν από 8,8 δισεκατομμύρια το 2018 σε 13,1 δισεκατομμύρια έως το 2023, μεταξύ των οποίων το 1,4 δισεκατομμύριο θα μπορεί να υποστηρίξει 5G. Η ταχύτερα αναπτυσσόμενη κατηγορία κινητών συσκευών είναι το M2M ακολουθούμενο από το smartphone. Η κατηγορία M2M για κινητά προβλέπεται να αυξηθεί κατά 30% του CAGR από το 2018 έως το 2023. Τα smartphones θα αυξηθούν κατά 7% του CAGR μέσα στο ίδιο χρονικό διάστημα.

Οι συνδρομές που σχετίζονται με smartphones αντιπροσωπεύουν περισσότερο από το 70 % όλων των συνδρομών κινητών τηλεφώνων. Οι συνδρομές για κινητά υπερβαίνουν τον πληθυσμό σε πολλές χώρες, γεγονός που οφείλεται σε μεγάλο βαθμό σε ανενεργές συνδρομές, την κατοχή πολλών συσκευών και τη χρήση διαφορετικών συνδρομών για διαφορετικούς τύπους κλήσεων. Ως αποτέλεσμα, ο αριθμός των συνδρομητών κινητής τηλεφωνίας είναι χαμηλότερος από τον αριθμό των συνδρομών σε κινητές συσκευές. Σήμερα, υπάρχουν περίπου 5,9 δισεκατομμύρια συνδρομητές παγκοσμίως σε σύγκριση με 8 δισεκατομμύρια συνδρομές. Η συνολική διείσδυση συνδρομής για κινητά είναι στο 104%. [2] Το 2025, το 90% των συνδρομών προβλέπεται πως θα προορίζεται για ευρυζωνική σύνδεση από κινητά. Υπολογίζεται ότι θα υπάρξουν 8,9 δισεκατομμύρια συνδρομές για κινητά έως το τέλος του 2025, εκ των οποίων περίπου το 90% θα προορίζεται για κινητές ευρυζωνικές συνδέσεις. Η διείσδυση των smartphones συνεχίζει

να αυξάνεται. Οι συνδρομές που σχετίζονται με smartphones αντιπροσωπεύουν περίπου το 70% όλων των συνδρομών κινητών τηλεφώνων. [2] Στο τρίτο τρίμηνο του 2019, η κίνηση δεδομένων κινητής τηλεφωνίας αυξήθηκε 68% σε ετήσια βάση. Ο υψηλός ρυθμός ανάπτυξης εξακολουθεί να επηρεάζεται από τον αυξημένο αριθμό συνδρομών smartphones. Σε γενικές γραμμές, η αύξηση της επισκεψιμότητας καθοδηγείται τόσο από τον αυξανόμενο αριθμό συνδρομών smartphones όσο και από τον αυξανόμενο μέσο όγκο δεδομένων ανά συνδρομή, που τροφοδοτείται κυρίως από περισσότερη προβολή περιεχομένου βίντεο. [2]

Η διεξόδυση των smartphone συνεχίζει να αυξάνεται. Οι συνδρομές που σχετίζονται με smartphones αντιπροσωπεύουν περίπου το 70% όλων των συνδρομών κινητών τηλεφώνων. [2] Στο τρίτο τρίμηνο του 2019, Η κίνηση δεδομένων κινητής τηλεφωνίας αυξήθηκε 68% σε ετήσια βάση. Ο υψηλός ρυθμός ανάπτυξης εξακολουθεί να επηρεάζεται από τον αυξημένο αριθμό συνδρομών smartphone. Σε γενικές γραμμές, η αύξηση της επισκεψιμότητας καθοδηγείται τόσο από τον αυξανόμενο αριθμό συνδρομών smartphone όσο και από τον αυξανόμενο μέσο όγκο δεδομένων ανά συνδρομή, που τροφοδοτείται κυρίως από περισσότερη προβολή περιεχομένου βίντεο. [2]

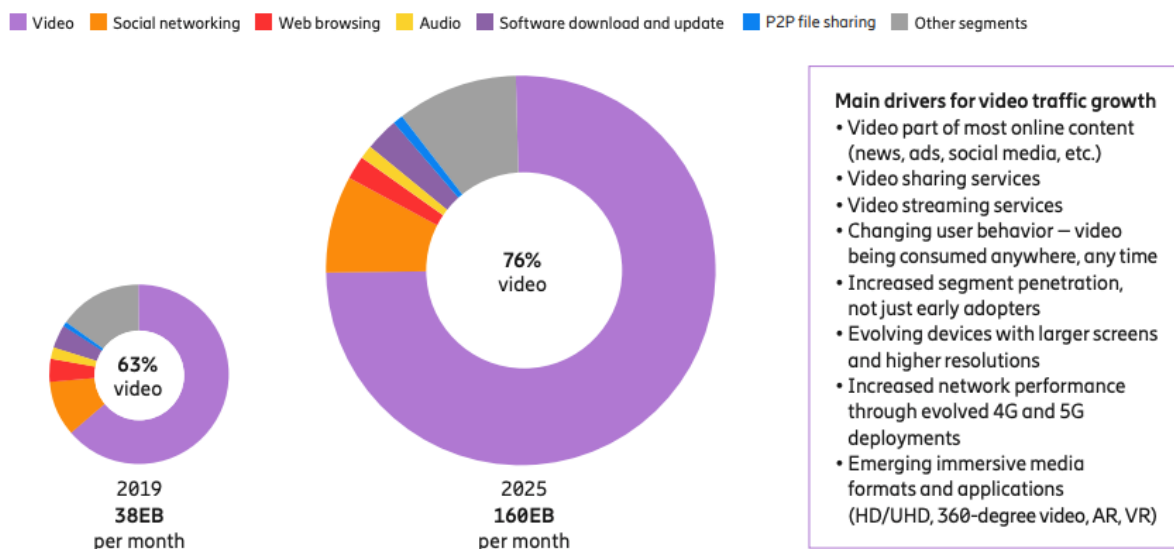


Εικόνα 2, Παγκόσμια κίνηση δεδομένων κινητής τηλεφωνίας και ετήσια αύξηση (EB ανά μήνα), Mobile Traffic Only. Ericsson Mobility Report 2019

Η επισκεψιμότητα από κινητά αναμένεται να αυξηθεί κατά 27% ετησίως μεταξύ 2019 και 2025. Συνεχίζοντας τις πρόσφατες τάσεις, τα περισσότερα από αυτά θα προέρχονται από την επισκεψιμότητα βίντεο. Η επισκεψιμότητα βίντεο σε δίκτυα κινητής τηλεφωνίας προβλέπεται να αυξηθεί κατά περίπου 30% ετησίως έως το 2025, αντιπροσωπεύοντας τα τρία τέταρτα της κίνησης δεδομένων κινητής τηλεφωνίας, από λίγο περισσότερο από

60% το 2019. Η αύξηση της επισκεψιμότητας βίντεο καθοδηγείται από την αύξηση του ενσωματωμένου βίντεο σε πολλές διαδικτυακές εφαρμογές video-on-demand (VoD) streaming services από την άποψη τόσο των συνδρομητών όσο και του χρόνου προβολής ανά συνδρομητή, και η εξέλιξη προς υψηλότερες αναλύσεις οθόνης σε έξυπνες συσκευές. Όλοι αυτοί οι παράγοντες επηρεάστηκαν από την αυξανόμενη διείσδυση έξυπνων συσκευών με δυνατότητα βίντεο. Η κυκλοφορία των κοινωνικών δικτύων αναμένεται επίσης να αυξηθεί 20% ετησίως κατά τα επόμενα 6 χρόνια. Ωστόσο, το σχετικό μερίδιο επισκεψιμότητας προβλέπεται πως θα μειωθεί από 10% το 2019 σε 8% περίπου το 2025, λόγω της ισχυρότερης ανάπτυξης του βίντεο.

Η πιο συνηθισμένη ανάλυση για ροή βίντεο μέσω κυψελοειδών δικτύων εκτιμάται ότι είναι περίπου 480p (ποικίλλει από δίκτυο σε δίκτυο). Με τα smartphone και τα δίκτυα να βελτιώνονται συνεχώς, η ροή βίντεο HD (720p) και Full HD (1080p) γίνεται πιο κοινή. Οι πιο συναρπαστικές μορφές και εφαρμογές πολυμέσων αναμένεται να αποτελέσουν σημαντικό παράγοντα που θα συμβάλλει στην αύξηση της κίνησης δεδομένων κινητής τηλεφωνίας, καθώς τα δίκτυα 5G θα παρέχουν την απαιτούμενη απόδοση για μια καλή εμπειρία χρήστη. Για παράδειγμα, παρακολουθώντας e-streaming sports event in multi-view θα ήταν δυνατό να καταναλωθούν περίπου 7 GB ανά ώρα, ενώ είναι υψηλής ποιότητας Augmented Reality/Virtual Reality stream με ρυθμό μέσων (bit) 25Mbps θα καταναλώνει έως και 12 GB ανά ώρα. [2]



Εικόνα 3, Κατανάλωση από κινητά ανά κατηγορία εφαρμογής ανά μήνα (ποσοστό), Ericsson Mobility Report 2019

1.3 Παγκόσμια απόδοση δικτύου και τάσεις

Κινητές Επικοινωνίες (cellular): Οι ταχύτητες αναμένεται ότι θα υπερδιπλασιαστούν έως το 2023. Η μέση ταχύτητα σύνδεσης δικτύου κινητής τηλεφωνίας ήταν 13,2 Mbps το 2018 και υπολογίζεται ότι θα είναι 43,9 Mbps έως το 2023.

Οι ταχύτητες του 5G: Η μέση ταχύτητα σύνδεσης του 5G αναμένεται να φτάσει τα 575 Mbps έως το 2023.

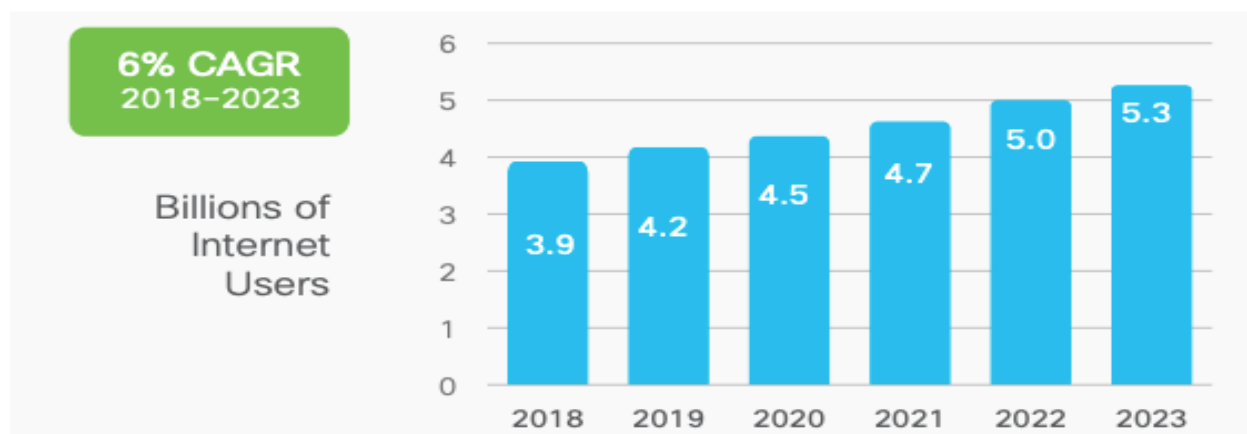
Mobile applications: Σχεδόν 300 εκατομμύρια εφαρμογές για κινητές συσκευές θα ληφθούν έως το 2023. Εφαρμογές κοινωνικής δικτύωσης, παιχνίδια και επιχειρηματικές εφαρμογές θα είναι οι πιο δημοφιλείς λήψεις.

Wi-Fi momentum: Οι ταχύτητες Wi-Fi από κινητές συσκευές εκτιμάται ότι θα τριπλασιαστούν έως το 2023. Σε παγκόσμιο επίπεδο, οι μέσες ταχύτητες Wi-Fi θα αυξηθούν από 30,3 Mbps το 2018 σε 92 Mbps έως το 2023. Τα σημεία πρόσβασης Wi-Fi εκτιμάται ότι θα αυξηθούν κατά 4 φορές από το 2018 έως το 2023. Σε παγκόσμιο επίπεδο, θα υπάρχουν σχεδόν 628 εκατομμύρια δημόσια σημεία πρόσβασης Wi-Fi έως το 2023, σε σύγκριση με τα 169 εκατομμύρια hotspots που υπήρχαν το 2018. Τα σημεία πρόσβασης Wi-Fi6 θα αυξηθούν 13 φορές από το 2020 έως το 2023 και θα αντιπροσωπεύουν το 11% όλων των δημόσιων σημείων πρόσβασης Wi-Fi έως το 2023.

Ανάλυση ασφάλειας: Ο αριθμός των παραβιάσεων και οι συνολικές εγγραφές που εκτίθενται ανά παραβίαση συνεχίζουν να αυξάνονται. Σε παγκόσμιο επίπεδο, σημειώθηκε αύξηση 776% στις επιθέσεις μεταξύ 100 Gbps και 400 Gbps από το 2018 έως το 2019 και ο συνολικός αριθμός επιθέσεων DDoS θα διπλασιαστεί από 7,9 εκατομμύρια το 2018 σε 15,4 εκατομμύρια έως το 2023.

1.3.1 Χρήστες, συσκευές και συνδέσεις

Προβλέπεται ανάπτυξη των χρηστών του Διαδικτύου παγκοσμίως. Ειδικότερα, ο συνολικός αριθμός χρηστών του Διαδικτύου προβλέπεται να αυξηθεί από 3,9 δισεκατομμύρια (51% του παγκόσμιου πληθυσμού) το 2018 σε 5,3 δισεκατομμύρια (66% της παγκόσμιας διείσδυσης του πληθυσμού) έως το 2023, μία αύξηση της τάξεως του 6% του CAGR. (Εικόνα 4)

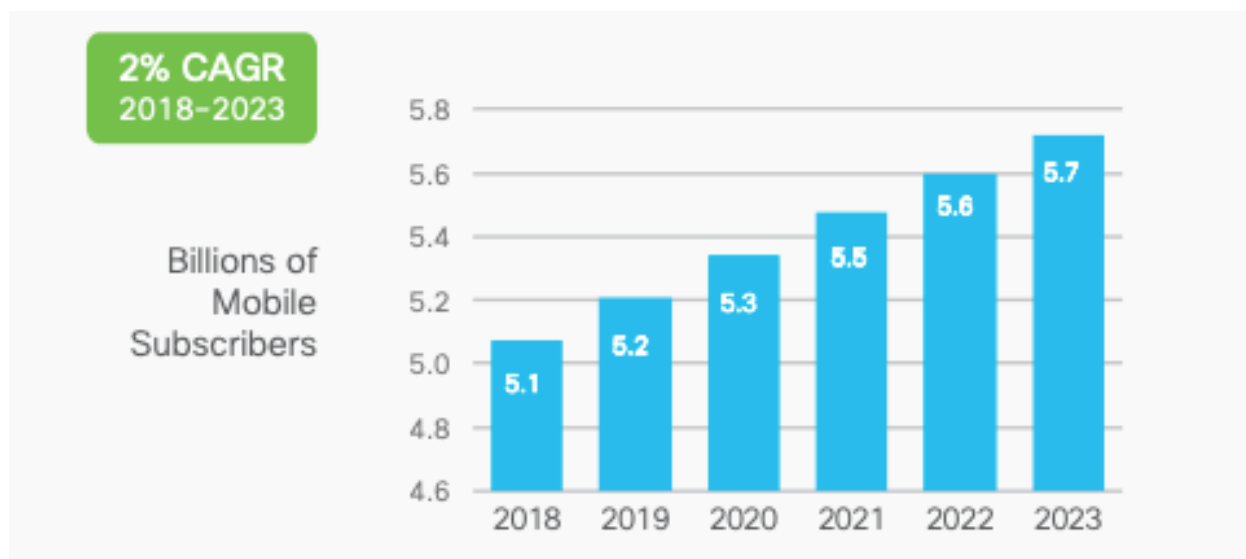


Εικόνα 4, Παγκόσμια ανάπτυξη Διαδικτύου, Source: Cisco Annual Internet Report, 2018-2023

1.3.2 Αύξηση κινητικότητας παγκοσμίως

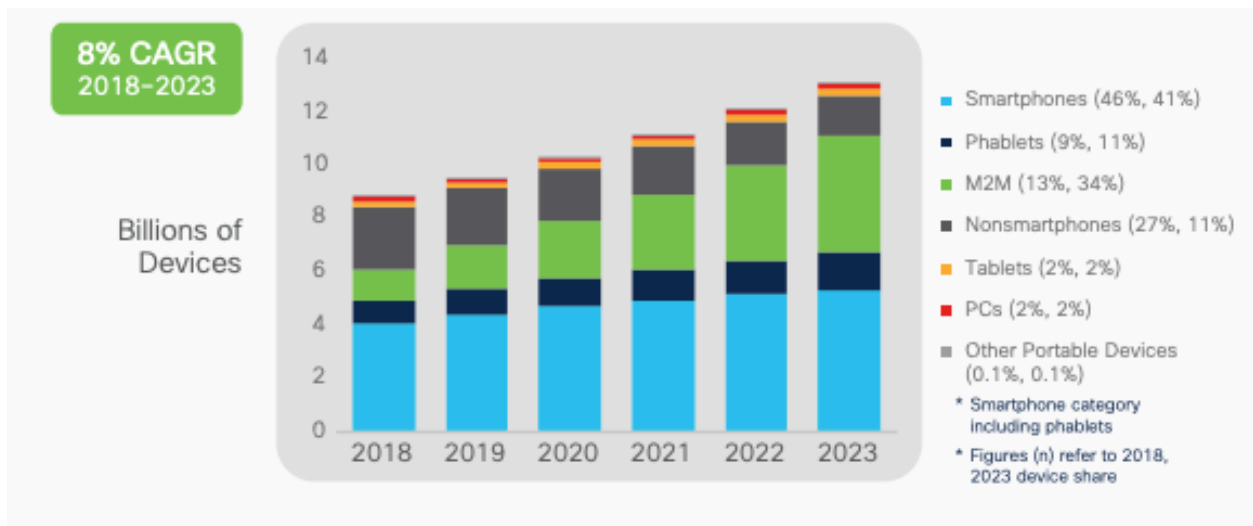
Ο συνολικός αριθμός συνδρομητών κινητής τηλεφωνίας (αυτοί που εγγράφονται σε μια υπηρεσία κινητής τηλεφωνίας) θα αυξηθεί από 5,1 δισεκατομμύρια το 2018 σε 5,7 δισεκατομμύρια έως το 2023 σε ένα ποσοστό του 2% επί του CAGR. Όσον αφορά τον πληθυσμό, αυτός αντιπροσώπευε το 66% του παγκόσμιου πληθυσμού το 2018 και αναμένεται να φτάσει το 71% της παγκόσμιας διείσδυσης του πληθυσμού έως το 2023 (Εικόνα 5).

Σε σχέση με την αύξηση των χρηστών του Διαδικτύου παρατηρείται επιβράδυνση στην ανάπτυξη των συνδρομητών κινητής τηλεφωνίας - αυτό συμβαίνει κυρίως επειδή τα επίπεδα διείσδυσης έχουν ήδη ξεπεράσει το 60%.



Εικόνα 5, Παγκόσμια αύξηση συνδρομητών κινητής τηλεφωνίας, Source: Cisco Annual Internet Report, 2018-2023

Ο συνεχώς μεταβαλλόμενος συνδυασμός και ανάπτυξη ασύρματων συσκευών που έχουν πρόσβαση σε δίκτυα κινητής τηλεφωνίας παγκοσμίως είναι ένας από τους κύριους συντελεστές στην παγκόσμια αύξηση της κυκλοφορίας κινητών. Κάθε χρόνο εισάγονται στην αγορά αρκετές νέες συσκευές με διαφορετικούς παράγοντες και αυξημένες δυνατότητες και ευφυΐα. Τα τελευταία δύο χρόνια, έχει παρατηρηθεί αύξηση των phablets και πιο πρόσφατα έχουν πραγματοποιηθεί πολλές νέες συνδέσεις M2M. Υπήρχαν 8,8 δισεκατομμύρια παγκόσμιες κινητές συσκευές και συνδέσεις το 2018, οι οποίες εκτιμάται ότι θα αυξηθούν σε 13,1 δισεκατομμύρια έως το 2023 με CAGR 8% (Εικόνα 6). Μέχρι το 2023, αναμένεται να υπάρχουν 8,7 δισεκατομμύρια φορητές ή προσωπικές συσκευές και 4,4 δισεκατομμύρια συνδέσεις M2M (π.χ. συστήματα GPS σε αυτοκίνητα, συστήματα παρακολούθησης περιουσιακών στοιχείων σε τομείς ναυτιλίας και κατασκευής ή ιατρικές εφαρμογές που καθιστούν πιο εύκολα διαθέσιμα τα αρχεία ασθενών και την κατάσταση υγείας, κλπ.).



Εικόνα 6, Παγκόσμια ανάπτυξη κινητών συσκευών και σύνδεσεων, Source: Cisco Annual Internet Report, 2018–2023

1.4 Δεδομένα ανά περιοχή

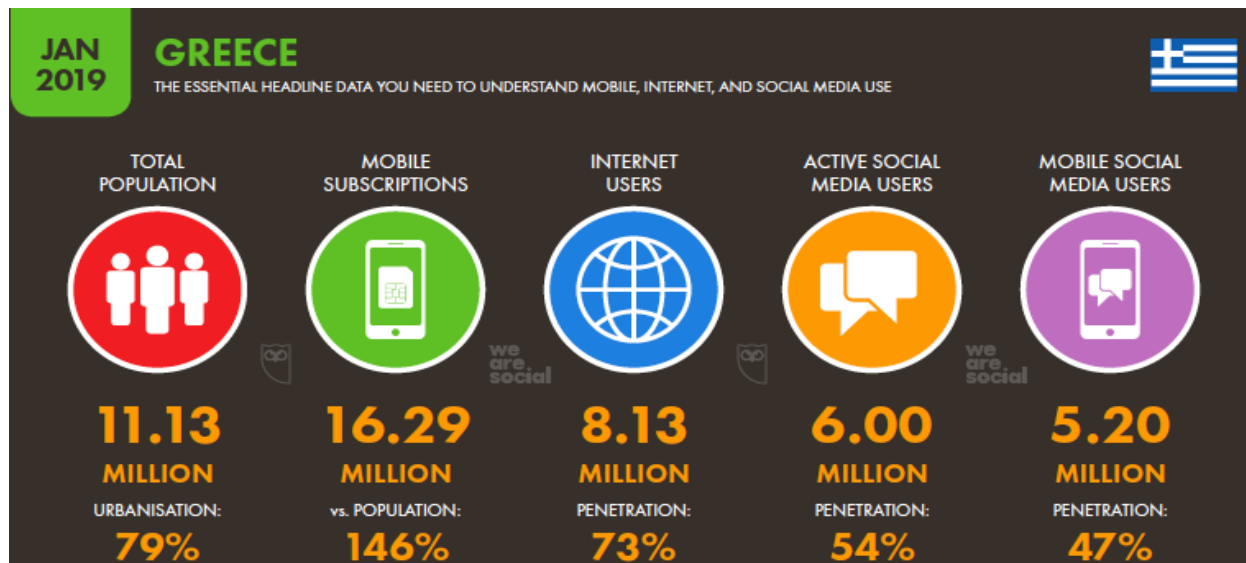
Αυτή η ενότητα παρέχει μία σύνοψη για χρήστες του Διαδικτύου, συσκευές και συνδέσεις καθώς και για την απόδοση του δικτύου για τη Δυτική Ευρώπη. Η Δυτική Ευρώπη έως το 2023, εκτιμάται ότι θα έχει 370 εκατομμύρια χρήστες του Διαδικτύου (87% του περιφερειακού πληθυσμού), από 345 εκατομμύρια (82% του περιφερειακού πληθυσμού) το 2018. Έως το 2023, η Δυτική Ευρώπη υπολογίζεται ότι θα έχει 365 εκατομμύρια χρήστες κινητής τηλεφωνίας (85% του περιφερειακού πληθυσμού), από 357 εκατομμύρια (84% του περιφερειακού πληθυσμού) το 2018.

Έως το 2023, η Δυτική Ευρώπη προβλέπεται να έχει 4,0 δισεκατομμύρια συσκευές / συνδέσεις δικτύου, από 2,4 δισεκατομμύρια το 2018.

Έως το 2023, στην Δυτική Ευρώπη η μέση ταχύτητα σύνδεσης κινητής τηλεφωνίας αναμένεται να φτάσει τα 62,4 Mbps, που αντιπροσωπεύει αύξηση 2,6 φορές από το 2018 (23,6 Mbps).

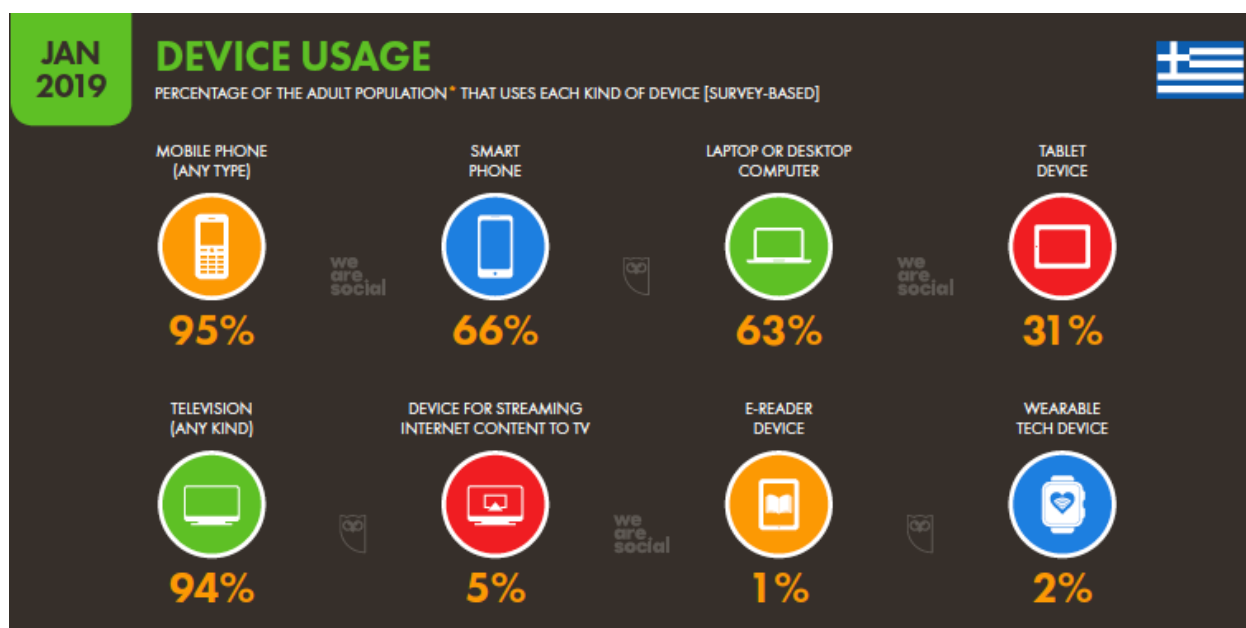
Έως το 2023, στην Δυτική Ευρώπη οι ταχύτητες Wi-Fi από κινητές συσκευές υπολογίζεται ότι θα φτάσουν τα 97 Mbps, που αντιπροσωπεύουν αύξηση 3,2 φορές από το 2018 (30,8 Mbps).

1.5 Δεδομένα κινητικότητας για την Ελλάδα



Εικόνα 7, Δεδομένα Χρήσης στην Ελλάδα, Source Hootsuite

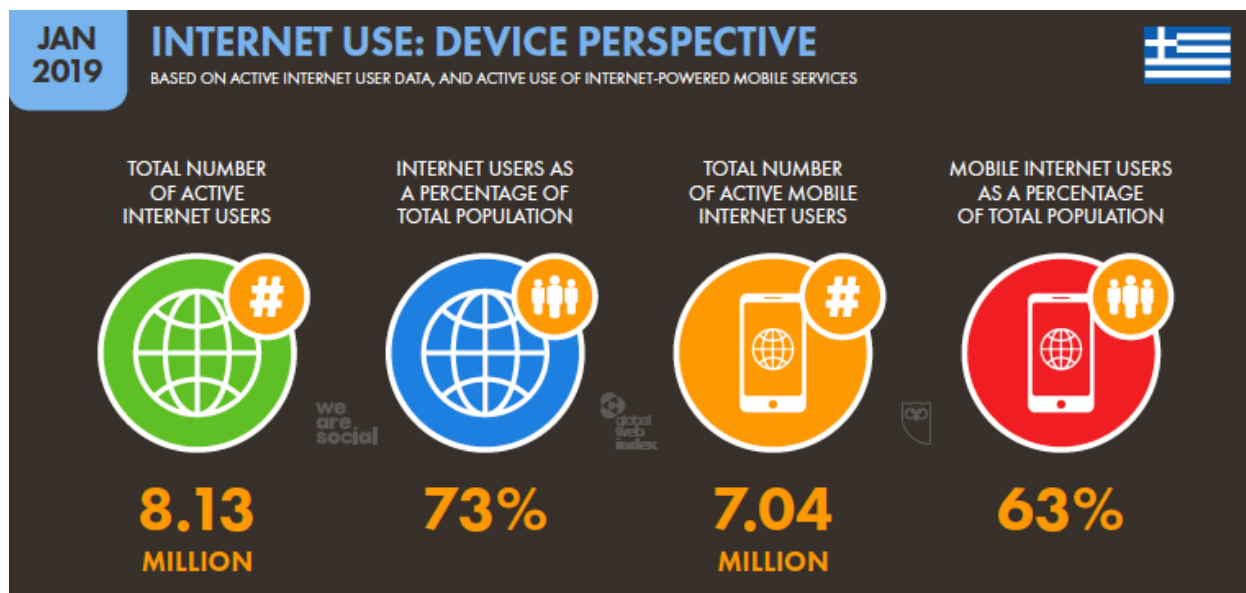
Όπως φαίνεται και στην παραπάνω εικόνα οι εγγραφές στα κυψελωτά δίκτυα επικοινωνιών στην Ελλάδα είναι 16,29 εκατομμύρια, οι ενεργές κάρτες SIM δηλαδή, είναι 6 εκατομμύρια παραπάνω από τον πληθυσμό της Ελλάδας. Ενώ η χρήση του διαδικτύου φτάνει σε ποσοστό το 73% του πληθυσμού.



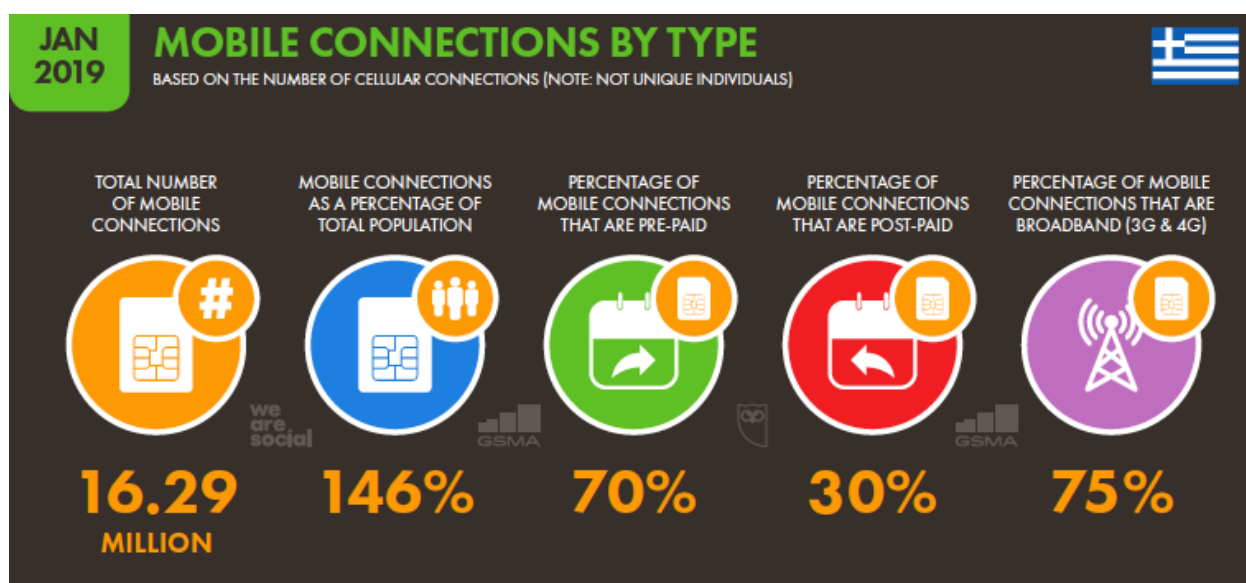
Εικόνα 8, Χρήση Κινητών Συσκευών στην Ελλάδα, Source Hootsuite

Στην παραπάνω εικόνα φαίνεται ο τύπος των συσκευών που χρησιμοποιούνται πιο πολύ από τον ελληνικό πληθυσμό. Όπως αποτυπώνεται, το κινητό τηλέφωνο φτάνει σε ποσοστό χρήσης το 95% από το οποίο το 66% είναι smartphones. Αν προστεθούν σε αυτό το ποσοστό και τα ποσοστά των υπόλοιπων συσκευών που συνδέονται σε κάποιο δίκτυο επικοινωνιών, είτε αυτό είναι κάποιο οικιακό ή εταιρικό ασύρματο δίκτυο, είτε αυτό είναι το δίκτυο του παρόχου κινητής επικοινωνίας, γίνεται αντιληπτός ο τεράστιος και

διαφορετικού τύπου όγκος δεδομένων που απαιτείται για να διαχειριστούν τα υπάρχοντα δίκτυα επικοινωνιών.



Εικόνα 9, Χρήση Διαδικτύου μέσω κινητών συσκευών, Source Hootsuite



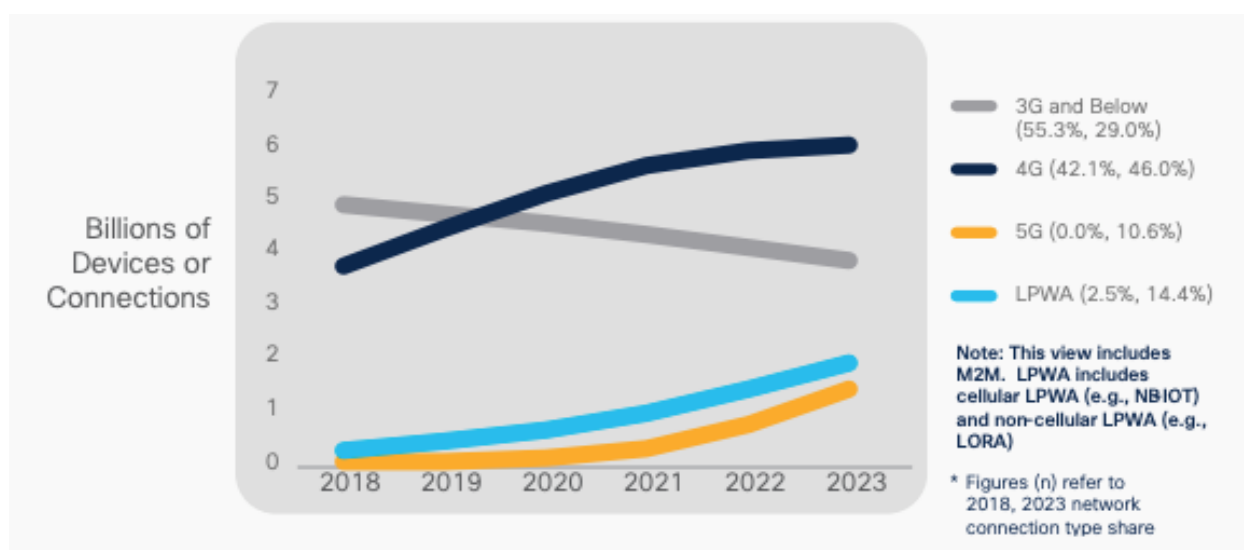
Εικόνα 10, κινητές συνδέσεις ανά τύπο, Source Hootsuite

Στην παραπάνω εικόνα γίνεται εύκολα αντιληπτό ότι από το σύνολο των συνδρομητών και ως συνέπεια των συνδέσεων, το 75% αφορούν συνδέσεις 3G και 4G και αυτό λόγω της δυνατότητας που παρέχουν αυτές οι τεχνολογίες να συνδεθούν στο διαδίκτυο.

1.6 Καθορισμός εξέλιξης κυψελωτών δικτύων

Οι φορητές συσκευές εξελίσσονται από συνδεσιμότητα δικτύου χαμηλότερης γενιάς (2G) σε συνδεσιμότητα δικτύου υψηλότερης γενιάς (3G, 3.5G, 4G ή LTE και τώρα επίσης 5G). Ο συνδυασμός δυνατοτήτων συσκευής με γρηγορότερο, υψηλότερο εύρος ζώνης και πιο έξυπνα δίκτυα θα διευκολύνει τον ευρύ πειραματισμό και την υιοθέτηση προηγμένων

εφαρμογών πολυμέσων που συμβάλλουν στην αύξηση της δικτυακής κυκλοφορίας των κινητών και του Wi-Fi. Η έκρηξη των εφαρμογών για κινητά και η διευρυμένη εμβέλεια της συνδεσιμότητας κινητής τηλεφωνίας σε έναν αυξανόμενο αριθμό τελικών χρηστών προκάλεσαν την ανάγκη βελτιστοποιημένης διαχείρισης εύρους ζώνης και νέων μοντέλων δημιουργίας εισόδων δικτύου για τη διατήρηση μιας ώριμης βιομηχανίας κινητής τηλεφωνίας. Μέχρι το 2023, οι συνδέσεις 4G αναμένεται να είναι το 46% των συνολικών συνδέσεων κινητής τηλεφωνίας, σε σύγκριση με το 42% το 2018 (Εικόνα 11). Οι παγκόσμιες συνδέσεις κινητής τηλεφωνίας 4G θα αυξηθούν από 3,7 δισεκατομμύρια το 2018 σε 6,0 δισεκατομμύρια έως το 2023 σε ένα CAGR της τάξεως του 10%. Οι συνδέσεις 5G που εμφανίστηκαν το 2019 αναμένεται να αυξηθούν πάνω από 100 φορές από περίπου 13 εκατομμύρια το 2019 σε 1,4 δισεκατομμύρια έως το 2023. Η συνδεσιμότητα 5G αναδύεται σε έναν ισχυρό υποψήφιο για συνδεσιμότητα μέσω κινητής τηλεφωνίας που οδηγείται από την ανάπτυξη IoT για κινητές συσκευές. Μέχρι το 2023, το 11% των συσκευών και συνδέσεων θα έχουν δυνατότητα 5G.



Εικόνα 11, Παγκόσμια ανάπτυξη κινητών συσκευών και σύνδεσεων, Source: Cisco Annual Internet Report, 2018–2023

Οι Low-Power Wide-Area (LPWA) συνδέσεις είναι αναγκαίο να συμπεριληφθούν στην ανάλυση. Αυτός ο τύπος ultra-narrowband wireless network διασύνδεσης προορίζεται ειδικά για M2M συσκευές που απαιτούν χαμηλό εύρος ζώνης και ευρεία γεωγραφική κάλυψη. Παρέχει υψηλή κάλυψη με χαμηλή κατανάλωση ενέργειας, λειτουργική μονάδα και κόστος σύνδεσης, δημιουργώντας έτσι νέες περιπτώσεις χρήσης M2M για διαχειριστές κινητών δικτύων (Mobile Network Operators) που μόνα τους τα δίκτυα κινητής τηλεφωνίας δεν μπορούσαν να αντιμετωπίσουν. Παραδείγματα αποτελούν, μετρητές αερίου ή νερού που δεν έχουν σύνδεση ρεύματος, φώτα δρόμου και ιχνηλάτες κατοικίδιων ή προσωπικών στοιχείων. Το μερίδιο των LPWA συνδέσεων (οι οποίες θα

είναι εξ ολοκλήρου M2M) προβλέπεται να αυξηθούν από περίπου 2,5% το 2018 σε 14% έως το 2023, από 223 εκατομμύρια το 2018 σε 1,9 δισεκατομμύρια έως το 2023. Αυτή η μετάβαση από 3G και κάτω σε 4G και πλέον η ανάπτυξη 5G είναι μια παγκόσμια τάση. Στην πραγματικότητα, έως το 2023, σχεδόν το 60% των κινητών συσκευών και συνδέσεων παγκοσμίως θα έχουν δυνατότητα 4G +, ξεπερνώντας τις συσκευές 3G και 4G.

1.6.1 Απόδοση δικτύου και εμπειρία χρήστη

Μία από τις κύριες λύσεις για την κάλυψη των απαιτήσεων της αυξανόμενης ζήτησης για εύρος ζώνης ήταν η από καιρό εξέλιξη των δικτύων Wi-Fi, η οποία επιτρέπει στους διαχειριστές να κλιμακώσουν τη χωρητικότητα για να καλύψουν τις ανάγκες των συνδρομητών τους. Με πρόοδο και επικύρωση στα πρότυπα Wi-Fi, πυκνά περιβάλλοντα με πολλές ταυτόχρονες συσκευές σύνδεσης και συνδέσεις IoT όπως αεροδρόμια, δημόσια μέσα μεταφοράς, λιανική, υγειονομική περίθαλψη, έξυπνες πόλεις, στάδια κ.λπ. έχουν ως αποτέλεσμα δημόσιες περιπτώσεις χρήσης Wi-Fi σε τομείς της βιομηχανίας. Σε παγκόσμιο επίπεδο, εκτιμάται ότι θα υπάρξουν σχεδόν 628 εκατομμύρια δημόσια hotspots Wi-Fi έως το 2023, από 169 εκατομμύρια hotspots το 2018, μια τετραπλάσια αύξηση. Τα καταστήματα λιανικής αναμένεται ότι θα έχουν τον υψηλότερο αριθμό hotspots έως το 2023 παγκοσμίως, και η ταχύτερη ανάπτυξη είναι σε εγκαταστάσεις υγειονομικής περίθαλψης (νοσοκομεία), όπου τα hotspots θα τριπλασιαστούν κατά την περίοδο πρόβλεψης. Ο πρωταρχικός στόχος του Wi-Fi στα νοσοκομεία είναι η βελτίωση της παροχής υπηρεσιών υγειονομικής περίθαλψης και της παραγωγικότητας του προσωπικού, με δευτερεύον όφελος την πρόσβαση στο Διαδίκτυο για τους ασθενείς, τις οικογένειές τους και τους επισκέπτες τους. Σε παγκόσμιο επίπεδο, τα Wi-Fi 6 hotspots θα αυξηθούν 13 φορές από το 2020-2023 και θα είναι το 11% όλων των δημόσιων hotspots Wi-Fi έως το 2023.

Το 802.11ax ή Wi-Fi 6 όπως ονομάζεται επίσης το High-Efficiency Wireless (HEW), έχει ως στόχο τη βελτίωση της μέσης απόδοσης ανά χρήστη κατά τουλάχιστον τέσσερις φορές σε πυκνά περιβάλλοντα χρήστη γεγονός που θα επιτρέψει πυκνές αναπτύξεις IoT. Μέχρι το 2023, το 27,4% όλων των τελικών σημείων WLAN θα είναι εξοπλισμένο με 802.11ax.



Εικόνα 12, Ιστορική αναδρομή και εξέλιξη των ενσύρματων και ασύρματων τεχνολογιών, Source: Cisco Annual Internet Report, 2018–2023

Το Wi-Fi θα παίξει ισχυρό ρόλο μαζί με άλλες τεχνολογίες μικρών κυψελών για την παράδοση βασικών περιπτώσεων χρήσης στο μέλλον για το πέρασμα στην εποχή 5G. [1]

1.7 Ανάγκη για την ανάπτυξη νέων συστημάτων κινητών επικοινωνιών

Για όλους τους λόγους που αναφέρθηκαν παραπάνω και περιγράφονται και συνοπτικά παρακάτω, είναι επιτακτική η ανάγκη δημιουργίας νέων δικτύων, τα οποία θα είναι ικανά και σχεδιασμένα με τέτοιο τρόπο έτσι ώστε να μπορούν να ανταποκριθούν στις νέες αυξημένες απαιτήσεις, τόσο για εύρος ζώνης όσο και για χαμηλό latency και υψηλό βαθμό ασφάλειας των επικοινωνιών.

- Δραματική εκθετική αύξηση του Mobile Internet
- Περισσότεροι χρήστες
- Περισσότερες συσκευές
- Διαφορετικού τύπου συσκευές που θα αιτηθούν πρόσβαση στο δίκτυο, όπως για παράδειγμα Machine-to-Machine επικοινωνίες
- Νέες εφαρμογές που θα απαιτούν μειωμένη καθυστέρηση
- Βελτιωμένη αξιοπιστία (Reliability) και μεγαλύτερη διάρκεια ζωής της μπαταρίας για συσκευές
- Internet of Things

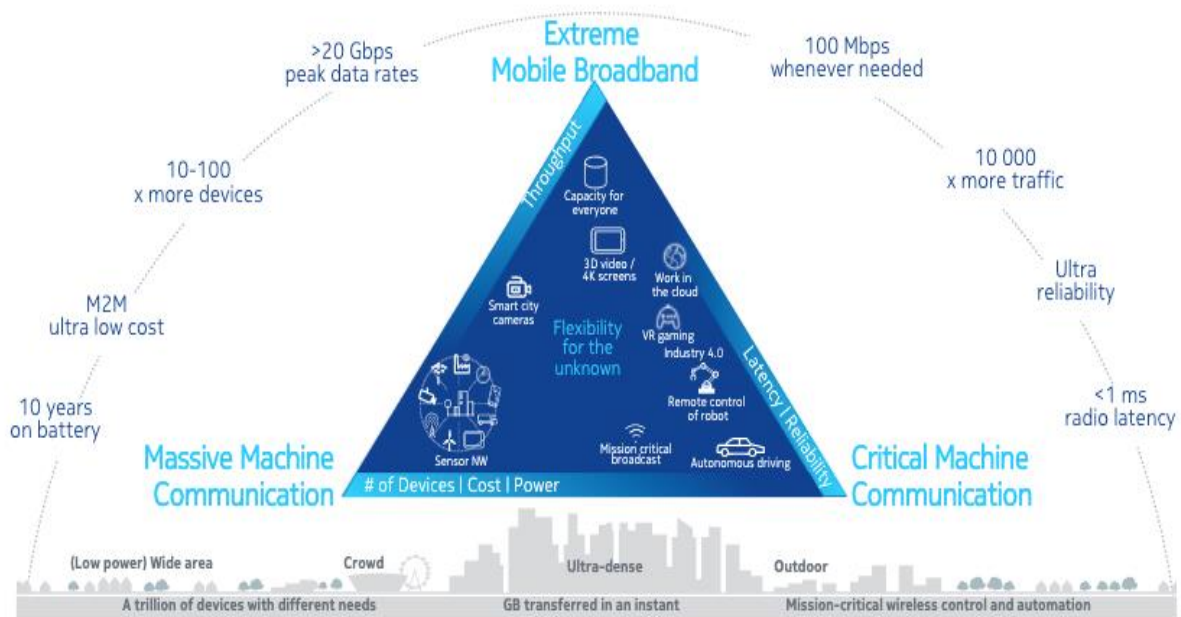
Η τεράστια αύξηση της κίνησης δεδομένων κινητής τηλεφωνίας και η εμφάνιση ασύρματων εφαρμογών που θέλουν εύρος ζώνης υπογραμμίζουν την επικείμενη ανάγκη για μεγάλο εύρος ζώνης και υψηλό ρυθμό δεδομένων σε δίκτυα κινητής τηλεφωνίας επόμενης γενιάς. Οι ασύρματες επικοινωνίες εξελίσσονται και καθοδηγούνται από περισσότερες συσκευές, περισσότερες συνδέσεις και περισσότερες εφαρμογές που απαιτούν εύρος ζώνης. Τα μελλοντικά δίκτυα θα χρειαστούν περισσότερη ασύρματη χωρητικότητα και αξιοπιστία. Εκεί έρχεται η έκτη γενιά Wi-Fi. Η έκτη γενιά Wi-Fi, το Wi-Fi 6, επίσης γνωστό ως 802.11ax, παρέχει περισσότερη ταχύτητα, χαμηλότερη καθυστέρηση και αυξημένη πυκνότητα συσκευών. Το IEEE 802.11ax επιτρέπει στα σημεία πρόσβασης να υποστηρίζουν περισσότερους πελάτες σε πυκνά περιβάλλοντα και να παρέχουν μια καλύτερη εμπειρία για τυπικά δίκτυα ασύρματου LAN. Εξασφαλίζει επίσης πιο προβλέψιμη απόδοση για προηγμένες εφαρμογές, όπως βίντεο 4K, Ultra HD, ασύρματο γραφείο και Internet of Things (IoT). Ο ευέλικτος προγραμματισμός χρόνου αφύπνισης επιτρέπει στις συσκευές πελατών να κοιμούνται πολύ περισσότερο από ό, τι με το 802.11ac και να ξυπνούν με λιγότερη διαμάχη, παρατείνοντας τη διάρκεια ζωής της μπαταρίας των έξυπνων τηλεφώνων, του IoT και άλλων συσκευών. Ένας από τους στόχους του 802.11ax, επίσης γνωστό και ως ασύρματο δίκτυο υψηλής αποτελεσματικότητας (High Efficiency), είναι να προσφέρει υψηλότερα επίπεδα απόδοσης στα υπάρχοντα δίκτυα Wi-Fi. Το IEEE 802.11ax επιτυγχάνει αυτά τα οφέλη προχωρώντας σε αλλαγές σε τρεις διαφορετικές λειτουργίες:

- Πιο πυκνή διαμόρφωση χρησιμοποιώντας 1024-QAM, επιτρέποντας ριπή(burst) ταχύτητας άνω του 35%
- Orthogonal Frequency Division Multiple Access (OFDMA) για την μείωση της καθυστέρησης
- Εύρωστη και αποτελεσματική σηματοδότηση υψηλής απόδοσης για καλύτερη λειτουργία σε σημαντικά χαμηλότερο Received Signal Strength Indication (RSSI)

Η πέμπτη γενιά ασύρματων, ή 5G, είναι η τελευταία τεχνολογία κινητής τηλεφωνίας, σχεδιασμένη για να αυξάνει την ταχύτητα και την χωρητικότητα των ασύρματων δικτύων. Οι απαιτήσεις από το νέο αυτό σύστημα είναι:

- 1) Βελτιστοποιημένες ραδιο-διεπαφές (radio interfaces)
- 2) Πιο προσαρμόσιμο ραδιοσύστημα
- 3) Πολύ χαμηλό end-to-end καθυστέρηση υπηρεσίας
- 4) Πιο προσαρμόσιμο (adaptable) core δίκτυο
- 5) Νέες τεχνολογίες πρόσβασης (access radio technologies)

Η 5^η γενιά κινητών επικοινωνιών θα βασίζεται σε 3 Τεχνολογίες 'πυλώνες'. Στην παρακάτω εικόνα απεικονίζονται οι 3 βασικοί πυλώνες του νέου συστήματος 5^{ης} γενιάς της 3GPP όπως και οι απαιτήσεις και οι προϋποθέσεις που αυτό πρέπει να πληροί.



Εικόνα 13, IMT 2020 Βασικές Κατευθύνσεις ανάπτυξης του 5G

2. IEEE 802.11ax ΚΑΙ ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΣΥΣΤΗΜΑΤΟΣ WIFI

Τα ασύρματα δίκτυα βλέπουν μία συνεχώς αυξανόμενη δημοτικότητα, προσελκύνοντας έναν συνεχώς αυξανόμενο αριθμό χρηστών. Αυτό είχε ως αποτέλεσμα την σημαντική αύξηση της κατανάλωσης εύρους ζώνης. Στην ενότητα αυτή θα περιγραφεί το νέο σύστημα κινητών επικοινωνιών, IEEE 802.11ax το οποίο είναι γνωστό και ως Wi-Fi 6 και το οποίο αναπτύχθηκε για την κάλυψη των νέων αυξημένων αναγκών. Στο κεφάλαιο αυτό περιγράφεται το νέο πρότυπο καθώς και οι νέες Τεχνολογικές του δυνατότητες. Γίνεται ανάλυση της διαμόρφωσης OFDMA και επεξήγηση του BSS Coloring, το οποίο είναι ένας νέος τρόπος αναγνώρισης των επικαλυπτόμενων BSS. Τέλος, περιγράφεται με αναλυτικό τρόπο η αρχιτεκτονική ενός εταιρικού ασύρματου δικτύου και ο τρόπος αυθεντικοποίησης του ασύρματου χρήστη.

2.1 IEEE 802.11ax (Wi-Fi 6)

Η παρουσία πλούσιου περιεχομένου ψηφιακών μέσων και η επιθυμία των χρηστών για συνεχή συνδεσιμότητα φέρνουν αυξανόμενες απαιτήσεις απόδοσης σε κάθε συσκευή Wi-Fi®. Αυτό με τη σειρά του απαιτεί μεγάλη αύξηση της συνολικής χωρητικότητας του δικτύου, καθώς και νέους τρόπους λειτουργίας για τον μετριασμό των ανεπαρκειών που θα μπορούσαν να εκδηλωθούν σε εφαρμογές μεγάλης κλίμακας. Καθώς οι εγκαταστάσεις δικτύων Wi-Fi συνεχίζουν να αυξάνονται, οι συσκευές Wi-Fi πρέπει να συνεχίσουν να λειτουργούν αξιόπιστα σε πολυσύχναστα περιβάλλοντα. Οι χρήστες αναμένουν όλο και περισσότερο σταθερές συνδέσεις Wi-Fi σε πυκνά περιβάλλοντα δικτύου που συχνά περιλαμβάνουν πολλές πηγές παρεμβολών, και μια μεγάλη ποικιλία συσκευών πελατών. Η επόμενη γενιά Wi-Fi, βάσει του προτύπου Ινστιτούτου Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (IEEE) 802.11ax, είναι το Wi-Fi 6. Αυτή η νέα γενιά Wi-Fi παρέχει δυνατότητες που ανταποκρίνονται αποτελεσματικά στην αυξανόμενη, εξελισσόμενη χρήση της τεχνολογίας του Wi-Fi. Τα τελευταία 20 χρόνια, το Wi-Fi έχει εξελιχθεί από μια νέα τεχνολογία σε παγκόσμια, ζωτική ανάγκη για επαγγελματικές και προσωπικές εφαρμογές. Η καινοτομία Wi-Fi έχει δώσει στα άτομα περισσότερη ευελιξία για να εργαστούν, να διασκεδάσουν και να συνδεθούν με φίλους και συγγενείς σε μια αυξανόμενη ποικιλία τόπων. Η ικανότητα αύξησης της παραγωγικότητας χωρίς ενσύρματη σύνδεση άλλαξε τον τρόπο που εργαζόμαστε και ζούμε. Οι παγκόσμιες επιχειρήσεις έχουν αναπτυχθεί με βάση το Wi-Fi, οι πάροχοι κινητής τηλεφωνίας εξαρτώνται από το Wi-Fi για να βελτιώσουν και να επεκτείνουν τα δίκτυά τους και το Wi-Fi χρησιμοποιείται για να γεφυρώσει το οικονομικό ψηφιακό χάσμα. Τώρα κάθε άτομο αναμένει να μπορεί να συνδεθεί με Wi-Fi, οποιαδήποτε στιγμή και παντού. Σχεδόν κάθε smartphone, tablet και υπολογιστής αποστέλλεται με Wi-Fi και νέοι τύποι συσκευών με δυνατότητα Wi-Fi με διάφορους παράγοντες μορφής, από τους ιχνηλάτες γυμναστικής έως τα ψυγεία, εισέρχονται στην αγορά κάθε χρόνο. Κάθε γενιά Wi-Fi προσφέρει στους χρήστες γρηγορότερες ταχύτητες, υψηλότερη πυκνότητα, πρόσθετες ζώνες συχνοτήτων και ταχύτερη απόδοση για να επιτρέπουν στους χρήστες να ενσωματώνουν το Wi-Fi σε ό, τι κάνουν στο σπίτι, στην εργασία και εν κινήσει. Καθώς ο κόσμος μπαίνει στην επόμενη γενιά συνδεσιμότητας κινητής τηλεφωνίας, το Wi-Fi 6 εισάγει νέες δυνατότητες για αποτελεσματική αντιμετώπιση των απαιτήσεων κίνησης.

Η ζήτηση για ασύρματη πρόσβαση από χρήστες έχει μετατοπιστεί από διασκέδαση σε ανάγκη. Λόγω αυτού, οι επιδόσεις του δικτύου έχουν καταστεί κρίσιμη προϋπόθεση για τις επιχειρήσεις. Τόσο οι εργαζόμενοι όσο και οι καταναλωτές περιμένουν μία αξιόπιστη Wi-Fi σύνδεση - η απουσία της οποίας μπορεί να επηρεάσει την απόφασή τους να

εισέλθουν σε μια εγκατάσταση ή να φύγουν από αυτή. Το ασύρματο εξελίσσεται, καθοδηγείται από περισσότερες συσκευές, περισσότερες συνδέσεις και περισσότερες εφαρμογές που απαιτούν εύρος ζώνης. Τα μελλοντικά δίκτυα θα χρειαστούν περισσότερη ασύρματη χωρητικότητα και αξιοπιστία. Εκεί έρχεται η έκτη γενιά Wi-Fi. Προκειμένου να προσελκύσουν και να διατηρήσουν πελάτες και εργαζόμενους, οι εταιρείες πρέπει να προσφέρουν αξιόπιστο Wi-Fi και ταυτόχρονα μία εκπληκτική εμπειρία πλοήγησης στο διαδίκτυο μέσω του ασύρματου δικτύου, διαφορετικά υπάρχει ο κίνδυνος της απώλειας πελατών. Προκειμένου να ικανοποιήσει τον αυξανόμενο αριθμό συσκευών κινητής τηλεφωνίας και IoT, χρειάζονται βελτιώσεις στην αποτελεσματικότητα του ασύρματου δικτύου καθώς και του τρόπου που χειρίζεται τη συμφόρηση. Η ανάπτυξη και η διαφορετικότητα των πελατών, καθώς και οι διαφορετικοί τύποι εφαρμογών που χρησιμοποιούνται πλέον δημιουργήσε την ανάγκη εξέλιξης το ασύρματων προτύπων (wireless standards) έτσι ώστε να μπορούν να συμβαδίζουν. Η φωνή και το video αποτελούν ευαίσθητες εφαρμογές, γιατί ακόμα και μία μικρή απώλεια δεδομένων θα έχει σαν αποτέλεσμα σημαντική αλλοίωση των δεδομένων του χρήστη το οποίο με την σειρά του θα οδηγήσει σε σχεδόν ταυτόχρονη απώλεια της υπηρεσίας. Αυτά κάνουν κοινή χρήση του εναέριου χώρου με συσκευές IoT που στέλνουν μικρά δεδομένα πακέτα - τα οποία επιβραδύνουν ένα ασύρματο δίκτυο. Για την επίλυση αυτού του προβλήματος, τα ασύρματα δίκτυα πρέπει να παρέχουν έναν πιο αποτελεσματικό τρόπο αντιμετώπισης αυτού του αυξανόμενου και διαφορετικού τύπου δεδομένων κυκλοφορίας, καθώς και τις ανάγκες εύρους ζώνης.

Το Institute of Electrical and Electronics Engineers (IEEE) και η Wi-Fi Alliance συνεργάστηκαν για να προσδιορίσουν τους τομείς βελτίωσης του ισχύοντος προτύπου (802.11ac). Το συμπέρασμα ήταν να επικεντρωθούν στις επιδόσεις υπό τις «τυπικές» συνθήκες για να αυξήσουν ολιστικά τις επιδόσεις ολόκληρου του δικτύου. Πρόκειται για μια απόκλιση από το προηγούμενο μοντέλο - όπου το επίκεντρο ήταν να ξεταστούν τα προχωρημένα ποσοστά κορυφής (peak data rates) δεδομένων σε "τέλειες" συνθήκες.

Ένας από τους τομείς στον οποίο έχουν εστιάσει είναι να βελτιωθεί η αποτελεσματικότητα με την οποία τα σημεία πρόσβασης (access points) χειρίζονται ταυτόχρονα πολλές διαφορετικές συσκευές. Οπότε πλέον δεν συγκρίνονται ταχύτητες Wi-Fi αλλά πρόκειται περισσότερο για την ικανότητα του δικτύου να παρέχει τη βέλτιστη απόδοση σε όλους τους χρήστες. Σκεφτείτε ότι προσθέτουμε περισσότερες λωρίδες σε έναν αυτοκινητόδρομο. Η χρήση λεωφορείο λωρίδων επιτρέπει στους ανθρώπους να χρησιμοποιούν τον αυτοκινητόδρομο περισσότερο αποτελεσματικά και τελικά ανακουφίζει από τη συμφόρηση.

Το νέο 802.11ax (Wi-Fi 6), το οποίο ονομάζεται επίσης και ασύρματη τεχνολογία υψηλής απόδοσης (High Efficiency Wireless), σχεδιάστηκε με σκοπό να αντιμετωπίσει προβλήματα συνδεσιμότητας σε δίκτυα υψηλής πυκνότητας βελτιώνοντας έτσι συνολικά την επίδοση ολόκληρου του δικτύου. Το πρότυπο IEEE 802.11ax είναι το τελευταίο βήμα σε ένα ταξίδι ασταμάτητης καινοτομίας. Βασίζεται στα δυνατά σημεία του 802.11ac, ενώ προσθέτει ευελιξία και επεκτασιμότητα που επιτρέπει στα νέα και υπάρχοντα δίκτυα να τροφοδοτούν εφαρμογές επόμενης γενιάς. Το IEEE 802.11ax συνδυάζει την ελευθερία και την υψηλή ταχύτητα του ασύρματου gigabit με την προβλεψιμότητα που βρίσκουμε στο αδειοδοτημένο ραδιόφωνο (LTE). Τα νέα χαρακτηριστικά επιτρέπουν σε πολλούς ταυτόχρονους χρήστες να μεταδίδουν ταυτόχρονα, αυξάνοντας με αυτό τον τρόπο την χωρητικότητα του δικτύου έως και 4 φορές σε σύγκριση με το 802.11ac. Το νέο πρότυπο προορίζεται να χρησιμοποιήσει τεχνικές που θα μπορούν να αυξήσουν τον φυσικό ρυθμό bit, αλλά και να μειώσουν το ρυθμό σφάλματος καρέ (FER) και να βελτιώσουν την επαναχρησιμοποίηση του διαθέσιμου φάσματος επιτρέποντας την πολύ αποτελεσματική πρόσβαση πολλαπλών χρηστών ταυτόχρονα με τον περιορισμό / μείωση των παρεμβολών, οι οποίες σε αντάλλαγμα θα αυξήσουν την απόδοση του συστήματος. Το

IEEE 802.11ax επιτρέπει σε επιχειρήσεις και παρόχους υπηρεσιών να υποστηρίζουν νέες και αναδυόμενες εφαρμογές στην ίδια υποδομή ασύρματου LAN (WLAN), ενώ παρέχει υψηλότερου βαθμού υπηρεσίες σε παλαιότερες εφαρμογές. Αυτό το σενάριο θέτει το στάδιο για νέα επιχειρηματικά μοντέλα και αυξημένη υιοθέτηση Wi-Fi.



Εικόνα 14, Source Aruba Networks

Το 802.11ax έχει επίσης σχεδιαστεί για εκφόρτωση δεδομένων (data offloading) κινητής τηλεφωνίας. Σε αυτό το σενάριο, το δίκτυο κινητής τηλεφωνίας εκφορτώνει την ασύρματη κίνηση σε ένα συμπληρωματικό δίκτυο Wi-Fi σε περιπτώσεις όπου η λήψη τοπικών κυψελών είναι κακή ή σε καταστάσεις όπου το δίκτυο κινητής τηλεφωνίας φορολογείται. [3], [4]

2.2 Τι είναι και τι περιλαμβάνει το νέο πρότυπο 802.11ax

Το πρότυπο 802.11ax στοχεύει στη βελτίωση της φασματικής απόδοσης και της απόδοσης της κάθε περιοχής κάλυψης μέσω της πυκνής κάλυψης access points. Επίσης, με τεχνολογία που θα παρουσιαστεί παρακάτω μπορεί και αυξάνει το συνολικό εύρος ζώνης μειώνοντας τις περιοχές αλληλοκάλυψης μεταξύ των access points. Το 802.11ax παρέχει μεγαλύτερη χωρητικότητα δικτύου, υψηλότερη απόδοση και μειωμένη καθυστέρηση.

2.2.1 Βασικά οφέλη του IEEE 802.11ax

- Αύξηση της συνολικής χωρητικότητας του δικτύου
- Υψηλότεροι ρυθμοί μετάδοσης
- Βελτιωμένη απόδοση σε πυκνό περιβάλλον
- Βελτιωμένη απόδοση ισχύος

2.2.2 Δυνατότητες του IEEE 802.11ax

- Ταυτόχρονη λειτουργία πολλαπλών χρηστών στο ίδιο κανάλι
- Αυξημένη δυνατότητα ταυτόχρονης μεταφόρτωσης (Upload) δεδομένων
- Καλύτερη χρήση φάσματος
- Νέες λειτουργίες διαμόρφωσης
- Βελτιωμένη σήμανση ελέγχου (Control Signaling) στο MAC επίπεδο

Το IEEE 802.11ax επιτρέπει στα σημεία πρόσβασης να υποστηρίζουν περισσότερους χρήστες σε πυκνά περιβάλλοντα και να παρέχουν μια καλύτερη εμπειρία για τυπικά δίκτυα ασύρματου LAN. Εξασφαλίζει επίσης πιο προβλέψιμη απόδοση για προηγμένες εφαρμογές, όπως βίντεο 4K, Ultra HD, ασύρματο γραφείο και Internet of Things (IoT). Επίσης, εξασφαλίζεται ευέλικτος προγραμματισμός χρόνου αφύπνισης, επιτρέποντας στις συσκευές των πελατών να 'κοιμούνται' πολύ περισσότερο από ό, τι με το 802.11ac, παρατείνοντας τη διάρκεια ζωής της μπαταρίας των έξυπνων τηλεφώνων, του IoT και άλλων συσκευών.

Το IEEE 802.11ax επιτυγχάνει αυτά τα οφέλη με την βοήθεια των 3 παρακάτω τεχνολογιών:

- Πυκνότερη Διαμόρφωση χρησιμοποιώντας την 1024-QAM διαμόρφωση, επιτρέποντας με αυτό τον τρόπο ριπή ταχύτητας(burst) άνω του 35%
- (OFDMA)-based προγραμματισμός για την μείωση της καθυστέρησης
- Εύρωστη σηματοδότηση υψηλής απόδοσης για καλύτερη λειτουργία σε σημαντικά χαμηλότερο επίπεδο Received Signal Strength Indication (RSSI)

Η τεχνολογία IEEE 802.11ax OFDMA επιτρέπει ακόμη και τα σημεία πρόσβασης 802.11ax πρώτου κύματος(wave 1) να υποστηρίζουν οκτώ χωρικές ροές (spatial streams) και να παρέχουν έως και 4800 Mbps στο φυσικό επίπεδο, ανάλογα με την υλοποίηση του προμηθευτή (vendor). Όλοι οι πελάτες θα επιτύχουν αποτελεσματικότερη απόδοση στο επίπεδο MAC, για καλύτερη συνολική εμπειρία χρήστη. Το πρότυπο 802.11ax έχει δύο τρόπους λειτουργίας, δηλαδή λειτουργία ενός χρήστη και λειτουργία για πολλαπλούς χρήστες. Στη λειτουργία ενός χρήστη, η ασύρματη διαδοχική λειτουργία RSTA στέλνει και λαμβάνει δεδομένα ταυτόχρονα μετά την ασφαλή πρόσβαση σε πολυμέσα. Ενώ βρίσκεται σε κατάσταση λειτουργίας πολλών χρηστών, μπορεί να πραγματοποιήσει ταυτόχρονες λειτουργίες πολλών STA εκτός AP. Το πρότυπο χωρίζει αυτή τη λειτουργία περαιτέρω σε Downlink και Uplink Multi-user. Η κατερχόμενη σύνδεση πολλαπλών χρηστών βασίζεται σε δεδομένα που εκτελούνται από το AP για πολλά σχετικά ασύρματα STA ταυτόχρονα. Το Multilink MU-MIMO παρέχει δυνατότητες τόσο στα σημεία πρόσβασης 802.11ac όσο και 802.11ax έτσι ώστε να μπορούν να λαμβάνουν και να στέλνουν ταυτόχρονα σε πολλούς χρήστες (MU) από ένα σημείο πρόσβασης. Αυτή η δυνατότητα παρέχει ευελιξία στα σημεία πρόσβασης για την εξυπηρέτηση πελατών-χρηστών στην περιοχή κάλυψης του σημείου πρόσβασης. Οι μέθοδοι που χρησιμοποιούνται και στα δύο πρωτόκολλα είναι MIMO πολλαπλών χρηστών και OFDMA. Η τεχνολογία που χρησιμοποιείται στο κινητό 4G εφαρμόζεται στο IEEE 802.11ax για να φιλοξενήσει περισσότερους χρήστες στο ίδιο κανάλι. Αυτή η τεχνολογία ονομάζεται OFDMA.

2.2.3 Αύξηση ταχύτητας δεδομένων στο 802.11ax

Η μέγιστη ασύρματη ταχύτητα είναι το προϊόν τεσσάρων παραγόντων: εύρος ζώνης καναλιού, πυκνότητα αστερισμού, αριθμός χωρικών ροών και overhead ανά σύμβολο (εύρος καναλιού, πυκνότητα αστερισμού, αριθμός χωρικών ροών, και overhead ανά σύμβολο). Το IEEE 802.11ax προωθεί την πυκνότητα αστερισμού 1024 QAM, αλλά βελτιώνει σημαντικά την επιβάρυνση ανά σύμβολο με ευέλικτες παραμέτρους χρονισμού PHY. Πρώτον, η μετάβαση από 256 QAM σε 1024 QAM αυξάνει τον μέγιστο ρυθμό δεδομένων κατά $10/8 = 1.25$ φορές. Η διαμόρφωση 256 QAM είναι πιο αξιόπιστη, αλλά η διαμόρφωση 1024 QAM δεν απαιτεί περισσότερο φάσμα ή περισσότερες κεραιές από την 256 QAM. Μπορεί να εφαρμοστεί εύκολα με τα υπάρχοντα φυσικά συστήματα.

Στη συνέχεια, η ταχύτητα είναι άμεσα ανάλογη με τον αριθμό των χωρικών ροών (spatial streams). Περισσότερα spatial streams απαιτούν και περισσότερες κεραιές, RF connectors, και RF chains στον πομπό και στον δέκτη. Τα 802.11ax access points, έχουν την δυνατότητα να υποστηρίζουν μέχρι και 8 spatial streams, που είναι διπλάσιος από τον μέγιστο αριθμό που παρέχεται στο 802.11ac. [6] Στην παρακάτω εικόνα φαίνεται ο υπολογισμός των μέγιστων ταχυτήτων κάθε πρότυπο, με βάση τα spatial streams που χρησιμοποιούνται.

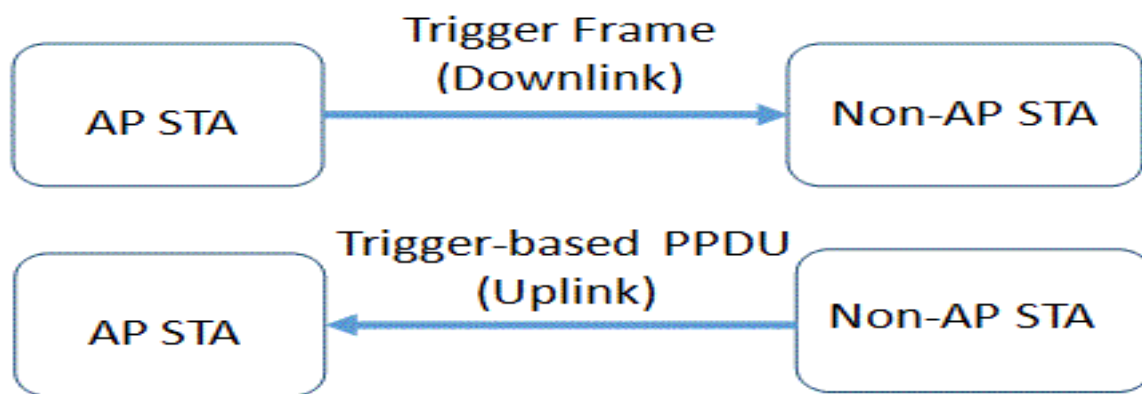
PHY	Bandwidth (as number of data subcarriers)		Data bits per subcarrier	Time per OFDM symbol (800ns GI)	1 SS	3 SS	4 SS	8 SS
802.11ac	234 (80 MHz)	X	$5/6 \times \log_2(256)$ ≈ 6.67	4 μ s	390 Mbps	1.17 Gbps	1.56 Gbps	-
	2 x 234 (160 MHz)		/	=	780 Mbps	-	3.12 Gbps	-
802.11ax	980 (80 MHz)		$5/6 \times \log_2(1024)$ ≈ 8.33	13.6 μ s	600 Mbps	1.8 Gbps	2.4 Gbps	4.8 Gbps
	2 x 980 (160 MHz)				1.2 Gbps	3.6 Gbps	4.8 Gbps	-

Εικόνα 15 Cisco, Υπολογίζοντας την ταχύτητα του 802.11ac και του 802.11ax

2.3 Επιλογή σημείου πρόσβασης στο 802.11ax

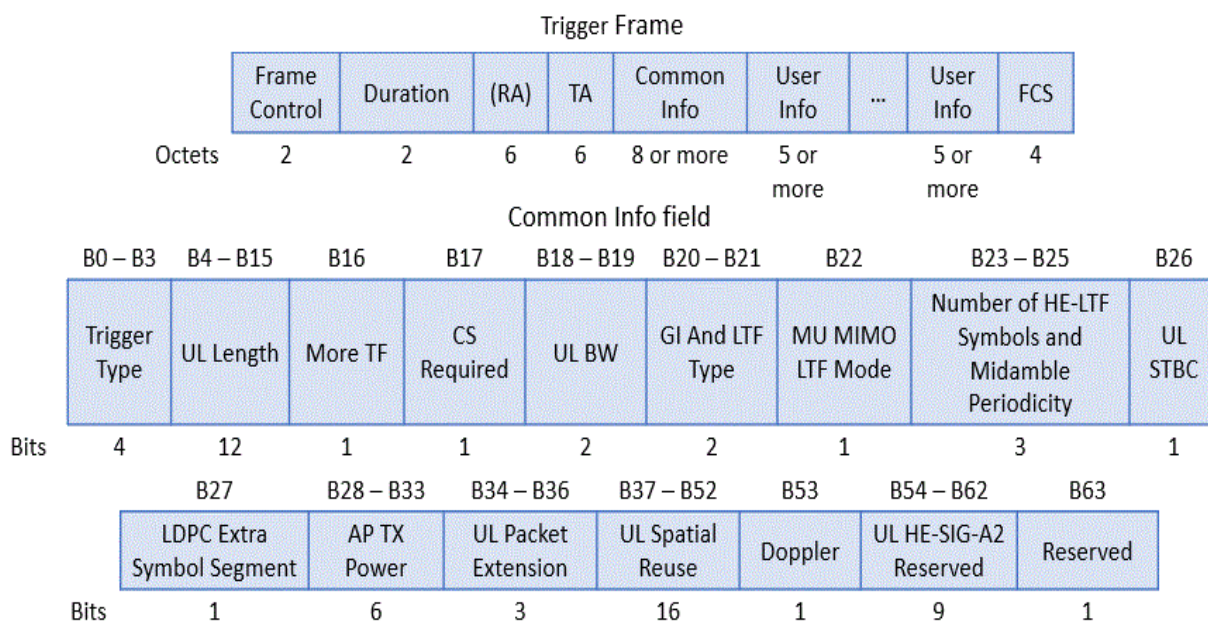
Η σύνδεση σε ένα access point στα έως τώρα ασύρματα 802.11 δίκτυα ήταν απόφαση της συσκευής του πελάτη. Οι συσκευές 'ακούν' τα beacons που στέλνει το access point ή στέλνουν αιτήματα ανίχνευσης για να ανακαλύψουν AP που διαφημίζουν το προτιμώμενο SSID. Έπειτα οι drivers της συσκευής του πελάτη χρησιμοποιούν την ισχύ του σήματος λήψης των beacons ή των απαντήσεων του αισθητήρα για να αποφασίσουν σε ποιο AP θα συνδεθεί. Η επιλογή του STA θα γίνει βάση των τιμών του RSSI που μπορεί να υποστηρίξει η συσκευή. Το RSSI (Received Signal Strength Indicator) είναι μία μέτρηση για το πόσο καλά η συσκευή μας μπορεί να 'ακούσει' ένα σήμα από κάποιο access point. Η τιμή αυτή είναι πολύ σημαντική διότι καθορίζει για τον εάν το σήμα επαρκεί προκειμένου να υπάρχει μία καλή ασύρματη σύνδεση. Επειδή η τιμή RSSI λαμβάνεται από την κάρτα Wi-Fi της συσκευής του πελάτη (εξ ου και η ένταση σήματος που έχει «ληφθεί»), δεν είναι ίδια με την ισχύ μετάδοσης από έναν δρομολογητή ή ένα AP. Το RSSI είναι ένας όρος που χρησιμοποιείται για τη μέτρηση της σχετικής ποιότητας ενός ληφθέντος σήματος σε μια συσκευή πελάτη, αλλά δεν έχει απόλυτη τιμή. Το πρότυπο IEEE 802.11 καθορίζει ότι το RSSI μπορεί να είναι σε κλίμακα από 0 έως και 255 και ότι κάθε κατασκευαστής chipset μπορεί να καθορίσει τη δική του τιμή "RSSI_Max". Η Cisco, για παράδειγμα, χρησιμοποιεί κλίμακα 0-100, ενώ η Atheros χρησιμοποιεί 0-60. Όλα εξαρτώνται από τον κατασκευαστή (αυτός είναι ο λόγος για τον οποίο το RSSI είναι ένας σχετικός δείκτης), αλλά γίνεται αντιληπτό ότι όσο υψηλότερη είναι η τιμή RSSI, τόσο καλύτερο είναι το σήμα. Το RSSI μετριέται σε dBm. Όσο πιο κοντά στα 0 dBm είναι η τιμή, τόσο καλύτερο είναι το λαμβανόμενο σήμα. Η απαιτούμενη ισχύς του σήματος στο access point για τη μετάδοση προς τον χρήστη υπολογίζεται από τον χρήστη, χρησιμοποιώντας το επίπεδο ισχύος μετάδοσης του access point, το επίπεδο του RSSI του πελάτη και την παραδοχή της αμοιβαιότητας του καναλιού. Η τιμή του RSSI τραβιέται από την κάρτα Wi-Fi της συσκευής του πελάτη (εξ ου και "ισχύς σήματος λήψης").

Στο Wi-Fi 6 και λόγω του Mu-MIMO ένας user equipment μπορεί να συνδεθεί σε περισσότερες από μία κεραίες πάνω στο ίδιο access point και πάντα με βάση το RSSI έχοντας έτσι ως αποτέλεσμα να επιτυγχάνει πολύ μεγαλύτερες αποδόσεις. Αυτό που αλλάζει στον νέο ασύρματο πρότυπο είναι ότι η επιλογή του RSSI κατευθύνεται από το Access Point. Η μετάδοση πολλαπλών χρηστών στην ανερχόμενη ζεύξη στο 802.11ax (HE) ξεκινά με ένα trigger frame από ένα σταθμό σημείου πρόσβασης (AP STA), όπως φαίνεται και στο παρακάτω σχήμα. Το 802.11ax καθορίζει έναν μηχανισμό προ-διόρθωσης ισχύος, σύμφωνα με τον οποίο το AP υποδεικνύει στο trigger frame την τρέχουσα ισχύ μετάδοσης και την ισχύ σήματος στόχου (target signal strength) που αναμένεται να λάβει το AP από ένα STA στην ακόλουθη μετάδοση UL. Έτσι, γνωρίζοντας την ισχύ μετάδοσης του AP και την ισχύ σήματος του ληφθέντος trigger frame, το STA μπορεί να εκτιμήσει την απώλεια διαδρομής προς το AP και μπορεί να υπολογίσει την κατάλληλη ισχύ μετάδοσης για την ακόλουθη μετάδοση UL. Σημειώνεται ότι αφού το AP (όχι ένα STA!) επιλέγει το Σχήμα κωδικοποίησης διαμόρφωσης, Modulation Coding Scheme για τις μεταδόσεις UL, κάθε STA περιλαμβάνει επίσης πληροφορίες σχετικά με το UL power headroom του, δηλαδή τη διαφορά μεταξύ της μέγιστης ισχύος μετάδοσης και της τρέχουσας ισχύος μετάδοσης για το εκχωρημένο MCS. [5]



Εικόνα 16 Trigger Frame

Όπως ορίζεται στο πρότυπο IEEE P802.11ax / D3.0; το πλαίσιο ενεργοποίησης περιέχει όλες τις πληροφορίες που σχετίζονται με τον χρήστη και κοινές πληροφορίες μεταξύ των χρηστών. Η παρακάτω εικόνα απεικονίζει τη μορφή του trigger frame.



Εικόνα 17 Trigger Frame

Για το UL- OFDMA, το trigger frame που αποστέλλεται από το AP χρησιμοποιείται για να ενημερώσει τους χρήστες πόσες χωρικές ροές (spatial streams) και ποιο σχήμα διαμόρφωσης και κωδικοποίησης (MCS) να χρησιμοποιήσουν κατά τη μετάδοση ανερχόμενης ζεύξης στις RU που τους έχουν αποδοθεί. Αυτές οι πληροφορίες μπορούν να βρεθούν στην κατανομή SS και στα υποπεδία UL MCS στο πεδίο πληροφοριών χρήστη μέσα στο σώμα ενός trigger frame. Τα trigger frames μπορούν επίσης να χρησιμοποιηθούν από ένα AP για να πει στους πελάτες να προσαρμόσουν τις ρυθμίσεις ισχύος τους για συγχρονισμένες μεταδόσεις uplink. Μέσα σε ένα trigger frame, το υποπεδίο UL Target RSSI υποδηλώνει, σε τιμές dBm, την αναμενόμενη ισχύ λήψης στο AP σε όλες τις κεραίες για τις μεταβιβαζόμενες μονάδες πόρων (RU) μεταδόσεις από τους πελάτες 802.11ax. Το υποπεδίο UL Target RSSI χρησιμοποιεί τιμές από 0 έως 90 οι οποίες αντιστοιχίζονται απευθείας σε -110 dBm έως -20 dBm. Μια τιμή 127 υποδεικνύει

στο σταθμό χρήστη (STA) να μεταδίδει στη μέγιστη ισχύ του για το εκχωρημένο MCS. Με βάση αυτές τις πληροφορίες που παρέχονται από το trigger frame, η ισχύς μετάδοσης θα μπορούσε να ρυθμιστεί από τους uplink χρήστες. Ας ληφθεί υπόψη, ότι ένας σταθμός πελάτη ενδέχεται να μην μπορεί να ικανοποιήσει τον στόχο RSSI λόγω των περιορισμών του υλικού ή των κανονιστικών ρυθμίσεων.

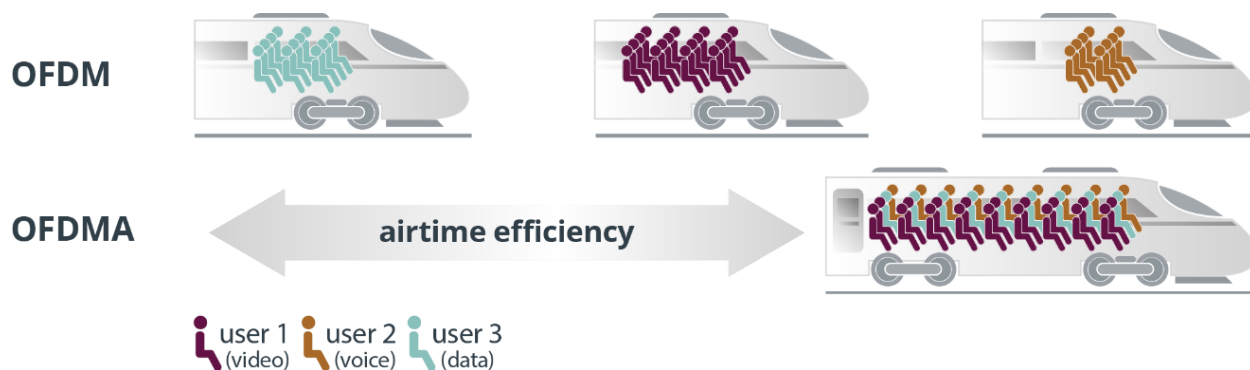
2.4 Επισκόπηση τεχνολογικών δυνατοτήτων του IEEE 802.11ax

Για την αποδοτικότερη χρήση του φάσματος, η νέα έκδοση του Wi-Fi εισάγει καλύτερες μεθόδους ελέγχου της ισχύος για την αποφυγή παρεμβολών σε γειτονικά δίκτυα, υποστηρίζει OFDMA (Orthogonal Frequency-Division Multiple Access), μία εξέλιξη της τεχνικής διαμόρφωσης με την ονομασία «Ορθογώνια Πολυπλεξία Διαίρεσης Συχνότητας», έχει υψηλότερης τάξης 1024-QAM, παρέχει υποστήριξη MIMO και MU-MIMO (Multi-User MIMO) για περαιτέρω αύξηση της απόδοσης καθώς και βελτιώσεις στην κατανάλωση ενέργειας σε συνδυασμό με διάφορα πρωτόκολλα για την αύξηση της ασφαλείας, όπως τα Target Wake Time αντίστοιχα.

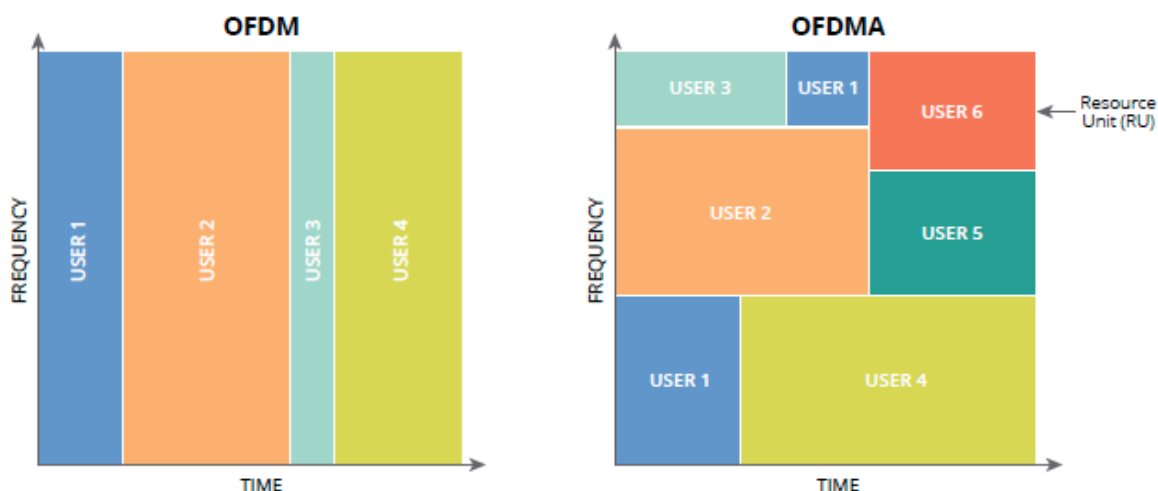
2.4.1 OFDMA - Orthogonal Frequency Division Multiple Access

Η υποστήριξη της διαμόρφωσης OFDMA (Orthogonal Frequency-Division Multiple Access), uplink και downlink, επιτρέπει σε έως και 30 συσκευές να μοιράζονται το ίδιο κανάλι ταυτόχρονα, αυξάνοντας τη «χωρητικότητα του δικτύου» και βελτιώνοντας σημαντικά την υστέρηση (latency, έως και κατά 75%). Με αυτή την τεχνική που δανείζεται από τα δίκτυα κινητής τηλεφωνίας, υπολογίζονται οι ανάγκες ευρυζωνικότητας (bandwidth) κάθε χρήστη ξεχωριστά και επομένως επιλύει ζητήματα που έχουν να κάνουν με τη συμφόρηση του δικτύου διαμοιράζοντας το bandwidth αποτελεσματικά σε όλους τους συνδεδεμένους χρήστες/ συσκευές.

Το OFDMA επιφέρει βελτίωση σε σχέση με προηγούμενες εκδόσεις Wi-Fi που χρησιμοποιούν ορθογώνια πολυπλεξία διαίρεσης συχνότητας (OFDM). Υποδιαιρεί το κανάλι Wi-Fi σε μικρότερες εκχωρήσεις συχνότητας που ονομάζονται μονάδες πόρων (resource units). Με το διαχωρισμό του καναλιού, πραγματοποιούνται ταυτόχρονα παράλληλες μεταδόσεις μικρότερων καρτέ (frame) σε πολλούς χρήστες (Εικόνα 18). Για παράδειγμα, ένα παραδοσιακό κανάλι 20 MHz μπορεί να χωριστεί σε εννέα μικρότερα κανάλια. Χρησιμοποιώντας το OFDMA, ένα Wi-Fi 6 AP θα μπορούσε ταυτόχρονα να μεταδώσει μικρότερα καρτέ σε εννέα χρήστες Wi-Fi 6. [3]



Εικόνα 18 Το OFDMA στο Wi-Fi 6 επιτρέπει σε πολλούς χρήστες με διαφορετικά προφίλ κυκλοφορίας να μεταδίδουν ταυτόχρονα μέσω του ίδιου καναλιού



Εικόνα 19 OFDM vs OFDMA Block

2.4.1.1 Ανερχόμενη ζεύξη OFDMA

Το Uplink OFDMA είναι ένα από τα βασικά χαρακτηριστικά που εισήγαγε το Wi-Fi 6 και είναι από τις σημαντικότερες διαφορές σε σχέση με το 802.11ac. Το Uplink OFDMA επιτρέπει την ταυτόχρονη μετάδοση πλαισίων δεδομένων (data frames) από πολλούς σταθμούς, κάτι που οδηγεί στην απόσβεση του preamble overhead και το medium contention overhead, τα οποία οδηγούν σε υψηλή απόδοση δικτύου. Το Uplink OFDMA μπορεί να προσφέρει πρόσθετα κέρδη επιτρέποντας μεγαλύτερο επίπεδο ισχύος μετάδοσης ανά συσκευή, με την επιφύλαξη ρυθμιστικών απαιτήσεων, και επομένως κάλυψη σήματος στην ανερχόμενη ζεύξη, καθώς η ισχύς μετάδοσης κάθε συσκευής πελάτη μπορεί να συγκεντρωθεί σε μικρότερες εκχωρημένες μονάδες πόρων (can be concentrated on smaller allocated resource units).

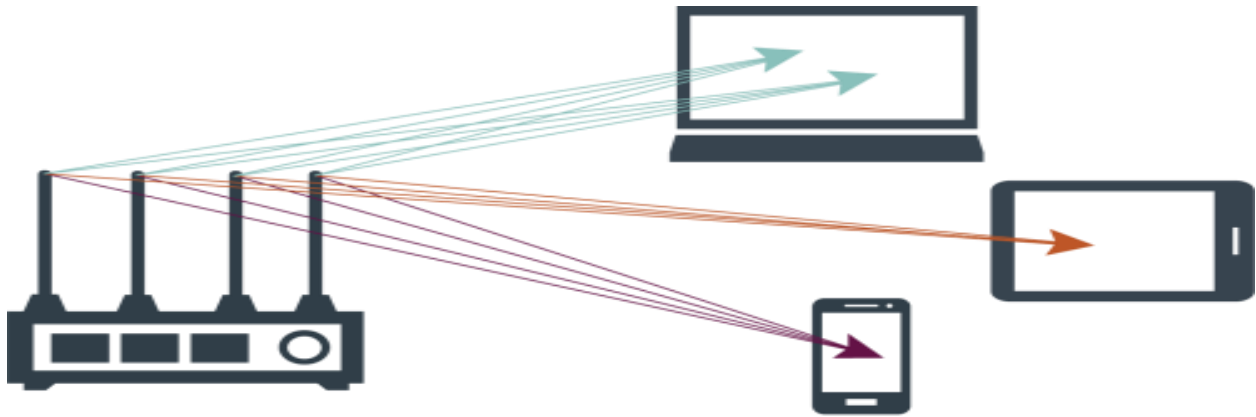
2.4.1.2 Κατερχόμενη ζεύξη OFDMA

Το Downlink OFDMA επιτρέπει τη μετάδοση πολλαπλών data frames σε μία μόνο μονάδα δεδομένων (single data unit) προς πολλούς σταθμούς, αποσβένοντας έτσι το preamble overhead και το medium contention overhead, οδηγώντας σε υψηλότερη απόδοση δικτύου. Το Downlink OFDMA μπορεί να βελτιστοποιήσει περαιτέρω τη συνολική απόδοση εξισορροπώντας την κατανομή ισχύος μεταξύ των χρηστών σε υψηλές και χαμηλές αναλογίες σήματος προς θόρυβο, με την επιφύλαξη των συνολικών περιορισμών ισχύος και των κανονιστικών απαιτήσεων. [3]

2.4.1.3 Κατερχόμενη ζεύξη multi-user MIMO

Με το downlink MU MIMO, ένα σημείο πρόσβασης (AP) μπορεί να μεταδίδει ταυτόχρονα σε πολλαπλούς σταθμούς/ συσκευές και με uplink MU MIMO μπορεί ταυτόχρονα να λαμβάνει από πολλαπλούς σταθμούς/ συσκευές. Στην ουσία, χάρη στην υποστήριξη MU MIMO, επιτρέπει τον σωστότερο ή και δικαιότερο καταμερισμό του εύρους ζώνης (bandwidth) μεταξύ των συνδεδεμένων συσκευών (αρκεί να το υποστηρίζουν) καθώς η μετάδοση δεδομένων γίνεται ταυτόχρονα και όχι διαδοχικά. Το MU MIMO υποστηρίζεται μαζί και με beamforming. Το Downlink multi-user MIMO επιτρέπει υψηλότερη απόδοση σε περιβάλλοντα με συσκευές που περιέχουν περιορισμένο αριθμό

κεραίων, πολυπλέκοντας τις μεταδόσεις τους στον χωρικό τομέα (spatial domain). Παρουσιάστηκε στο 802.11ac για να υποστηρίξει ταυτόχρονα έως και τέσσερις χρήστες, το Wi-Fi 6 επεκτείνει το MIMO πολλαπλών χρηστών και διπλασιάζει τον αριθμό των συσκευών που μπορούν να υποστηριχθούν αποτελεσματικά σε οκτώ χρήστες. Μαζί με το downlink OFDMA, το οποίο λειτουργεί στον τομέα συχνοτήτων, αυτή η δυνατότητα επιτρέπει σε ένα Wi-Fi 6 AP να προγραμματίζει μεταδόσεις πολλαπλών χρηστών downlink σε χωρικές ροές (spatial streams) ή συχνοτήτες. [3]



Εικόνα 20 Multi-user multiple input, multiple output

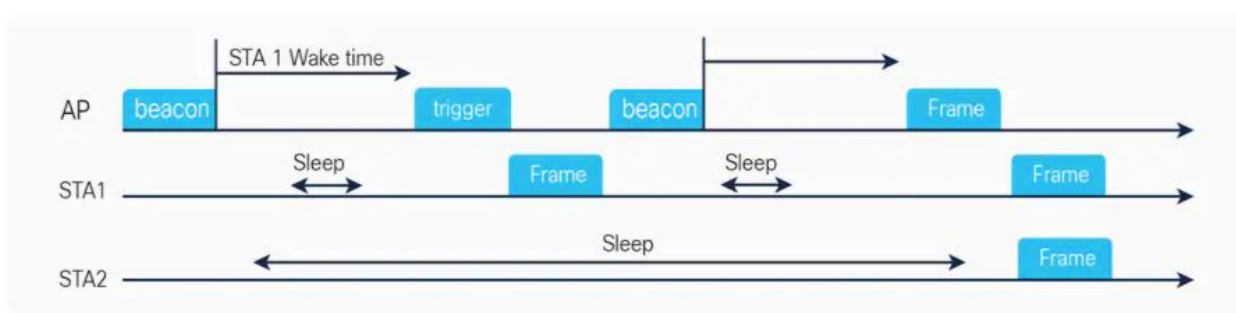
Είναι ένας άλλος τρόπος για την διαχείριση της δικτυακής κίνησης από πολλές συσκευές, ο οποίος αρχικά εισήχθη στο 802.11ac. Στο 802.11ax, αυτή η δυνατότητα έχει βελτιωθεί επιτρέποντας την μετάδοση έως και 8 συσκευών ταυτόχρονα χρησιμοποιώντας ένα ειδικό κανάλι ανά συσκευή. Αυτό επιτρέπει σε μεγάλα πακέτα, όπως streaming HD video να μπορούν να διαχειριστούν πιο αποτελεσματικά, ενώ μικρότερα πακέτα από IoT συσκευές καθώς και voice traffic να μπορούν να διαχειριστούν καλύτερα χρησιμοποιώντας το OFDMA.

2.4.2 Μετάδοση μορφής δέσμης (Transmit beamforming)

Παραδοσιακά, τα σημεία πρόσβασης διαθέτουν πανκατευθυντικές (omnidirectional) κεραίες, οι οποίες ονομάζονται έτσι επειδή στέλνουν ενέργεια προς όλες τις κατευθύνσεις. Συχνά, η omnidirectional κάλυψη εμφανίζεται ως ένας κύκλος με επίκεντρο το AP. Οι omnidirectional κεραίες μεταδίδουν ραδιοκύματα προς κάθε κατεύθυνση, απελευθερώνοντας το AP από την ανάγκη παρακολούθησης κάθε πελάτη. Μια εναλλακτική μέθοδος μετάδοσης η ενέργεια να εστιάζεται προς έναν δέκτη, μια διαδικασία που ονομάζεται beamforming. Το Beamforming εστιάζει την ενέργεια προς έναν ασύρματο χρήστη. Η μετάδοση δέσμης επιτρέπει σημαντικά υψηλότερους ρυθμούς δεδομένων σε ένα δεδομένο εύρος που οδηγεί σε συνολικά υψηλότερη απόδοση δικτύου. Η μετάδοση δέσμης εστιάζει την ενέργεια προς έναν δέκτη για τη βελτίωση του SNR ενός συνδέσμου (link). Σε αυτό το σχήμα, ο πομπός ονομάζεται beamformer και ο δέκτης ονομάζεται beamformee. Ένα σύστημα διεύθυνσης χρησιμοποιείται από τον διαμορφωτή δέσμης για να κατευθύνει την ενέργεια προς τον beamformee. Το Wi-Fi 6 προσθέτει σημαντική βελτίωση υποστηρίζοντας έως και οκτώ χωρικές ροές (spatial-streams).

2.4.3 Target Wake Time

Το Target Wait Time (TWT) είναι ένας μηχανισμός που επιτρέπει τον προγραμματισμό των ανταλλαγών κίνησης μεταξύ ενός AP και μιας συσκευής πελάτη. Η προγραμματισμένη συμπεριφορά μειώνει το overhead και την αναποτελεσματικότητα της μεθόδου πρόσβασης καναλιού για την απόκτηση ευκαιριών μετάδοσης και επιτρέπει στις συσκευές πελάτη εξοικονόμηση ενέργειας με την μείωση της κατανάλωσης ενέργειας, προσδιορίζοντας ρητά τους χρόνους που πρέπει να είναι ξύπνιοι. Η διάρκεια ζωής της μπαταρίας των χρηστών βελτιώνεται με μια λειτουργία που ονομάζεται χρόνος αφύπνισης στόχου (TWT, Target Wake Time), ο οποίος επιτρέπει στις συσκευές να παραμείνουν ανενεργές μέχρι να είναι η σειρά τους για να μεταδώσουν δεδομένα. Αυτό γίνεται με την χρήση ενός προγράμματος προγραμματισμού που συμφωνήθηκε με τα AP (Access Points). Επειδή οι συσκευές μπορούν να μεταβούν στην ανενεργή λειτουργία, η διάρκεια ζωής της μπαταρίας των έξυπνων τηλεφώνων, των tablet και των συσκευών IoT αποτελεί ένα υποκειμενικό όφελος. Το αποτέλεσμα είναι να υπάρχει λιγότερη συμφόρηση, εξοικονόμηση ενέργειας και συνολικά καλύτερη εμπειρία χρήστη. [3] Γενικά, η συσκευή μπορεί να ζητήσει ένα πρόγραμμα για να ξυπνήσει ανά πάσα στιγμή στο μέλλον. Το αποτέλεσμα είναι η σημαντική εξοικονόμηση ενέργειας για συσκευές με μπαταρία, ιδίως εκείνες που βρίσκονται στο χώρο του IoT.



Εικόνα 21 Λειτουργία του Target Wakeup Time (TWT)

Ένα σχετικό αλλά σημαντικό πλεονέκτημα του TWT είναι ότι μπορεί επίσης να χρησιμοποιηθεί ως μέθοδος προγραμματισμού ανερχόμενης ζεύξης που μοιάζει με το UL-OFDMA. Δηλαδή, επειδή το TWT θέτει αποτελεσματικά τους πελάτες να κοιμούνται με έναν προκαθορισμένο χρόνο αφύπνισης (με βάση το αίτημά τους), είναι δυνατός ο ντετερμινιστικός χρόνος μετάδοσης και επομένως ο προγραμματισμός ανερχόμενων ζεύξεων. Το σημείο πρόσβασης μπορεί να χρησιμοποιήσει αυτήν την ικανότητα τόσο για τη μείωση της διαμάχης (μεγαλύτερη κατανομή χρήσης καναλιών) όσο και για την αντιμετώπιση της ευαισθησίας καθυστέρησης των εφαρμογών.

2.4.4 Χωρική επαναχρησιμοποίηση και λειτουργία Overlapping BSS (OBSS)

Το Wi-Fi 6 εισάγει πολλές τεχνικές που επιτρέπουν σε μια συσκευή υπό ορισμένες συνθήκες να είναι πιο 'επιθετική' στην πρόσβαση στο μέσο κατά τη διάρκεια της μετάδοσης δεδομένων από συσκευές που βρίσκονται σε άλλα ασύρματα δίκτυα. Αυτό είναι γνωστό ως χωρική επαναχρησιμοποίηση (spatial reuse). Μία τέτοια τεχνική είναι ο μηχανισμός χρωματισμού, ο οποίος επιτρέπει σε μια συσκευή να προσδιορίσει γρήγορα εάν μια μετάδοση ανήκει στο δίκτυό της. Με οποιοδήποτε ασύρματο σύστημα συμπεριλαμβανομένων των δικτύων που βασίζονται σε CSMA 802.11, η κοινή χρήση του ίδιου καναλιού RF στον ίδιο φυσικό χώρο ήταν πάντα μια πρόκληση. Παρόλο που το 802.11 το κάνει πιο εύρωστο από τις εναλλακτικές λύσεις, οι πελάτες (STA) και τα σημεία πρόσβασης εξακολουθούν να ενεργούν ανεξάρτητα για να μεγιστοποιήσουν τη δική τους Ποιότητα Εμπειρίας (QoE). Για παράδειγμα, ορισμένοι πελάτες ενδέχεται να χρησιμοποιούν υπερβολική ισχύ δεδομένης της εγγύτητας με το σχετικό σημείο πρόσβασης, δημιουργώντας περιττές παρεμβολές ή μπορεί να χρησιμοποιούν πολύ μικρή ισχύ λόγω της παρεμβολής και δεν μπορούν να φτάσουν στο σημείο πρόσβασης. Το επίπεδο του σήματος (RSSI) στο οποίο ένα STA καθορίζει ότι το κανάλι είναι «ελεύθερο να μεταδώσει» ή αυτό που ονομάζουμε Carrier Sense (CS) ήταν ιστορικά συντηρητικό με βάση τις ελάχιστες προσδοκίες απόδοσης και στην πράξη συμπληρωμένο από μεμονωμένους προμηθευτές για τη βελτίωση της απόδοσης. Ωστόσο, με την εξέλιξη της τεχνολογίας, το 802.11ax τυποποιεί αυτήν τη συμπεριφορά για να εξασφαλίσει βέλτιστες βελτιώσεις απόδοσης επισημοποιώντας τέσσερις έννοιες:

1. Overlapping Basic Service Set (OBSS) είναι η αλληλοεπικάλυψη ή παρεμβολή μεταξύ ενός BSS (δηλαδή, το σημείο πρόσβασης και τα σχετικά STA) με τα οποία σχετίζεται το STA και ένα γειτονικό BSS με το οποίο δεν σχετίζεται το STA.
2. BSS Color είναι μια μέθοδος διαφοροποίησης μεταξύ BSS (δηλαδή, σημεία πρόσβασης και οι πελάτες τους) στο ίδιο κανάλι RF.
3. OBSS Packet Detection (PD) είναι η ικανότητα ανίχνευσης σημάτων από άλλα BSS (OBSS).
4. Clear Channel Assessment έλεγχος κατωφλίου είναι η ικανότητα μιας συσκευής να αλλάζει την ευαισθησία CCA με βάση το σχετικό σημείο πρόσβασης και την τρέχουσα μετάδοση.

Clear Channel Assessment (CCA): Το Clear Channel Assessment (CCA) είναι ένας μηχανισμός για τον προσδιορισμό του αν το μέσο είναι αδρανές ή όχι. Το CCA περιλαμβάνει ανίχνευση φορέα και ανίχνευση ενέργειας. Πριν από τη μετάδοση ενός πακέτου, η συσκευή εκτελεί ένα CCA (Clear Channel Assessment) στο κανάλι για να προσδιορίσει εάν το κανάλι είναι διαθέσιμο για μετάδοση. Η ανιχνευόμενη ενέργεια στο κανάλι συγκρίνεται με την τιμή παραμέτρου CA (Clear Channel Assessment). Εάν η ανιχνευθείσα ενέργεια υπερβαίνει την τιμή παραμέτρου CA, η συσκευή δεν μεταδίδει το πακέτο. Όταν συνδυάζονται αυτές τις έννοιες, υπάρχει η δυνατότητα αποτελεσματικής διαχείρισης των παρεμβολών σε διαχειριζόμενα δίκτυα, όπως αυτά που αναπτύσσονται από επιχειρήσεις και παρόχους υπηρεσιών. Συγκεκριμένα, αυτή η δυνατότητα επιτρέπει στους πελάτες και τα σημεία πρόσβασης να συμφωνούν σιωπηρά για τα απαιτούμενα επίπεδα ανίχνευσης πακέτων ή «απασχολημένων» ορίων σήματος και ισχύος μετάδοσης (TX).

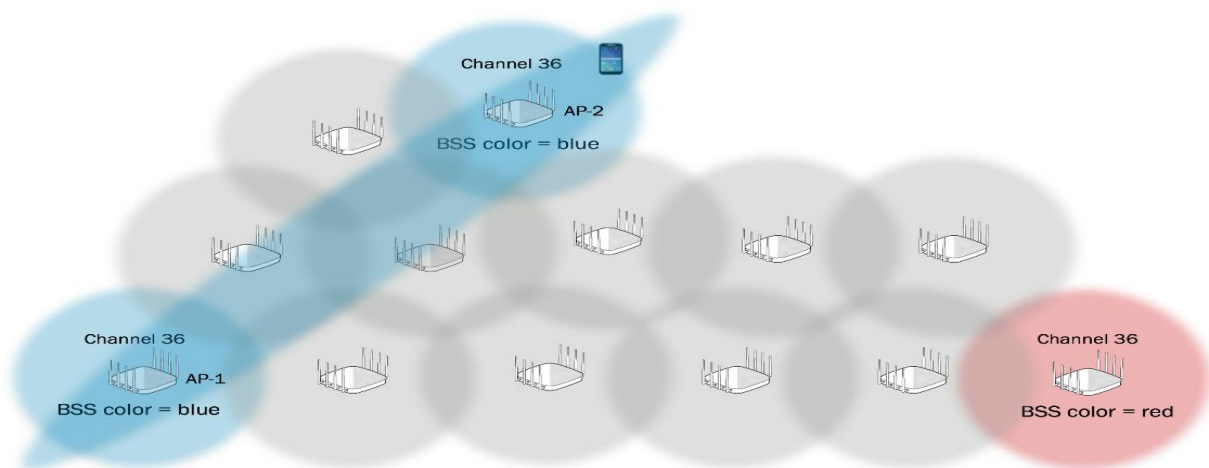
Η λειτουργία του BSS Color είναι η παρακάτω:

- Κάθε BSS (access point) χρησιμοποιεί ένα διαφορετικό χρώμα (6 bits στο preamble του σήματος).
- Κάθε STA μαθαίνει το δικό του BSS κατά τη σύνδεση και έτσι άλλα BSS είναι OBSS.
- Σήματα με το ίδιο χρώμα BSS χρησιμοποιούν ένα χαμηλό RSSI threshold, μειώνοντας έτσι τις συγκρούσεις στο ίδιο BSS.
- Σήματα με διαφορετικό χρώμα BSS χρησιμοποιούν ένα υψηλότερο RSSI threshold, επιτρέποντας έτσι περισσότερες ταυτόχρονες μεταδόσεις.

Το σχήμα αυτό εκφράζει μία πιο δίκαια διαδικασία (κάθε STA έχει την ίδια ευκαιρία να διεκδικήσει ένα TXOP, Transmit Opportunity) για υψηλότερη χωρητικότητα ανά σημείο πρόσβασης (STAs που βρίσκονται στο BSS μου υπερσχύουν). Σε διαχειρίσιμα (managed) υψηλής πυκνότητας, High-Density (HD) εταιρικά δίκτυα, η τεχνική αυτή είναι αποτελεσματική, ενώ σε μη διαχειρίσιμα (unmanaged) περιβάλλοντα, ο αντίκτυπος αυτής της ικανότητας μπορεί να είναι λιγότερο αποτελεσματικός ή ακόμη και επιζήμιος για την απόδοση του πελάτη.

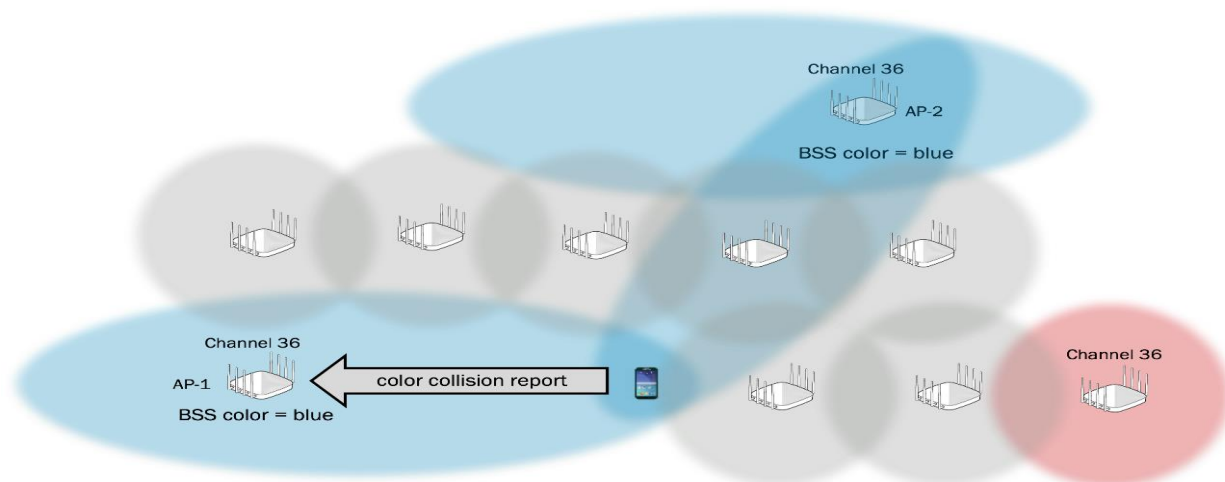
2.4.5 BSS Coloring

Οι συσκευές επικοινωνίας που συνθέτουν ένα BSS αποτελούνται από ένα access point το οποίο εκπέμπει σε μία συγκεκριμένη συχνότητα με έναν ή περισσότερους σταθμούς πελατών. Το 802.11ax μπορεί να διακρίνει μεταξύ BSS χρησιμοποιώντας ένα αναγνωριστικό χρώματος BSS όταν άλλα ραδιόφωνα μεταδίδουν στο ίδιο κανάλι. Εάν το χρώμα είναι το ίδιο, αυτό θεωρείται ως μετάδοση πλαισίου εντός του BSS (intra-BSS). Με άλλα λόγια, η συσκευή που εκπέμπει ανήκει στο ίδιο BSS με τον δέκτη. Εάν το ανιχνευμένο πλαίσιο έχει διαφορετικό χρώμα BSS από το δικό του, τότε το STA θεωρεί αυτό το πλαίσιο ως πλαίσιο μεταξύ BSS (inter-BSS) από ένα επικαλυπτόμενο BSS. Ένα 802.11ax AP έχει τη δυνατότητα να αλλάξει το χρώμα του BSS εάν ανιχνεύσει ένα OBSS χρησιμοποιώντας το ίδιο χρώμα. Η διπλή ανίχνευση χρώματος ενός OBSS αναφέρεται επίσης ως σύγκρουση χρώματος. Όπως φαίνεται στο Σχήμα 1, ένα 802.11ax AP μπορεί να ανιχνεύσει μια σύγκρουση χρώματος εάν ακούσει μια μετάδοση από ένα AP ή πελάτη σε διαφορετικό BSS που τυχαίνει να έχει το ίδιο χρώμα.



Εικόνα 22 Λειτουργία BSS Coloring

Επιπλέον, ένας συσχετισμένος πελάτης 802.11ax μπορεί να στείλει μια αναφορά σύγκρουσης χρώματος στο συσχετισμένο AP, εάν ο πελάτης εντοπίσει μια σύγκρουση χρώματος. Όπως φαίνεται στο Σχήμα 2, το AP-1 δεν μπορεί να ακούσει το AP-2, ωστόσο, ένας συνδεδεμένος πελάτης στο AP-1 μπορεί να ακούσει το OBSS με το ίδιο χρώμα και μπορεί στη συνέχεια να στείλει μια αναφορά σύγκρουσης χρώματος. Η αυτόνομη αναφορά του σταθμού πελάτη θα περιλαμβάνει πληροφορίες χρώματος BSS για όλα τα OBSS που μπορεί να εντοπίσει ο πελάτης. [7]



Εικόνα 23 Λειτουργία BSS Coloring, Εύρεση Σύγκρουσης

Όταν ένα AP ανιχνεύει μια σύγκρουση χρώματος από μόνο του ή με βάση τις πληροφορίες σύγκρουσης χρώματος που το AP συγκεντρώθηκε από τις αυτόνομες αναφορές πελατών, το AP μπορεί να αποφασίσει να αλλάξει το χρώμα του BSS. Θα πρέπει να σημειωθεί ότι τα κριτήρια αλλαγής του χρώματος BSS και η μέθοδος επιλογής ενός νέου χρώματος BSS δεν εμπίπτουν στο πεδίο εφαρμογής της τρέχουσας πρότασης τροποποίησης 802.11ax. Πιθανότατα, οι προμηθευτές WLAN θα ενσωματώσουν αλλαγές χρώματος BSS σε προσαρμοστικά(adaptive) πρωτόκολλα RF. [7] Το 802.11ax αυξάνει τη χωρητικότητα έως και τέσσερις φορές πιο πολύ από αυτή του 802.11ac. Επιπροσθέτως, οι βελτιώσεις περιλαμβάνουν και τη δυνατότητα χρήσης τόσο των 2,4 Gigahertz (GHz) και 5GHz για πολλές περιπτώσεις χρήσης.



Εικόνα 24 Source Aruba Networks

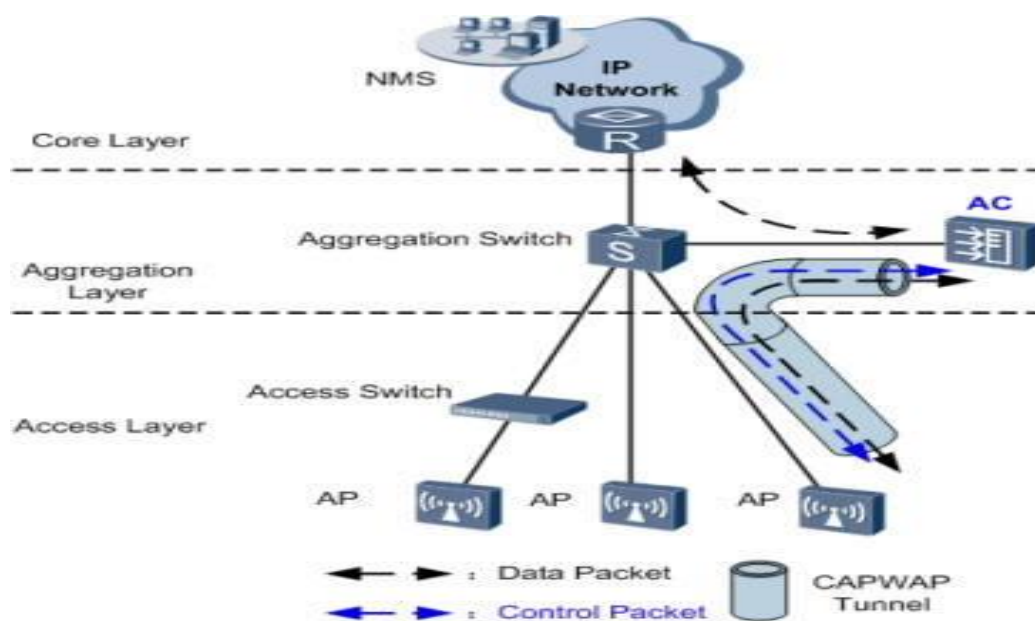
Αναμφισβήτητα, το σημαντικότερο νέο χαρακτηριστικό στο πρότυπο 802.11ax είναι η βελτιωμένη λειτουργία πολλαπλών χρηστών που ονομάζεται OFDMA (Orthogonal Frequency Division Multiple Access). Πολλαπλές συσκευές με ποικίλες ανάγκες εύρους ζώνης μπορούν να εξυπηρετηθούν ταυτόχρονα αντί για το υπάρχον μοντέλο όπου οι συσκευές ανταγωνίζονται μεταξύ τους για την αποστολή δεδομένων. Με το 802.11ax δεν υπάρχει συμφόρηση καθώς κάθε συσκευή έχει προγραμματιστεί για την παράλληλη μετάδοση δεδομένων. Η διαχείριση των πακέτων με αυτόν τον τρόπο βελτιώνει την απόδοση, καθώς ένας μεγάλος αριθμός πακέτων - ειδικά εκείνων που είναι ευαίσθητα στην καθυστέρηση όπως για παράδειγμα μεταγωγή φωνής (Voice Traffic) - μπορούν να μεταδοθούν ταυτόχρονα. Σε πυκνά περιβάλλοντα, αντί να χρησιμοποιεί ένα μόνο όχημα για τη μεταφορά της κυκλοφορίας-δεδομένων, είναι σαν να χρησιμοποιεί το μοντέλο του car pooling, όπου γίνεται χρήση του ίδιου μέσου από παραπάνω από ένα άτομα. Η κυκλοφορία συγκεντρώνεται σε ένα μέσο μεταφοράς, μία μέθοδος η οποία επιτρέπει πολλές συνομιλίες να συμβαίνουν ταυτόχρονα. Αυτό επιτρέπει στα σημεία πρόσβασης (access points) να διαχειρίζονται αποτελεσματικότερα την κίνηση δεδομένων (data traffic) από πολλαπλές συσκευές 802.11ax. [4]

2.5 Αρχιτεκτονική εταιρικού ασύρματου δικτύου

Το υλικό και το λογισμικό (hardware and software) που χρειάζεται για την υλοποίηση μίας ασύρματης υποδομής είναι :

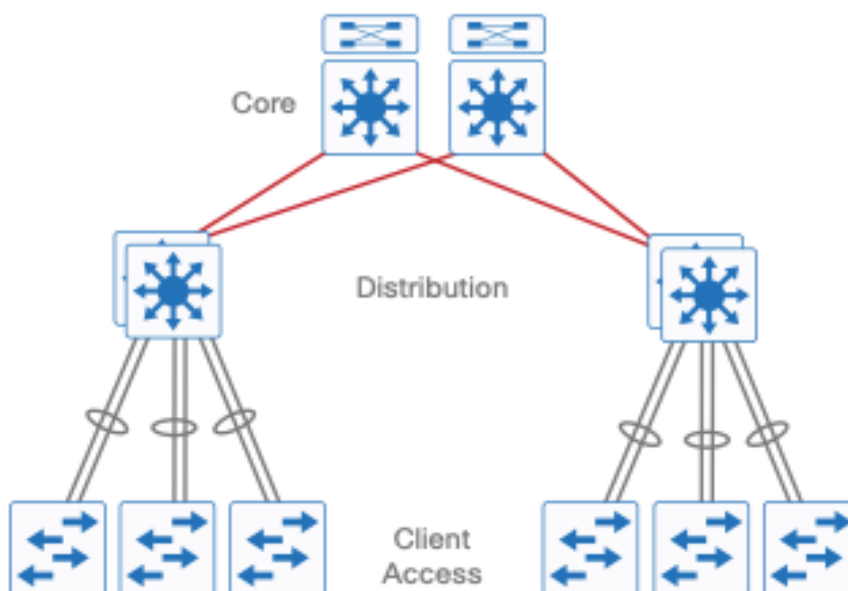
- Client devices
- Access points
- Access Switches τα οποία υποστηρίζουν PoE (Power-over-Ethernet)
- Wireless controllers
- Δίκτυο Κορμού

Το λειτουργικό σύστημα (Operating System) που είναι απαραίτητο προκειμένου να λειτουργήσει η ασύρματη δικτυακή υποδομή βρίσκεται ήδη μέσα στο μηχανήματα που περιγράφηκαν παραπάνω. Όλα τα μηχανήματα έρχονται με ένα βασικό license ενώ εάν επιθυμείται η ενεργοποίηση παραπάνω χαρακτηριστικών τότε πρέπει να αγοραστεί και το αντίστοιχο license έτσι ώστε να “ξεκλειδωθούν” και τα επιπλέον χαρακτηριστικά . Παρακάτω απεικονίζεται η αρχιτεκτονική ενός Ασύρματου Δικτύου όπου φαίνεται η ροή της δικτυακής κίνησης καθώς και οι εξοπλισμοί που αναφέρονται παραπάνω. Στην εικόνα 27 αποτυπώνεται ότι μεταξύ του access point και του Wireless Lan Controller σχηματίζεται το CAP WAP Tunnel. Όταν ένα access point εντάσσεται σε έναν Δικτυακό Ασύρματο Controller, τότε δημιουργείται μέσω του Control and Provisioning of Wireless Access Points protocol (CAPWAP) ένα tunnel μεταξύ των 2 συσκευών. Όλη η κίνηση, μέσα στην οποία συμπεριλαμβάνεται και η κίνηση των χρηστών, στέλνεται μέσω του CAPWAP tunnel.



Εικόνα 25 Λογική Διασύνδεση ενός Access Point

Στην περίπτωση του Controller για το ασύρματο δίκτυο, όπως φαίνεται και στην παραπάνω εικόνα, τοποθετείται/συνδέεται στο Distribution Layer και δημιουργείται το CAP WAP tunnel μεταξύ του Access Point και του Controller. Στην παρακάτω εικόνα απεικονίζεται μία end-to-end δικτυακή υλοποίηση καθώς και όλοι οι δικτυακοί εξοπλισμοί που είναι απαραίτητοι για την υλοποίηση του ασύρματου δικτύου.

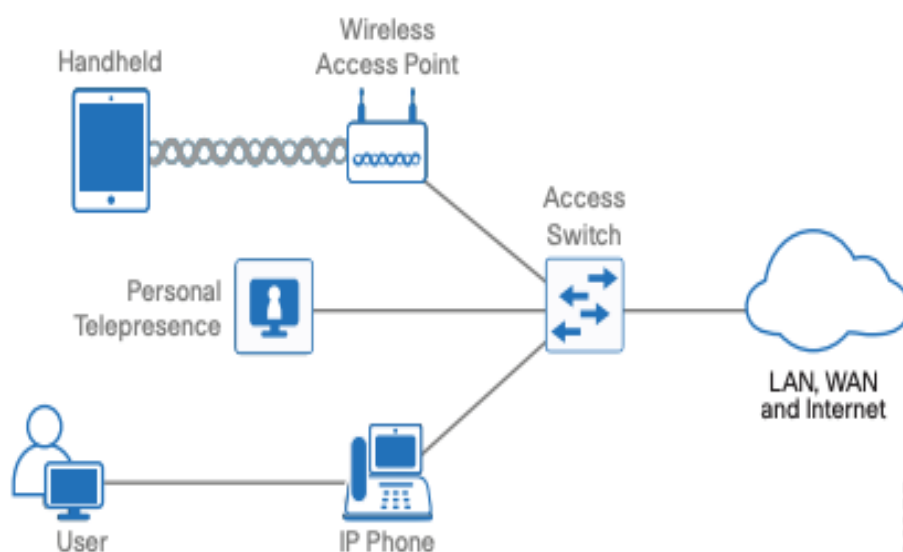


Εικόνα 26 Ιεραρχία ενός Δικτύου

Η παραπάνω εικόνα δείχνει την Αρχιτεκτονική ενός Ιεραρχικού Δικτύου. Ένα Ιεραρχικό δίκτυο αποτελείται από 3 επίπεδα (Layers) το Core, το Distribution και το Access.

Access Layer: Το access layer είναι το πρώτο επίπεδο ενός δικτύου όπου συνδέονται οι τελικές συσκευές (τηλέφωνα, εκτυπωτές, υπολογιστές, κλπ.). Είναι επίσης το σημείο

όπου συνδέονται συσκευές οι οποίες επεκτείνουν το δίκτυο (access points, switches, routers, κλπ.). Η μεγάλη ποικιλία πιθανών τύπων συσκευών που μπορούν να συνδεθούν καθώς και οι διάφορες υπηρεσίες και οι δυναμικοί μηχανισμοί διαμόρφωσης που είναι απαραίτητοι (brdu guard, 802.1x, QoS, PVST+, κλπ.), καθιστούν το στρώμα πρόσβασης ένα από τα πλούσια σε χαρακτηριστικά μέρη του δικτύου. Το access layer παρέχει την έξυπνη οριοθέτηση μεταξύ της υποδομής δικτύου και των υπολογιστικών συσκευών που αξιοποιούν αυτή την υποδομή. Ως εκ τούτου, αποτελεί το σημείο διατήρησης της ασφάλειας, του QoS και της διατήρησης των πολιτικών ασφαλείας του δικτύου. Σύμφωνα με το την Αρχιτεκτονική Ασφαλείας ενός δικτύου, το access layer είναι το πρώτο επίπεδο άμυνας και το πρώτο σημείο επικοινωνίας των διαφόρων συσκευών με την δικτυακή υποδομή. Εν ολίγοις το access layer είναι το σημείο εκείνο του δικτύου όπου ενεργοποιούνται τα περισσότερα χαρακτηριστικά και υπηρεσίες. [8]



Εικόνα 27 Σύνδεση Χρήστη στο Access Layer

Distribution Layer: Το Distribution Layer έχει ένα μοναδικό ρόλο διότι λειτουργεί ως το επίπεδο ελέγχου μεταξύ του access και του core layer. Και το access layer και το core layer αποτελούν layers ειδικού σκοπού και εκτελούν συγκεκριμένες λειτουργίες. Σκοπός του access layer είναι η παροχή συνδεσιμότητας της τελικής συσκευής ενώ σκοπός του core layer είναι η παροχή αδιάκοπης σύνδεσης με το υπόλοιπο δίκτυο. Αντίθετα, το Distribution layer εξυπηρετεί πολλούς σκοπούς. Είναι το σημείο συγκέντρωσης όλων των access switches καθώς και το σημείο όπου εφαρμόζονται πολλές πολιτικές του δικτύου. Αποτελεί επίσης μέρος του core δικτύου και λαμβάνει μέρος στην δρομολόγηση των πακέτων. Επιπλέον, αποτελεί και το σημείο διαχωρισμού και ομαδοποίησης του access δικτύου και του υπόλοιπου δικτύου. [8]

Core layer: Το Core Layer είναι το σχετικά πιο απλό μέρος του δικτύου αλλά ταυτόχρονα και το πιο κρίσιμο. Παρέχει ένα πολύ μικρό αριθμό υπηρεσιών ενώ είναι σχεδιασμένο με τέτοιο τρόπο έτσι ώστε να είναι πάντα διαθέσιμο. Το Core Layer πρέπει να μπορεί να λειτουργεί 7x24x365. Το σχεδιαστικό στοιχείο κλειδί για το Core Layer είναι η ύπαρξη εναλλακτικών/διαθέσιμων δικτυακών μονάδων τα οποία θα μπορέσουν να αναλάβουν την προώθηση των πακέτων και την απρόσκοπτη λειτουργία των υπηρεσιών στην περίπτωση που κάποιος μηχανισμός παρουσιάσει βλάβη και τεθεί εκτός λειτουργίας. Στο Core Layer δεν θα πρέπει να υλοποιηθεί κανένας περίπλοκος μηχανισμός εφαρμογής πολιτικών όπως ούτε και να έχει απευθείας συνδεδεμένα συσκευές όπως servers ή

τερματικά χρηστών. Θα πρέπει επίσης να έχει το ελάχιστο δυνατό control plane configuration. Με λίγα λόγια το Core Layer είναι αυτό το κομμάτι του δικτύου το οποίο παρέχει την συνδεσιμότητα μεταξύ όλων των υπόλοιπων δικτυακών οντοτήτων όπως για παράδειγμα παρέχει την σύνδεση μεταξύ του Data Center και του των τελικών χρηστών που χρησιμοποιούν την εφαρμογή που φιλοξενείται σε έναν από τους servers που βρίσκονται μέσα σε αυτό. [8]

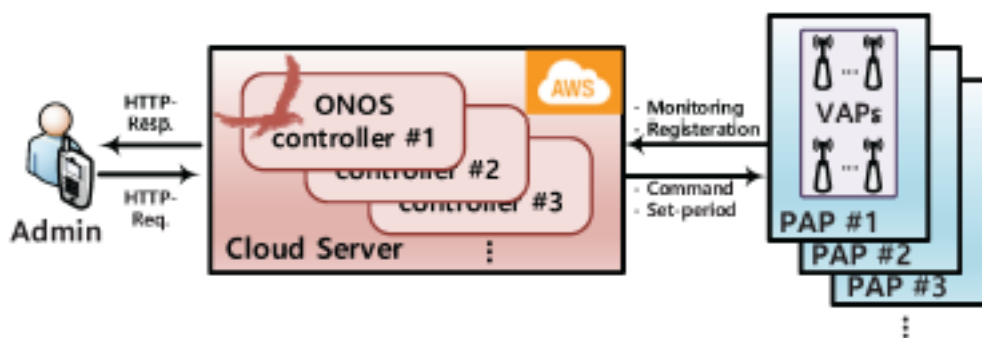
2.6 Αρχιτεκτονική εταιρικού ασύρματου Cloud Based Controller

Η ιδέα της μεταφοράς της διαχείρισης και της διαμόρφωσης ολόκληρου του ασύρματου δικτύου στο Cloud και πιο συγκεκριμένα σε κάποιον Cloud Provider είναι μία ιδέα που όλο και περισσότερες επιχειρήσεις έχουν στα πλάνα τους προς υλοποίηση. Αυτό που πρέπει να ληφθεί πολύ σοβαρά υπόψιν σε κάθε νέα υλοποίηση είναι η δομή της εταιρείας, αν για παράδειγμα υπάρχει ένα και μόνο site ή εάν υπάρχουν πολλά site που πρέπει να επικοινωνούν με τον Cloud WLAN Controller, ο σχεδιασμός του δικτύου της εταιρείας καθώς και οι ασύρματες απαιτήσεις που υπάρχουν. Όταν ξεκίνησε η ανάπτυξη των ασύρματων δικτύων στις επιχειρήσεις η διαχείριση και ο προγραμματισμός του κάθε access point γινόταν ξεχωριστά και ανεξάρτητα από τα υπόλοιπα access points που βρίσκονταν στο ίδιο δίκτυο. Αυτό δεν αποτελούσε πρόβλημα γιατί οι εταιρείες ακόμα είχαν συγκεκριμένους χώρους που παρείχαν ασύρματο δίκτυο και για συγκεκριμένους σκοπούς και χρήστες. Παραδείγματα τέτοιων χώρων ήταν τα δωμάτια διασκέψεων ή διάφοροι υπαίθριοι χώροι και γενικά όπου δεν υπήρχε η δυνατότητα ενσύρματης σύνδεσης με το δίκτυο. Καθώς η ζήτηση για ασύρματη κάλυψη μέσα στην εταιρία μεγάλωνε οι διαχειριστές ήρθαν αντιμέτωποι με έναν τεράστιο αριθμό αιτημάτων για την τοποθέτηση ασύρματου δικτύου παντού μέσα στην εταιρείες. Ακόμα μεγαλύτερα όμως ήταν τα προβλήματα που προέκυψαν από τις παρεμβολές μεταξύ των access point, τις ενδοκαναλικές παρεμβολές μεταξύ των access point και την μετακίνηση των χρηστών από το ένα access point στο άλλο. Όλα αυτά είχαν σαν συνέπεια πολλά δίκτυα να μην είναι σταθερά και να είναι απρόβλεπτα. [9] Προκειμένου να επιλυθούν όλα τα παραπάνω προβλήματα οι κατασκευαστές ασυρμάτων δικτύων δημιούργησαν τους WLAN Management Controllers έτσι ώστε όλο το data και management control plane να επιστρέφει σε ένα συγκεκριμένο σημείο. Η δουλειά του WLAN Management Controller είναι να αποτελεί το μοναδικό σημείο συγκέντρωσης στο ασύρματο δίκτυο όπου από εκεί θα δίνεται ο προγραμματισμός των Access point, η νέα πολιτική στα access point και θα επικοινωνούν τα access point μεταξύ τους. Αυτό που επιτυγχάνεται με αυτό είναι ότι ο WLAN Management Controller γίνεται το 'μυαλό' του δικτύου ενώ τα access point χάνουν οποιαδήποτε ικανότητα αποφάσεων είχαν έως τώρα. Το νέο αυτό μοντέλο δικτύου έχει αρκετά πλεονεκτήματα. Πρώτον ο Management Controller επιβλέπει όλα τα access points σε όλο το δίκτυο και ως εκ τούτου έχει πλήρη εικόνα του WLAN. Οι διαχειριστές του δικτύου μπορούν να χρησιμοποιήσουν τον Management Controller για να πραγματοποιήσουν έξυπνες ρυθμίσεις ραδιοσυχνοτήτων ανάλογα με τις ανάγκες. Αυτό επιτρέπει στους διαχειριστές του WLAN να τροποποιούν τα ασύρματα κανάλια όταν συμβαίνουν παρεμβολές, να αλλάζουν την ισχύ του ασύρματου σήματος όταν τα access points βρίσκονται εκτός ή εντός δικτύου καθώς και να αλλάζουν πελάτες από ένα access point σε άλλο. Δεύτερον, όλη η κίνηση του Control και του Data Plane επιστρέφουν πίσω στον Controller προτού μεταδοθούν στο τοπικό δίκτυο. Αυτό μπορεί να είναι θετικό και αρνητικό από την άποψη του data plane. Είναι θετικό, υπό την έννοια ότι οι ασύρματες πολιτικές για όλα τα SSID επιβάλλονται κεντρικά, καθιστώντας απίστευτα εύκολη τη διαχείριση της πολιτικής. Προσφέρει επίσης καλύτερη ασφάλεια, καθώς η κίνηση από ένα access point μεταφέρεται μέσω κρυπτογραφημένης σήραγγας. Αλλά η συνολική σχεδίαση μπορεί να δημιουργήσει σημεία συμφόρησης και μεμονωμένα σημεία

αποτυχίας, αν δεν προγραμματιστεί σωστά. [9] Με έναν Cloud-Managed Controller, τα access points συνδέονται σε έναν εικονικό Controller, ο οποίος φυσικά είναι εγκατεστημένος σε κάποια Cloud υποδομή ενός παρόχου υπηρεσιών. Η πληροφορία του Control Plane, η διαχείριση των access points και διάφορα άλλα services εκτελούνται μεταξύ του Cloud Controller και των τοπικών access points μέσω μίας σύνδεσης στο διαδίκτυο. Η αρχική αρχιτεκτονική διαφοροποίηση μεταξύ ενός Controller που βρίσκεται φυσικά εγκατεστημένος εντός του δικτύου μας και ενός Cloud Controller είναι ο τρόπος της ροής δεδομένων του Data Plane. Σε έναν Controller που βρίσκεται φυσικά εγκατεστημένος εντός του δικτύου μας η κίνηση των δεδομένων και από το Control Plane και από το Data plane επιστρέφουν πίσω στον Controller. Η διαδικασία επιστροφής της κίνησης πίσω στον Controller ονομάζεται Wireless Backhaul. Σε αντίθεση, σε έναν Cloud Controller η κίνηση του Data Plane δεν χρειάζεται να φτάσει μέχρι τον Cloud Controller αλλά παραμένει στο επίπεδο του τοπικού LAN. Αυτό έχει ως συνέπεια η νέα γενιά access points να μπορούν να πάρουν αποφάσεις για τον τρόπο διαχείρισης της κίνησης καθώς και της εφαρμογής νέων πολιτικών.

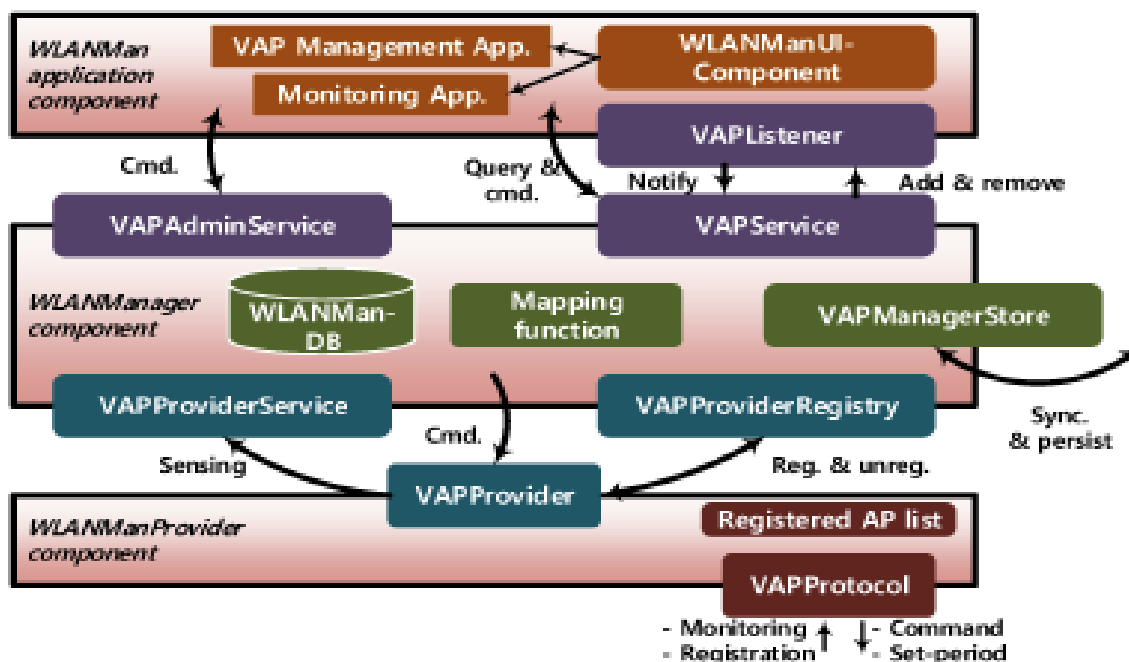
Τα πλεονεκτήματα από την χρήση ενός Cloud Controller είναι η ευκολία διαχείρισης και διαμόρφωσης των επιμέρους στοιχείων του ασύρματου δικτύου για παράδειγμα στην περίπτωση που ένας οργανισμός ή μία εταιρεία είναι γεωγραφικά διασκορπισμένη η αρχιτεκτονική και ο τρόπος λειτουργίας του Cloud Controller μειώνει δραστικά τον χρόνο για την πραγματοποίηση μίας αλλαγής από τον διαχειριστή του δικτύου. Επίσης με την αρχιτεκτονική του Cloud-based Controller και στο παράδειγμα που αναφέρθηκε παραπάνω θα χρειαστεί μόνο ένας WLAN Management Controller αντί για την φυσική τοποθέτηση ενός Controller σε κάθε σημείο παρουσίας της εταιρείας. Αυτό πέραν του διαχειριστικού φόρτου που αφαιρεί από τους διαχειριστές του δικτύου έχει και οικονομικά οφέλη για τους οργανισμούς και τις εταιρείες καθώς δεν θα χρειάζεται πλέον η αγορά της ίδιας δικτυακής συσκευής για όλα τα σημεία που υπάρχει φυσική παρουσία της εταιρείας. Κάτι επίσης πολύ σημαντικό που πρέπει να σημειωθεί είναι με το Cloud WLAN Controller γίνεται και η διαχείριση των Virtual Access Points που κάθε access point εκπέμπει.

Όσο αναφορά την αρχιτεκτονική και τον σχεδιασμό από την μεριά του Cloud πρέπει να σημειωθεί ότι προκειμένου να αποφύγουμε την δημιουργία Bottleneck το δίκτυο από την μεριά του Controller, κάτι το οποίο θα συμβεί εάν η κίνηση που φτάνει στο Controller είναι πολύ μεγαλύτερη από αυτή που μπορεί να διαχειριστεί. Ο τρόπος αντιμετώπισης μίας τέτοιας συνθήκης είναι η δημιουργία μίας ομάδας από Controller οι οποίοι θα λειτουργούν και θα επεξεργάζονται δεδομένα και κίνηση ταυτόχρονα. Το καθεστώς λειτουργίας αυτής της ομάδας θα είναι Master and Slave όπου ένας Controller θα είναι ο Master και οι υπόλοιποι οι Slaves. [9] Ένα τέτοιο παράδειγμα WLAN Management Controller είναι ο ONOS Controller και ο οποίος παρέχει την διαχείριση των virtual access points και την παρακολούθηση όλων των δικτυακών οντοτήτων του ασύρματου δικτύου. Μέσω της εφαρμογής διαχείρισης των virtual access points μπορεί κάποιος να δημιουργήσει ή να καταργήσει virtual access points σε οποιοδήποτε φυσικό access point χρησιμοποιώντας ένα μήνυμα εντολής(command message). Η εφαρμογή παρακολούθησης μπορεί να παρακολουθεί τόσο τα φυσικά access points όσο και τα virtual access points. Για την σωστή λειτουργία και παρακολούθηση του ασύρματου δικτύου, κάθε φυσικό access point αποστέλλει περιοδικά ένα μήνυμα παρακολούθησης το οποίο περιλαμβάνει την παρακολούθηση τα δεδομένα από την παρακολούθηση τόσο του φυσικού access point όσο και των virtual access point που είναι διαμορφωμένα σε αυτό προς την ομάδα των Cloud Controller. Η περίοδος παρακολούθησης μπορεί να αλλάξει μεταδίδοντας ένα μήνυμα ορισμένης περιόδου(set-period message) σε επιλεγμένα φυσικά access points. Για την υποστήριξη όλης της παραπάνω διαδικασίας τόσο τα φυσικά access points όσο και οι Controllers θα πρέπει να έχουν το ίδιο λογισμικό.



Εικόνα 28 Αρχιτεκτονική Cloud Controller

Η διαχείριση όλου του συστήματος γίνεται από τον διαχειριστή μέσω του ONOS web service. Η διαδικασία προσθήκης και αφαίρεσης ενός virtual access point ή ενός φυσικού access point γίνεται μόνο με μερικά κλικ στα αντίστοιχα πεδία. Ακόμα, μέσω του ONOS web service ο διαχειριστής μπορεί να δει συγκεντρωτικά όλα τα αποτελέσματα που προκύπτουν από την παρακολούθηση του δικτύου. [9] Κάθε φυσικό access point έχει εγκατεστημένο ένα WLAN Management agent software έτσι ώστε να μπορεί να παρακολουθεί και να διαμορφώνει τον εαυτό του καθώς και τα virtual access points που είναι διαμορφωμένα σε αυτό μόνο του χωρίς την παρέμβαση του WLAN Management Controller. Κάθε ONOS controller που βρίσκεται μέσα στην ομάδα των Controllers αποτελείται από ένα υποσύστημα το οποίο απεικονίζεται στην παρακάτω εικόνα.



Εικόνα 29 Σχεδιασμός του WLANMan υποσυστήματος στον ONOS controller

Το υποσύστημα αυτό περιέχει το WLAN Management πρωτόκολλο και 3 συστατικά μέρη τα WLANManProvider, WLANMan, και WLANMan application. Το WLAN Management πρωτόκολλο είναι υπεύθυνο για την επικοινωνία με τα φυσικά access points μέσω της TCP δικτυακής πόρτας επικοινωνίας. Όλων των ειδών τα μηνύματα μεταδίδονται ή λαμβάνονται από και προς όλα τα φυσικά access points μέσω του πρωτοκόλλου αυτού.

Το στοιχείο του WLANMANProvider βρίσκεται στο provider επίπεδο του ONOS Controller. Το στοιχείο αυτό περιέχει την λίστα με τον ποια access points είναι εγγεγραμμένα στον Controller. Το στοιχείο του WLANManager ορίζεται στο Core layer του ONOS controller. [9]

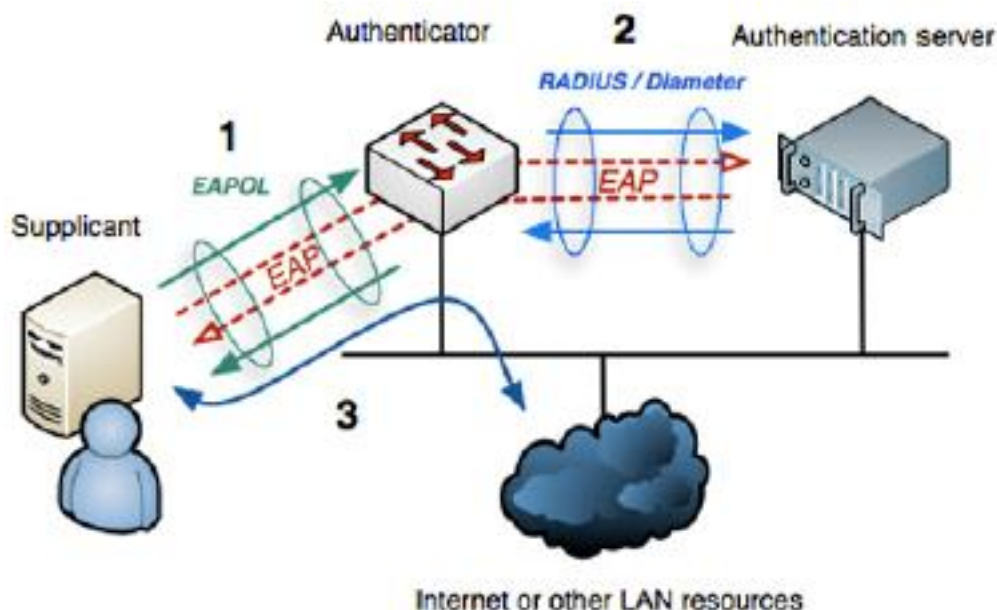
Το στοιχείο αυτό εμπεριέχει τα ακόλουθα 3 συστατικά μέρη:

- WLANManStore, το οποίο είναι υπεύθυνο για τον συγχρονισμό και την διατήρηση των υπόλοιπων ONOS controller στην ίδια ομάδα (ίδιο group).
- WLANManager, το οποίο είναι υπεύθυνο για την αντιστοίχιση του κάθε φυσικού access point με τον κατάλληλο controller μέσα από την ομάδα. Στο σημείο αυτό πρέπει να γίνει σωστή κατανομή των φυσικών access points προς του Controllers έτσι ώστε να μην υπάρξουν φαινόμενα όπου ένας Controller θα είναι υπερφορτωμένος με συσκευές ενώ κάποιος άλλος θα εξυπηρετεί ελάχιστα access point. Επιπλέον, ο WLANManager αποθηκεύει και στοιχεία από την παρακολούθηση του ασύρματου δικτύου σε μία βάση που ονομάζεται WLANManDB.
- WLANManApplication, το οποίο περιέχει μία web based εφαρμογή για τον χρήστη και η οποία ονομάζεται WLANManUIComponent και η οποία υποστηρίζει τις εφαρμογές για την παρακολούθηση και την διαχείριση των Virtual Access points. Μέσω της εφαρμογής αυτής οι χρήστες ή οι διαχειριστές μπορούν εύκολα να παρακολουθήσουν και να διαχειριστούν τα ασύρματα δίκτυα της εταιρείας ή του οργανισμού με την χρήση οποιουδήποτε web browser.

Καταλήγοντας, η αρχιτεκτονική του Cloud-based Controller αποτελεί μία ευέλικτη, εύκολη στη ρύθμιση και εύκολα επεκτάσιμη λύση και η οποία αλλάζει το μέχρι τώρα μοντέλο επικοινωνίας το οποίο επιβάλλει την δημιουργία του CAPWAP tunnel μεταξύ του Controller και του κάθε access point που έχουμε εγκατεστημένο στο ασύρματο δίκτυο.

2.7 Έλεγχος πρόσβασης σε ένα ασύρματο δίκτυο

Για να εξασφαλιστεί η ασφάλεια ενός δικτύου είναι απαραίτητο να αναπτυχθεί μία λύση για Authentication, Authorization και Accounting (AAA) η οποία θα χρησιμοποιεί εξειδικευμένο λογισμικό και εξοπλισμό δικτύου. Η επιτυχής ασφαλής σύνδεση ενός χρήστη με το δίκτυο θα απαιτεί, στο τμήμα πρόσβασης του δικτύου, δύο διαμεσολαβητές συσκευές που ονομάζονται authenticator και RADIUS server. Η διαδικασία του Authentication, Authorization και Accounting των χρηστών που συνδέονται στο δίκτυο επιτυγχάνεται με την βοήθεια 2 μεθόδων του Extensible Authentication Protocol (EAP), του Transport Layer Security και του Tunnelled Transport Layer Security.



Εικόνα 30 The topology indicating the AAA mechanisms using the EAP Authentication Protocol

Supplicant – Ο supplicant αποκτά πρόσβαση στις διαθέσιμες υπηρεσίες μέσω του authenticator. Ο supplicant είναι υπεύθυνος για να απαντά σε αιτήματα που γίνονται από τον authenticator για τον έλεγχο της ταυτότητας του.

Authenticator – Ο authenticator επιβάλλει τον έλεγχο ταυτότητας πριν επιτρέψει την πρόσβαση σε υπηρεσίες που είναι προσβάσιμες μέσω αυτής της δικτυακής πόρτας. Ο authenticator είναι υπεύθυνος για την επικοινωνία με τον supplicant και για την προώθηση των πληροφοριών που λαμβάνει από τον supplicant σε έναν κατάλληλο διακομιστή ελέγχου ταυτότητας (authentication server). Αυτό επιτρέπει την επαλήθευση των στοιχείων του χρήστη και καθορίζει την επακόλουθη κατάσταση του authorization. Είναι σημαντικό να σημειωθεί ότι η λειτουργία του authenticator είναι ανεξάρτητη από την πραγματική μέθοδο ελέγχου ταυτότητας. Λειτουργεί αποτελεσματικά ως ένα μέσο διασύνδεσης για την ανταλλαγή στοιχείων ταυτότητας μεταξύ του supplicant και του Authentication server.

EAP – Το Extensible Authentication Protocol (EAP) είναι μία μέθοδος της διεξαγωγής της επικοινωνίας μεταξύ ενός χρήστη και ενός authentication server.

Authentication / RADIUS Server - RADIUS είναι το Remote Access Dial in User Service. Είναι ο βασικός τρόπος παροχής Authentication, Authorization και Accounting σε ένα δίκτυο.

Authentication – Είναι η διαδικασία επαλήθευσης των χρηστών όταν προσπαθούν να συνδεθούν στον Controller. Οι χρήστες πρέπει να πληκτρολογήσουν ένα έγκυρο όνομα χρήστη και έναν κωδικό πρόσβασης, προκειμένου ο Controller να πιστοποιήσει τους χρήστες στο διακομιστή RADIUS. Εάν έχουν ρυθμιστεί πολλές βάσεις δεδομένων, μπορεί να καθοριστεί η ακολουθία την οποία θα ακολουθήσει ταυτοποίηση του χρήστη στις βάσεις δεδομένων.

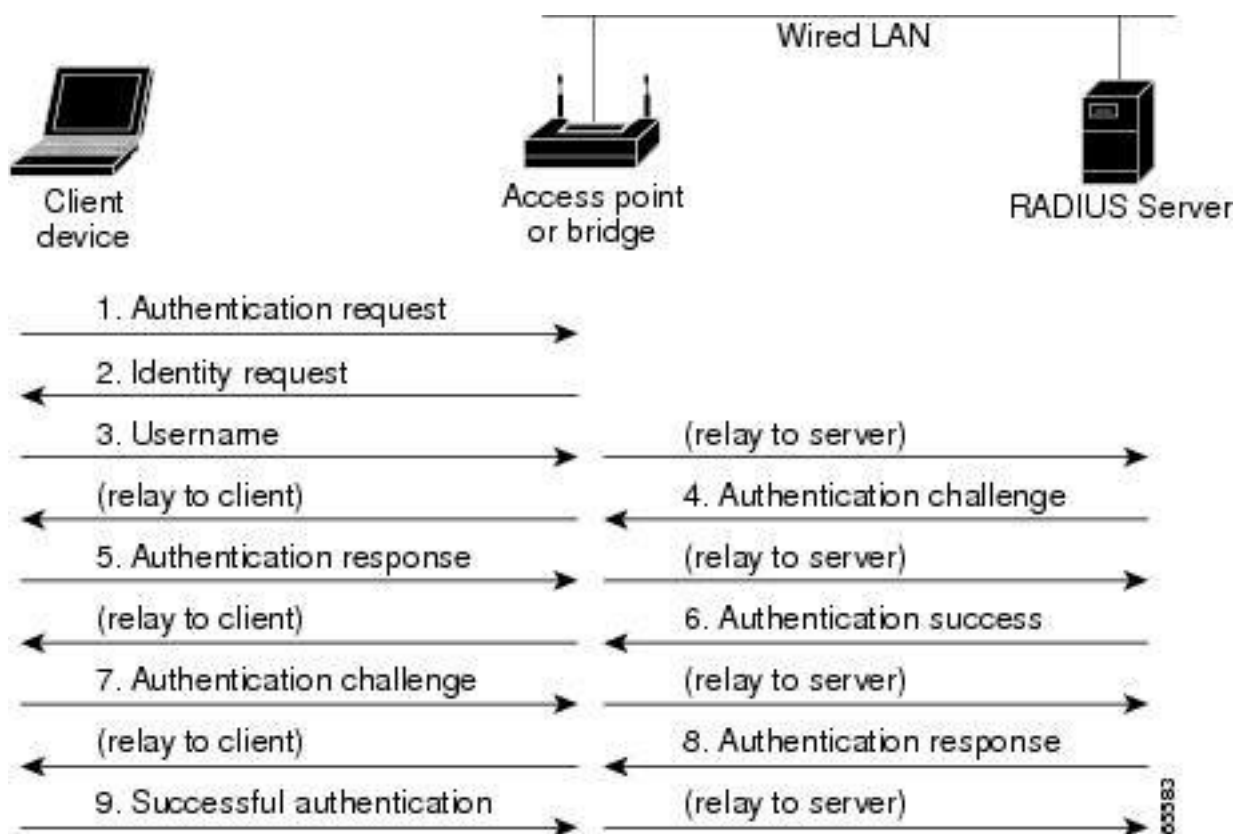
Authorization – Είναι η διαδικασία με την οποία ο RADIUS server βλέπει εάν ο χρήστης έχει δικαιώματα για να αποκτήσει πρόσβαση σε κάποιο αρχείο/φάκελο ή να εκτελέσει κάποια ενέργεια.

Accounting - Είναι η διαδικασία καταγραφής των ενεργειών του χρήστη και των αλλαγών που πραγματοποιεί. Κάθε φορά που ένας χρήστης εκτελεί επιτυχώς μια ενέργεια, ο RADIUS accounting server καταγράφει τις αλλαγές, το αναγνωριστικό του χρήστη που έκανε την αλλαγή, τον απομακρυσμένο κεντρικό υπολογιστή όπου έχει συνδεθεί ο χρήστης, την ημερομηνία και την ώρα εκτέλεσης της εντολής, το επίπεδο του χρήστη και την περιγραφή της ενέργειας που εκτελέστηκε και των παρεχόμενων τιμών. Εάν ο RADIUS accounting server βγει εκτός λειτουργίας, οι χρήστες μπορούν να συνεχίσουν τις συνεδρίες τους χωρίς διακοπή.

Το RADIUS είναι ένα πρωτόκολλο για τη μεταφορά πληροφοριών σχετικά με τον έλεγχο ταυτότητας, την εξουσιοδότηση και το accounting μεταξύ ενός χρήστη που επιθυμεί να πιστοποιήσει τους συνδέσμούς του και σε έναν διακομιστή ελέγχου ταυτότητας. Το πρωτόκολλο RADIUS χρησιμοποιεί το UDP για την μεταφορά των δεδομένων. Διατηρεί μια βάση δεδομένων και ακούει στη θύρα UDP 1812 για τις εισερχόμενες αιτήσεις πιστοποίησης(authentication) και τη θύρα UDP 1813 για εισερχόμενα accounting αιτήματα. Μπορούν να διαμορφωθούν πολλοί RADIUS Authentication και Accounting servers. Για παράδειγμα, μπορεί να υπάρξει ένας κεντρικός διακομιστής ελέγχου ταυτότητας RADIUS αλλά πολλοί RADIUS Accounting servers. Εάν δημιουργηθούν πολλοί servers του ίδιου τύπου και ο πρώτος βγει εκτός λειτουργίας τότε ο Controller αυτόματα προσπαθεί να επικοινωνήσει με τον δεύτερο, έπειτα με τον τρίτο κλπ. Πολλοί οργανισμοί έχουν επενδύσει στην τεχνολογία του Authentication (έλεγχος ταυτότητας), Authorization (εξουσιοδότησης) και Accounting, AAA, για τον έλεγχο της πρόσβασης των χρηστών τους στο δίκτυο, συνήθως μέσω του πρωτοκόλλου RADIUS (Remote Authentication Dial In User Service) ή μέσω ενός Firewall. Το 802.1X μπορεί να αξιοποιήσει τους εγκατεστημένους διακομιστές AAA, μέσω του RADIUS πρωτοκόλλου, για να παρέχει αυτές τις λειτουργίες σε νέους χρήστες 802.1X. Το IEEE 802.1X αποτελεί μία port-based μέθοδο ελέγχου της ταυτότητας του χρήστη η οποία διαμορφώνεται σε μία δικτυακή συσκευή. Στην μεγαλύτερη πλειοψηφία τους αυτές οι δικτυακές συσκευές είναι switch. Όταν ένας χρήστης είναι ρυθμισμένος να χρησιμοποιεί RADIUS τότε οποιοσδήποτε χρήστης του client θα πρέπει να δίνει ένα username και ένα password για να αποκτήσει πρόσβαση στο service που δίνεται μέσω του δικτύου. Το RADIUS είναι ένα κατακεκομμένο σύστημα client/server το οποίο εξασφαλίζει τα δίκτυα από μη εξουσιοδοτημένη πρόσβαση. Οι RADIUS clients τρέχουν στις τελικές δικτυακές συσκευές και στέλνουν αιτήματα για αυθεντικοποίηση (authentication) στον κεντρικό RADIUS server ο οποίος περιέχει όλες τις πληροφορίες για την ταυτοποίηση των χρηστών καθώς και σε ποια service μπορεί ο καθένας να έχει πρόσβαση. Ο τρόπος που ένας RADIUS server χρησιμοποιείται μέσα σε ένα ασύρματο δίκτυο περιγράφεται παρακάτω:

2.7.1 Radius Authentication

Καθώς ο ασύρματος χρήστης προσπαθεί να συνδεθεί στο επιθυμητό ασύρματο δίκτυο θα πρέπει να δώσει ένα username και ένα password. Και οι δύο αυτές μεταβλητές θα μεταφερθούν στον RADIUS server όπου εκεί θα γίνει ο έλεγχος για το εάν οι μεταβλητές που έδωσε ο χρήστης συμφωνούν με αυτές που είναι καταχωρημένες στην βάση δεδομένων του server. Στην παρακάτω εικόνα φαίνεται και η ακριβής διαδικασία που ακολουθείται κάθε φορά που ένας χρήστης ή ένα service πρέπει να ταυτοποιηθεί.



Εικόνα 31 Αλληλουχία Επικοινωνιών μεταξύ Radius Server και Client

Στην παραπάνω εικόνα, και τα βήματα 1 έως 9 απεικονίζονται ένας ασύρματος χρήστης και ένας RADIUS server όπου φαίνεται η διαδικασία της αυθεντικοποίησης του χρήστη μέσω ενός access point το οποίο συνδέεται ενσύρματα με τον Radius server. Ο RADIUS server στέλνει ένα Authentication Challenge στον χρήστη. Ο χρήστης χρησιμοποιεί one-way encryption για να δημιουργήσει μία απάντηση στο challenge και στέλνει την απάντηση στον RADIUS server. Χρησιμοποιώντας πληροφορίες από την βάση δεδομένων του ο RADIUS server δημιουργεί την δική του απάντηση και την συγκρίνει με την απάντηση που έλαβε από τον client. Όταν ο RADIUS server πιστοποιήσει τον χρήστη τότε ξεκινάει η αντίστροφη διαδικασία όπου ο χρήστης πρέπει να τακτοποιήσει τον RADIUS server. Όταν ολοκληρωθεί ο αμοιβαίος έλεγχος ταυτότητας και από τις δύο δικτυακές οντότητες ο RADIUS server και ο client καθορίζουν ένα Wired Equivalent Privacy(WEP) κλειδί για τον client το οποίο είναι μοναδικό και παρέχει στον client το κατάλληλο επίπεδο δικτυακής πρόσβασης. Ο client αποθηκεύει αυτό το κλειδί και το χρησιμοποιεί κατά την διαδικασία της αυθεντικοποίησης όταν προσπαθήσει να αποκτήσει πρόσβαση στο δίκτυο. Κατά την διάρκεια του login session, ο RADIUS server κρυπτογραφεί και στέλνει το WEP κλειδί, το οποίο ονομάζεται session key, μέσω του ενσύρματου δικτύου στο access point. Το access point κρυπτογραφεί το broadcast κλειδί με το session κλειδί και στέλνει το κρυπτογραφημένο broadcast κλειδί στον χρήστη, ο οποίος χρησιμοποιεί το session κλειδί για να το αποκρυπτογραφήσει. Ο client και το access point ενεργοποιούν το WEP και χρησιμοποιούν τα session και broadcast WEP κλειδιά για όλες τις επικοινωνίες που πραγματοποιούνται κατά την διάρκεια του session.

2.7.2 Local Authentication

Πέραν του authentication με την χρήση του RADIUS server μπορεί να γίνει και authentication με την χρήση τοπικής βάσης δεδομένων αυθεντικοποίησης στο access point. Το access point μπορεί να αυθεντικοποιήσει τους χρήστες χρησιμοποιώντας MAC-based ταυτοποίηση. Η διαμόρφωση για την ταυτοποίηση τοπικά σε κάθε access point γίνεται χειροκίνητα μέσω του controller. Για κάθε Virtual Access Point πρέπει να δημιουργηθούν από τον διαχειριστή τα απαραίτητα username και password στον Controller τα οποία θα μπορούν να έχουν πρόσβαση στο δίκτυο μέσω του συγκεκριμένου SSID.

2.7.3 Multifactor Authentication

Τα τελευταία χρόνια και λόγω της πολύ μεγάλης αύξησης των κυβερνοεπιθέσεων με σκοπό την κλοπή προσωπικών στοιχείων των χρηστών και των εταιριών, ήταν επιτακτική η δημιουργία ενός επιπλέον βήματος αυθεντικοποίησης του χρήστη. Το Multifactor Authentication είναι ένα σύστημα ασφαλείας που απαιτεί περισσότερες από μία μεθόδους ελέγχου ταυτότητας από ανεξάρτητες κατηγορίες διαπιστευτηρίων για την επαλήθευση της ταυτότητας του χρήστη για σύνδεση ή άλλη συναλλαγή. Ο έλεγχος ταυτότητας πολλαπλών παραγόντων συνδυάζει δύο ή περισσότερα ανεξάρτητα διαπιστευτήρια: τι γνωρίζει ο χρήστης (κωδικός πρόσβασης), τι έχει ο χρήστης (διακριτικό ασφαλείας) και τι είναι ο χρήστης (βιομετρική επαλήθευση). Ο στόχος του MFA είναι να δημιουργήσει μια πολυεπίπεδη άμυνα και να δυσκολέψει την πρόσβαση ενός μη εξουσιοδοτημένου ατόμου σε έναν στόχο, όπως μια φυσική τοποθεσία, μια υπολογιστική συσκευή, ένα δίκτυο ή μια βάση δεδομένων. Εάν ένας παράγοντας έχει παραβιαστεί ή σπάσει, ο εισβολέας εξακολουθεί να έχει τουλάχιστον ένα ακόμη εμπόδιο για να παραβιάσει πριν επιτύχει με επιτυχία στον στόχο. Στο παρελθόν, τα συστήματα MFA βασίζονταν συνήθως σε έλεγχο ταυτότητας δύο παραγόντων. Όλο και περισσότερο, οι προμηθευτές χρησιμοποιούν την ετικέτα "multifactor" για να περιγράψουν οποιοδήποτε σχήμα ελέγχου ταυτότητας που απαιτεί περισσότερα από ένα διαπιστευτήρια ταυτότητας.

2.8 Σύγκριση προτύπου 802.11ac και 802.11ax

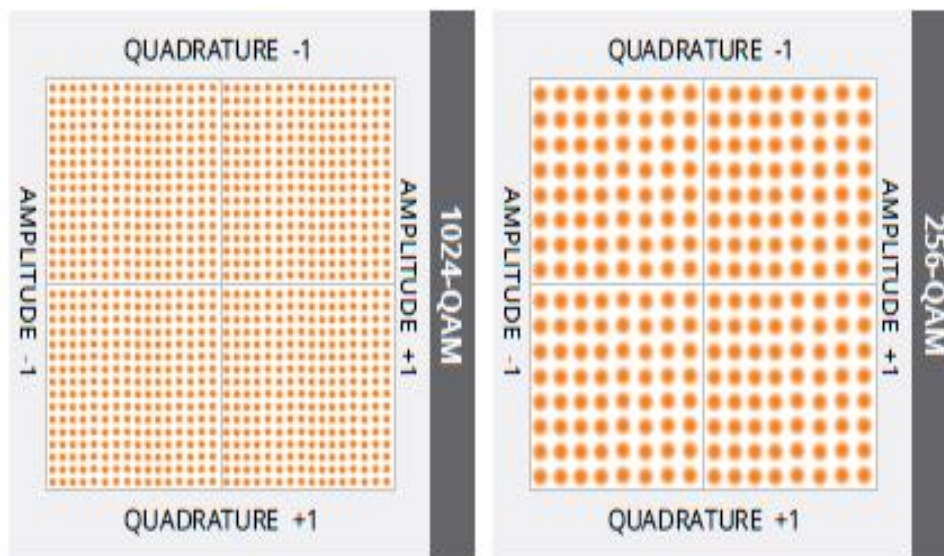
Σε σχέση με το προηγούμενο πρότυπο, το Wi-Fi 6 προσφέρει θεωρητικά 37%-40% υψηλότερη περίπτωση ταχύτητα. Όμως οι υψηλότερες υποστηριζόμενες ταχύτητες δεν αποτελούν το μοναδικό πλεονέκτημα της νέας έκδοσης του προτύπου, καθώς βελτιώνει την απόδοση σε περιβάλλοντα με πολλές συνδεδεμένες συσκευές ταυτόχρονα – ουσιαστικά επιλύοντας ζητήματα συμφόρησης του δικτύου- ενώ παράλληλα επιδεικνύει καλύτερη ασφάλεια και «μειωμένο ενεργειακό αποτύπωμα».

802.11AC WAVE 2 (WI- FI 5)	802.11AX (WI - FI 6)
<ul style="list-style-type: none"> • Multi-User MIMO (Downlink) • 4 Spatial Streams (4SS) • 20/40/80/160 MHz channel • 256-QAM modulation and coding • Explicit transmit beamforming 	<ul style="list-style-type: none"> • 4x Average throughput per station in 2.4 & 5 GHz bands • Multi-User MIMO (Uplink & Downlink) • OFDMA uplink and downlink • Higher Rates(1024-QAM) • Wait to Wake (Target Wake Time)

	<ul style="list-style-type: none">• Enhanced outdoor long-range performance
--	---

Πίνακας 1 802.11ac vs 802.11ax

Το Wi-Fi 6 διαθέτει δυνατότητα διαμόρφωσης 1024-QAM. Κάθε OFDM σύμβολο αντιπροσωπεύει 10bits δεδομένων σε σχέση με 8bits δεδομένων στο Wi-Fi 5 όπου η μέγιστη διαμόρφωση ήταν 256-QAM, κάτι το οποίο είναι 25% αύξηση σε bit ανά σύμβολο και το οποίο μεταφράζεται ως 25% μείωση στο περιθώριο λάθους.



Εικόνα 32 1024-QAM vs 256-QAM

Στον παρακάτω πίνακα φαίνονται και οι διαφορές στα τεχνικά χαρακτηριστικά-προδιαγραφές μεταξύ των 2 προτύπων.

	802.11ac	802.11ax
BANDS	5GHz	2.4 GHz and 5GHz
CHANNEL BANDWIDTH	20MHz, 40 MHz, 80 MHz, 80+80 MHz & 160 MHz	20MHz, 40 MHz, 80 MHz, 80+80 MHz & 160 MHz
FFT SIZES	64, 128, 256, 512	256, 512, 1024, 2048
SUBCARRIER SPACING	312.5 kHz	78.125 kHz
OFDM SYMBOL DURATION	3.2 us + 0.8/0.4 CP	12.8 us + 0.8/1.6/3.2 us CP
HIGHEST MODULATION	256-QAM	1024-QAM
DATA RATES	433 Mbps (80MHz, 1SS) 6933 Mbps (160 MHz, 8SS)	600.4 Mbps (80 MHz, 1SS) 9607.8 Mbps (160 MHz, 8SS)

Εικόνα 33 802.11ac vs 802.11ax Τεχνικές Προδιαγραφές

2.9 Περίληψη

Το IEEE 802.11ax είναι ένα συναρπαστικό νέο βήμα για τα ασύρματα LAN. Αυτή η έκτη γενιά Wi-Fi όχι μόνο θα προσφέρει υψηλότερες ταχύτητες, αλλά θα επιτρέψει και νέα επιχειρηματικά μοντέλα και περιπτώσεις χρήσης, όπως:

- IoT
- Εφαρμογές σε πραγματικού χρόνου, βίντεο 4K/8K ή επταυξημένη ή εικονική πραγματικότητα

Όπως συμβαίνει και με κάθε άλλη εξέλιξη του Wi-Fi, το 802.11ax είναι συμβατό με παλαιότερες εκδόσεις, αξιοποιώντας τις υπάρχουσες τεχνολογίες και τις καθιστά πιο αποτελεσματικές. Αυτό το σενάριο επιτρέπει μια ομαλή Εν τω μεταξύ, οι πελάτες εταιρειών και παρόχων υπηρεσιών που εξετάζουν μακροπρόθεσμες επενδύσεις σε ασύρματα LAN πρέπει να λάβουν σοβαρά υπόψη τα σημεία πρόσβασης 802.11ac και πως αυτά θα αντικατασταθούν από σημεία πρόσβασης 802.11ax.

Feature	Benefit					
	Overhead Reduction	Dense Network Efficiency	Increased Throughput, Reduced Latency	Performance at Network Edge	Robust Outdoor Experience	Client Power Efficiency
Uplink OFDMA	✓	✓	✓	✓	✓	
Downlink OFDMA	✓	✓			✓	
Downlink multi-user MIMO	✓	✓	✓		✓	
Transmit beamforming		✓	✓	✓	✓	
Per-link enhancement (benefits via one or more of): • 1024-QAM • Incr. symbol time, varied guard interval combinations • Multi-TID AMPDU	✓	✓	✓	✓	✓	
Target wake time	✓					✓
Operation mode indication						✓

Εικόνα 34 Πλεονεκτήματα του 802.11ax

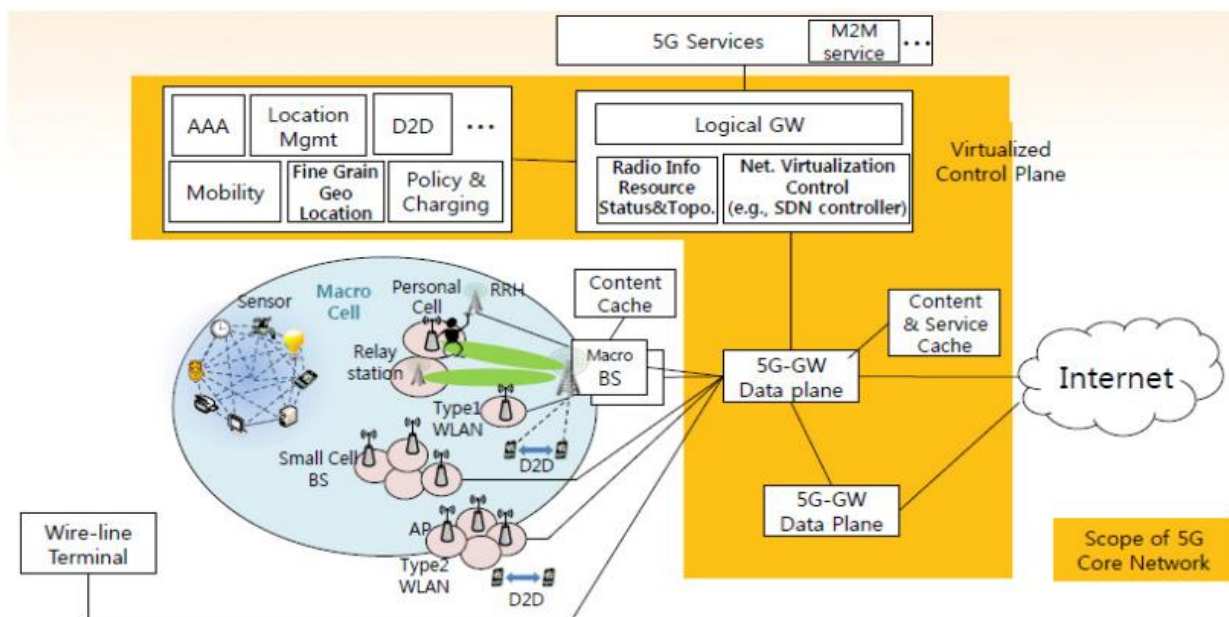
3. ΠΕΡΙΦΡΑΦΗ LTE RELEASE 15 (5G) ΚΑΙ ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΣΥΣΤΗΜΑΤΟΣ

Στην ενότητα αυτή θα αναλυθεί το νέο σύστημα κινητών επικοινωνιών, 3GPP LTE Release 15 (5G). Στα παρακάτω κεφάλαια περιγράφεται η αρχιτεκτονική του νέου συστήματος καθώς και ο τρόπος αυθεντικοποίησης του χρήστη. Επιπλέον, περιγράφονται οι νέες τεχνολογικές δυνατότητες του 3GPP Release 15 καθώς επίσης και το περιεχόμενο των Release 15 και 16. Τέλος, περιγράφεται η διαδικασία εύρεσης κυψέλης καθώς και οι νέες οντότητες του Δικτύου κορμού του LTE Release 15.

3.1 3GPP LTE RELEASE 15 (5G)

Στην ενότητα αυτή περιγράφεται το νέο πρότυπο κινητών επικοινωνιών της 3GPP. Το νέο αυτό πρότυπο δημιουργήθηκε με σκοπό την υποστήριξη των αυξημένων απαιτήσεων των τελικών συσκευών/ χρηστών για εύρος ζώνης, για χαμηλό latency και αξιοπιστία μετάδοσης. Βασικό συστατικό στοιχείο του νέου προτύπου είναι η δημιουργία ενός πυκνού ασύρματου δικτύου μέσω της εγκατάστασης νέου τύπου κυψελών. Το 5G περιλαμβάνει ένα σύνολο προτύπων και τεχνολογιών για ένα ριζικά πιο γρήγορο ασύρματο Internet που στην ιδανική περίπτωση είναι έως και 20 φορές πιο γρήγορο με 120 φορές λιγότερο λανθάνοντα χρόνο από το 4G, θέτοντας το στάδιο για την πρόοδο της δικτύωσης IoT και την υποστήριξη για νέο υψηλό εύρος ζώνης εφαρμογές. Τα τεχνολογικά θεμέλια του 5G καθορίζονται από μια σειρά προτύπων. Ένα από τα πιο σημαντικά από αυτά είναι το 5G New Radio, ή το 5G NR, που τυποποιήθηκε από το 3rd Generation Partnership Project (3GPP), έναν οργανισμό τυποποίησης που αναπτύσσει πρωτόκολλα για κινητή τηλεφωνία. Σε σύγκριση με τις προηγούμενες γενιές, η αρχιτεκτονική του συστήματος 3GPP 5G θα βασίζεται στις υπηρεσίες, θα είναι δηλαδή ένα service-based σύστημα. Αυτό σημαίνει ότι θα είναι δυνατό τα νέα αρχιτεκτονικά στοιχεία, τα οποία θα είναι ορισμένα ως δικτυακές λειτουργίες οι οποίες θα παρέχουν υπηρεσίες τους μέσω διασυνδέσεων ενός κοινού πλαισίου, να παρέχουν την υπηρεσία τους σε οποιαδήποτε δικτυακή εφαρμογή έχει την απαραίτητη πιστοποίηση ότι μπορεί να χρησιμοποιήσει αυτή την υπηρεσία. Οι Network Repository Functions (NRF) επιτρέπουν σε κάθε λειτουργία του δικτύου (network function) να ανακαλύψει τις υπηρεσίες που προσφέρουν άλλες λειτουργίες δικτύου. Θα πρέπει να αναφερθεί πως στο 5G σύστημα ως network functions αναφέρονται αυτά που στο 4G σύστημα αναφέρθηκαν ως network nodes. Αυτό το μοντέλο αρχιτεκτονικής, υιοθετεί περαιτέρω αρχές όπως modularity και επαναχρησιμοποίηση των λειτουργιών του δικτύου και επιτρέπει στις εφαρμογές να επωφεληθούν από τις πιο πρόσφατες τεχνολογίες λογισμικού εικονικοποίησης (virtualization) και λογισμικού. Η service-based αρχιτεκτονική απεικονίζει τις αρχές που βασίζονται στις υπηρεσίες, παρουσιάζοντας τις λειτουργίες του δικτύου (network functions), κυρίως τις λειτουργίες του κεντρικού δικτύου(Core Network), με μια ενιαία διασύνδεση με το υπόλοιπο σύστημα. Τα νέα 5G συστήματα θα πρέπει να μπορούν να συνεργάζονται άψογα και με πάρα πολύ μικρούς χρόνους με υποδομές αποθήκευσης δεδομένων (storage networks) καθώς και με πολλά δωμάτια δεδομένων (Data Centers). Οι πάροχοι κινητών επικοινωνιών θα πρέπει να σχεδιάζουν την εγκατάσταση πυκνότερων πλεγμάτων κυψελών και μικρών κυψελών ακόμα και στο επίπεδο του δρόμου. Ο ευέλικτος και προγραμματιζόμενος χαρακτήρας των νέων δικτύων 5G αντιπροσωπεύει μια ριζική εξέλιξη στα δίκτυα κινητών επικοινωνιών από την άποψη της χωρητικότητας, των επιδόσεων και του φάσματος. Εκεί όπου θα χρειαστεί ριζικός επανασχεδιασμός είναι επίσης και στην συνολική χωρητικότητα του Backhaul δικτύου. Η προβλεπόμενη αύξηση της πυκνότητας των δικτύων 5G θα οδηγήσει με την σειρά της σε ανάγκη για μεγαλύτερη χωρητικότητα ανά Radio Access Network και ένα πολύ πυκνότερο πλέγμα σταθμών βάσης 5G. Αυτό το πυκνότερο πλέγμα επιτρέπει το

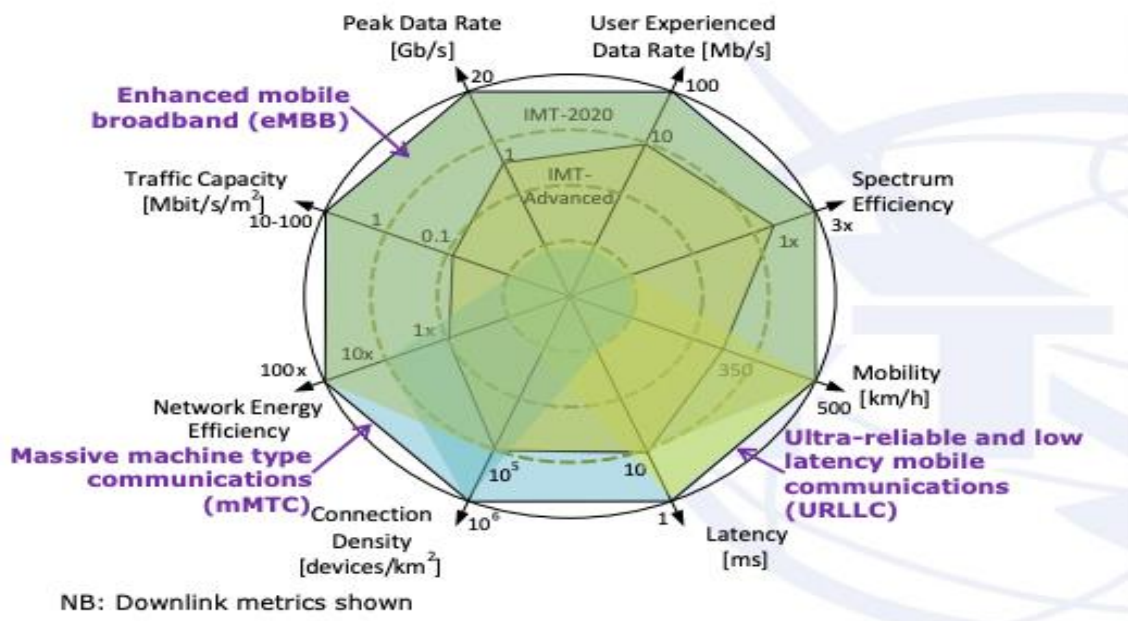
ασύρματο Backhauling δεδομένων από μικροκυψέλες σε μακροκυψέλες. Αυτό σημαίνει ότι οι απαιτήσεις αναβαθμίσεων για την υποδομή 5G επεκτείνεται σε πολλούς σταθμούς βάσης. Με βάση του παραπάνω, σε πολλές περιπτώσεις τα δεδομένα που διέρχονται από το δίκτυο έχουν μικρότερη απόσταση να διανύσουν, λιγότερα δικτυακά hops, μεταξύ του χρήστη και του προορισμού του. Το Backhauling και το Fronthauling αποτελούν σημαντικά χαρακτηριστικά στον δρόμο προς το 5G Cloud-Centric δίκτυο. Σύμφωνα με την 5GPPP, το Centric Cloud θα συνδέεται μέσω ενός Backhaul δικτύου σε διάφορα άλλα Edge-Computing-Clouds τα οποία δεν θα απέχουν απόσταση μεγαλύτερη των 20 χιλιομέτρων από το χρήστη. Εάν ακόμα οι υπηρεσίες μπορούν να εκτελεστούν στην άκρη του δικτύου (Mobile Edge Computing), αυτό θα οδηγήσει την κυκλοφορία μακριά από το Cloud RAN. Στην παρακάτω εικόνα απεικονίζεται το νέο RAN και 5G Core δίκτυο.



Εικόνα 35 5G RAN και Core Δίκτυο

3.2 Προϋποθέσεις (Standards) ενός 5G Συστήματος

Σύμφωνα με την ITU, International Telecommunications Union όλα τα 5G συστήματα θα πρέπει να πληρούν τα specifications που έχουν οριστεί στο IMT-2020 Standard.



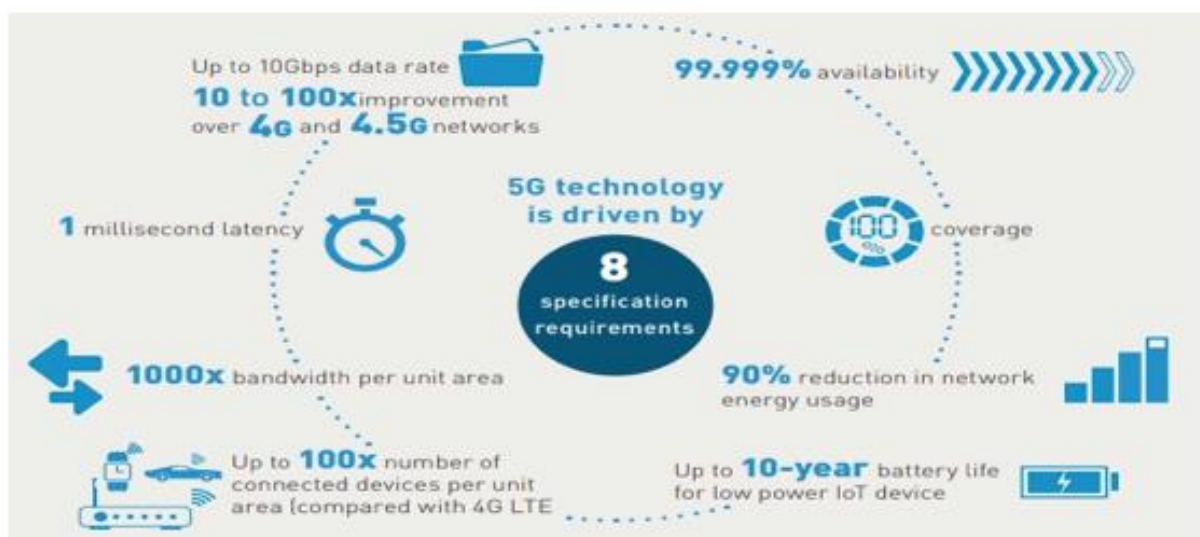
Εικόνα 36 IMT-2020 Standard

Η παρακάτω εικόνα παρέχει μια επισκόπηση των ειδικών τεχνικών απαιτήσεων που ορίζονται ως ελάχιστες απαιτήσεις για το IMT- 2020.

Metric	Requirement	Comments
Peak Data Rate	DL: 20 Gb/s UL: 10 Gb/s	Single eMBB mobile in ideal scenarios assuming all resources utilized
Peak Spectral Efficiency	DL: 30 b/s/Hz (assuming 8 streams) UL: 15 b/s/Hz (assuming 4 streams)	Single eMBB mobile in ideal scenarios assuming all resources utilized
User Experienced Data Rate	DL: 100 Mb/s UL: 50 Mb/s	5% CDF of the eMBB user throughput
Area Traffic Capacity	Indoor hotspot DL: 10 Mb/s/m ²	eMBB
User Plane Latency	eMBB: 4 ms URLLC: 1 ms	Single user for small IP packets, for both DL and UL (eMBB and URLLC)
Control Plane Latency	20 ms (encouraged to consider 10 ms)	Transition from Idle to Active (eMBB and URLLC)
Connection Density	1M devices per km ²	For mMTC
Reliability	99.9999% success prob.	32 L2 bytes within 1 ms at cell edge
Bandwidth	>100 MHz; up to 1 GHz in > 6 GHz	Carrier aggregation allowed

Εικόνα 37 IMT- 2020 Ελάχιστες Απαιτήσεις

Στην παρακάτω εικόνα απεικονίζεται τι θα πρέπει να πληροί ένα 5G σύστημα. Πιο συγκεκριμένα φαίνονται οι 8 προδιαγραφές :



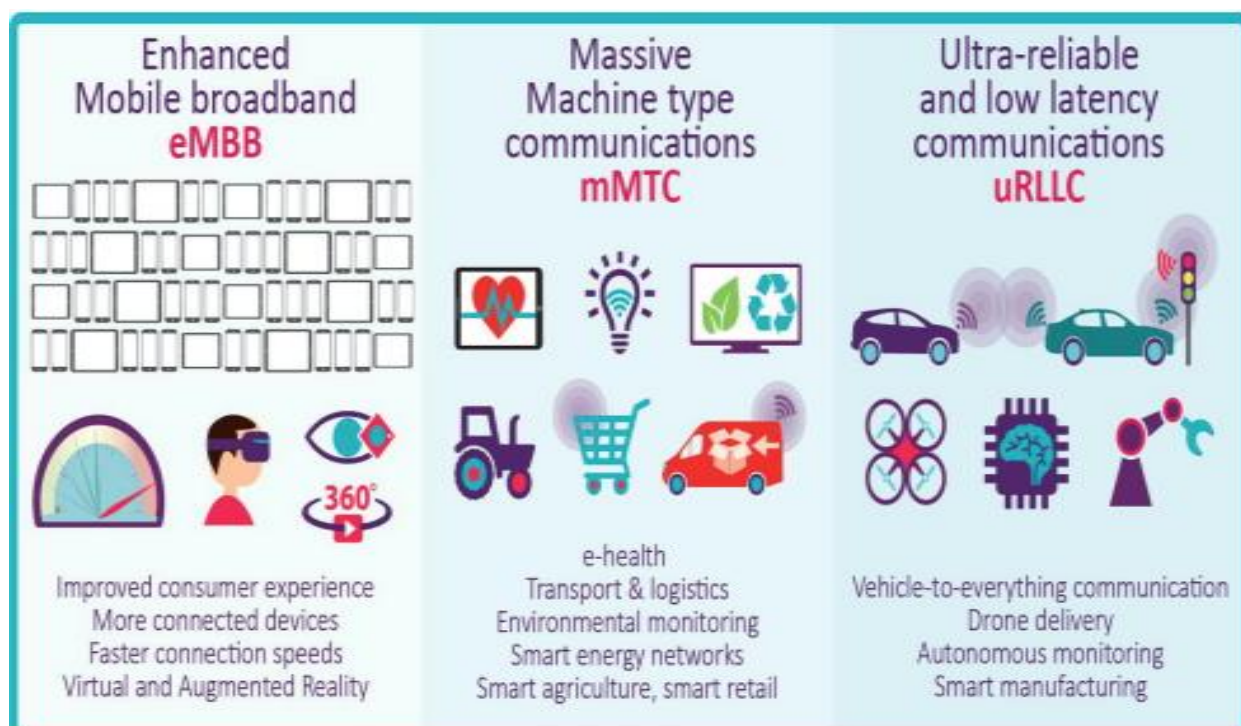
Εικόνα 38 Απαιτήσεις που καθοδηγούν την Αρχιτεκτονική 5G

- Έως 10Gbps ρυθμό μετάδοσης
- x10 έως x100 βελτίωση σε σχέση με τα δίκτυα 4G και 4.5G
- Latency = 1ms
- Εύρος ζώνης 1000 ανά μονάδα επιφάνειας
- Έως 100 x αριθμός συνδεδεμένων συσκευών ανά μονάδα μονάδας (σε σύγκριση με 4G LTE)
- Διαθεσιμότητα 99,999%
- Κάλυψη 100%
- Μείωση κατά 90% στη χρήση ενέργειας δικτύου
- Έως 10 χρόνια ζωής μπαταρίας για συσκευές χαμηλής κατανάλωσης IoT

3.3 Επισκόπηση νέων τεχνολογιών συστήματος

Η 5^η γενιά κινητών επικοινωνιών θα βασίζεται στις παρακάτω Τεχνολογίες ‘πυλώνες’

- **Extreme Mobile Broadband:** Παρέχει πολλαπλά gigabyte εύρους ζώνης αναλόγως την ζήτηση (on-demand). Βελτιώνει την απόδοση και αυξάνει σημαντικά την εμπειρία του χρήστη.
- **Massive Machine Types:** Θα μπορεί να διασυνδέει δισεκατομμύρια αισθητήρες και συσκευές. Θα είναι ικανό να διατηρεί μεγάλη την διάρκεια ζωής των μπαταριών.
- **Critical Machine Communications:** Επιτρέπει την άμεση σύγχρονη ανατροφοδότηση που επιτρέπει τον έλεγχο των ρομπότ. Απαιτεί εξαιρετικά αξιόπιστες (ultra-reliable) και χαμηλής καθυστέρησης (low-latency) επικοινωνίες και διαθεσιμότητα.
- **Small Cells και Pico Cells:** Τα small cells είναι σταθμοί βάσης χαμηλής ισχύος που χρησιμοποιούνται σε προηγμένες εκδόσεις LTE και τεχνολογία 5G για τροφοδοσία συσκευών σε μικρότερη γεωγραφική περιοχή, όπως μερικές εκατοντάδες μέτρα έως ακτίνα 2 km. Τα small cells θα χρησιμοποιούν κύματα χιλιοστών (millimeter wave) για τη μετάδοση και τη λήψη δεδομένων. Τα κύματα χιλιοστών δεν είναι κατάλληλα για επικοινωνία μεγάλων αποστάσεων λόγω υψηλότερης εξασθένισης από την ατμόσφαιρα και εμπόδια. Σε σύγκριση με τους συμβατικούς σταθμούς βάσης, απαιτείται μεγάλος αριθμός μονάδων μικρών κυψελών για την κάλυψη μιας μεγαλύτερης περιοχής. Ωστόσο, μπορεί να παρέχει υψηλότερο ρυθμό δεδομένων και χαμηλή καθυστέρηση κάλυψης δικτύου για τους χρήστες κάτω από κάθε μονάδα.
- **Massive MIMO:** Η έννοια του MIMO (Multiple Input Multiple Output) χρησιμοποιείται για την αύξηση του ρυθμού δεδομένων με την προσθήκη κεραίας για μετάδοση και λήψη σημάτων. Μεγάλος αριθμός συστοιχιών κεραιών μικρού μεγέθους χρησιμοποιούνται στην τεχνολογία 5G. Οι συσκευές χρηστών θα μπορούν επίσης να λαμβάνουν και να στέλνουν δεδομένα χρησιμοποιώντας πολλαπλές κεραίες ενσωματωμένες σε κινητές συσκευές. Σημαντική ποσότητα δεδομένων μπορεί να μεταδοθεί ταυτόχρονα με την εφαρμογή της τεχνολογίας MIMO.
- **Beamforming:** Το Beamforming είναι μια άλλη έξυπνη τεχνολογίας για την αποτελεσματική μετάδοση δεδομένων σε συσκευές χρήστη. Η ακριβής τοποθεσία της συσκευής χρήστη παρακολουθείται συνεχώς χρησιμοποιώντας προηγμένους αλγόριθμους λογισμικού και οι σταθμοί βάσης μεταδίδουν σήματα μόνο προς την κατεύθυνση της τοποθεσίας του χρήστη. Οι συμβατικοί σταθμοί βάσης μεταδίδουν δεδομένα σε πολλές κατευθύνσεις που προκαλούν υψηλότερη κατανάλωση ενέργειας και περιττή χρήση πόρων. Το Beamforming μπορεί να παρομοιαστεί ως ένας προβολέας που ακολουθεί έναν κινούμενο ερμηνευτή σε μια σκηνή. Η δέσμη σήματος θα ακολουθήσει τον χρήστη σύμφωνα με την αλλαγή θέσης.



Εικόνα 39 IMT 2020 Βασικές Κατευθύνσεις ανάπτυξης του 5G

Στην παραπάνω εικόνα περιγράφεται με λίγα λόγια η βιομηχανία στην οποία στοχεύει κάθε μία από τις νέες υπηρεσίες.

3.3.1 Enhanced Mobile Broadband (eMBB)

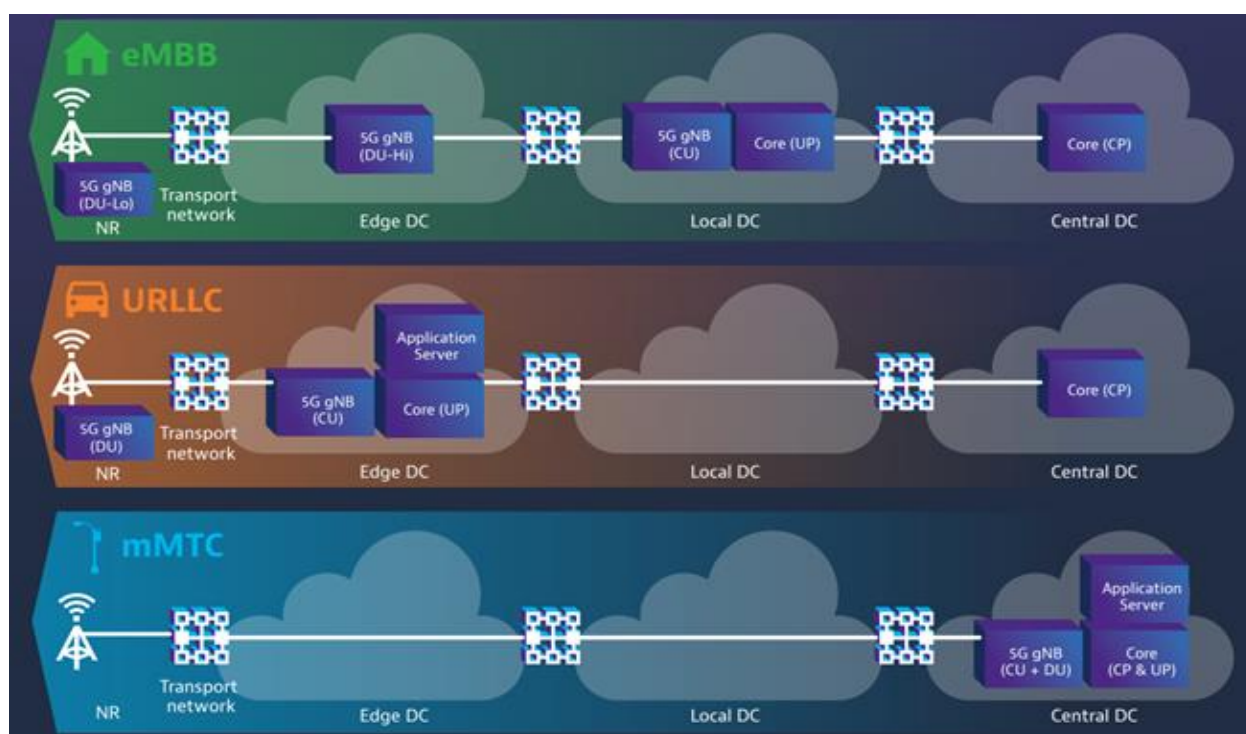
Υποστηρίζει υψηλή χωρητικότητα και υψηλή κινητικότητα, μέχρι και 500km/h, για τη ράδιο πρόσβαση, με 4ms user plane latency). Παρέχοντας επικοινωνίες εξαιρετικά υψηλού ρυθμού δεδομένων και χαμηλού λανθάνοντος χρόνου, το extreme mobile broadband (eMBB) προσφέρει επίσης εξαιρετική κάλυψη - πολύ πέρα από αυτήν που παρέχεται από την 4G. Η συνδεσιμότητα και το εύρος ζώνης είναι πιο ομοιόμορφα στην περιοχή κάλυψης και η απόδοση υποβαθμίζεται σταδιακά καθώς αυξάνεται ο αριθμός των χρηστών.

3.3.2 Ultra-Reliable and Low Latency Communications (URLCC)

Υποστηρίζει επείγουσες και αξιόπιστες ανταλλαγές δεδομένων (με 0.5ms user plane latency). Το URLLC είναι μια υπηρεσία επικοινωνίας για την επιτυχή παράδοση πακέτων με αυστηρές απαιτήσεις, ιδίως όσον αφορά διαθεσιμότητα, καθυστέρηση και αξιοπιστία. Το URLLC θα υποστηρίξει την ενεργοποίηση των αναδυόμενων εφαρμογών και υπηρεσιών. Παραδείγματα υπηρεσιών που περιλαμβάνουν τον ασύρματο έλεγχο και τον αυτοματισμό αποτελούν τα βιομηχανικά εργοστασιακά περιβάλλοντα, επικοινωνίες μεταξύ οχημάτων για βελτιωμένη ασφάλεια και αποτελεσματικότητα. Με βάση τα παραπάνω γίνεται αντιληπτό ότι το URLLC αποτελεί μία σημαντική νέα τεχνολογία του 5G, ιδίως λαμβάνοντας υπόψη την αποτελεσματική υποστήριξη των κατακόρυφων (vertical) βιομηχανιών τις οποίες φέρνει στον κόσμο των τηλεπικοινωνιών.

3.3.3 Massive Machine-Type Communications (mMTC)

Όχι πολύ συχνές, μαζικές και μικρές μεταδόσεις πακέτων για mMTC (με 10s latency). Αλλιώς γνωστό και ως Massive IoT, το mMTC έχει σχεδιαστεί για να παρέχει κάλυψη ευρείας περιοχής και βαθιά διείσδυση (deep penetration) για εκατοντάδες χιλιάδες συσκευές ανά τετραγωνικό χιλιόμετρο κάλυψης. Ένας επιπλέον στόχος του mMTC είναι να παρέχει συνδεσιμότητα παντού με σχετικά χαμηλή πολυπλοκότητα λογισμικού και υλικού και λειτουργία χαμηλής ενέργειας. Παραδείγματα που εμπίπτουν σε αυτήν την κατηγορία υπηρεσιών περιλαμβάνουν την παρακολούθηση και αυτοματοποίηση κτιρίων και υποδομών, έξυπνη γεωργία, εφοδιαστική, παρακολούθηση και διαχείριση στόλου.



Εικόνα 40 Λογική Διασύνδεση 5G RAN με 5G Core Δίκτυο

Στην παραπάνω εικόνα φαίνεται ο τρόπος και τα σημεία με τα οποία η κάθε τεχνολογία αλληλοεπιδρά με το δίκτυο. Όπως μπορεί να παρατηρηθεί η λειτουργία της κάθε τεχνολογίας εξυπηρετεί και διαφορετικό σκοπό, κάτι το οποίο φαίνεται και στην παραπάνω εικόνα από το γεγονός ότι το σημείο στο οποίο βρίσκεται ο server που φιλοξενεί την εφαρμογή είναι διαφορετικό μεταξύ του uRLLC και του mMTC ενώ στο eMBB δεν υπάρχει καθόλου.

3.3.4 Φάσμα και Συχνότητα

Το φάσμα και οι συχνότητες στις οποίες θα εκπέμπει το 5G κυμαίνονται από 30GHz – 300GHz. Το συγκεκριμένο τμήμα του ραδιοφάσματος είναι γνωστό ως millimeter wave καθώς τα μήκη κύματος από 1-10mm. Αυτή την στιγμή παγκοσμίως συχνότητες από 24GHz – 100GHz έχουν αποδοθεί για την χρήση του 5G. Εκτός από τις mmWave συχνότητες που χρησιμοποιούνται στο 5G, επαναχρησιμοποιούνται επίσης και οι χαμηλές UHF συχνότητες μεταξύ των 300 MHz και 3GHz. Το διαφορετικό εύρος των χρησιμοποιούμενων συχνοτήτων μπορεί να προσαρμοστεί στις διαφορετικές εφαρμογές που μπορούν να αναπτυχθούν για το 5G. Οι συχνότητες των mmWave είναι ιδανικές για

πυκνοκατοικημένες περιοχές, αλλά αναποτελεσματικές για επικοινωνία μεγάλων αποστάσεων. Μέσα σε αυτές τις ζώνες υψηλής και χαμηλότερης συχνότητας που έχουν αποδοθεί στο 5G, κάθε φορέας έχει αρχίσει να αποκτά τα δικά του ξεχωριστά τμήματα του φάσματος.

3.3.5 MEC

Το Multi-Access Edge Computing (MEC) αποτελεί ένα σημαντικό στοιχείο της αρχιτεκτονικής του 5G. Το MEC είναι μια εξέλιξη στο cloud computing που φέρνει τις εφαρμογές από τα κεντρικά κέντρα δεδομένων στην άκρη του δικτύου και επομένως πιο κοντά στους τελικούς χρήστες και τις συσκευές τους. Αυτό ουσιαστικά αυξάνει την ταχύτητα παράδοσης του περιεχομένου μεταξύ του χρήστη και του κεντρικού υπολογιστή. Αυτή η τεχνολογία δεν είναι αποκλειστικότητα του 5G, αλλά είναι αναπόσπαστο μέρος της αποτελεσματικότητάς του. Τα χαρακτηριστικά του MEC περιλαμβάνουν την χαμηλή καθυστέρηση, το υψηλό εύρος ζώνης και την πρόσβαση σε πραγματικό χρόνο σε πληροφορίες του RAN και είναι αυτά που ξεχωρίζουν την αρχιτεκτονική του 5G από τους προκατόχους του.

3.3.6 Beamforming

Μια άλλη πρωτοποριακή τεχνολογία που αποτελεί αναπόσπαστο μέρος της αρχιτεκτονικής του 5G είναι το beamforming. Οι συμβατικοί σταθμοί βάσης μεταδίδουν σήματα σε πολλές κατευθύνσεις, ανεξάρτητα από τη θέση των στοχευμένων χρηστών ή των συσκευών. Μέσω της χρήσης συστοιχιών πολλαπλών εισόδων, πολλαπλών εξόδων (MIMO) με δεκάδες μικρές κεραίες σε ένα μόνο σχηματισμό, μπορούν να χρησιμοποιηθούν αλγόριθμοι επεξεργασίας σήματος για τον προσδιορισμό της πιο αποτελεσματικής διαδρομής μετάδοσης σε κάθε χρήστη, ενώ μεμονωμένα πακέτα μπορούν να σταλούν μέσω πολλαπλών κατευθύνσεων και στη συνέχεια να προσεγγίσουν τον τελικό χρήστη σε μια προκαθορισμένη ακολουθία.



Εικόνα 41 Beamforming

Με τη μετάδοση των δεδομένων 5G να καταλαμβάνει την συχνότητα των mmWave, η απώλεια διάδοσης ελεύθερου χώρου, η οποία είναι ανάλογη με το μικρότερο μέγεθος της κεραίας και την απώλεια διάθλασης, οι απώλειες που υπάρχουν σε υψηλότερες συχνότητες και η έλλειψη διείσδυσης στο τοίχωμα, είναι σημαντικά μεγαλύτερες. Από την

άλλη πλευρά, το μικρότερο μέγεθος κεραίας επιτρέπει επίσης πολύ μεγαλύτερες συστοιχίες από κεραίες να καταλαμβάνουν τον ίδιο φυσικό χώρο. Με κάθε μία από αυτές τις μικρότερες κεραίες να αλλάζει πιθανώς την κατεύθυνση της δέσμης αρκετές φορές ανά χιλιοστό του δευτερολέπτου, γίνεται πιο εφικτό το massive beamforming για την υποστήριξη των προκλήσεων το μεγάλο εύρος ζώνης που απαιτεί το 5G. Με μεγαλύτερη πυκνότητα κεραιών στον ίδιο φυσικό χώρο, στενότερες δέσμες μπορούν να επιτευχθούν με massive MIMO, παρέχοντας έτσι ένα μέσο για την επίτευξη υψηλής απόδοσης με πιο αποτελεσματικό εντοπισμό των χρηστών.

3.4 3GPP Phases

Η 3GPP χώρισε το 5G standard σε 2 Releases: Το Release 15 το οποίο αντιστοιχεί στην Φάση 1 του New Radio (NR) και στο Release 16 το οποίο αντιστοιχεί στην Φάση 2 του New radio (NR). Στην Φάση 1 υπάρχουν κοινά στοιχεία μεταξύ του LTE και του NR, όπως για παράδειγμα και τα δύο συστήματα χρησιμοποιούν OFDM. Στον παρακάτω πίνακα φαίνονται οι διαφορές μεταξύ του LTE και το NR. [12]

3.4.1 5G Φάση Πρώτη (Release 15)

- Διόρθωση σφαλμάτων μέσω κωδικών ισοτιμίας χαμηλής πυκνότητας (LDPC) για μετάδοση δεδομένων, οι οποίοι είναι υπολογιστικά πιο αποτελεσματικοί από τους κωδικούς turbo LTE σε υψηλότερους ρυθμούς δεδομένων. Τα κανάλια ελέγχου χρησιμοποιούν πολικούς κωδικούς οι οποίοι καθορίζουν μια διαφορά μεταξύ των επιπέδων πρωτοκόλλου PDCP και Radio Link Control (RLC)
- Αυτόνομα ενσωματωμένα υποπλάισια που συνδυάζουν προγραμματισμό, δεδομένα και αναγνώριση. Τα οφέλη περιλαμβάνουν γρήγορη και ευέλικτη εναλλαγή TDD, χαμηλότερο λανθάνοντα χρόνο και αποτελεσματικό τεράστιο MIMO
- Παροχή ενός ευέλικτου ράδιο πλαισίου που έχει συμβατότητα προς τα εμπρός για την υποστήριξη μελλοντικών, επί του παρόντος άγνωστων υπηρεσιών, όπως το URLLC που θα καθοριστεί στην Έκδοση 16 και σε μη αδειοδοτημένο / κοινόχρηστο φάσμα
- Επεκτάσιμα χρονικά διαστήματα μετάδοσης, με σύντομα χρονικά διαστήματα για χαμηλό λανθάνοντα χρόνο (low latency) και μεγαλύτερα χρονικά διαστήματα για υψηλότερη φασματική απόδοση
- Υποστήριξη ενός νέου μοντέλου QoS
- Δυναμική συνύπαρξη με το LTE στα ίδια ράδιο κανάλια
- Network slicing

3.4.2 5G Φάση Δεύτερη (Release 16)

- URLLC (Ultra Reliable Low Latency Communications)
- Λειτουργία σε μη αδειοδοτημένο φάσμα κάτω από τα 7 GHz, πιθανότατα θα βασίζεται σε τρέχουσες προσεγγίσεις του LTE όπως το LAA
- Integrated access and backhaul

- NR-based C-V2X
- Θέση για εμπορική και κανονιστική χρήση
- NR για μη επίγεια δίκτυα, συμπεριλαμβανομένων των δορυφόρων
- Υποστήριξη για ράδιο ζώνες πάνω από τα 52.6 GHz
- Dual-carrier, carrier-aggregation, και ενίσχυση κινητικότητας
- Μείωση κατανάλωσης ισχύος του χρήστη

Το Release 16 θα αποτελέσει την φάση 2 του 5G και αναμένεται να ολοκληρωθεί έως το τέλος του 2020. [12] Προκειμένου να ολοκληρωθεί πλήρως το νέο 5G σύστημα χρειάζεται εντελώς νέος εξοπλισμός. Παρ' όλα αυτά επειδή αυτό είναι μία μετάβαση πολύ κοστοβόρα για όλες τις εταιρείες τηλεπικοινωνιών προτάθηκε μία νέα προσέγγιση μετάβασης στο νέο σύστημα και αυτή είναι ότι θα λειτουργούν ταυτόχρονα και το LTE Core δίκτυο και το νέο υπό ανάπτυξη NR δίκτυο. Αυτά τα δύο δίκτυα θα επικοινωνούν μεταξύ τους. Οι νέες δικτυακές συσκευές που θα εισάγονται στο δίκτυο θα διαμορφώνονται εξ αρχής προκειμένου να επικοινωνούν μόνο με το νέο NR Core δίκτυο. Για να καταστεί σαφές ποιες συσκευές μπορούν να επικοινωνούν μεταξύ τους, έχει εισαχθεί νέα ορολογία:

3.5 Ορολογία του 3GPP Release 15 (5G)

- LTE eNB - Συσκευή που μπορεί να συνδεθεί στο EPC ή στο τρέχον βασικό δίκτυο LTE
- eLTE eNB: The eLTE eNB είναι η εξέλιξη του eNB που υποστηρίζει τη σύνδεση με το EPC και το NGC (Next Generation Core)
- gNB: Ένας κόμβος που υποστηρίζει το NR καθώς και συνδεσιμότητα με το NGC
- New RAN: Είναι ένα Ράδιο Δίκτυο Πρόσβασης που υποστηρίζει είτε το NR είτε το E-UTRA ή και τα δύο μαζί, έχοντας διασύνδεση με το NGC
- New Radio: Αποτελεί την νέα τεχνολογία Ράδιο Δικτύου Πρόσβασης
- Network Slice: Το Network Slice είναι ένα νέο εικονικό δίκτυο που δημιουργήθηκε από τον διαχειριστή προσαρμοσμένο για να παρέχει μια βελτιστοποιημένη λύση για ένα συγκεκριμένο σενάριο αγοράς/πελάτη
- Network Function: Το Network Function είναι ένας λογικός κόμβος σε μια υποδομή δικτύου που έχει καλά καθορισμένες εξωτερικές διεπαφές και καλά καθορισμένη λειτουργική συμπεριφορά
- NG2 – Αποτελεί την Control plane διεπαφή μεταξύ του core δικτύου και του RAN (S1-C in LTE)
- NG3 – Αποτελεί την User plane διεπαφή μεταξύ του core δικτύου και του RAN (S1-U in LTE)

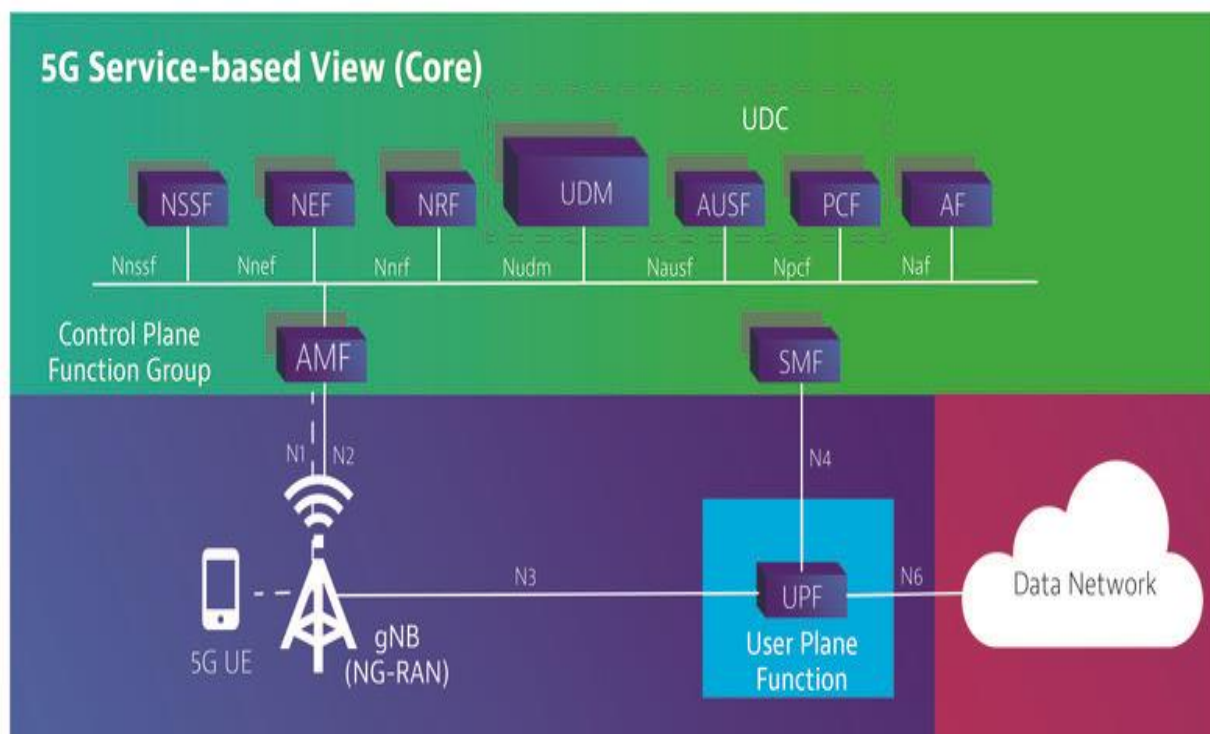
- NG-C: Είναι μία control plane διεπαφή που χρησιμοποιείται στο NG2 για επικοινωνία μεταξύ του New RAN και του NGC
- NG-U: Είναι μία user plane διεπαφή που χρησιμοποιείται στο NG3 για επικοινωνία μεταξύ του New RAN και του NGC
- Non-standalone NR: Είναι μια δικτυακή διαμόρφωση όπου το gNB απαιτεί ένα LTE eNB ως σημείου εισόδου για control plane συνδεσιμότητα στο EPC, ή ένα eLTE eNB ως σημείου εισόδου για control plane συνδεσιμότητα στο NGC
- Non-standalone E-UTRA: Είναι μια δικτυακή διαμόρφωση όπου το eLTE eNB απαιτεί ένα gNB ως σημείου εισόδου για control plane συνδεσιμότητα στο NGC
- User Plane Gateway: Σημείο τερματισμού της ραδιο-επαφής NG-U

3.6 Διαφορές από την 4G Αρχιτεκτονική

Οι διαφορές στο επίπεδο του Core δικτύου μεταξύ του 4G και του 5G είναι τεράστιες καθώς πλέον στην αρχιτεκτονική του 5G εισήχθησαν νέα αρχιτεκτονικά στοιχεία όπως millimeter wave, massive MIMO και network slicing. Η μεγαλύτερη διαφορά όμως μεταξύ των δύο Core Αρχιτεκτονικών είναι ότι το 5G Core αξιοποιεί την εικονικοποίηση (virtualization) και το σχεδιασμό λογισμικού cloud σε πρωτοφανή επίπεδα. Μεταξύ των άλλων αλλαγών που διαφοροποιούν το 5G Core από τον προκάτοχό του 4G είναι η λειτουργία επιπέδου χρήστη (UPF) για την αποσυσχέτιση του packet gateway control, του user plane function και του access and mobility function (AMF) έτσι ώστε να μπορέσει να γίνει ο διαχωρισμός των λειτουργιών διαχείρισης συνεδρίας (session management functions) από τις εργασίες σύνδεσης και διαχείρισης κινητικότητας (connection and mobility management tasks).

3.7 Οντότητες και διεπαφές δικτύου κορμού 5G

Η αρχιτεκτονική του 5G Core βρίσκεται στο επίκεντρο της νέας προδιαγραφής για το 5G και επιτρέπει την αυξημένη ζήτηση για εύρος ζώνης που πρέπει να υποστηρίξει το 5G. Το νέο 5G Core, όπως έχει οριστεί από την 3GPP, χρησιμοποιεί service-based αρχιτεκτονική (SBA) η οποία επεκτείνεται σε όλα τα συστατικά μέρη του νέου δικτύου και στις μεταξύ τους αλληλεπιδράσεις και περιλαμβάνει τα αυθεντικοποίηση, ασφάλεια, διαχείριση συνεδρίας και συνάθροιση της κυκλοφορίας των τερματικών συσκευών. Το νέο 5G Core δίνει έμφαση στο NFV ως αναπόσπαστο κομμάτι του σχεδιασμού με εικονικοποιημένες λειτουργίες λογισμικού (virtualized software functions) ικανές να αναπτυχθούν χρησιμοποιώντας την υποδομή MEC. [15]



Εικόνα 42 Συστατικά Μέρη - Λειτουργίες του 5G Core

3.7.1 AMF - Access and Mobility Function

1. Διαχειρίζεται το αρχικό μήνυμα του UE από το gNB. Αυτό το μήνυμα φέρει το αίτημα εγγραφής από τον UE.
2. Κατά τη λήψη του αιτήματος εγγραφής, το νέο AMF αποκτά το περιεχόμενο του UE από το παλιό AMF
3. Στη συνέχεια, το AMF αυθεντικοποιεί τον UE έπειτα και από την απόκτηση των κλειδιών από το AUSF. Η ασφάλεια στο επίπεδο του NAS δημιουργείται μεταξύ του UE και του AMF
4. Το AMF ελέγχει επίσης το 5G-EIR(Equipment Identity Register) για να επαληθεύσει ότι η εγγραφή δεν επιχειρείται από κλεμμένη συσκευή
5. Στη συνέχεια, το AMF αποκτά δεδομένα συνδρομής από το UDM
6. Στη συνέχεια, το AMF δημιουργεί μια πολιτική σύνδεσης με το PCF
7. Στη συνέχεια, το AMF ενημερώνει το περιεχόμενο του SMF και αποστέλλει ένα Initial Context Setup Request για να ενεργοποιήσει την προεπιλεγμένη περίοδο λειτουργίας PDU. Το μήνυμα περιέχει επίσης και το μήνυμα Αποδοχή της καταχώρησης από το AMF.
8. Όταν το gNB ενημερώσει για την ολοκλήρωση της αρχικής ρύθμισης του περιεχομένου, το AMF ενημερώνει το περιεχόμενο του SMF

3.7.2 AUSF - Authentication Server Function

Το AUSF συμμετέχει στη διαδικασία ελέγχου ταυτότητας. Λαμβάνει τις πληροφορίες ελέγχου ταυτότητας του UE από το UDM.

3.7.3 UDM - Unified Data Management

Το UDM παρέχει δεδομένα επαλήθευσης ταυτότητας κατά τη διάρκεια της διαδικασίας εγγραφής. Το νέο AMF που εξυπηρετεί τον χρήστη καταχωρεί επίσης το UDM. Το παλιό AMF διαγράφεται από το UDM. Το UDM παρέχει επίσης πληροφορίες διαχείρισης των δεδομένων των συνδρομητών στο νέο AMF.

3.7.4 PCF - Policy Control Function

Το νέο AMF δημιουργεί μια συσχέτιση πολιτικής (policy-association) με το PCF. Το παλιό AMF διαγράφει το policy-association με το PCF. Το PCF εγγράφεται με το AMF, ώστε να μπορεί να ειδοποιηθεί σε γεγονότα όπως αλλαγή τοποθεσίας και αποτυχία επικοινωνίας.

3.7.5 SMF - Session Management Function

Το SMF βρίσκεται στο Control plane και είναι υπεύθυνο για διαχείριση των session. Εμπλέκεται στις ακόλουθες αλληλεπιδράσεις:

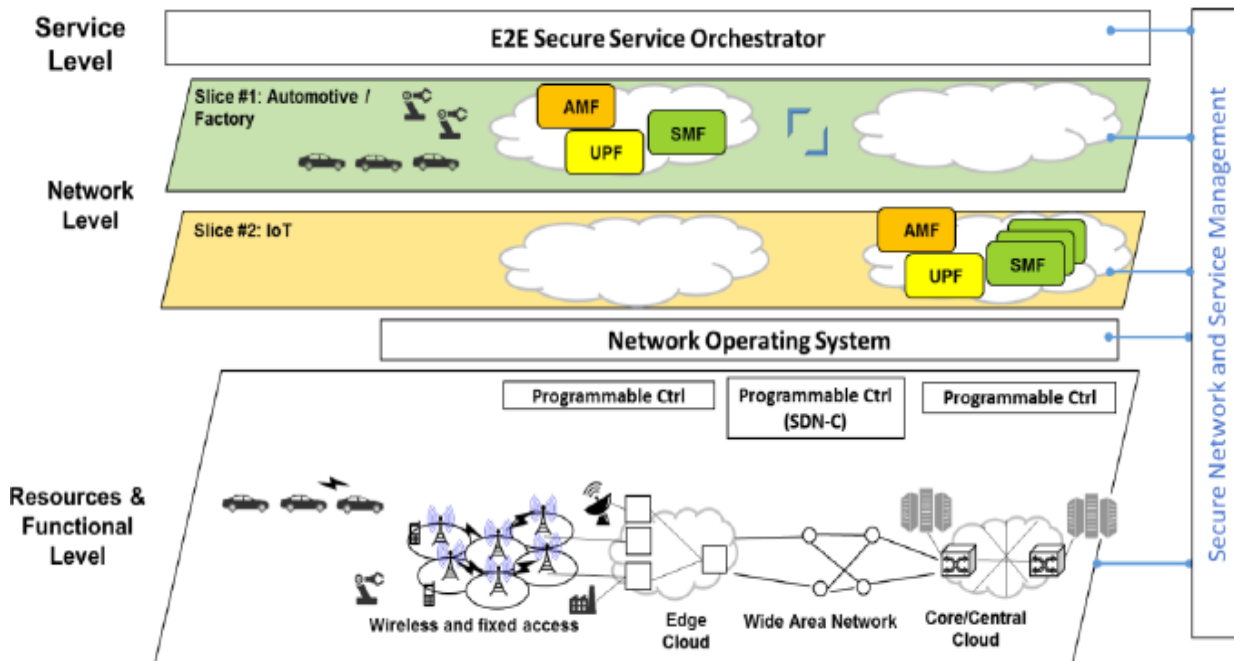
1. Το παλιό AMF απεγγράφεται από το SMF
2. Το νέο AMF ενημερώνει το περιεχόμενο διαχείρισης των sessions. Το SMF αποδίδει μια διεύθυνση IP και το αναγνωριστικό σήραγγας (tunnel id) που θα χρησιμοποιηθεί για την αποστολή δεδομένων ανερχόμενης ζεύξης.
3. Το SMF επιλέγει το UPF που θα χρησιμοποιηθεί για το session.
4. Το SMF ενημερώνει το UPF χρησιμοποιώντας μηνύματα PFCP μέσω της διασύνδεσης επιπέδου δεδομένων ελέγχου N4.
5. Το νέο AMF ειδοποιεί επίσης το SMF όταν το session είναι έτοιμο για μεταφορά δεδομένων ανερχόμενης ζεύξης και κατερχόμενης.

3.7.6 UPF - User Plane Function

Το UPF είναι ένα στοιχείο που ανήκει στο data plane και διαχειρίζεται τα δεδομένα χρήστη. Το UPF ελέγχεται πλήρως από το SMF χρησιμοποιώντας τη διεπαφή N4. Το SMF χρησιμοποιεί το Packet Flow Control Protocol (PFCP) για να ανανεώσει το data plane. Το πρώτο PFCP Session Modification Request ετοιμάζει το UPF προκειμένου να λάβει uplink data. Το UPF επίσης ξεκινά την προσωρινή αποθήκευση (buffering) των downlink data. Μόλις δημιουργηθεί το default PDU session, το SMF ανανεώνει το PFCP session έτσι ώστε να ξεκινήσει να στέλνει downlink data. [16]

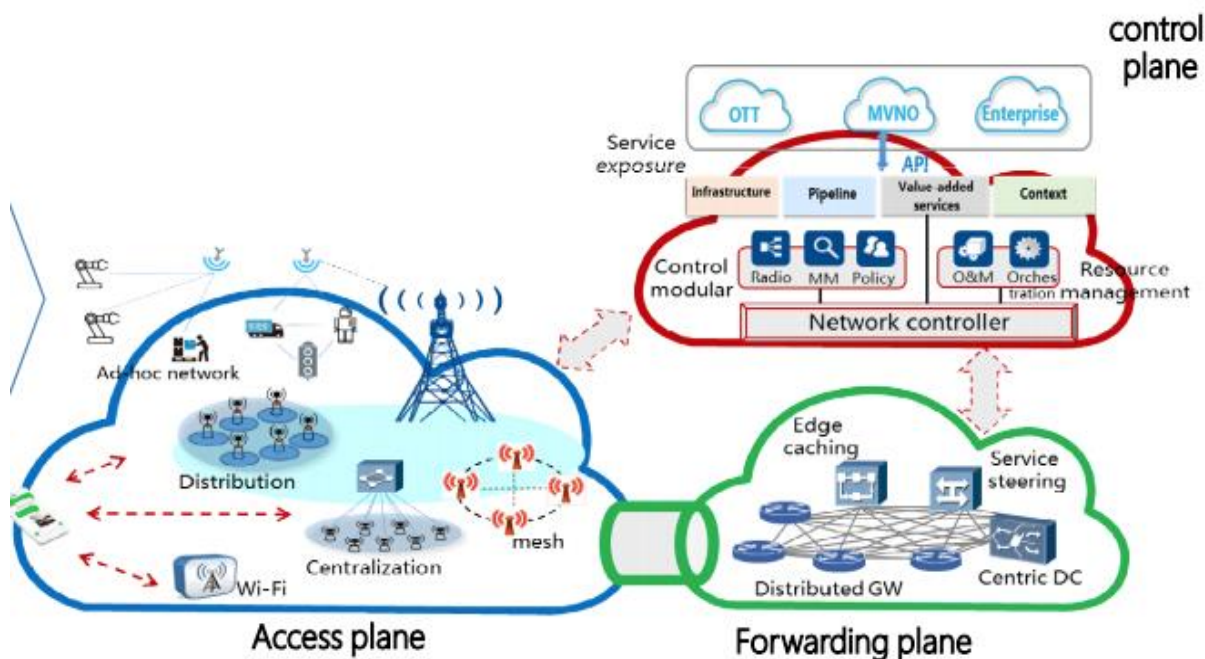
3.8 Σενάρια ανάπτυξης/ Επιλογές αρχιτεκτονικής 5G

Η Συνολική Αρχιτεκτονική του νέου συστήματος απεικονίζεται παρακάτω



Εικόνα 43 End-to-End 5G Αρχιτεκτονική

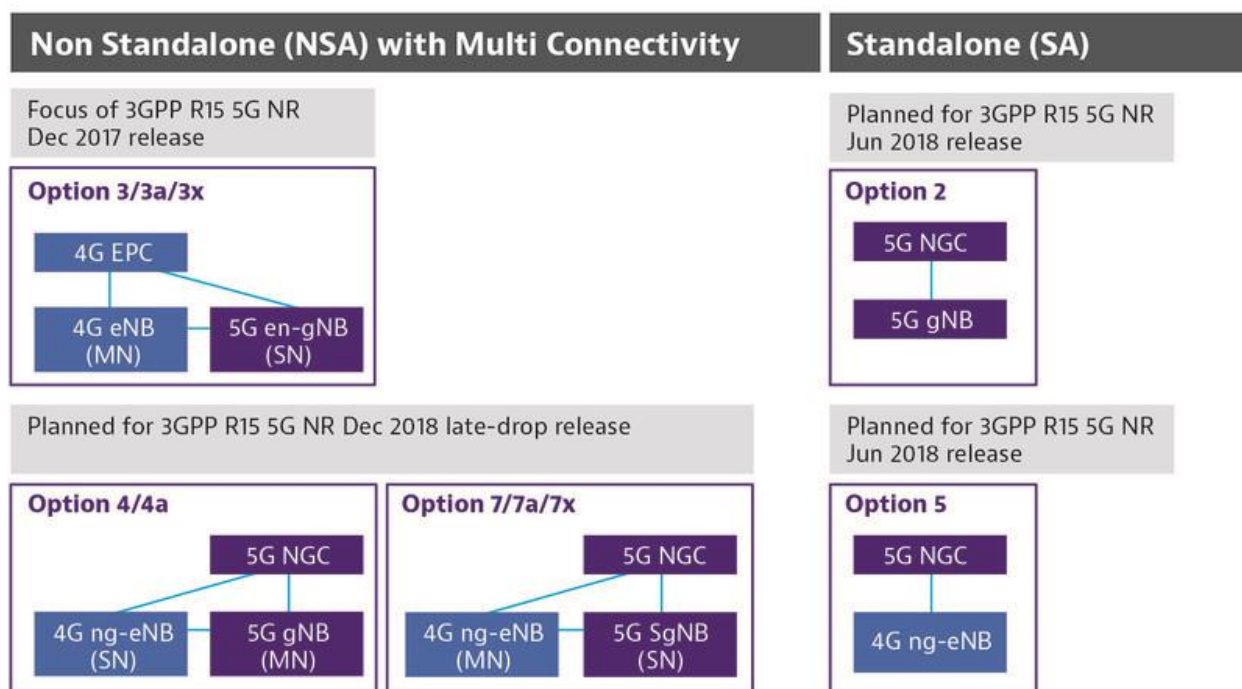
Η πλήρης περιγραφή του νέου 5G Αρχιτεκτονικού Συστήματος περιγράφεται μέσα από τα specifications TS 23.501 (System Architecture for the 5G System), TS 23.502 (Procedures for the 5G System) and TS 23.503 (Policy and Charging Control Framework for the 5G System). Η νέα αρχιτεκτονική του 5G συστήματος θα βασίζεται στο Access plane, Control Plane και το Forwarding Plane. [13], [14]



Εικόνα 44 5G Επίπεδα Πρόσβαση, Προώθησης και Ελέγχου

Ο ρόλος του NFV (Network Function Virtualization) στην νέα αρχιτεκτονική του 5G θα είναι να διαχωρίσει το software από το hardware παρέχοντας έτσι ευέλικτη νέα υποδομή. Ο ρόλος του SDN (Software Define Networking) στην νέα αρχιτεκτονική του 5G θα είναι ο διαχωρισμός του Control plane από το Forwarding plane. Η αρχιτεκτονική του συστήματος 5G έχει σχεδιαστεί για να υποστηρίζει τη συνδεσιμότητα δεδομένων και τις υπηρεσίες, επιτρέποντας στις εφαρμογές να χρησιμοποιούν τεχνικές όπως Network Function Virtualization και Software Defined Networking. Η αρχιτεκτονική του συστήματος 5G θα πρέπει να αξιοποιεί τις υπηρεσίες οι οποίες βασίζονται στην αλληλεπίδραση με τις δικτυακές λειτουργίες του Control Plane. Το 5G χρησιμοποιεί μια πιο έξυπνη αρχιτεκτονική, με τα Δίκτυα Radio Πρόσβασης (RAN) να μην περιορίζονται πλέον από την εγγύτητα σταθμών βάσης ή από πολύπλοκες υποδομές. Το 5G οδηγεί προς ένα ευέλικτο και εικονικό RAN με νέες διεπαφές δημιουργώντας πρόσθετα σημεία πρόσβασης δεδομένων. [13]

Η γεφύρωση του χάσματος μεταξύ 4G και 5G απαιτεί σταδιακά βήματα και ένα καλά οργανωμένο σχέδιο μετάβασης. Σημείο κλειδί θα είναι η σταδιακή μετάβαση από μη αυτόνομη λειτουργία (Non-Standalone Mode) σε αυτόνομη (Standalone Mode) λειτουργία αρχιτεκτονικής 5G. Το μη αυτόνομο (Non-Standalone) πρότυπο 5G ολοκληρώθηκε στα τέλη του 2017 και χρησιμοποιεί τα υπάρχοντα ασύρματα δίκτυα LTE και LTE Core δίκτυο ως βασικά δικτυακά στοιχεία, με την προσθήκη μόνο σταθμών βάσεων 5G. Παρά την εξάρτηση από την υπάρχουσα αρχιτεκτονική, η μη αυτόνομη λειτουργία θα αυξήσει το εύρος ζώνης αγγίζοντας τις συχνότητες mmWave (24GHz – 100GHz). Η αυτόνομη λειτουργία (Standalone Mode) 5G είναι ουσιαστικά η ανάπτυξη του νέου 5G δικτύου από την αρχή με τη νέα αρχιτεκτονική πυρήνα και πλήρη ανάπτυξη όλου του υλικού, των λειτουργιών και των λειτουργιών 5G. Καθώς η μη αυτόνομη λειτουργία υποχωρεί σταδιακά σε νέες αναπτύξεις αρχιτεκτονικής δικτύου κινητής τηλεφωνίας 5G, ο προσεκτικός σχεδιασμός και η εφαρμογή θα κάνουν αυτήν τη μετάβαση απρόσκοπτη για τους χρήστες.



Εικόνα 45 Non-Standalone & Standalone Αρχιτεκτονική

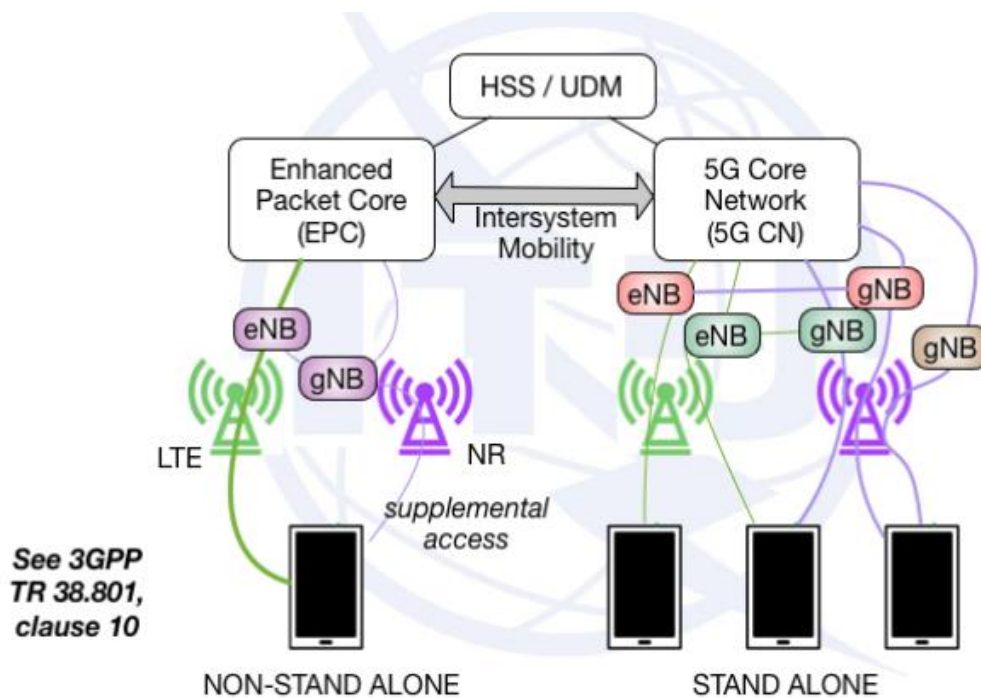
Non-standalone (NSA) και Standalone (SA) είναι δύο 5G διαφορετικοί δρόμοι που οι πάροχοι υπηρεσιών κινητής επικοινωνίας μπορούν να επιλέξουν κατά τη μετάβασή τους από την 4G γενιά στην επόμενη γενιά, το 5G. Η πρώτη ανάπτυξη των δικτύων 5G είναι αναπτύξεις NSA που εστιάζουν στην ενισχυμένη ευρυζωνική τεχνολογία για την παροχή υψηλότερου εύρους ζώνης δεδομένων και αξιόπιστης συνδεσιμότητας. Είναι σύμφωνες με την προδιαγραφή 3GPP ότι οι πρώιμες εκκινήσεις δικτύων και συσκευών 5G θα τεθούν υπό τη λειτουργία της NSA - δηλαδή, τα δίκτυα 5G θα βοηθηθούν από την υπάρχουσα υποδομή 4G. Έτσι, οι πάροχοι υπηρεσιών που θέλουν να είναι οι πρώτοι που θα προσφέρουν ταχύτητες 5G θα ξεκινήσουν με την NSA και, μόλις δημιουργηθεί κάλυψη 5G, θα εφαρμόσουν αυτόνομο 5G. Ωστόσο, η ψηφιοποίηση της βιομηχανίας είναι αυτό που θα ανοίξει το δρόμο για νέες ροές εσόδων για παρόχους υπηρεσιών. Οι περιπτώσεις χρήσης 5G που απαιτούν ultra-low latency και πολύ μεγαλύτερη χωρητικότητα θα είναι εφικτές μόνο με την υποδομή του SA 5G NR και την αρχιτεκτονική δικτύου πυρήνα 3GPP 5G Core (5GC). Ακολουθεί μια πιο λεπτομερής των χαρακτηριστικών των δύο επιλογών της αρχιτεκτονικής 5G από την άποψη των χαρακτηριστικών και της επιπρόσθετης αξίας που φέρνουν στο νέο σύστημα.

3.8.1 Non-Standalone 5G

- Εισάγει νέα 5G φάσματα για την αύξηση της χωρητικότητας και της αποδοτικότητας
- Μεγιστοποιεί την χρήση των ήδη εγκατεστημένων LTE σταθμών βάσεων
- Απαιτείται ένας κεντρικός LTE κόμβος για control plane επικοινωνία and διαχείριση κινητικότητας
- 5G Evolved Packet Core
- Παρέχει πρόωρη υιοθέτηση για 5G-enabled συσκευές
- Επιτρέπει το video streaming, AR/VR
- Δημιουργεί ευκαιρίες για νέες περιπτώσεις χρήσης όπως Critical IoT

3.8.2 Standalone 5G

- Ολοκληρωμένο 5G σύστημα
- Απλοποιημένη αρχιτεκτονική RAN και συσκευών
- Νέο cloud-native 5G Core
- Εισάγει ultra-low latency
- Υποστηρίζει προηγμένες λειτουργίες network-slicing
- Υποστηρίζει ένα ευρύτερο φάσμα περιπτώσεων χρήσης για νέες 5G συσκευές



[17]

Υπάρχουν δύο τρόποι με τους οποίους ένα UE μπορεί να συνδεθεί σε μία 5G NR κυψέλη.

1. EUTRA- NR- Dual Connectivity - ENDC
2. Standalone NR Κυψέλες

Με τον 1^ο τρόπο, ENDC, οι πληροφορίες της αναζήτησης κυψέλης, όπως η συχνότητα, το αναγνωριστικό κυψέλης, οι RACH (Random Access Channel) παράμετροι, κλπ, παρέχονται από το δίκτυο μέσω του RRC Reconfiguration μηνύματος και το οποίο στέλνεται από το eNB. Ο UE μπορεί μέσω του RACH να αποκτήσει πρόσβαση στην κυψέλη(gNB) του νέου 5G NR δικτύου.

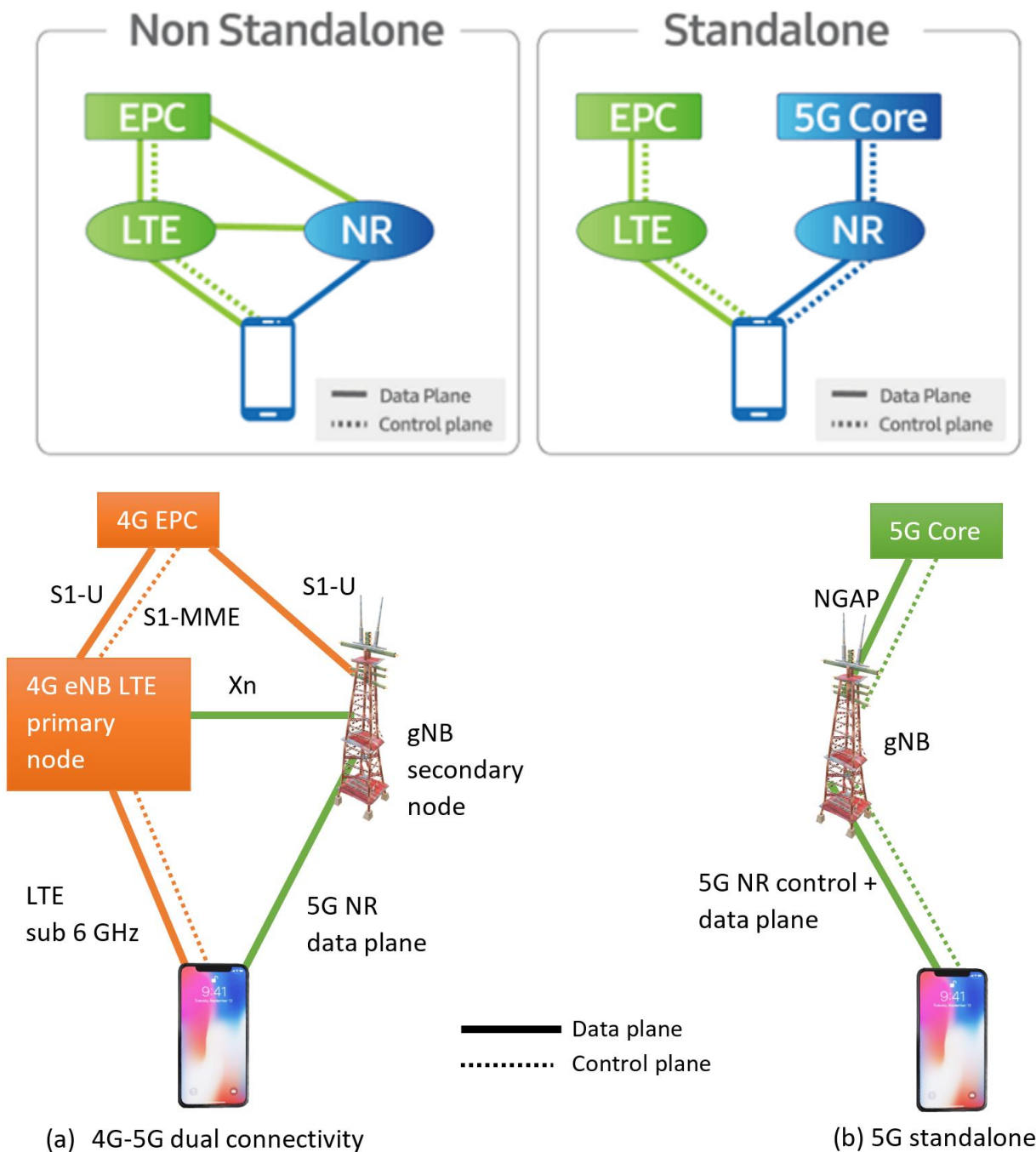
Με τον 2^ο τρόπο, Standalone NR αναζήτηση κυψέλης, ο UE σαρώνει την ζώνη συχνοτήτων sync raster βασισμένος στη ζώνη συχνοτήτων που ο UE είναι ρυθμισμένος να πραγματοποιεί την αναζήτηση κυψελών κάτι το οποίο ορίζεται από το 3GPP 38.104, 5.4.3.3. Το synchronization raster υποδηλώνει την θέση που πρέπει να έχει το synchronization block στο πεδίο της συχνότητας και αποτελεί μία πληροφορία που μπορεί

να χρησιμοποιηθεί από τον UE για πρόσβαση στο σύστημα όταν δεν είναι μπορεί να προσδιοριστεί μέσω της σηματοδότησης η ακριβής τοποθεσία του synchronization block. Το synchronization raster και το subcarrier spacing για κάθε synchronization block ορίζεται ξεχωριστά για κάθε ζώνη συχνοτήτων. Το RACH σημαίνει Random Access Channel και είναι το πρώτο μήνυμα που στέλνει ο UE προς το eNB όταν ανοίγει. Από την οπτική γωνία του eNB, φαίνεται ότι παίρνει αυτό το αρχικό σήμα του UE σχεδόν τυχαία (π.χ. σε τυχαίο χρόνο, τυχαία συχνότητα και τυχαία αναγνώριση) επειδή δεν έχει ιδέα το πότε ένας χρήστης ενεργοποιεί το UE (στην πραγματικότητα δεν είναι εντελώς τυχαίο, υπάρχει ένα ορισμένο εύρος συμφωνίας μεταξύ UE και δικτύου σχετικά με το χρονοδιάγραμμα, τη θέση συχνότητας και την πιθανή αναγνώριση, αλλά σε μεγάλη κλίμακα θα έμοιαζε να είναι εντελώς τυχαίο). Όσον αφορά την υλοποίηση του δικτύου πρόσβασης (RAN), η διαχείριση του RACH θα ήταν μία από τις πιο απαιτητικές εργασίες. Ακόμη και όσον αφορά το σχεδιασμό του πρωτοκόλλου, ο σχεδιασμός του RACH μπορεί να είναι ένα από τα πιο σημαντικά και κρίσιμα τμήματα.

Η αναζήτηση κυψέλης (cell search) είναι η διαδικασία με την οποία το UE αποκτά συγχρονισμό χρόνου και συχνότητας με μία κυψέλη και αποκωδικοποιεί το αναγνωριστικό κυψέλης της κυψέλης. Στο 5G NR, η διαδικασία αναζήτησης κυψέλης είναι παρόμοια με του LTE όσον αφορά την αποκωδικοποίηση του Primary Sync Signal (PSS) και Secondary Sync Signal (SSS). Όπως αναφέρθηκε και παραπάνω το Radio Access του νέου 5G NR συστήματος, το οποίο βασίζεται στην OFDM μέθοδο διαμόρφωσης, βασίζεται σε δύο μεθόδους με τις οποίες ένα UE μπορεί να έχει πρόσβαση σε ένα κύτταρο 5G-NR:

- ⇒ **Non-Standalone 5G New Radio (NR) : EUTRA – NR Dual Connectivity [EN-DC]:** Είναι η πρώτη έκδοση του Standalone 5G New Radio (NR) και στο οποίο το 5G σύστημα υποστηρίζεται από την ήδη υπάρχουσα 4G υποδομή. Το Non-Standalone 5G New Radio (NR) επικεντρώνεται κυρίως στο enhanced mobile broadband (eMBB) όπου οι κινητές συσκευές που υποστηρίζουν 5G θα χρησιμοποιούν mm-Wave συχνότητες για αυξημένη χωρητικότητα δεδομένων αλλά θα χρησιμοποιούν την ήδη υπάρχουσα 4G υποδομή για τις επικοινωνίες φωνής.

- ⇒ **Standalone 5G New Radio (NR) Deployment:** Θα είναι μία εντελώς νέα end-to-end αρχιτεκτονική η οποία θα χρησιμοποιεί mm-Waves και sub-GHz συχνότητες. Η αρχιτεκτονική αυτή δεν θα χρησιμοποιεί το ήδη υπάρχον 4G σύστημα. Το Standalone 5G New Radio (NR) θα χρησιμοποιεί enhanced mobile broadband (eMBB), Ultra-reliable low latency communications (URLLC) και Massive machine type communications (mMTC) για να παρέχει multi-gigabit ρυθμούς δεδομένων με βελτιωμένη αποτελεσματικότητα και χαμηλότερα κόστη.

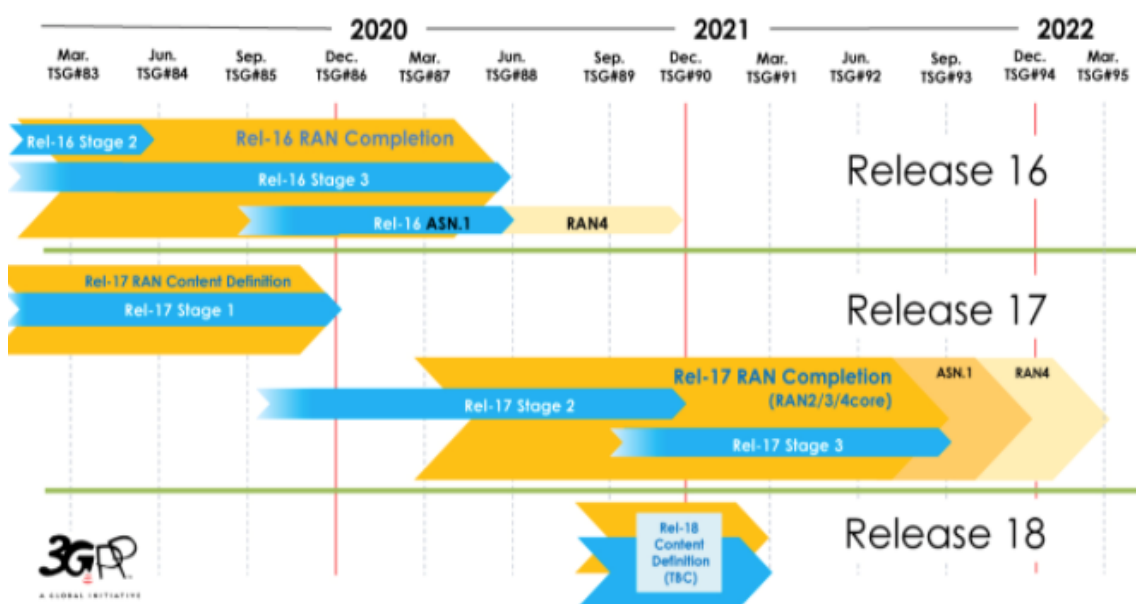


Εικόνα 46 Non-Standalone & Standalone Αρχιτεκτονική

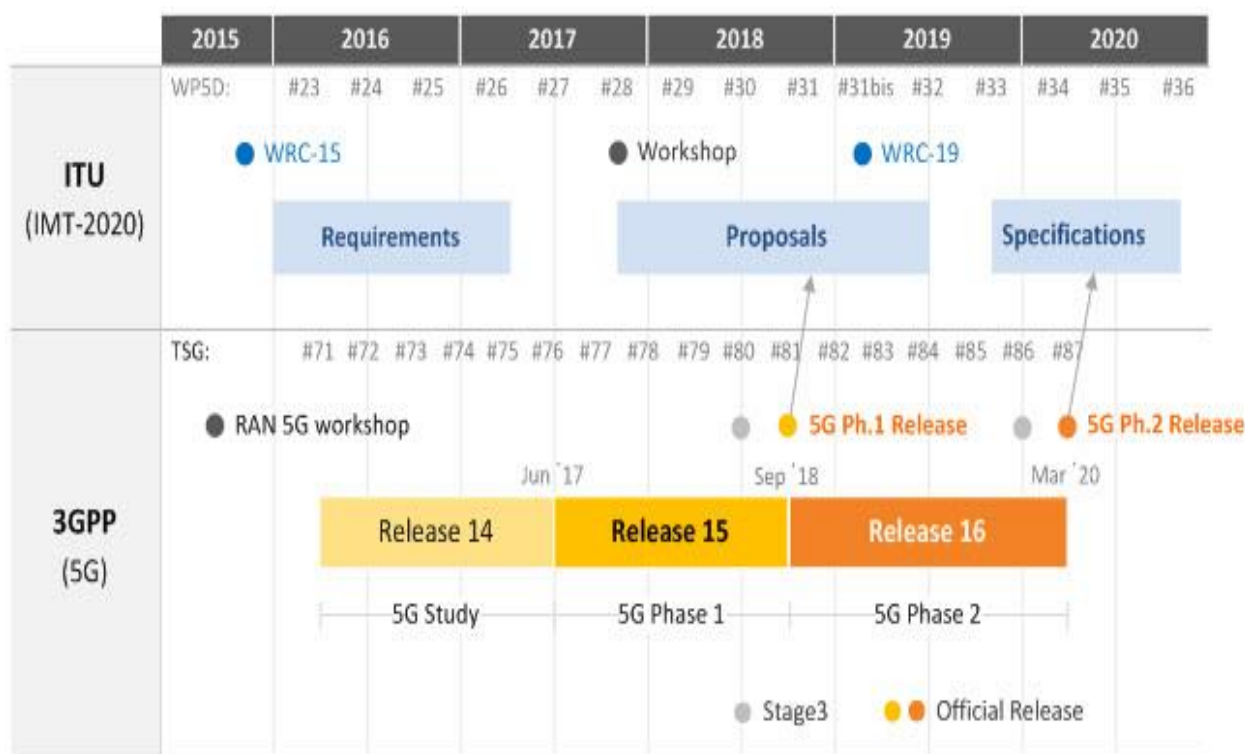
Στην πρώτη περίπτωση, Non-Standalone 5G New Radio (NR), οι πληροφορίες από την αναζήτηση της κυψέλης όπως η συχνότητα (NR-ARFCN), το αναγνωριστικό κυψέλης, οι RACH παράμετροι κλπ. παρέχονται από το δίκτυο και μηνύματος μέσω του LTE eNB. Ο UE μπορεί να προσπαθήσει μέσω κάποιου Random Access Channel (RACH) να αποκτήσει πρόσβαση στην κυψέλη του 5G NR. Το RACH χρησιμοποιείται από τον UE για να μπορέσει να αιτηθεί την δημιουργία νέας σύνδεσης (connection setup). Η διαδικασία αυτή ονομάζεται random access. Στην δεύτερη περίπτωση, Standalone 5G New Radio (NR), η διαδικασία αναζήτησης κυψέλης είναι η παρακάτω:

1. Ο UE συντονίζεται σε μια συγκεκριμένη συχνότητα
2. Ο UE προσπαθεί να ανιχνεύσει το PSS/SSS. Εάν ο UE δεν το ανιχνεύσει, πηγαίνει να συντονιστεί στην επόμενη συχνότητα
3. Μόλις ανιχνευτεί με επιτυχία το PSS / SSS, ο UE προσπαθεί να αποκωδικοποιήσει το PBCH
4. Μόλις ο UE αποκωδικοποιήσει με επιτυχία το PBCH, προσπαθεί να PDCCCH και PDSCH για RMSI και OSI

Η 3GPP έχει ορίσει ένα συγκεκριμένο χρονοδιάγραμμα για την ολοκλήρωση του κάθε νέου Release με σκοπό να διασφαλίσουν ότι όλα τα Release ολοκληρώνονται στην ώρα τους και πως η μετάβαση από το 4G σύστημα στο νέο 5G σύστημα θα παραδοθεί στην ώρα του. Στην παρακάτω εικόνα φαίνεται το χρονοδιάγραμμα που έχει δοθεί μέχρι και την ολοκλήρωση του Release 18.



Εικόνα 47 3GPP Release 18 Timeplan



Εικόνα 48 3GPP 5G Timeline

Στη παραπάνω εικόνα αποτυπώνεται συνολικά το χρονοδιάγραμμα από τότε που το 5G σύστημα ξεκίνησε να σχεδιάζεται.

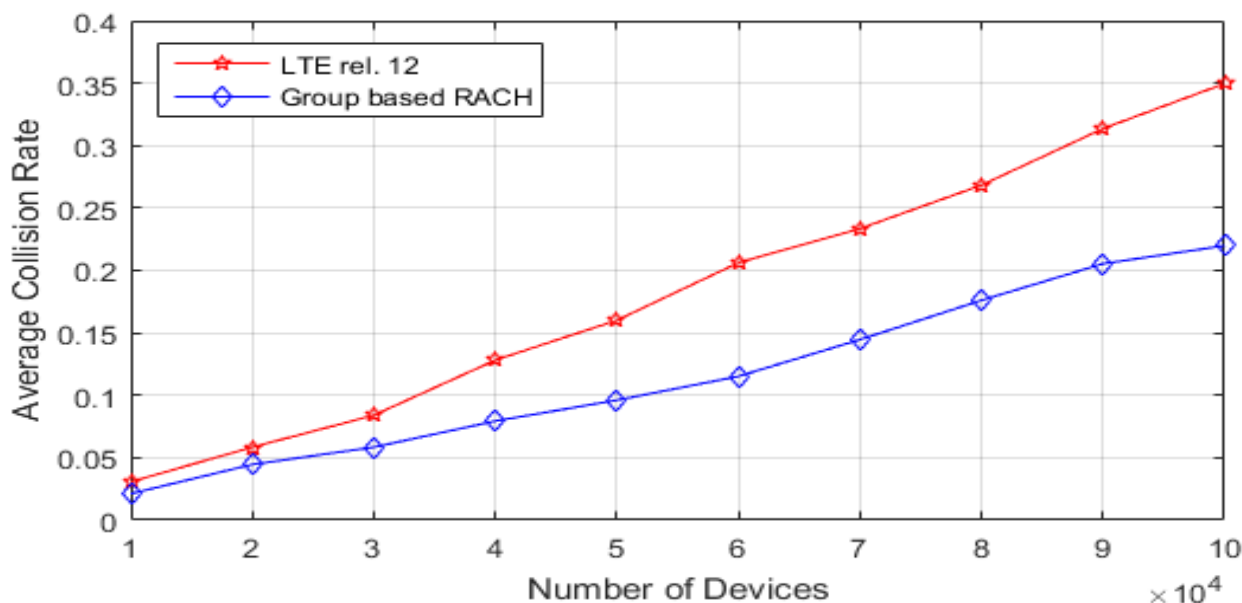
3.9 Διαδικασία αρχικής πρόσβασης του UE – Διαδικασία Εύρεσης Κυψέλης

Τον Σεπτέμβριο του 2018 η 3GPP δημοσίευσε την 15^η έκδοση της τεχνικής προδιαγραφής ETSI 38.211, η οποία περιγράφει τις διαδικασίες του φυσικού επιπέδου του 5G New Radio(NR). Μία από τις απαιτήσεις του 5G NR είναι να μπορεί να παρέχει την δυνατότητα για γρήγορο radioframe synchronization έτσι ώστε να μειωθεί ο χρόνος σύνδεσης του UE προς το δίκτυο του σταθμού βάσης. Για να επιτευχθεί αυτό οι προγραμματιστές θα πρέπει να αυξήσουν την πολυπλοκότητα και να μειώσουν την περιοδικότητα μετάδοσης της σηματοδοσίας συγχρονισμού. Έτσι το NR επιτρέπεται να χρησιμοποιεί από 8 έως 64 μπλοκ συγχρονισμού κατά την διάρκεια ενός radioframe. Ο UE χρησιμοποιώντας οποιοδήποτε μπλοκ ανιχνεύει, συγχρονίζει και μεταδίδει άμεσα ένα access request προς το gNB. Η διαδικασία συγχρονισμού έχει αλλάξει σημαντικά σε σύγκριση με το 4G LTE και πλέον χρησιμοποιείται ολόκληρο το signal block το οποίο αποτελείται από παραπάνω από δύο σήματα σηματοδοσίας. Το Synchronization Signal Block (SSB) αποτελείται από τρία ειδικά σήματα και ένα φυσικό κανάλι. Ένα Synchronization Signal Block καταλαμβάνει 300 υποφέρουσες για κάθε ένα από τα τέσσερα OFDM σύμβολα στο πεδίο του χρόνου. Με άλλα λόγια, 1200 resource elements του resource grid, χρησιμοποιούνται για να μεταφέρουν το ένα μπλοκ συγχρονισμού (σε αντίθεση με τα 288 resource elements του LTE). Το Initial Access αναφέρεται σε ένα σύνολο από Control Plane λειτουργίες που λαμβάνουν χώρα σε πολλαπλά επίπεδα του RAN protocol stack όπως π.χ. το PHY, MAC και RRC και, σε κάποιο βαθμό, το CN / RAN interface όπως στην περίπτωση του paging και του state handling. Στο LTE, μερικές από αυτές τις λειτουργίες είναι το synchronization (στον χρόνο και την συχνότητα, Uplink/Downlink), αναζήτηση κυψέλης, διανομή και απόκτηση των πληροφοριών του συστήματος, random access and paging. Οι λύσεις για το initial access υποστηρίζουν

την διαχείριση τόσο των initial access bottlenecks εξαιτίας των μαζικών αιτήσεων για συνδεσιμότητα καθώς και της διαχείρισης της προτεραιότητας ανά service. Οι προτεινόμενες αρχιτεκτονικές λειτουργίες που προτείνονται είναι:

- **Group based RACH:** Οι συσκευές ομαδοποιούνται από το δίκτυο με βάση την κινητικότητά τους και τα χαρακτηριστικά επικοινωνίας τους (π.χ. δεδομένα προς μετάδοση, απαιτήσεις καθυστέρησης πακέτου) για τη μείωση του ρυθμού σύγκρουσης. Το δίκτυο προγραμματίζει την μετάδοση του κάθε cluster από σταθμούς βάσης σύμφωνα με τις απαιτήσεις μετάδοσής τους.
- **URLLC:** Συλλέγει τα preambles από τις μεταδόσεις συγκεκριμένων UE's για να μπορέσει να δώσει προτεραιότητα σε αιτήματα υπηρεσίας σε περίπτωση σύγκρουσης(collision).
- **5G RAN lean design:** Με κατ' απαίτηση (on-demand) πληροφορίες συστήματος, αποφεύγοντας πάντα τα σύμβολα αναφοράς και μεγαλύτερο χρόνο μεταξύ των σημάτων συγχρονισμού, το νέο 5G σύστημα μπορεί να μειώσει σταθερά την κατανάλωση ενέργειας σε σύγκριση με το LTE.

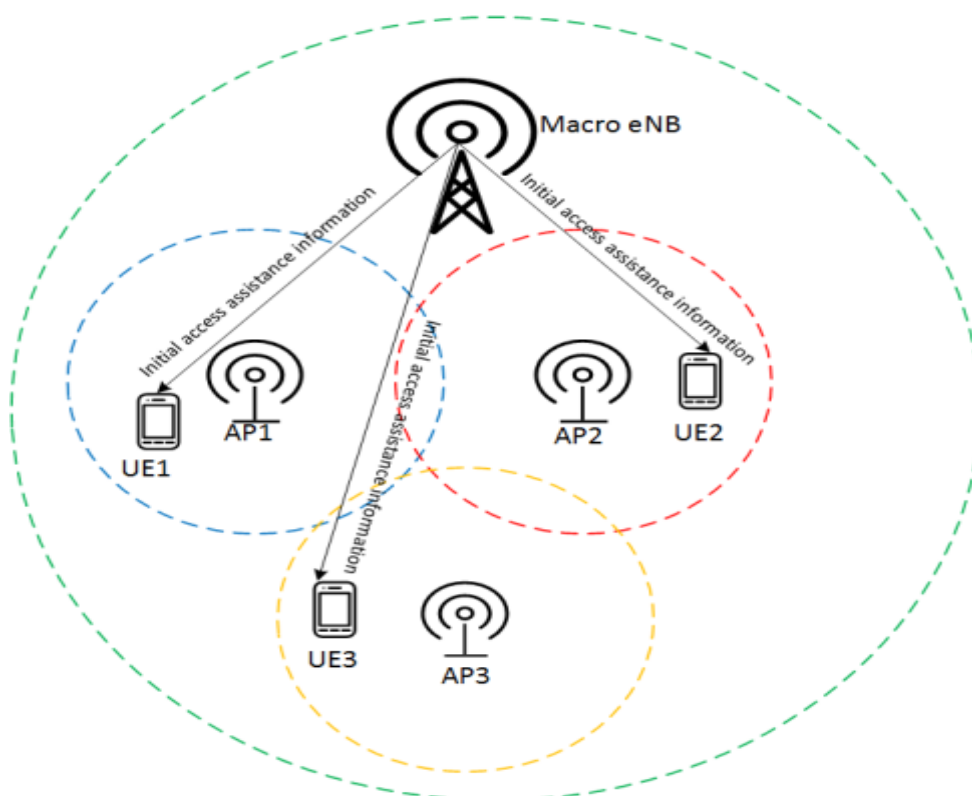
Από τα αποτελέσματα της αξιολόγησης που απεικονίζονται στο παρακάτω σχήμα παρατηρείται ότι η χρήση του group based system access μειώνει σημαντικά τον ρυθμό σύγκρουσης. Επιπλέον, η μέση αρχική καθυστέρηση πρόσβασης μειώνεται, όπως φαίνεται στο παρακάτω σχήμα, καθώς οι συσκευές έχουν πρόσβαση στο σύστημα με λιγότερες συγκρούσεις και συνεπώς αντιμετωπίζουν λιγότερες αναμεταδόσεις.



Εικόνα 49 Group-based αρχικά κέρδη πρόσβασης σε σχέση με τη μέση μείωση του ρυθμού σύγκρουσης

Η αρχική διαδικασία πρόσβασης περιλαμβάνει τις τρεις φάσεις συγχρονισμού του downlink στο πεδίο του χρόνου και του συγχρονισμού συχνότητας, απόκτησης πληροφοριών συστήματος και συγχρονισμού του uplink στο πεδίο του χρόνου. Κατά την αρχική πρόσβαση, ένας UE πρέπει να δημιουργήσει μια σύνδεση RRC με το αντίστοιχο

mmWave Access Point. Η επίδοση αυτής της διαδικασίας επηρεάζει άμεσα την εμπειρία του χρήστη. Επομένως, στο στρώμα PHY πρέπει να επιτευχθεί ευθυγράμμιση της δέσμης μέσα σε σύντομο χρονικό διάστημα. Η αξιοποίηση των περιορισμένων a-priori πληροφοριών σχετικά με την προτιμώμενη διεύθυνση μετάδοσης και στα δύο άκρα του link θα το υποστηρίξει. Σε μία Non-Standalone υλοποίηση, όπως π.χ. σε ένα ετερογενές δίκτυο, όπως αυτό που απεικονίζεται στο παρακάτω σχήμα, όπου τα mmWave small cells βρίσκονται εντός της περιοχής κάλυψης ενός macro cell που λειτουργεί σε χαμηλή συχνότητα, η βοήθεια RAT χαμηλής συχνότητας μπορεί να βελτιώσει την αρχική απόδοση πρόσβασης σημαντικά. Ειδικά η κατανάλωση ισχύος και η καθυστέρηση του UE μπορούν να μειωθούν σημαντικά.



Εικόνα 50 Αρχική πρόσβαση με υποβοηθούμενη συχνότητα σε ετερογενές δίκτυο

Στη συνέχεια, επισημαίνονται οι ενέργειες της βοήθειας που παρέχει η χαμηλής συχνότητας RAT (Radio Access Technology).

3.9.1 Συγχρονισμός κατερχόμενης ζεύξης

Για το downlink synchronization ο UE χρησιμοποιεί τα σήματα συγχρονισμού που εκπέμπονται από τον σταθμό βάσης. Τα σήματα συγχρονισμού εκπέμπονται σε συγκεκριμένες συχνότητες ανά συγκεκριμένα χρονικά διαστήματα, και έχουν ως σκοπό την απόκτηση συμβόλων, slot και sub-frame συγχρονισμού. Μετά την επίτευξη αυτού, ο UE μπορεί να μάθει το cell ID. Εάν ο UE βρίσκεται σε περιοχή κάλυψης RAT χαμηλής συχνότητας, τότε το χαμηλής συχνότητας RAT μπορεί να μεταδώσει πληροφορίες σχετικά με τις συχνότητες και των αναγνωριστικών των mmWave κυψελών που βρίσκονται μέσα στη περιοχή κάλυψης του, στέλνοντας σηματοδοσία μόνο προς τον συγκεκριμένο UE. Λαμβάνοντας την σηματοδοσία αυτή ο UE δεν χρειάζεται να εφαρμόσει

εκτεταμένη αναζήτηση σε ολόκληρο το διάστημα συχνοτήτων που εκπέμπουν οι μικροκυψέλες, αλλά προσπαθεί να ανιχνεύσει μόνο τα σηματοδοτημένα αναγνωριστικά κυψέλης. Ως συνέπεια, η κατανάλωση ενέργειας του UE για την κατερχόμενη ζεύξη συγχρονισμού (downlink synchronization) είναι σημαντικά μειωμένη.

3.9.2 Πληροφορίες συστήματος μετάδοσης

Το δεύτερο μέρος της διαδικασίας της αρχικής πρόσβασης είναι η απόκτηση των πληροφοριών του συστήματος που παρέχουν όλες τις βασικές πληροφορίες για την πρόσβαση του UE στο δίκτυο. Η κάλυψη των πληροφοριών συστήματος καθορίζει την κάλυψη της κυψέλης. Μερικά από τα στοιχεία πληροφοριών του συστήματος, όπως π.χ. ο αριθμός του frame, αλλάζουν γρήγορα με βάση ένα ή περισσότερα mmWave RAT frames. Άλλα στοιχεία πληροφοριών συστήματος αλλάζουν σχετικά αργά, οπότε έτσι πληροφορίες για το εύρος ζώνης του συστήματος, τους διαθέσιμους πόρους για την διαδικασία τυχαίας πρόσβασης, τους διαθέσιμους πόρους για το paging και ο προγραμματισμός διαφόρων άλλων στοιχείων πληροφοριών είναι συνήθως ημι-στατικό. Για τον λόγο αυτό, μπορεί να είναι ενεργειακά αποδοτικό να μεταφερθούν μερικές από τις αργά μεταβαλλόμενες πληροφορίες του συστήματος να εκπέμπονται από την ζώνη χαμηλών συχνοτήτων RAT αξιοποιώντας την υπάρχουσα χαμηλή συχνότητα RAT. Ωστόσο, τα γρήγορα μεταβαλλόμενα στοιχεία πληροφοριών συστήματος πρέπει να μεταδίδονται από την mm-wave RAT.

3.9.3 Συγχρονισμός ανερχόμενης ζεύξης

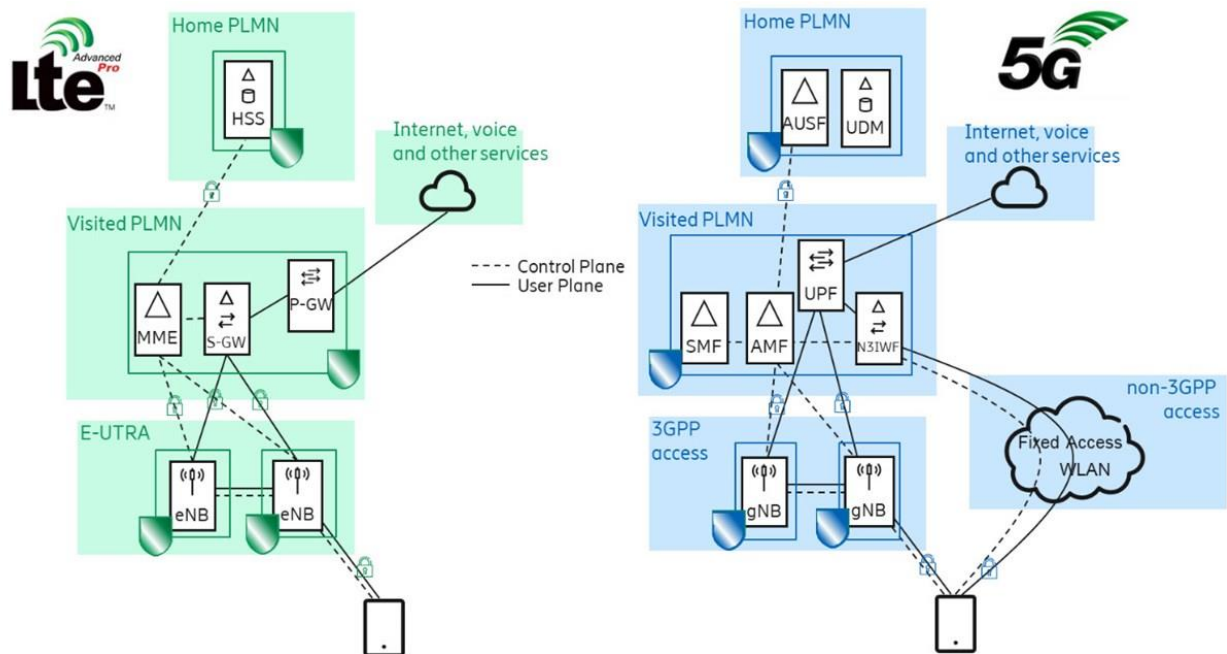
Είναι σημαντικό να υποστηρίζεται η αποτελεσματική μετάδοση δεδομένων στην ανερχόμενη ζεύξη (uplink) στην χαμηλή ζώνη συχνοτήτων mm-wave RAT, ειδικά για “UL data traffic dominant” περιπτώσεις χρήσης, π.χ., ανέβασμα περιεχομένου, όπως βίντεο υψηλής ανάλυσης στα μέσα κοινωνικής δικτύωσης κατά τη διάρκεια αθλητικών εκδηλώσεων, συναυλίες κλπ. Ο συγχρονισμός του Uplink χρειάζεται να επιτευχθεί πριν από οποιαδήποτε μετάδοση πακέτου για να εξασφαλιστεί ότι όλα τα προγραμματισμένα Uplink σήματα των UE είναι ευθυγραμμισμένα με το χρόνο στο eNB. Μπορεί να χρησιμοποιηθεί και η διαδικασία RACH, η οποία είναι παρόμοια με αυτή που έχει τυποποιηθεί για το LTE. Οι ράδιο πόροι για την μετάδοση του preamble είναι συνήθως μέρος των πληροφοριών του συστήματος. Τέτοιου είδους πληροφορίες μπορούν να σηματοδοτηθούν από χαμηλής συχνότητας RAT. Αυτό μπορεί να θεωρηθεί ως μια βασική βοήθεια για τον συγχρονισμό του Uplink. Για να διασφαλιστεί μία συγκεκριμένη κάλυψη για το preamble του UL, εάν υποστηρίζονται από το σύστημα αρκετές preamble μορφές, οι RAT που εκπέμπουν σε χαμηλές ζώνες συχνοτήτων μπορούν να σηματοδοτήσουν μία συγκεκριμένη μορφή preamble προς τον UE έτσι ώστε να υποδείξουν στον UE την μορφή του preamble που υποστηρίζει το δίκτυο. Σε περίπτωση μη συμφωνίας μεταξύ τους, οι χαμηλών συχνοτήτων RAT μπορούν να σηματοδοτήσουν την ακριβή αλληλουχία του preamble που θα χρησιμοποιηθεί από τον UE. Κατά την διάρκεια της διαδικασίας, το RACH σήμα απόκρισης μπορεί να μεταδοθεί και από RAT χαμηλών συχνοτήτων. Εκτός από τις προαναφερθείσες επιλογές για την βοήθεια στον συγχρονισμό του Uplink, οι χαμηλών συχνοτήτων RAT μπορούν επίσης να παρέχουν βοήθεια στις πιθανές λειτουργίες ευθυγράμμισης δέσμης κατά την αρχική διαδικασία συγχρονισμού UL. [18]

3.10 Έλεγχος πρόσβασης σε ένα 5G Network

Η υλοποίηση του 5G θα αποφέρει τεράστια οφέλη απόδοσης και ποικιλία εφαρμογών μέσω της εκτεταμένης χρήσης των πόρων που βασίζονται στο cloud, στην

εικονικοποίηση (virtualization), το network slicing και άλλων αναδυόμενων τεχνολογιών. Με αυτές τις αλλαγές έρχονται νέοι κίνδυνοι ασφαλείας και πρόσθετες «επιφάνειες επίθεσης» που εκτίθενται στην αρχιτεκτονική ασφαλείας 5G. Η διάδοση του IoT και η εξάπλωση των χρηστών δημιουργούν έναν εκθετικά υψηλότερο αριθμό τελικών σημείων πρόσβασης με πολλά από αυτά να μην επιβλέπονται πλέον από ανθρώπινα χέρια. Μεταξύ των βελτιωμένων λειτουργιών ασφαλείας του 5G που περιγράφονται λεπτομερώς από τα πρότυπα 3GPP είναι και ο ενοποιημένος έλεγχος της ταυτότητας του χρήστη για την αποσυσχέτιση του ελέγχου ταυτότητας από τα σημεία πρόσβασης, το extensible authentication protocol για την υποδοχή ασφαλών συναλλαγών, ευέλικτες πολιτικές ασφαλείας για την αντιμετώπιση περισσότερων περιπτώσεων χρήσης και μόνιμων αναγνωριστικών συνδρομητών (SUPI) για τη διασφάλιση της ιδιωτικότητας (privacy) στο δίκτυο. Καθώς η ανάπτυξη του 5G συνεχίζεται και οι κρίσιμοι για την απόδοση κόμβοι γίνονται όλο και πιο εικονικοί (virtualized), οι διαχειριστές θα πρέπει να παρακολουθούν συνεχώς και να αξιολογούν την απόδοση ασφαλείας. Η συμμόρφωση με τις βέλτιστες πρακτικές ασφαλείας σημαίνει συνεχόμενη παρακολούθηση ασφάλειας του δικτύου από άκρο σε άκρο σε όλη την αρχιτεκτονική του συστήματος, τις συσκευές και τις εφαρμογές. Στα 5G δίκτυα, το authentication των end devices θα είναι access agnostic, δεν θα μας ενδιαφέρει δηλαδή από ποια access συσκευή ζητήθηκε η πρόσβαση στο περιεχόμενο αλλά θα μας ενδιαφέρει το ποιο περιεχόμενο/service ζητήθηκε. Οι ίδιες μέθοδοι ταυτοποίησης χρησιμοποιούνται και για 3GPP και μη-3GPP δίκτυα πρόσβασης όπως για παράδειγμα 5G radio access και Wi-Fi access. Όπως φαίνεται και στο παρακάτω σχήμα υπάρχουν πολλές ομοιότητες μεταξύ των LTE/4G και 5G σε ό,τι αφορά τους δικτυακούς κόμβους, όπου στο 5G αναφέρονται ως functions, που εμπλέκονται στα χαρακτηριστικά ασφαλείας, τους συνδέσμους επικοινωνίας ασφαλείας κ.λπ. Και στα δύο συστήματα, οι μηχανισμοί ασφαλείας μπορούν να ομαδοποιηθούν σε δύο ομάδες

- Το πρώτο σετ περιέχει όλους τους λεγόμενους μηχανισμούς ασφάλειας πρόσβασης στο δίκτυο. Αυτά είναι τα χαρακτηριστικά ασφαλείας που παρέχουν στους χρήστες ασφαλή πρόσβαση στις υπηρεσίες μέσω της συσκευής (συνήθως ένα τηλέφωνο) και προστατεύουν από επιθέσεις στην διεπαφή αέρα (radio interface) μεταξύ της συσκευής και του ασύρματου κόμβου (eNB σε LTE και gNB σε 5G)
- Το δεύτερο σετ περιέχει τους επανομαζόμενους μηχανισμούς ασφάλειας τομέα του δικτύου (network domain security mechanisms). Αυτό περιλαμβάνει τις λειτουργίες που επιτρέπουν στους κόμβους να ανταλλάσσουν ασφαλή δεδομένα σηματοδότησης και δεδομένα χρήστη, για παράδειγμα, μεταξύ των ράδιο κόμβων και των κόμβων του κεντρικού δικτύου



Εικόνα 51 4G vs 5G Ροή κυκλοφορίας Αρχιτεκτονικής Ασφάλειας

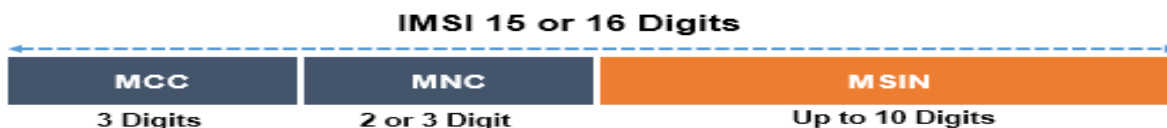
Η παραπάνω εικόνα απεικονίζει απλοποιημένες αρχιτεκτονικές ασφαλείας των LTE και 5G NR που δείχνουν την ομαδοποίηση των οντοτήτων του δικτύου που πρέπει να εξασφαλιστούν στο Home Network και στο Visited Network καθώς και όλους τους συνδέσμους επικοινωνίας που πρέπει να προστατευθούν.

Το 5G εισάγει την έννοια του anchor key με την εισαγωγή της λειτουργίας του Security Anchor Function (SEAF). Το SEAF επιτρέπει το re-authentication της συσκευής καθώς αυτή μετακινείται σε διαφορετικά access networks ή ακόμα και serving networks χωρίς να χρειάζεται να ξανατρέξει από την αρχή όλη την διαδικασία του authentication. Αυτό έχει ως αποτέλεσμα την μείωση της σηματοδότησης στον HSS server κατά την διαδικασία του mobility. Το SEAF και το AMF μπορούν να βρίσκονται μαζί αλλά και το κάθε ένα μόνο του. Στο 3GPP Release 15 το SEAF και το AMF βρίσκονται μαζί. Στο 5G αποδίδεται ένας μοναδικός Subscriber Permanent Identifier (SUPI) σε κάθε χρήστη-συνδρομητή. Το SUPI δεν αποκαλύπτεται ποτέ στον αέρα όταν ο φορητός υπολογιστής δημιουργεί μια σύνδεση. Αυτό είναι διαφορετικό από τα 3G και 4G δίκτυα όπου το IMSI αποκαλύπτεται κατά την μετάδοση στο αέρα κατά την διαδικασία της αρχικής σύνδεσης στο δίκτυο προτού ακόμα προλάβει η συσκευή να γίνει authenticate από το δίκτυο. Αντί του να αποκαλύπτεται το SUPI χρησιμοποιείται το Subscription Concealed Identifier (SUCI) μέχρι να γίνουν authenticated η συσκευή και το δίκτυο. Μόνο όταν ολοκληρωθεί το authentication αποκαλύπτεται ο Subscriber Permanent Identifier (SUPI). Η διαδικασία αυτή ακολουθείται για την αποτροπή των IMSI catchers, γνωστοί κι ως false base stations, από το να μπορέσουν να υποκλέψουν την ταυτότητα του χρήστη 'αναγκάζοντας' την κινητή συσκευή να συνδεθεί στον rogue base station ή να με το να 'αναγκάσει' την κινητή συσκευή να ξεκινήσει την διαδικασία του attachment με τον σταθμό βάσης και να μπορέσει να υποκλέψει όλη την μη-κρυπτογραφημένη κίνηση που ανταλλάσσουν.

3.10.1 Subscription Permanent Identifier (SUPI)

Το Subscription Permanent Identifier (SUPI) είναι ένας 5G παγκόσμια μοναδικός αριθμός ο οποίος αποδίδεται σε κάθε συνδρομητή και ο οποίος έχει οριστεί στο specification TS 23.501 της 3GPP. Το SUPI ID δημιουργείται στη USIM και σε συνεργασία με το UDM/UDR του 5G Core. Το SUPI είναι συνήθως μια σειρά 15 δεκαδικών ψηφίων. Τα

πρώτα τρία ψηφία αντιπροσωπεύουν τον Mobile Country Code (MCC) ενώ τα επόμενα δύο ή τρία σχηματίζουν τον Mobile Network Code (MNC) προσδιορίζοντας έτσι τον πάροχο του δικτύου κινητής επικοινωνίας. Τα υπόλοιπα εννέα ή δέκα ψηφία που απομένουν είναι γνωστά ως Mobile Subscriber Identification Number (MSIN) και αντιπροσωπεύουν τον κάθε χρήστη ξεχωριστά. Το SUPI ID είναι ισοδύναμο με το IMSI το οποίο προσδιορίζει με μοναδικό τρόπο το ME, και είναι επίσης μία σειρά από 15 ψηφία.



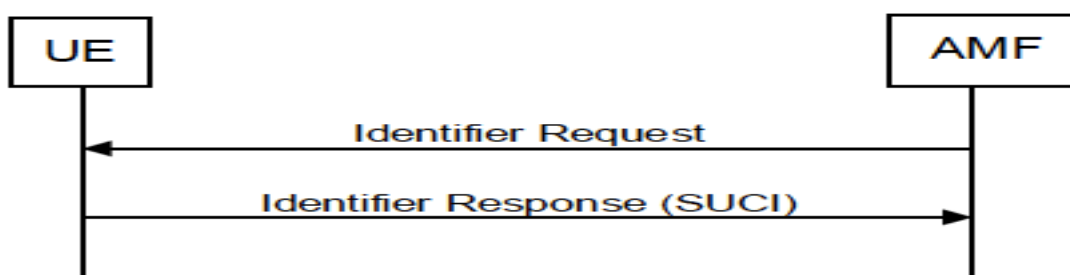
Εικόνα 52 SUPI Frame

3.10.2 Subscription Concealed Identifier (SUCI)

Το Subscription Concealed Identifier (SUCI) είναι ένα αναγνωριστικό διατήρησης της ιδιωτικότητας του συνδρομητή και το οποίο περιέχει το κρυπτογραφημένο το SUPI. Ο UE παράγει το SUCI χρησιμοποιώντας ένα σχήμα που βασίζεται στο ECIES, χρησιμοποιώντας το δημόσιο κλειδί του Home Network το οποίο δημιουργήθηκε με ασφάλεια στην USIM κατά την διαδικασία εγγραφής της USIM στο δίκτυο. Μόνο το MSIN μέρος του SUPI ID προστατεύεται από το πλαίσιο ασφαλείας ενώ το home network identifier όπως π.χ το MCC/MNC μεταδίδεται σαν απλό κείμενο. Παρακάτω φαίνονται τα πεδία δεδομένων που αποτελούν το SUCI.

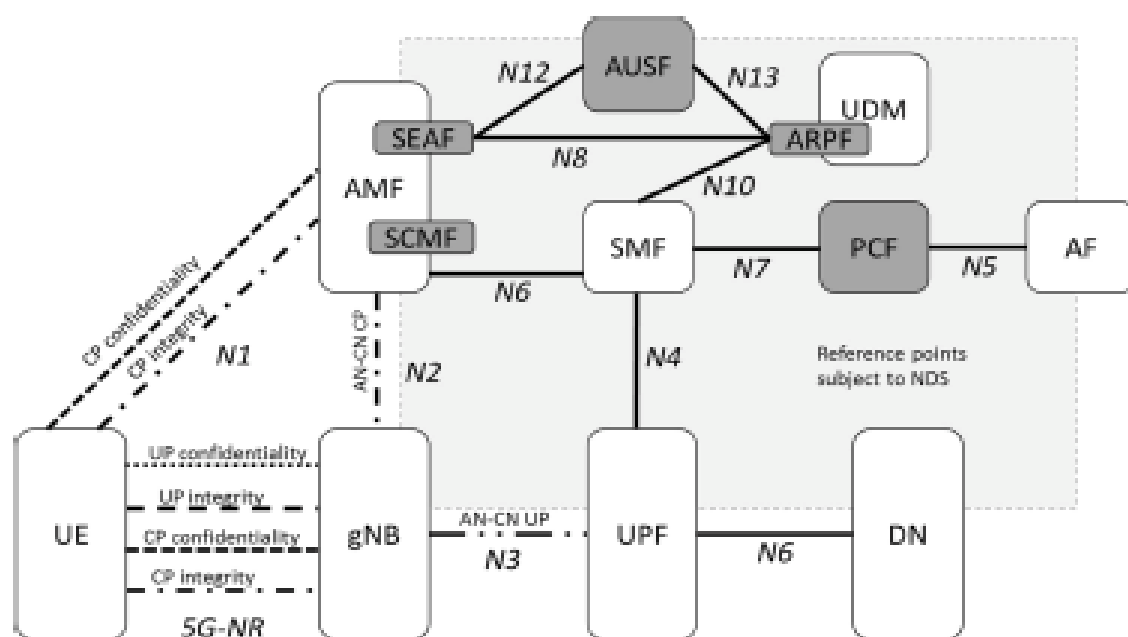


Εικόνα 53 SUCI Frame



Εικόνα 54 Subscriber Identification Mechanism

Το νέο σύστημα 5G έχει σχεδιαστεί για να μπορεί να υποστηρίξει διαφορετικές υπηρεσίες όπως Mission Critical Communications (MCC), Internet of Things (IoT), Αυτοκινητοβιομηχανία, κλπ. Η παρακάτω εικόνα απεικονίζει το Αρχιτεκτονικό διάγραμμα ασφαλείας του 5G όπου φαίνονται όλες οι νέες οντότητες που σχετίζονται με την ασφάλεια του δικτύου και οι οποίες είναι Security Anchor Function (SEAF), Authentication Server Function (AUSF), Authentication Credential Repository and Processing Function (ARPF), Security Context Management Function (SCMF) και Security Policy Control Function ((S)PCF). [20]



Εικόνα 55 Αρχιτεκτονική ασφαλείας 5G και Απεικόνιση Διεπαφών

Όλες οι λειτουργίες δικτύου στο σύστημα είναι ασφαλισμένες με την χρήση του Network Domain Security, η οποία βασίζεται στην διαμόρφωση των πολιτικών ασφαλείας του κάθε χρήστη.

3.10.3 Σημείο τερματισμού του επιπέδου του χρήστη (User Plane)

Ο τερματισμός του user plane security στο 4G γίνεται στο eNB. Ωστόσο, η τοποθεσία του gateway μπορεί να διαφέρει αναλόγως το είδος της υπηρεσίας.

Ο σχεδιασμός του 3GPP αυτή την στιγμή υποδεικνύει ότι το User plane security τερματίζει στο Packet Data Convergence Protocol (PDCP) επίπεδο του gNB. Αυτό συμβαδίζει με την ασφάλεια του LTE, δηλαδή η ασφάλεια της ραδιο επαφής παρέχεται από το PDCP επίπεδο και για το control και για το user plane. Η λύση αυτή επιτρέπει την τοποθέτηση του σημείου τερματισμού ασφαλείας σε μία κεντρική μονάδα του gNB. [20]

3.10.4 Έλεγχος ταυτότητας και εξουσιοδότηση

Ευέλικτες μέθοδοι ελέγχου ταυτότητας για τις συσκευές θα απαιτούνται για το 5G, καθώς θα υπάρχουν περισσότερες περιπτώσεις χρήσης, συμπεριλαμβανομένου του IoT, ιδιωτικά δίκτυα εργοστασίων και καθώς και διαφορετικές τεχνολογίες πρόσβασης. Το 3GPP SA3 έχει ορίσει έναν κύριο και υποχρεωτικό μηχανισμό για ταυτοποίηση του

χρήστη και έναν δεύτερο μη-υποχρεωτικό μηχανισμό ταυτοποίησης. Ο δεύτερος μηχανισμός ταυτοποίησης ενεργοποιείται μόνο όταν γίνει με επιτυχία η πρώτη και υποχρεωτική ταυτοποίηση του χρήστη. Η πρώτη ταυτοποίηση του χρήστη του δίνει πρόσβαση στο 5G δίκτυο. Η δεύτερη ταυτοποίηση βασίζεται στο Protocol Configuration Options (PCO) όπου ο χρήστης δίνει τα PAP/CHAP διαπιστευτήρια χρήστη. Και οι δύο μέθοδοι ταυτοποίησης του χρήστη υποστηρίζουν EAP. Με τον τρόπο αυτό, η ταυτοποίηση του χρήστη στο 5G μπορεί να διαφέρει αναλόγως την υπηρεσία που θέλει να χρησιμοποιήσει.

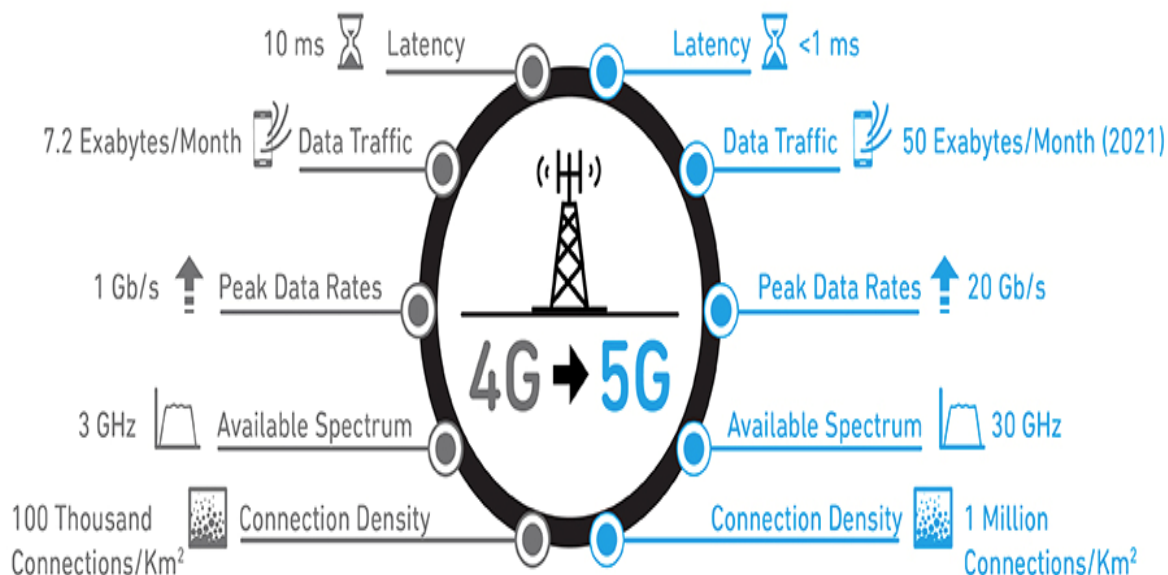
Ακόμα μία αλλαγή που θα γίνει στο πλαίσιο της ασφάλειας για το 5G είναι η διασφάλιση της ιδιωτικότητας του International Mobile Subscriber Identity (IMSI) το οποίο στέλνεται σαν απλό κείμενο κατά της διαδικασία της αρχικής σύνδεσης του χρήστη στο LTE δίκτυο. Η προστασία του 5G IMSI, το οποίο είναι γνωστό και ως SUPI- Subscriber Permanent Identifier) κατά την μετάδοσή του θα επιτυγχάνεται με Public Key Encryption Infrastructure (PKI). [20]

3.10.5 5G SIM

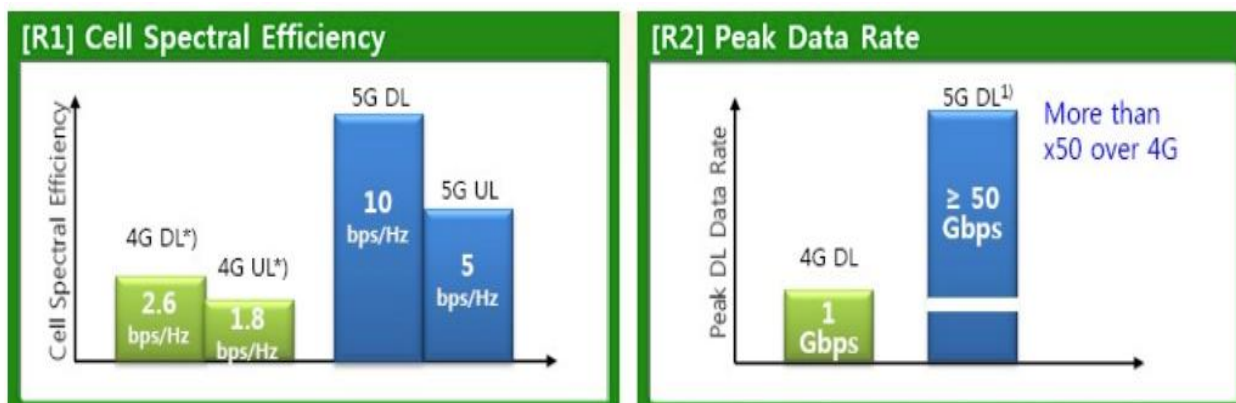
Μια κάρτα SIM 5G είναι ένα ασφαλές στοιχείο, το οποίο είναι το μόνο που επιτρέπει τη διασφάλιση της ασφαλούς πρόσβασης στο δίκτυο 5G. Έχει καθοριστεί από τον οργανισμό τυποποίησης 5G ETSI-3GPP στις προδιαγραφές UICC Release 15 (UICC: Universal Integrated Circuit Card, γνωστό ως SIM). Στόχος της είναι η άμεση αντιμετώπιση των βασικών χαρακτηριστικών του 5G: Βελτιωμένη ευρυζωνική τεχνολογία κινητής τηλεφωνίας, μαζικό IoT, κρίσιμες επικοινωνίες. Το 5G θα είναι διαθέσιμο παγκοσμίως σε 1,9 δισ. συνδρομητές έως το 2024 (δηλ. Το 20% όλων των συνδρομών κινητής τηλεφωνίας), καθιστώντας την ταχύτερη γενιά που θα κυκλοφορήσει ποτέ σε παγκόσμια κλίμακα.

3.11 Σύγκριση 4G και 5G

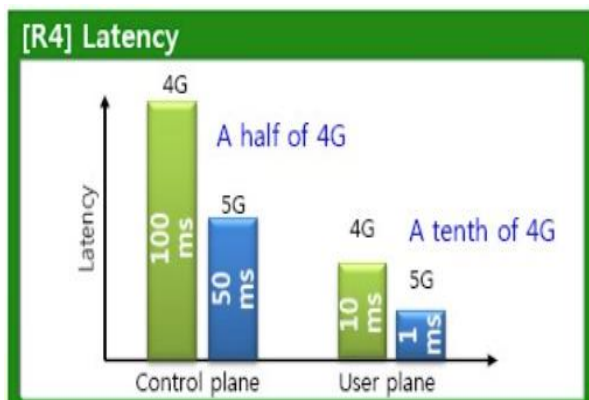
Παρακάτω απεικονίζεται η διαφορά στο κομμάτι του Radio Access μεταξύ 4G και 5G:



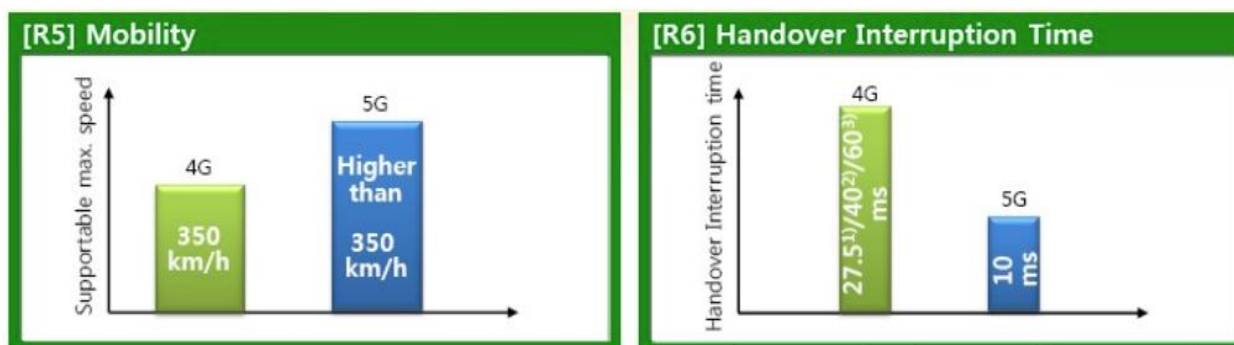
Εικόνα 56 Σύγκριση Δυνατοτήτων 4G και 5G



Εικόνα 57 Σύγκριση Δυνατοτήτων Αποδοτικότητας και Μέγιστου Ρυθμού Μετάδοσης μεταξύ 4G και 5G



Εικόνα 58 Σύγκριση Χρόνου Καθυστερήσης μεταξύ 4G και 5G



Εικόνα 59 Σύγκριση Κινητικότητας και Αλλαγής Κυψέλης μεταξύ 4G και 5G

	LTE	NR
Frequency of Operation	Μέχρι 6 GHz	Μέχρι 6 GHz, ~28 GHz, ~39 GHz, υπόλοιπες mmWave συχνότητες μέχρι 52GHz
Carrier Bandwidth	Μέχρι 20 MHz	Μέχρι 100 MHz (at <6 GHz) Μέχρι 1 GHz (at >6 GHz)
Carrier Aggregation	Μέχρι 32	Μέχρι 16
Analog Beamforming(dynamic)	Δεν υποστηρίζεται	Υποστηρίζεται
Digital Beamforming	Μέχρι 8 επίπεδα	Μέχρι 12 επίπεδα
Channel Coding	Data: Turbo Coding Control: Convolutional Coding	Data: LDPC Coding Control: Polar coding
Subcarrier Spacing	15 kHz	15 kHz, 30 kHz, 60 kHz, 120 kHz, 240 kHz
Self-Contained Subframe	Δεν υποστηρίζεται	Υποστηρίζεται
Spectrum Occurance	90% του Channel BW	Έως 98% του Channel BW

Πίνακας 2 Σύγκριση Τεχνικών Προδιαγραφών μεταξύ LTE και NR

Στον παρακάτω πίνακα απεικονίζεται η αντιστοιχία των ονομασιών του παλιού 4G και του νέου 5G συστήματος.

Marketing Name	ITU Name	3GPP Name	RAN Name	Core Name	System Name
4G	IMT- Advanced	LTE- Advanced	E-UTRAN	Evolved Packet Core (EPC)	Evolved Packet System (EPS)
5G	IMT- 2020	5G	New Radio (NR)	5G Core(5GC)	5G System(5GS)

Πίνακας 3 Αντιστοίχιση Ονοματοδοσίας Στοιχείων μεταξύ 4G και 5G

3.12 Περίληψη

Με την συνδεσιμότητα να βρίσκεται στο επίκεντρο του μετασχηματισμού της βιομηχανίας, τα συστήματα 5G μπορούν να διαδραματίσουν σημαντικό ρόλο - όχι μόνο στην εξέλιξη της επικοινωνίας, αλλά και στην εξέλιξη των επιχειρήσεων και της κοινωνίας στο σύνολό της. Το 5G θα αναπτύξει και θα επεκτείνει το δημόσιο ασύρματο δίκτυο, καθιστώντας το βιώσιμο για κάθε τύπο εφαρμογών. Κατά συνέπεια, το 5G θα είναι ο σημαντικότερος παράγοντας του διαδικτύου των πραγμάτων και της δικτυωμένης κοινωνίας. Ο μετασχηματισμός 5G έχει ήδη ξεκινήσει με NB-IoT, NFV και αυτοματισμό διαχείρισης, για παράδειγμα. Είναι μια σταδιακή διαδικασία, που βελτιώνει το τρέχον δίκτυο βήμα προς βήμα. Καθώς εξελίσσεται η διαδικασία, οι παγκόσμιες εταιρικές σχέσεις θα αποδειχθούν ουσιαστικές για να καταστεί δυνατή μια διεπαγγελματική δέσμευση στον καθορισμό και την οικοδόμηση του συστήματος 5G.

4. ΕΙΚΟΝΙΚΟΠΟΙΗΣΗ ΔΙΚΤΥΟΥ ΚΑΙ ΔΗΜΙΟΥΡΓΙΑ ΟΤΤ ΥΠΗΡΕΣΙΑΣ

Αρχικά, στην ενότητα αυτή αντικείμενο εξέτασης αποτελεί το Virtual Access Point (VAP) και ο τρόπος δημιουργίας του μέσω ενός Ασύρματου Κεντρικού Controller σε ένα παραγωγικό δίκτυο. Έπειτα θα εξεταστεί το πλήθος των VAP που μπορεί να δημιουργηθεί σε έναν Ασύρματο Controller. Τέλος, θα παρουσιαστεί η λύση ενός over the top service, που θα παρέχεται μέσω του Virtual Access Point, το οποίο μετά την ταυτοποίηση του χρήστη, μέσω ενός Social κοινωνικού δικτύου, π.χ. Facebook, LinkedIn, θα του επιτρέψει την σύνδεσή του στο διαδίκτυο.

4.1 Virtual Access Points

Η τεχνολογία του Virtual Access Point (VAP) είναι επωφελής γιατί ο διαχειριστής έχει την δυνατότητα να χωρίσει σε μικρότερα τμήματα ένα ασύρματο broadcast domain. Ένα Virtual Access Point προσομοιώνει πολλαπλά access points μέσω ενός φυσικού access point. Το επίπεδο ασφαλείας ενός Virtual Access Point μπορεί να διαμορφωθεί με τέτοιο τρόπο έτσι ώστε να μπορεί να γίνει έλεγχος της πρόσβασης πολλαπλών χρηστών. Αυτό παρέχει καλύτερο έλεγχο στην broadcast και multicast κίνηση που επηρεάζει την επίδοση του δικτύου. Κάθε Virtual Access Point μπορεί να διαμορφωθεί για να έχει πρόσβαση σε ξεχωριστά λογικά εικονικά δίκτυα (Vlans). Το SSID είναι μια συμβολοσειρά ASCII που χρησιμοποιούν οι συσκευές ασύρματης δικτύωσης για τη δημιουργία και τη συντήρηση της ασύρματης σύνδεσης. Τα πολλαπλά σημεία πρόσβασης σε ένα δίκτυο ή ένα υποσύστημα μπορούν να χρησιμοποιούν τα ίδια SSID. Συνήθως σε μία πραγματική ασύρματη τοπολογία, κάθε SSID αντιστοιχεί και σε ένα ξεχωριστό Vlan. Αυτό σημαίνει ότι τα διαφορετικά SSID τα οποία μοιράζονται την ίδια τοπολογία, τους ίδιους δικτυακούς controllers, τα ίδια φυσικά μονοπάτια (links), είναι εντελώς ανεξάρτητα μεταξύ τους κάτι που σημαίνει ότι οι χρήστες του ενός SSID δεν μπορούν να επικοινωνήσουν με τους χρήστες ενός άλλου SSID χωρίς την παρουσία ενός δρομολογητή. Το access point προσθέτει μία Vlan ID ετικέτα στην ασύρματη κίνηση βάση της IP διεύθυνσης που έχει διαμορφωθεί στο εικονικό δίκτυο (Vlan).

Τέλος, μπορεί να υλοποιηθεί Quality of Service (QoS) σε διαφορετικά SSIDs με βάση την υπηρεσία ή την εφαρμογή που εξυπηρετούν. Μία πτυχή της ασύρματης δικτύωσης που συχνά παραβλέπεται είναι ότι οι διαχειριστές δικτύου μπορούν να ελέγχουν τις παρεμβολές και τη χρήση καναλιών που δημιουργούνται από το δικό τους διαχειριζόμενο ασύρματο σύστημα. Ο πίνακας ελέγχου επιτρέπει στους διαχειριστές τη δυνατότητα ενεργοποίησης πολλαπλών SSID σε ένα φυσικό AP (Σημείο πρόσβασης). Κάθε SSID

που είναι ενεργοποιημένο σε ένα συγκεκριμένο AP ονομάζεται VAP (Virtual AP). Τα VAP συμπεριφέρονται ως το δικό τους ανεξάρτητο AP, λειτουργώντας στα κανάλια στα οποία έχει ρυθμιστεί το φυσικό AP. Επομένως, η ενεργοποίηση πέντε SSID σε ένα μεμονωμένο AP στον Πίνακα ελέγχου είναι σχεδόν ίδια με την ανάπτυξη πέντε φυσικών AP με ένα SSID το καθένα. Κανονικά, πολλαπλά SSID χρησιμοποιούνται για την παροχή διαφορετικών τύπων ασύρματης πρόσβασης δικτύου σε διαφορετικούς τύπους συσκευών και κατηγορίες χρηστών. Το μειονέκτημα της ενεργοποίησης περισσότερων SSID είναι ότι δημιουργεί περισσότερη χρήση καναλιών λόγω των γενικών εξόδων (more channel utilization due to overhead).

4.2 Πλήθος SSID που μπορεί να εκπέμπει ένα access point

Η απάντηση στην ερώτηση, πόσα VAP μπορεί να εκπέμπει ένα access point, είναι ότι εξαρτάται από τον κατασκευαστή και τον εξοπλισμό που αγοράζει ο διαχειριστής. Ο αριθμός των υποστηριζόμενων SSID ποικίλλει από 8 – 64.

Οι συνέπειες της χρήσης πολλών SSID είναι η μεγαλύτερη χρήση του διαθέσιμου καναλιού. Κάθε SSID που ενεργοποιείται σε ένα Access Point ονομάζεται Virtual Access Point (VAP). Κάθε VAP λειτουργεί ως ένα ανεξάρτητο Access Point και εκπέμπει στην συχνότητα στην οποία έχει ρυθμιστεί. Οπότε, ενεργοποιώντας πέντε VAP σε ένα Access Point είναι σαν να τοποθετούνται πέντε access point στο ίδιο σημείο τα οποία θα εκπέμπουν και από ένα SSID.

4.2.1 Σελίδα RF φάσματος σε Cisco Meraki ασύρματο controller

Τα Cisco Meraki AP που χρησιμοποιούν το ειδικό ράδιο ανάλυσης Φάσματος έχουν μια λίστα παρεμβολών AP στο Dashboard. Αυτή η λίστα βρίσκεται στη σελίδα λεπτομερειών του AP στην περιοχή Monitor → RF. Η λίστα εμφανίζει το BSSID (APs Wireless MAC), το επίπεδο ισχύος, το κανάλι και το όνομα SSID των AP που λειτουργούν εντός εμβέλειας. Αυτές οι πληροφορίες παρέχουν τη δυνατότητα εντοπισμού πιθανών πηγών συμφόρησης ή παρεμβολών.

Utilization Interfering APs

Channel: all channels ▼

BSSID	SSID ▲	dBm	Channel	Mode	On LAN
		██████████ -80	11	802.11g (open)	not seen
		██████████ -51	11	802.11n (WPA2)	00:18:0a:91:92:90
		██████████ -60	6	802.11n (WPA2)	00:18:0a:7a:c0:30
		██████████ -69	11	802.11n (WPA2)	00:18:0a:7a:d0:f0
		██████████ -77	1	802.11n (802.1x)	not seen
		██████████ -81	11	802.11n (802.1x)	00:18:0a:79:a4:60
		██████████ -74	1	802.11n (802.1x)	not seen
		██████████ -78	6	802.11n (WPA2)	00:18:0a:79:4e:70
		██████████ -68	1	802.11n (WPA2)	00:18:0a:91:92:a0
		██████████ -41	11	802.11n (WPA2)	00:18:0a:91:92:90
		██████████ -77	6	802.11n (open)	00:18:0a:79:4e:70
		██████████ -75	1	802.11n (802.1x)	not seen
		██████████ -79	6	802.11n (802.1x)	00:18:0a:79:12:70
		██████████ -77	1	802.11n (802.1x)	not seen
		██████████ -76	11	802.11n (WPA2)	00:18:0a:79:28:70

Εικόνα 60 Σελίδα Απεικόνισης Παρεμβολών στον Wireless Controller Cisco Meraki, Source: Channel Planning Best Practices, Cisco Meraki

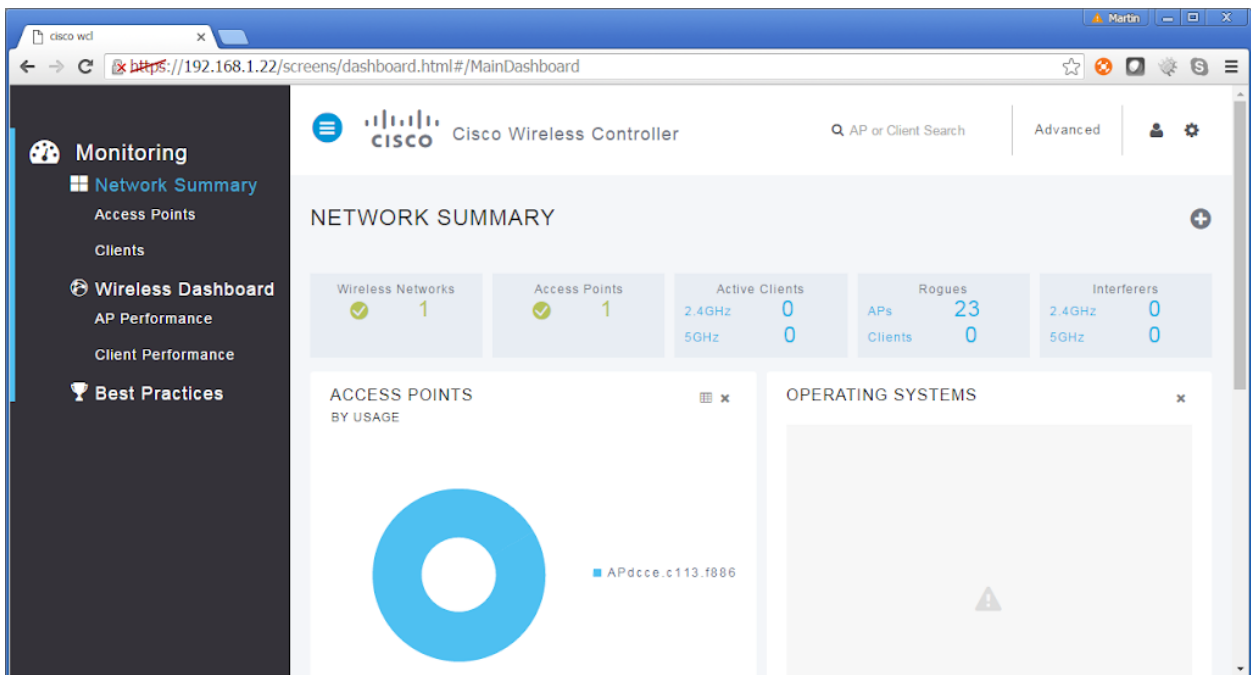
Στην παραπάνω εικόνα απεικονίζεται η σελίδα του Wireless Cisco Cloud Controller. Στην αριστερή στήλη βρίσκονται όλα τα Virtual Access Points – SSID που είναι διαμορφωμένα στον Controller ενώ επίσης φαίνεται το κανάλι στο οποίο εκπέμπει το κάθε VAP καθώς και το IEEE πρότυπο που είναι διαμορφωμένο σε κάθε ένα από αυτά. Επίσης υπάρχει και η στήλη με την ονομασία dBm και η οποία δείχνει την ισχύ εκπομπής του κάθε VAP. Η επιλογή αυτή μπορεί να οριστεί είτε χειροκίνητα από τον διαχειριστή του δικτύου είτε αυτόματα από τον Controller και σύμφωνα με τις παρεμβολές που δέχεται το κάθε VAP από γειτονικά του.

4.3 Εικονικοποίηση δικτύου σε Cisco WLAN Management Controller

Η παρακάτω διαδικασία έχει πραγματοποιηθεί σε Cisco 5520 WLC Controller.

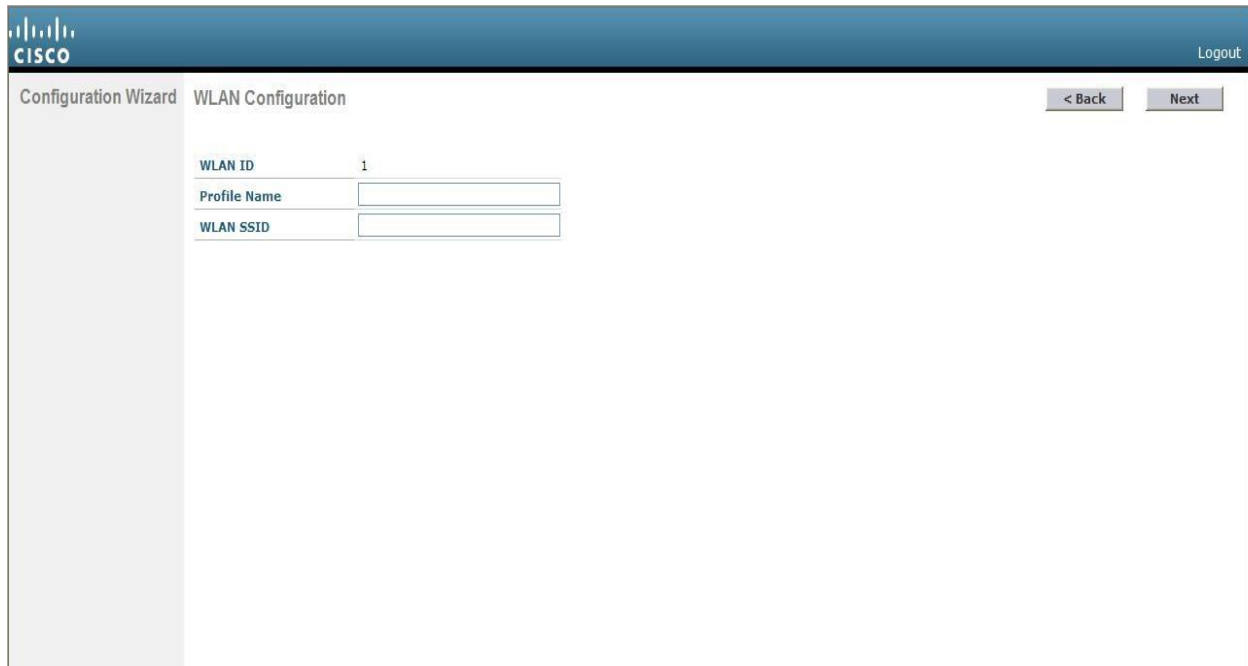


Για να εκκινήσει η διαδικασία δημιουργίας ενός virtual access point, ο διαχειριστής πρέπει πρώτα να εισέλθει στην Web σελίδα Διαχείρισης του Ασύρματου Controller. Αυτό γίνεται εισάγοντας στον browser τον σύνδεσμο <http://192.168.1.122>. Έπειτα, ξεκινάει την διαδικασία δημιουργίας του VAP, ακολουθώντας τα παρακάτω βήματα:



Σελίδα Διαμόρφωσης WLAN

WLAN → Create New



The screenshot displays the Cisco Configuration Wizard interface for WLAN configuration. The top header includes the Cisco logo and a 'Logout' link. The main content area is titled 'WLAN Configuration' and contains the following fields:

WLAN ID	1
Profile Name	<input type="text"/>
WLAN SSID	<input type="text"/>

Navigation buttons for '< Back' and 'Next' are located in the top right corner of the configuration area.

Εικόνα 61 Διαμόρφωση SSID (1)

- ⇒ Στο πεδίο Profile Name , είναι δυνατή η καταχώρηση έως και 32 αλφαριθμητικών χαρακτήρων για το όνομα που θα αντιστοιχιστεί σε αυτό το δίκτυο WLAN.
- ⇒ Στο πεδίο WLAN SSID , είναι δυνατή η καταχώρηση έως και 32 αλφαριθμητικών χαρακτήρων για το όνομα του δικτύου, ή του service set identifier (SSID). Το SSID ενεργοποιεί την βασική λειτουργία του controller και επιτρέπει στα access points τα οποία έχουν συνδεθεί με τον controller να ενεργοποιήσουν τα ραδιοκανάλια τους.
- ⇒ Για να προχωρήσει η διαδικασία, επιλέγεται το “Next”

Διαμόρφωση του RADIUS Server

Configuration Wizard RADIUS Server Configuration

< Back Apply Skip

Server IPv4 Address

Shared Secret Format ASCII ▾

Shared Secret

Confirm Shared Secret

Port Number 1812

Server Status Disabled ▾

Server IPv6 Address

Shared Secret Format ASCII ▾

Shared Secret

Confirm Shared Secret

Port Number 1812

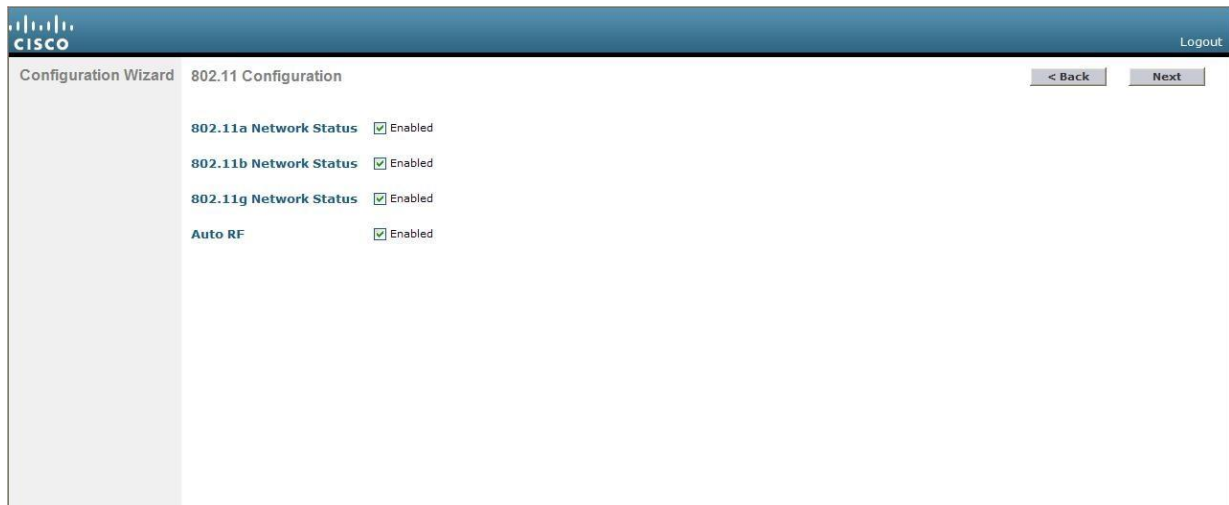
Server Status Disabled ▾

352938

Εικόνα 62 Διαμόρφωση SSID (2)

- ⇒ Στο πεδίο Server IP Address, εισάγεται η IP διεύθυνση του RADIUS server.
- ⇒ Στα πεδία Shared Secret και Confirm Shared Secret , εισάγεται το μυστικό κλειδί που θα χρησιμοποιείται από τον RADIUS server.
- ⇒ Στα πεδία Shared Secret και Confirm Shared Secret , εισάγεται το μυστικό κλειδί που χρησιμοποιεί ο RADIUS server.
- ⇒ Στο πεδίο Port Number , εισάγεται η πόρτα επικοινωνίας του RADIUS server. Η προεπιλεγμένη τιμή είναι 1812.
- ⇒ Για την ενεργοποίηση του RADIUS server, επιλέγεται “Enabled” από το πεδίο Server Status. Για την απενεργοποίηση του RADIUS server, παραμένει το πεδίο αυτό στην επιλογή Disabled.
- ⇒ Για να προχωρήσει η διαδικασία, επιλέγεται το “Apply”.

Διαμόρφωση του 802.11



Εικόνα 63 Διαμόρφωση SSID (3)

- ⇒ Για να ενεργοποιηθούν τα 802.11a, 802.11b, and 802.11g access point δίκτυα, επιλέγονται τα 802.11a Network Status, 802.11b Network Status, και 802.11g Network Status. Για να απενεργοποιηθούν αυτά τα δίκτυα αφαιρείται το σύμβολο από το κουτί επιλογής.
- ⇒ Για να ενεργοποιηθεί η δυνατότητα του controller να διαχειρίζεται τις ράδιο-συχνότητες (radio resource management (RRM)), το auto-RF feature, πρέπει να παραμείνει επιλεγμένο.
Σημείωση: Το χαρακτηριστικό auto-RF επιτρέπει στον controller να δημιουργεί αυτόματα ένα RF group με τους υπόλοιπους controllers. Το group αυτό δυναμικά εκλέγει έναν «αρχηγό» ο οποίος είναι υπεύθυνος για την βελτιστοποίηση των ρυθμίσεων των RRM παραμέτρων όπως είναι η επιλογή του καναλιού εκπομπής και η μετάδοση ισχύος μετάδοσης για ολόκληρο το group.
- ⇒ Για να προχωρήσει η διαδικασία, επιλέγεται το “Next”.

Ρύθμιση Ώρας

Configuration Wizard Set Time

< Back Next

Current Time Sun May 17 23:37:33 2009

Date

Month May

Day 17

Year 2009

Time

Hour 23

Minutes 37

Seconds 33

Timezone

Delta hours 0 mins 0

252073

Εικόνα 64 Διαμόρφωση SSID (4)

- ⇒ Ρυθμίζεται η ώρα.
- ⇒ Για να προχωρήσει η διαδικασία, επιλέγεται το “Next”.

Ολοκλήρωση Διαμόρφωσης νέου SSID

Configuration Wizard Configuration Wizard Completed

< Back Save And Reboot

The configuration wizard is now complete. It is now necessary to save and reboot the system for the changes to take effect.

252074

Εικόνα 65 Διαμόρφωση SSID (5)

- ⇒ Για να ολοκληρωθεί η διαδικασία, επιλέγεται το “Save and Reboot”.

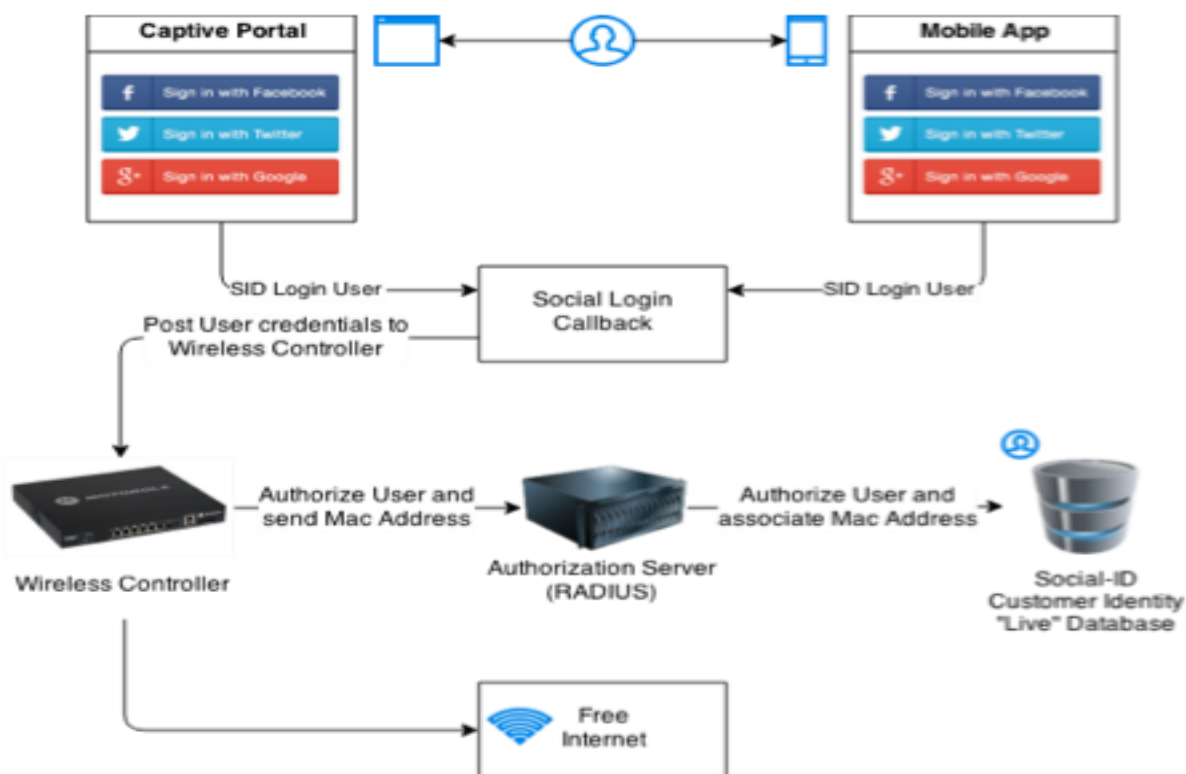
4.5 Διαδικασία δημιουργίας Over the Top σε Cisco εξοπλισμό

Αφού πλέον έχει δημιουργηθεί το νέο SSID στον Controller του δικτύου και έχουν επιλεγθεί ποια access points θα το εκπέμπουν, θα αναλυθεί η διαδικασία απόκτησης πρόσβασης στο διαδίκτυο. Κατά την διαδικασία αυτή θα πρέπει να επιλεγθεί να γίνει η σύνδεση με βάση τα στοιχεία πρόσβασης ενός από τους λογαριασμούς facebook, linkedin, κλπ. που διατηρεί ο χρήστης. Εφόσον επιλέξει να συνδεθεί στο SSID που μόλις δημιουργήθηκε, το επόμενο βήμα είναι να ανοίξει στην οθόνη της κινητής συσκευής μία ιστοσελίδα όπου θα πρέπει να εισάγει είτε κάποιο username ή password εάν διαθέτει ή θα πρέπει να συνδεθεί με κάποιον από τους λογαριασμούς κοινωνικής δικτύωσης που διαθέτει. Η ιστοσελίδα που εμφανίζεται ονομάζεται captive portal και είναι μια ιστοσελίδα με πρόσβαση σε ένα πρόγραμμα περιήγησης ιστού που εμφανίζεται συνδεδεμένους χρήστες ενός Wi-Fi ή ενσύρματου δικτύου πριν τους δοθεί ευρύτερη πρόσβαση σε πόρους του δικτύου. Η ιστοσελίδα ζητά επίσης από τους χρήστες την αποδοχή της πολιτικής χρήσης και των όρων πρόσβασης.

Υπάρχουν 2 ειδών Captive Portal:

- 1) **Εσωτερικό Captive portal** – Για τον έλεγχο ταυτότητας, χρησιμοποιείται ένας εσωτερικός διακομιστής για τη φιλοξενία της υπηρεσίας του Captive Portal.
- 2) **Εξωτερικό Captive portal** - Για τον έλεγχο ταυτότητας, χρησιμοποιείται ένας εξωτερικός διακομιστής στο Cloud για τη φιλοξενία της υπηρεσίας του Captive Portal.

Η αρχιτεκτονική του captive portal και η Social-ID πλατφόρμα παρουσιάζονται στο παρακάτω διάγραμμα:



Εικόνα 66 Αρχιτεκτονική Captive Portal και Social ID

Μόλις ο χρήστης συνδεθεί σε ένα δίκτυο Wi-Fi, το AP ή ο controller ανακατευθύνει τον χρήστη στο captive portal. Ο χρήστης μπορεί να συνδεθεί χρησιμοποιώντας ένα κοινωνικό δίκτυο ή παραδοσιακά διαπιστευτήρια όπως όνομα χρήστη και κωδικό πρόσβασης. Τα στοιχεία αυθεντικοποίησης του χρήστη από την σελίδα της κοινωνικής δικτύωσης γίνονται γνωστά στο ασύρματο AP ή τον controller.

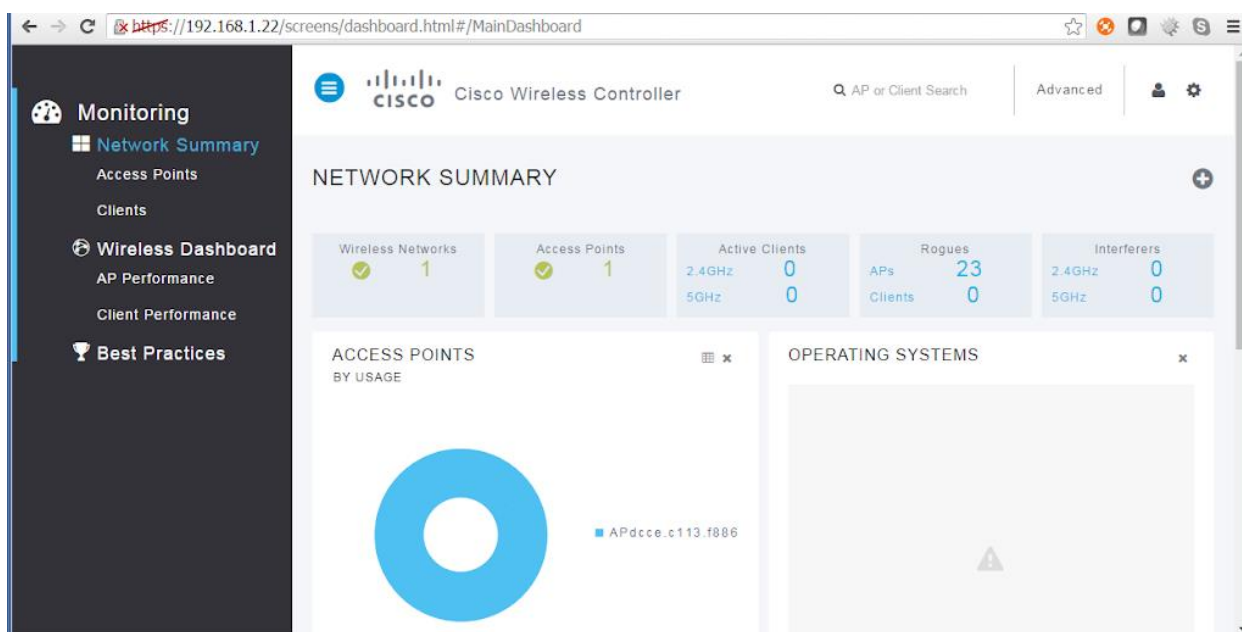
Το AP ή ο controller πρέπει να διαμορφωθούν για έλεγχο της ταυτότητας των χρηστών μέσω ελέγχου ταυτότητας RADIUS. Ένας διακομιστής RADIUS και ένα μυστικό κλειδί πελάτη ρυθμίζονται και υποβάλλονται σε ερώτηση κατά την άφιξη ενός αιτήματος ελέγχου ταυτότητας. Ο διακομιστής κοινωνικής σύνδεσης RADIUS επικυρώνει τον χρήστη και απαντά στο ασύρματο AP ή τον controller, το οποίο ανοίγει το Διαδίκτυο στον χρήστη και ανακατευθύνει πίσω σε κάποια σελίδα υποδοχής. Από αυτό το σημείο ο χρήστης μπορεί να απολαύσει δωρεάν Διαδίκτυο.

Παράμετροι διαμόρφωσης

Για την διαμόρφωση του Captive Portal σε σχεδόν όλους τους προμηθευτές, χρειάζονται αυτοί οι βασικοί παράμετροι:

- Η IP διεύθυνση του Social-ID RADIUS server που είναι υπεύθυνος για τον έλεγχο ταυτότητας των χρηστών.
- Το Μυστικό Κλειδί RADIUS: Το μυστικό κλειδί χρειάζεται για την επικοινωνία μεταξύ του RADIUS client και του server.
- Το Captive portal URL: Το URL της login σελίδας όπου θα ανακατευθύνονται οι χρήστες.

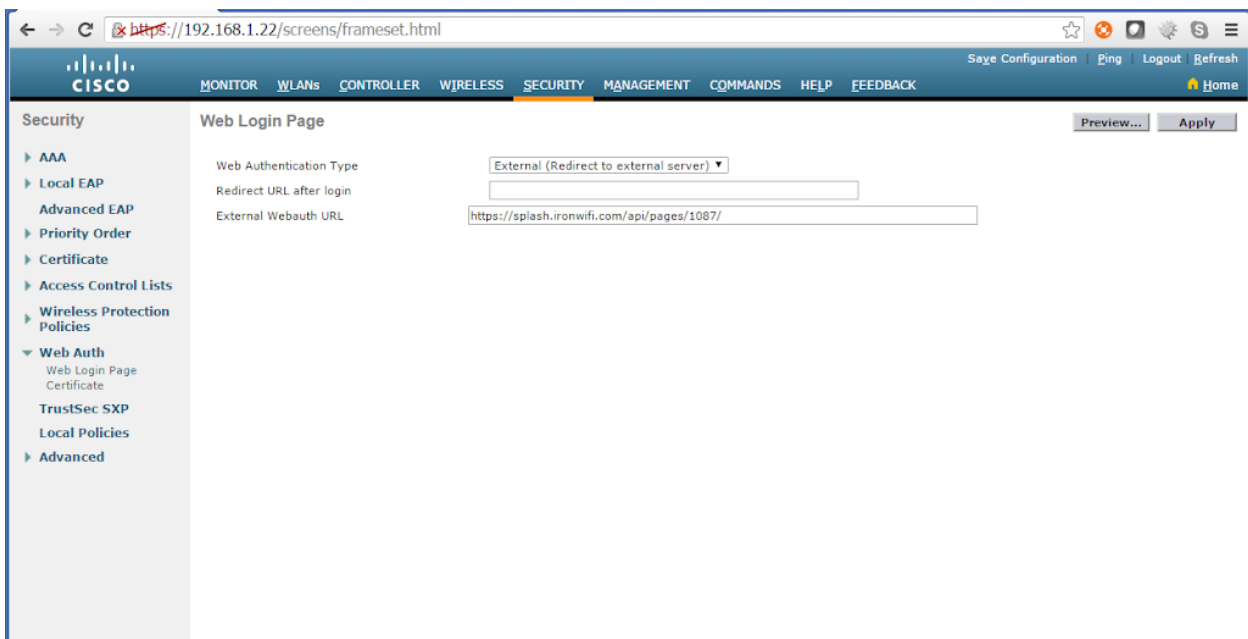
Είσοδος στον Cisco WLC Web-Browser και είσοδος στην σελίδα Advanced Settings.



Εικόνα 67 Ρύθμιση του Ασύρματου Controller για Ανακατεύθυνση του χρήστη στην σελίδα του Captive Portal (1)

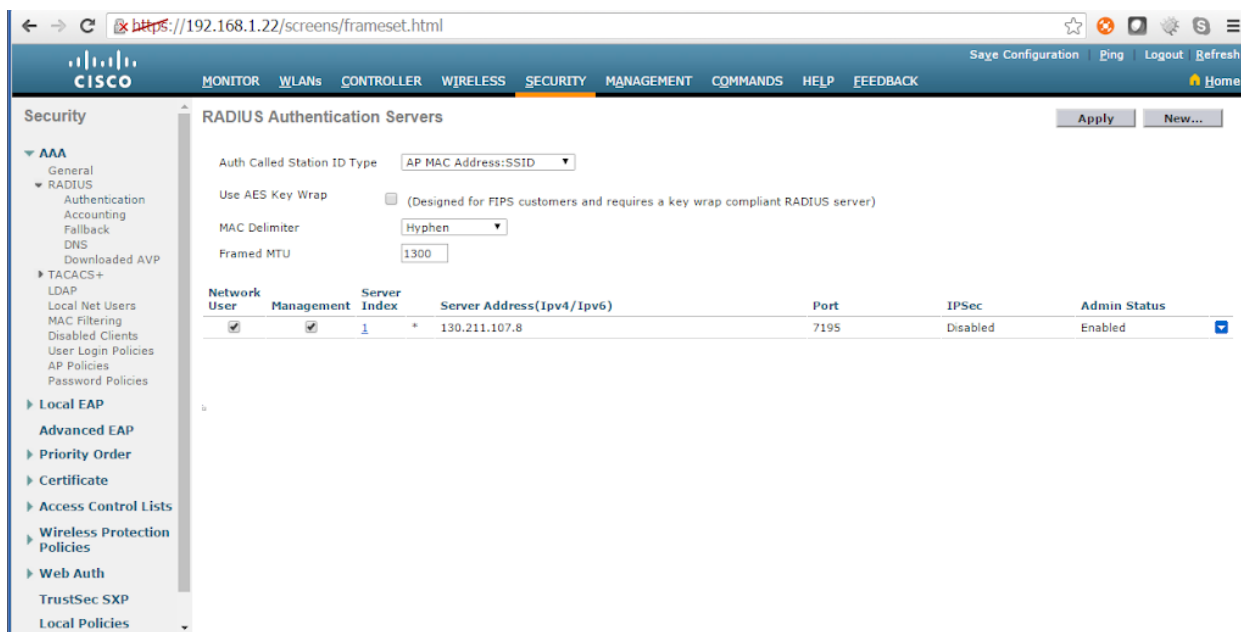
Ο διαχειριστής, αφού εισέλθει στην σελίδα διαχείρισης του ασύρματου controller, ακολουθεί την παρακάτω διαδρομή **Security** → **Web Auth** → **Web Login Page** και αλλάζει το Web Authentication Type σε External (redirect to an external server) και έπειτα προσθέτει το External URL του server.

- ⇒ **Web Authentication Type:** External (ανακατευθύνει τον χρήστη στον Cloud Captive Portal server)
- ⇒ **Redirect URL After Login:** Παραμένει κενό
- ⇒ **External Webauth URL:** Εισάγεται το URL του Captive Portal

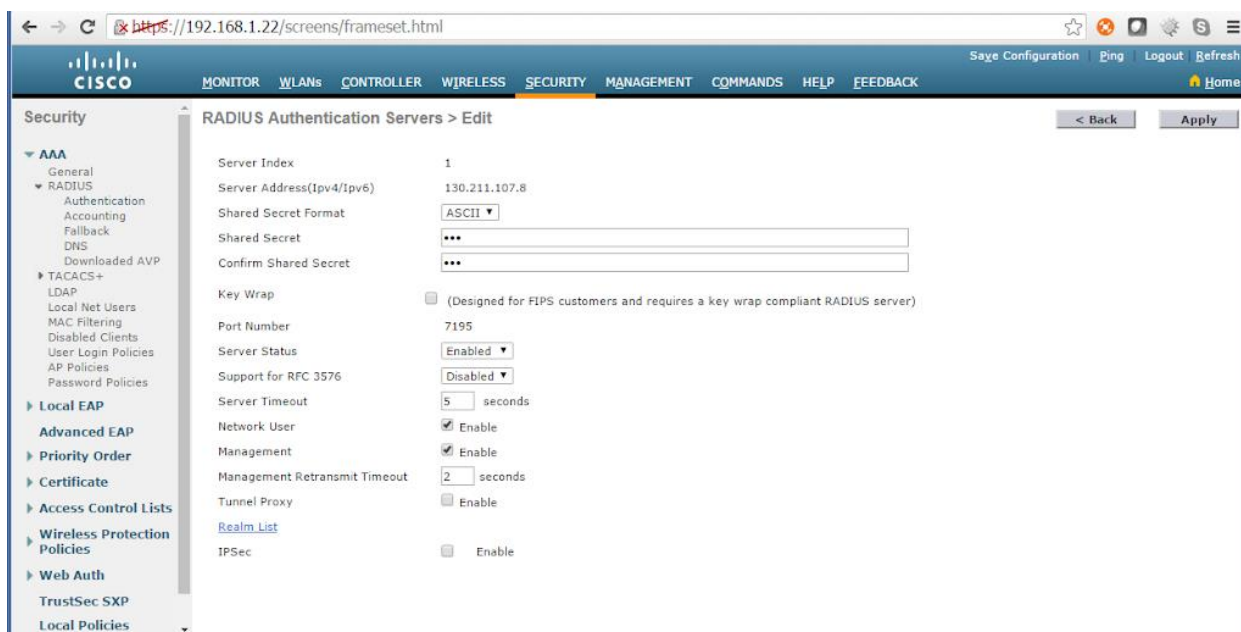


Εικόνα 68 Ρύθμιση του Ασύρματου Controller για Ανακατεύθυνση του χρήστη στην σελίδα του Captive Portal (2)

Ο διαχειριστής πλοηγείται στο πεδίο **Security** → **RADIUS** → **Authentication**, και προσθέτει τον νέο RADIUS Authentication Servers. Έπειτα εισάγει την IP διεύθυνση, την πόρτα και το μυστικό κλειδί.



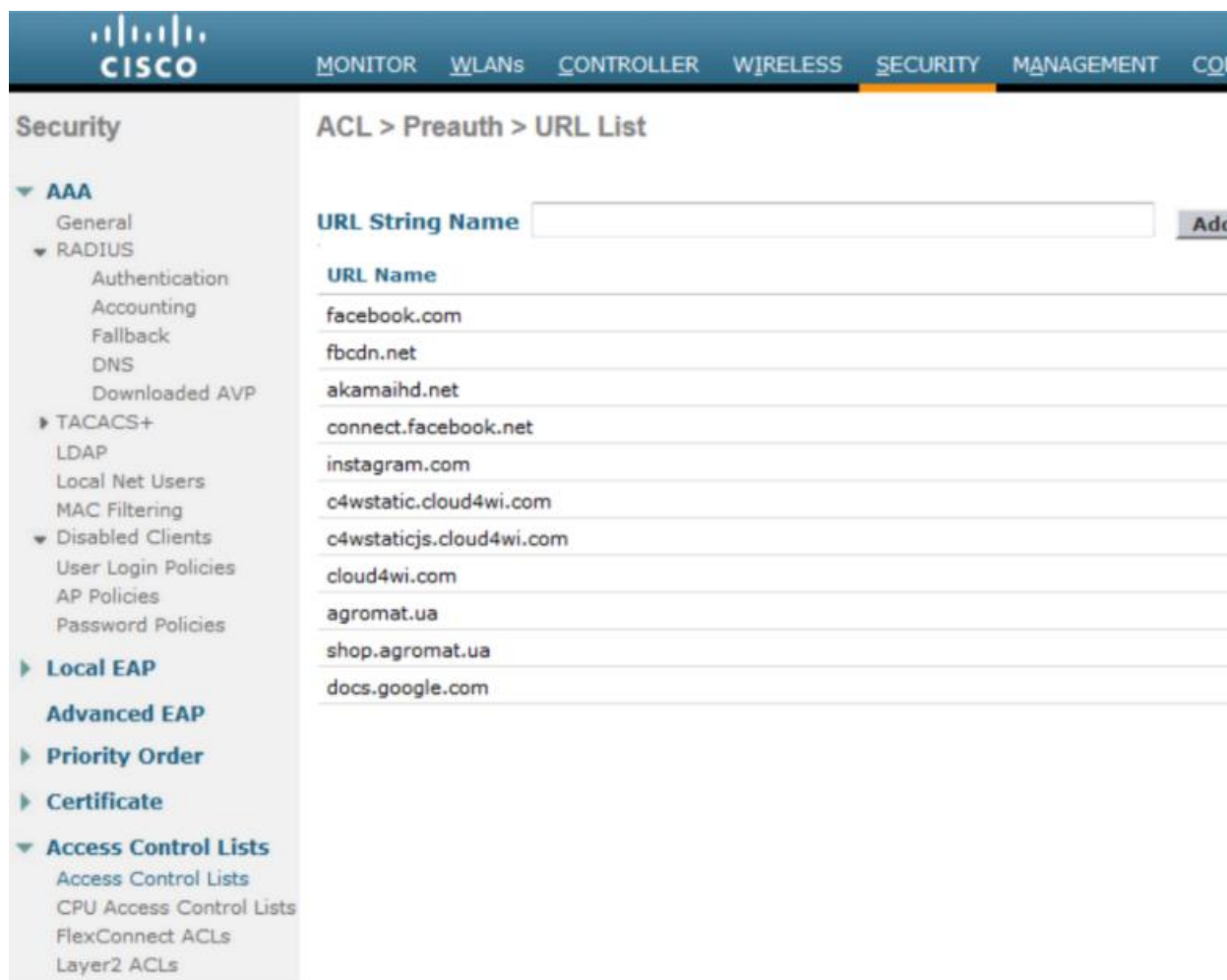
Εικόνα 69 Ρύθμιση του Ασύρματου Controller για Ανακατεύθυνση του χρήστη στην σελίδα του Captive Portal (3)



Εικόνα 70 Ρύθμιση του Ασύρματου Controller για Ανακατεύθυνση του χρήστη στην σελίδα του Captive Portal (4)

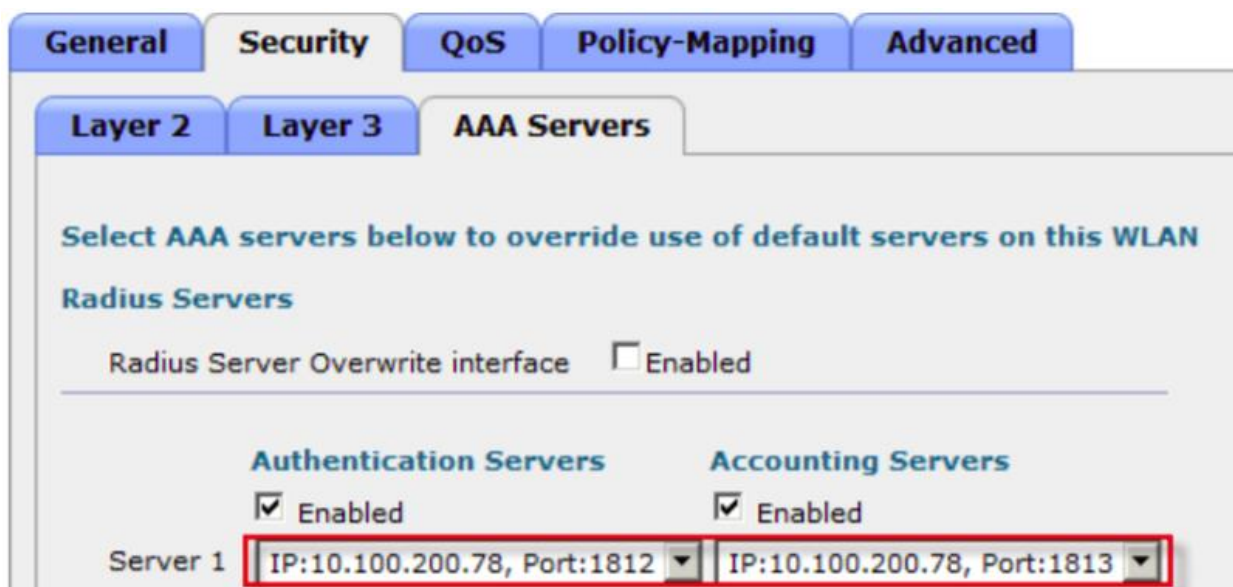
Προκειμένου να ενεργοποιηθεί η είσοδος στο ασύρματο δίκτυο μέσω των κοινωνικών σελίδων, θα πρέπει πρώτα να διαμορφωθεί μια λίστα διευθύνσεων URL στις οποίες οι χρήστες πρέπει να έχουν πρόσβαση χωρίς έλεγχο ταυτότητας στο δίκτυο Wi-Fi. Αυτή η λίστα διευθύνσεων URL, που ονομάζεται Walled Garden, μπορεί να διαμορφωθεί βάσει ονομάτων τομέα (domain names) ή IP. Η πιο αποτελεσματική διαμόρφωση βασίζεται σε domain names, μίας και τα περισσότερα από τα τρέχοντα κοινωνικά δίκτυα και εφαρμογές χρησιμοποιούν δυναμικές IP για την παροχή των υπηρεσιών τους, με αποτέλεσμα να

είναι πολύ δύσκολο να παρακολουθούνται όλες οι αλλαγές των IP που χρησιμοποιούνται. Το Social Login επιτρέπει στους χρήστες να συνδεθούν και να εγγραφούν με ένα κλικ στον ιστότοπο χρησιμοποιώντας τους υπάρχοντες λογαριασμούς τους από διάφορα κοινωνικά δίκτυα.



Εικόνα 83 Ρύθμιση του Ασύρματου Controller για Ανακατεύθυνση του χρήστη στην σελίδα του Captive Portal (5)

Πλέον και αφού έχει δημιουργηθεί η λίστα με τα URL τα οποία θα χρησιμοποιούν το External Captive Portal για είσοδο των χρηστών με την χρήση των στοιχείων που έχουν δηλώσει στα αντίστοιχα sites, δηλώνονται οι AAA servers του External Captive Portal στο SSID που δημιουργήθηκε στο προηγούμενο βήμα.



Εικόνα 84 Ρύθμιση του Ασύρματου Controller για Ανακατεύθυνση του χρήστη στην σελίδα του Captive Portal (6)

Μετά και από την ολοκλήρωση όλων των βημάτων, έχει ολοκληρωθεί η δημιουργία ενός νέου SSID, το οποίο κατά την διαδικασία σύνδεσης εμφανίζει ένα Web Portal στο οποίο αφού γίνει σύνδεση με τον Social Media λογαριασμό ή με κάποιο προσωπικό λογαριασμό, επιτρέπει στον χρήστη να πλοηγηθεί στο διαδίκτυο. [15]



Εικόνα 85 Ιστοσελίδα Captive Portal για Σύνδεση στο WI-FI με την διαδικασία του Social Login

ΠΙΝΑΚΑΣ ΟΡΟΛΟΓΙΑΣ

Ξενογλωσσος όρος	Ελληνικός Όρος
Reliability	Αξιοπιστία
Latency	Καθυστέρηση
Access Point	Ασύρματο Σημείο Πρόσβασης
VAP	Virtual Access Point
STA	Station
mMTC	massive Machine Type Communication
eNB	evolved NodeB
EPC	Evolved Packet Core
NR	New Radio
NFV	Network Function Virtualization
SDN	Software Defined Networking
MEC	Multi-Access Edge
OFDMA	Orthogonal Frequency Division Multiple Access
MIMO	Multiple Input – Multiple Output
RSSI	Received Signal Strength Indicator
SSID	Service Set Identifier
BSS	Basic Service Set
AP	Access Point
AAA	Authentication, Authorization, Accounting
eMBB	Enhanced Mobile Broadband
URLCC	Ultra-Reliable Low-Latency Communication

ΑΝΑΦΟΡΕΣ

- [1] Cisco VNI 2018 - 2023
- [2] Ericson Mobility Report 2019
- [3] WI-FI Alliance, WI-FI 6 White Paper, October 2018
- [4] Aruba Networking, White Paper 902.11ax
- [5] Evgeny Khorov, Anton Kiryanov, Andrey Lyakhov, and Giuseppe Bianchi, A tutorial on IEEE 802.11ax High Efficiency WLANS, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 21, NO. 1, FIRST QUARTER 2019
- [6] Cisco, Calculating the speed of 802.11ac and 802.11ax
- [7] Extreme Networks, How does BSS Coloring work in 802.11ax, 17 October 2019
- [8] Cisco, Campus Lan and Wireless Lan Design Guide, January 2018
- [9] Woojoong Kim, Seunggho Ryu, James Won-Ki Hong, and Young-Joo Suh, WLANMan: A Cloud-based Wireless LAN Management System in ONOS Controllers, 2016 IEEE Conference on Computer Communications Workshops
- [10] Cisco, IEE 802.11ax, The sixth Generation of WI-FI White Paper, 3 April 2020
- [11] Cisco Meraki, Channel Planning Best Practises
- [12] 3GPP LTE Release 15 & 16, <https://www.3gpp.org/release-15>,
<https://www.3gpp.org/release-16>
- [13] 3GPP TS 33.501, V15.1.0 (2018-07)
- [14] 3GPP TS 23.502, V15.2.0 (2018-06)
- [15] Viavisolutions.com/5G Architecture
- [16] EventHelix, 5G Standalone Access Registration
- [17] Ericsson Non-Standalone and Standalone: two standards-based paths to 5G, July 2019
- [18] 5GPPP Architecture Working Group, Version 2.0, July 2017
- [19] 5G Americas Whitepaper, October 2018
- [20] Xiaowei Zhang, Andreas Kunz, Stefan Schröder, Overview of 5G Security in 3GPP, IEEE Conference on Standards for Communications and Networking (CSCN)2017
- [21] Cisco, Wireless LAN Design Guide for High Density Environments in Higher Education, 22 July 2017
- [22] Cisco, Enterprise Mobility 4.1 Design Guide WLAN
- [23] Gabriel-Cătălin CRISTESCU, Victor CROITORU, Vlad SORICI, Implementing an AAA-Radius Solution based on EAP, IEEE 2016
- [24] Remote Authentication Dial In User Service (RADIUS), IETF RFC 2865