



ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ  
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ  
ΤΜΗΜΑ ΦΥΣΙΚΗΣ  
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ  
ΜΕΤΑΠΤΥΧΙΑΚΟ ΔΙΠΛΩΜΑ ΕΙΔΙΚΕΥΣΗΣ ΣΤΗΝ  
ΗΛΕΚΤΡΟΝΙΚΗ-ΡΑΔΙΟΗΛΕΚΤΡΟΛΟΓΙΑ

---

**Ανάλυση αρχιτεκτονικής αυτόνομου και μη  
αυτόνομου συστήματος πέμπτης γενιάς (5G) και  
υλοποίηση σε cloud περιβάλλον**

---

**ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ**  
ΤΟΥ  
**ΓΕΩΡΓΙΑΔΗ Γ. ΠΕΤΡΟΥ**  
**A.M.:2019102**

**Μέλη Τριμελούς Επιτροπής**

- 1] ΤΖΑΝΑΚΑΚΗ Άννα - Αν. Καθηγήτρια Ε.Κ.Π.Α. (Επιβλέπουσα)
- 2] ΡΕΪΣΗΣ Διονύσιος - Καθηγητής Ε.Κ.Π.Α.
- 3] ΝΙΣΤΑΖΑΚΗΣ Έκτορας-Εμμανουήλ - Αν. Καθηγητής Ε.Κ.Π.Α.

Πανεπιστήμιο Αθηνών  
Μάιος, 2021



# Περιεχόμενα

<b>I</b>	<b>Θεωρία</b>	<b>5</b>
<b>1</b>	<b>Εισαγωγή</b>	<b>1</b>
1.1	Ιστορική αναδρομή . . . . .	1
1.2	Ανάγκες που μας οδήγησαν στο 5G . . . . .	3
1.3	Προκλήσεις κατά την πραγματοποίηση του 5G δικτύου . . . . .	4
1.4	Επισκόπηση αρχιτεκτονικής και σχεδίασης του δικτύου 5G . . . . .	5
1.4.1	Αυτόνομη και μη αυτόνομη ανάπτυξη 5G δικτύου . . . . .	6
1.5	Έκδοσεις κυκλοφορίας 5G της κοινοπραξίας 3GPP . . . . .	9
1.5.1	Έκδοση-15 . . . . .	9
1.5.2	Έκδοση-16 . . . . .	9
1.5.3	Έκδοση-17 . . . . .	10
1.5.4	Έκδοση-18 . . . . .	10
1.6	Οργανισμοί ανάπτυξης 5G συστημάτων . . . . .	11
1.6.1	Περιφερειακή ανάπτυξη / προώθηση του 5G . . . . .	11
1.6.2	Ανάπτυξη προτύπων (Standard Development) . . . . .	14
<b>2</b>	<b>Δίκτυο Κορμού 5G</b>	<b>17</b>
2.1	Μη αυτόνομο δίκτυο κορμού 5G (Non-Stand Alone) . . . . .	17
2.1.1	Βασική Αρχιτεκτονική Evolved Packet Core(EPC) . . . . .	18
2.1.2	(Enhanced) Dedicated Core Network((e)DECOR ή DCN) . . . . .	20
2.1.3	Control and User Plane Separation(CUPS) . . . . .	22
2.2	Αυτόνομο δίκτυο κορμού 5G( Stand Alone) . . . . .	25
2.2.1	Access και Mobility Management Function (AMF) . . . . .	25
2.2.2	Session Management Function (SMF) . . . . .	28
2.2.3	User plane function(UPF) . . . . .	29
2.2.4	Network repository function (NRF) . . . . .	29
2.2.5	Unified data management function (UDM) . . . . .	30
2.2.6	Unified Data Repository(UDR) . . . . .	30
2.2.7	Unstructured data storage function( UDSF) . . . . .	31
2.2.8	AUthentication Server Function (AUSF) . . . . .	31
2.2.9	5G equipment identity registry(5G-EIR) . . . . .	31
2.2.10	Policy control function (PCF) . . . . .	31
2.2.11	Network slice selection function(NSSF ) . . . . .	32
2.2.12	Network exposure function(NEF) . . . . .	32
2.2.13	Network data analytics function(NWDAF) . . . . .	33
2.2.14	Security edge protection proxy(SEPP) . . . . .	33
2.2.15	Non-3GPP inter working function(N3IWF) . . . . .	33
2.2.16	Application function(AF) . . . . .	33

2.2.17	Short message service function(SMSF)	34
2.2.18	Location management function (LMF)	34
2.3	Μοντέλα αρχιτεκτονικής δικτύου κορμού 5G	36
2.3.1	Αρχιτεκτονική σημείου αναφοράς (Reference Point Architecture)	36
2.3.2	Αρχιτεκτονική βασιζόμενη στις υπηρεσίες (Service-Based Architecture, SBA)	38
2.4	Υπηρεσίες και λειτουργίες υπηρεσιών	42
2.4.1	Υπηρεσίες της AMF	43
2.4.2	Υπηρεσίες της SMF	44
2.4.3	Υπηρεσίες της PCF	45
2.4.4	Υπηρεσίες της UDM	45
2.4.5	Υπηρεσίες της AUSF	46
2.4.6	Υπηρεσίες της SMSF	46
2.4.7	Υπηρεσίες της UDR	46
2.4.8	Υπηρεσίες 5G-EIR	46
2.4.9	Υπηρεσίες της NWDAF	47
2.4.10	Υπηρεσίες της UDSF	47
2.4.11	Υπηρεσίες της NSSF	47
2.4.12	Υπηρεσίες της LMF	47
2.4.13	Υπηρεσίες της NEF	47
<b>3</b>	<b>Δίκτυο Πρόσβασης 5G</b>	<b>49</b>
3.1	Συνδεσμολογίες 5G RAN	50
3.1.1	Επιλογές συνδεσιμότητας 5G CN και 5G RAN	50
3.1.2	Ραδιοπρόσβαση	51
3.1.3	Βασική διασύνδεση δικτύου πρόσβασης	52
3.2	Χειρισμός διαφορετικών QoS	54
3.2.1	Hybrid Automatic Repeat reQuest(HARQ)	55
3.2.2	Forward Error Correction(FEC)	55
3.2.3	Χρονοπρογραμματισμός (Scheduling)	55
3.3	Αρχιτεκτονική Ραδιοπρωτοκόλλων	57
3.3.1	Πρωτόκολλα Επιπέδου Χρήστη(User Plane)	58
3.3.2	Πρωτόκολλα επιπέδου ελέγχου	62
3.4	Κανάλια μετάδοσης	63
3.4.1	Κανάλια επιπέδου MAC	63
3.4.2	Κανάλια επιπέδου PHY	69
3.5	Διεπαφές δικτύου πρόσβασης	72
3.5.1	Η διεπαφή Xn	72
3.5.2	Η διεπαφή NG	75
3.5.3	Η διεπαφή F1	76
3.5.4	Η διεπαφή E1	80
3.6	Τεχνικές Διαμόρφωσης 5G συστημάτων	82
3.6.1	Orthogonal Frequency-Division Multiplexing(OFDM)	82
3.6.2	Single Carrier- FDMA(SC-FDMA)	82
3.6.3	Non-Orthogonal Multiple Access(NOMA)	84
3.7	Το φάσμα συχνοτήτων του 5G	85
3.7.1	Παγκόσμια κατάσταση φάσματος 5G	85

3.7.2	Ζώνες συχνότητων για το NR . . . . .	86
<b>4</b>	<b>Καινοτόμες προσεγγίσεις στο 5G</b>	<b>91</b>
4.1	Πρωτόκολλα επικοινωνίας στο 5G . . . . .	91
4.1.1	5G στρώμα μη-πρόσβασης(5G Non-Access Stratum, 5G NAS)	91
4.1.2	NG Πρωτόκολλο εφαρμογών (NG Application Protocol, NGAP) . . . . .	94
4.1.3	Πρωτόκολλο μεταφοράς υπερκειμένου (Hypertext transfer protocol, HTTP) . . . . .	96
4.1.4	Πρωτόκολλο ελέγχου προώθησης πακέτων (Packet forwarding control protocol, PFCP) . . . . .	101
4.1.5	GPRS Tunneling Protocol για User Plane (GTP-U) . . . . .	102
4.1.6	Επεκτάσιμο πρωτόκολλο ελέγχου ταυτότητας (Extensible Authentication Protocol, EAP) . . . . .	104
4.1.7	IP security (IPSec) . . . . .	105
4.1.8	Πρωτόκολλο ελέγχου ροής μετάδοσης (Stream Control Transmission Protocol, SCTP) . . . . .	107
4.1.9	Γενική ενθυλάκωση δρομολόγησης (Generic Routing Encapsulation, GRE) . . . . .	111
4.2	Νέες Εφαρμοζόμενες τεχνολογίες . . . . .	114
4.2.1	Μικροϋπηρεσίες (Microservices) . . . . .	114
4.2.2	Τεχνικές Εικονικοποίησης (Virtualization και Containerization) . . . . .	115
4.2.3	Τεχνολογίες νέφους (Cloud computing) . . . . .	117
4.2.4	Δικτύωση βασισμένη στο λογισμικό (Software Defined Network, SDN) . . . . .	119
4.2.5	Αυτοματοποίηση . . . . .	120
4.3	Τεμαχισμός Δικτύου (Network Slicing) . . . . .	121
4.3.1	Η ανάγκη του τεμαχισμού του δικτύου . . . . .	121
4.3.2	Λειτουργία του Slicing . . . . .	122
4.3.3	Single Network Slice Selection Assistance Information (S-NSSAI) . . . . .	124
4.3.4	Πλεονεκτήματα χρήσης . . . . .	125
4.4	Διαχωρισμός Λειτουργιών (Function Split) . . . . .	126
4.4.1	Κίνητρα για διαχωρισμό λειτουργιών του 5G . . . . .	126
4.4.2	Επιλογές Λογικού διαχωρισμού 5G λειτουργιών . . . . .	128
<b>II</b>	<b>Πειραματική Διαδικασία</b>	<b>131</b>
<b>5</b>	<b>Υλοποίηση αυτόνομου και μη αυτόνομου συστήματος 5G</b>	<b>133</b>
5.1	Προετοιμασία υλικού και λογισμικού εξοπλισμού . . . . .	134
5.1.1	Δίκτυο Κορμού . . . . .	135
5.1.2	Δίκτυο Πρόσβασης . . . . .	136
5.1.3	Διεπαφές . . . . .	139
5.2	Υλοποίηση μη αυτόνομης λειτουργίας 5G . . . . .	139
5.2.1	Δίκτυο κορμού . . . . .	140
5.2.2	Δίκτυο πρόσβασης . . . . .	145
5.2.3	Εξοπλισμός χρήστη . . . . .	150

5.2.4	Λειτουργία . . . . .	153
5.3	Υλοποίηση αυτόνομης λειτουργίας 5G . . . . .	154
5.3.1	Δίκτυο κορμού . . . . .	155
5.3.2	Δίκτυο πρόσβασης και UE . . . . .	158
<b>6</b>	<b>Σχολιασμός αποτελεσμάτων και μελλοντικές εξελίξεις</b>	<b>161</b>
6.1	Σχολιασμός αποτελεσμάτων πειραματικής διαδικασίας . . . . .	161
6.1.1	Μη αυτόνομο σύστημα 5G . . . . .	161
6.1.2	Αυτόνομο σύστημα 5G . . . . .	164
6.2	Μελλοντικές εξελίξεις . . . . .	173
6.2.1	Βελτιώσεις του αυτόνομου 5G συστήματος . . . . .	173
6.2.2	Προσθήκη νέων δυνατοτήτων στο δίκτυο κορμού . . . . .	174
6.2.3	Προσθήκη νέων δυνατοτήτων στο δίκτυο πρόσβασης . . . . .	177
6.2.4	6G και Beyond: Το μέλλον των ασύρματων συστημάτων επικοινωνίας . . . . .	180
6.3	Επίλογος . . . . .	185

# Λίστα Εικόνων

1.1	Σχηματική αναπαράσταση ιστορικής εξέλιξης κυψελωδών συστημάτων[40] . . . . .	2
1.2	Περιπτώσεις αξιοποίησης 5G τεχνολογίας [34] . . . . .	4
1.3	Αναπαράσταση αρχιτεκτονικής σχεδίασης end-to-end [40] . . . . .	5
1.4	Περιοδική 5G συστήματος-Τοπικό σενάριο ξεμπλοκαρίσματος [40] . . . . .	7
1.5	Χρονοδιάγραμμα εκδόσεων 3GPP για το 5G-NR [42] . . . . .	10
1.6	Λογότυπα και σχέση μεταξύ ITU και 3GPP [41] . . . . .	15
2.1	Στοιχειώδης Αρχιτεκτονική δικτύου 4G . . . . .	18
2.2	(α)Όλες οι υπηρεσίες μοιράζονται το ίδιο δίκτυο κορμού (β)Χρήση λειτουργιών δικτύου κορμού με βάση τις ανάγκες της κάθε υπηρεσίας . . . . .	21
2.3	Αναπαράσταση πυρήνα δικτύου δομημένου με CUPS [2] . . . . .	23
2.4	Παράδειγμα ανάπτυξης αρχιτεκτονικής δικτύου με DECOR,CUPS και EN-DC [2] . . . . .	24
2.5	Βασικά στοιχεία 5G δικτύου [2] . . . . .	25
2.6	Αναπαράσταση συνδεσιμότητας AMF [3] . . . . .	26
2.7	Επιλογή AMF απο ένα σύνολο AMF set [3] . . . . .	27
2.8	Σύνολο λειτουργιών με εφαρμογή IMS Core και MEC συστήματος [43] . . . . .	34
2.9	Διαφορετικοί συνδυασμοί επιλογών χρήσης δικτύου κορμού[2] .	35
2.10	Οπτικοποίηση Αρχιτεκτονικής διεπαφών σημείο-προς-σημείο [2]	36
2.11	Οπτικοποίηση Αρχιτεκτονικής διεπαφών βασισμένες στις υπηρεσίες(SBA) [2] . . . . .	38
2.12	Ενοποιημένη ροή κλησεων[2] . . . . .	41
2.13	Απλή επισκόπηση υπηρεσιών 5G δικτύου [2] . . . . .	43
3.1	Διαφορετικοί συνδυασμοί CN και RAN[10] . . . . .	50
3.2	Διεπαφές Δικτύου ραδιο-πρόσβασης [10] . . . . .	52
3.3	Διπλή συνδεσιμότητα LTE-NR με χρήση της επιλογής 3. [10] . .	53
3.4	Ροές QoS και Radio Bearers σε μια PDU συνεδρία[10] . . . . .	54
3.5	Μορφή Μεταφοράς για κατερχόμενη και ανερχόμενη ζεύξη[10] .	56
3.6	Στοίβα πρωτοκόλλων για το Non-Stand Alone [14] . . . . .	57
3.7	Αρχιτεκτονική πρωτοκόλλου κατερχόμενης ζεύξης NR επιπέδου χρήστη όπως φαίνεται απο τη συσκευή[10] . . . . .	59
3.8	Αντιστοίχιση μεταξύ λογικών,μεταφοράς και φυσικού καναλιού[10]	67
3.9	Διεπαφές για τη διασύνδεση 5G-Core και 5G-RAN [17] . . . . .	72
3.10	Χn-U στοίβα πρωτοκόλλων. [17] . . . . .	73

3.11	Χη-C στοίβα πρωτοκόλλων. [17] . . . . .	74
3.12	Στοιβά πρωτοκόλλων διεπαφής NG (α) Επιπέδου ελέγχου και (β) Επιπέδου χρήστη [17] . . . . .	76
3.13	Στοιβά πρωτοκόλλων διεπαφής F1 επιπέδου ελέγχου [22] . . . . .	77
3.14	Στοιβά πρωτοκόλλων διεπαφής F1 επιπέδου χρήστη [22] . . . . .	79
3.15	Στοιβά πρωτοκόλλων διεπαφής E1 [23] . . . . .	81
3.16	Συνολική επισκόπηση των διαφόρων τύπων διεπαφών για το gNB του 5G NR [24] . . . . .	81
3.17	OFDM υποφέρουσες συχνότητες [12] . . . . .	83
4.1	Στοιβά Πρωτοκόλλου NAS[2] . . . . .	92
4.2	Δομή πλαισίου(frame) μηνυμάτων NAS για (α) 5GMM και (β) 5GSM[2] . . . . .	94
4.3	Στοιβά πρωτοκόλλου HTTP.[2] . . . . .	96
4.4	Απλή συναλλαγή HTTP [26] . . . . .	97
4.5	Στοιβά πρωτοκόλλου PFCP επιπέδου ελέγχου [29] . . . . .	102
4.6	Στοιβά πρωτοκόλλου επιπέδου χρήστη για PDU συνεδρία [27] .	103
4.7	Κεφαλίδα GTP-U[27] . . . . .	103
4.8	Στοιβά πρωτοκόλλου EAP [2] . . . . .	105
4.9	Συσχέτιση SCTP [2] . . . . .	108
4.10	Multistreaming με SCTP [2] . . . . .	110
4.11	Multi-homing με SCTP [2] . . . . .	110
4.12	Παράδειγμα στοίβας πρωτοκόλλου κατά τη χρήση GRE tunneling [2] . . . . .	111
4.13	Παράδειγμα GRE tunnel μεταξύ δύο κόμβων δικτύου με IPv4 πρωτόκολλο παράδοσης [2] . . . . .	112
4.14	Κεφαλίδα GRE και η επέκταση κλειδιού και αριθμού ακολουθίας [2] . . . . .	113
4.15	Παράδειγμα δομής 5G με microservices [43] . . . . .	114
4.16	Προσέγγιση βασισμένη σε NFV για τις λειτουργίες δικτύου [32] .	116
4.17	Τεχνικές εικονικοποίησης [13] . . . . .	117
4.18	Μοντέλα Cloud Υπηρεσιών [32] . . . . .	118
4.19	Δικτύωση Βασισμένη στο λογισμικό [32] . . . . .	119
4.20	Τεμαχισμός Δικτύου 5G [32] . . . . .	121
4.21	Επίπεδα Framework για τον τεμαχισμό δικτύου 5G [32] . . . . .	123
4.22	Παράδειγμα Network Slicing στο 5G [32] . . . . .	124
4.23	Κάτοψη του S-NSSAI [2] . . . . .	125
4.24	Δομή C-RAN με τρία RRHs συνδεδεμένα με το δίκτυο μεταφοράς [38] . . . . .	126
4.25	Ευέλικτος διαχωρισμός λειτουργιών Cloud-RAN [38] . . . . .	127
4.26	Επιλογές διαχωρισμού λειτουργιών [38] . . . . .	128
5.1	Υλική υποδομή εφαρμογής της πειραματικής διαδικασίας . . . . .	134
5.2	Σχέδιο υλοποίησης μη αυτόνομου 5G συστήματος . . . . .	140
5.3	Συνδεσιμότητα eNB/gNB server με το Docker δίκτυο κορμού [45] .	142
5.4	Διάγραμμα Block του OpenAirInterface[45] . . . . .	147
5.5	Διάγραμμα Block μητρικής κάρτας Ettus Usrp N310[46] . . . . .	149
5.6	Δομή κάρτας SIM [48] . . . . .	151
5.7	Αναπαράσταση λειτουργίας μη αυτόνομου 5G[45] . . . . .	153



5.8	Λειτουργίες αυτόνομου 5G που περιλαμβάνει η υλοποίηση[45]	154
5.9	Συνδεσιμότητα προσομοιωτών gNB και UE με το Docker δίκτυο κορμού [45]	159
6.1	Ανάλυση πακέτου δικτύου κορμού 5G NSA [45]	163
6.2	Ανάλυση πακέτου δικτύου κορμού 5G NSA-επισύναψη συσκευής χρήστη στο δίκτυο [45]	164
6.3	Ανταλλαγή μηνυμάτων μεταξύ SMF,NRF και UPF [45]	165
6.4	Ανάλυση πακέτου δικτύου κορμού 5G SA-αρχική σύνδεση	166
6.5	Ανάλυση πακέτου δικτύου πρόσβασης 5G SA-Πιστοποίηση εξωτερικού δικτύου	167
6.6	Ανάλυση πακέτου δικτύου πρόσβασης 5G SA-Επικοινωνία με εξωτερικό δίκτυο	168
6.7	Επικοινωνία μέσω μηνυμάτων NAS	169
6.8	Εγκαθίδρυση συνεδρίας SMF προς UPF — PFCP	170
6.9	Αποστολή N2 μηνύματος του SMF προς το AMF για το gNB	171
6.10	Αποστολή σημάτων ping για επιβεβαίωση σύνδεσης	171
6.11	Τυπική πρόσβαση σε ασύρματη γραμμή [2]	176
6.12	Το οραμα που επιτρέπει τεχνολογίες συστημάτων ασύρματης επικοινωνίας 6G και πέραν αυτών [50]	180
6.13	(Σύγκριση Cell-free MIMO και classic massive MIMO [50]	181
6.14	Περιπτώσεις χρήσης της 6G και Beyond τεχνολογίας [50]	183
6.15	Χρονοδιάγραμμα έργων για το 6G και Beyond συστήματα [50]	186



# Λίστα Πινάκων

2.1 Αναπαράσταση διαφορετικών υλοποιήσεων συνδυαστικών επιλογών [2] . . . . .	35
3.1 Είδη Λογικών καναλιών [14] . . . . .	65
3.2 Είδη καναλιών μεταφοράς[14] . . . . .	67
3.3 Εύρος Συχνοτήτων 2 (Frequency Range 2, FR2)[10] . . . . .	88
3.4 Εύρος Συχνοτήτων 1 (Frequency Range 1, FR1)[10] . . . . .	89
4.1 Σύγκριση πρωτοκόλλων μετάδοσης [2] . . . . .	109
6.1 Διευθυνσιοδότηση οντοτήτων . . . . .	165
6.2 Συγκεντρωτικός πίνακας νέων τεχνολογιών και ανοικτών θεμάτων	185

# Περίληψη

Οι σύγχρονες τεχνολογικές εξελίξεις απαιτούν την αναθεώρηση της αρχιτεκτονικής των δικτύων για την ικανοποίηση τους. Τα συστήματα 5G είναι μία υποψήφια τεχνολογία που αναμένεται να επιλύσει προβλήματα τόσο συνδεσιμότητας όσο και διακίνησης δεδομένων. Η εργασία αυτή πραγματεύεται την αρχιτεκτονική του 5G στις εκδόσεις που έχει δρομολογηθεί να υλοποιηθεί αλλά και σε αυτές που ήδη μελετούνται για το μέλλον, ώστε να αποτελέσουν σημείο εφαρμογής σε περιπτώσεις όπως αυτές που ορίζει το τρίπτυχο "χαμηλή καθυστέρηση, επικοινωνία μηχανών και ευρυζωνικές επικοινωνίες".

Εισάγοντας τα ανωτέρω στην έναρξη της εργασίας, εμβαθύνουμε στο δίκτυο κορμού που αποτελεί την πρώτη από τις δύο γενικές οντότητες που αποτελούν ένα τηλεπικοινωνιακό σύστημα και ειδικότερα ένα δίκτυο 5G. Αναλύονται οι περιπτώσεις δόμησης ενός τέτοιου δικτύου και διασυνδεσιμότητα μεταξύ των οντοτήτων. Επίσης, στο τρίτο κεφάλαιο αναλύουμε το δίκτυο πρόσβασης του 5G ως προς τα πρωτόκολλα επικοινωνίας, και γενικότερα τη λειτουργία του, και παρουσιάζεται η αρχιτεκτονική του και ορισμένα δομικά χαρακτηριστικά του.

Οι καινοτόμες προσεγγίσεις ενός 5G συστήματος το καθιστούν διαφορετικό από τα προγενέστερα τηλεπικοινωνιακά δίκτυα. Ένα πλήθος τέτοιων τεχνολογιών και τεχνικών αναδεικνύονται στο τέταρτο κεφάλαιο, που ολοκληρώνεται με την παρουσίαση πρωτοκόλλων που χρησιμεύουν για τη λειτουργία του συστήματος.

Το δεύτερο μέρος της εργασίας, αποτελεί το πρακτικό μέρος όπου καταγράφονται τα βήματα υλοποίησης αυτόνομου και μη αυτόνομου συστήματος 5G με έργα ανοικτού κώδικά, με πραγματικές συσκευές αλλά και με προσομοιωτές ανάλογα με την περίπτωση υλοποίησης. Η ανάλυση των αποτελεσμάτων και τα εξαγόμενα συμπεράσματα από τις υλοποιήσεις συγκεντρώνονται στο τελευταίο κεφάλαιο.

Κλείνοντας την εργασία, γίνεται αναφορά στις βελτιώσεις που επιδέχεται το αυτόνομο δίκτυο 5G, καθώς και στις ανάγκες που θα μας οδηγήσουν στην επόμενη από αυτό γενιά, την έκτη γενιά (6G) ή τα πιο μελλοντικά δίκτυα (Beyond) και θα γίνει κατανοητό ότι όλα αυτά τα συστήματα δεν αποτελούν απλά μια βελτίωση των προγενέστερων δικτύων αλλά μια νέα αρχή, μία επανάσταση, ένα άνοιγμα προς το μέλλον.

**Λέξεις-Κλειδιά:** Αυτόνομο σύστημα πέμπτης γενιάς(5G), Μη αυτόνομο σύστημα πέμπτης γενιάς(5G), Αρχιτεκτονική δικτύων, Δίκτυο κορμού, Δίκτυο πρόσβασης

# Summary

Modern technological developments require the revision of network architecture to their satisfaction. 5G systems are a candidate technology that is expected to solve both connectivity and data traffic problems. This thesis deals with the architecture of 5G in the versions that have been launched to be implemented but also in those that are already being studied for the future, so that they can be applied in cases such as those defined by the triptych "low latency, machine communication and broadband communications".

Introducing the above at the beginning of the thesis, we delve into the core network which is the first of the two general entities that constitute a telecommunications system and in particular a 5G network. The cases of building such a network and interconnection between entities are analyzed. Also, in the third chapter we analyze the 5G access network in terms of communication protocols, and its operation in general, and presents its architecture and some structural features.

Innovative approaches to a 5G system make it different from previous telecommunications networks. A number of such technologies and techniques are highlighted in the fourth chapter, which concludes with the presentation of protocols that serve the operation of the system.

The second part of the thesis, is the practical part where the steps of implementation of autonomous (stand alone) and non-autonomous (non-stand alone) 5G system are recorded with open source projects, with real devices but also with simulators depending on the case of implementation. The analysis of the results and the conclusions drawn from the implementations are summarized in the last chapter.

Closing the thesis, reference is made to the improvements that the stand alone 5G network can make, as well as to the needs that will lead us to the next generation, the sixth generation (6G) or the more future networks (Beyond) and it will be understood that all this systems are not just an improvement on previous networks but a new beginning, a revolution, an opening to the future.

**Keywords:** Fifth generation (5G) standalone system, Fifth generation (5G) non-standalone system, Network architecture, core network, Access network

# ΜΕΡΟΣ Ι

## Θεωρία





# Κεφάλαιο 1

## Εισαγωγή

### 1.1 Ιστορική αναδρομή

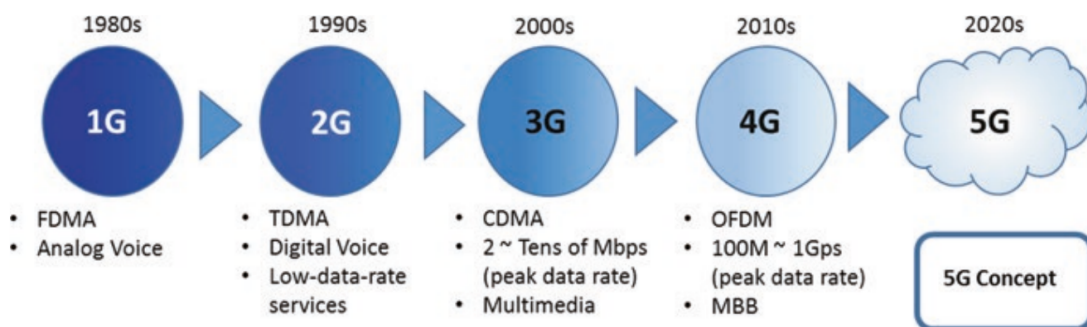
**Η** πρώτη γενιά (1G) κυψελοειδών συστημάτων εισήχθη το 1980 για μετάδοση φωνής. Η πολλαπλή πρόσβαση με διαίρεση συχνότητας (FDMA) χρησιμοποιήθηκε ως τεχνική πρόσβασης στο σύστημα RAN 1G και απαιτούσε μεγάλο κενό μεταξύ των καναλιών για να αποφευχθεί η παρεμβολή και επιπλέον, κάθε κανάλι, είχε τη δυνατότητα να εξυπηρετεί μόνο έναν χρήστη. Με την πάροδο του χρόνου ο αριθμός των χρηστών αυξήθηκε και το σύστημα 1G υπέφερε λόγω περιορισμένης χωρητικότητας, κακής ποιότητας φωνής καθώς και ζητημάτων κλιμάκωσης.[32]

Για να ξεπεραστούν αυτά τα μειονεκτήματα, αναπτύχθηκαν τεχνολογίες κινητής τηλεφωνίας 2G (δηλαδή, GSM, D-AMPS) που βασίστηκαν σε πολλαπλή πρόσβαση με διαίρεση χρόνου (TDMA). Παρόλο που το TDMA επέτρεπε σε πολλούς χρήστες ανά μεμονωμένο κανάλι να χρησιμοποιούν κοινό χρόνο μετάδοσης, εξακολουθούσε να απαιτεί μεγάλα κενά μεταξύ των καναλιών για να αποφευχθούν παρεμβολές. Έτσι, για να βελτιωθεί περαιτέρω η απόδοση των κυψελοειδών δικτύων, εισήχθη η τρίτη γενιά (3G) των οποίων τα βασικά χαρακτηριστικά ήταν υψηλότερη χωρητικότητα και υψηλότεροι ρυθμοί δεδομένων. Το 3G χρησιμοποιούσε την τεχνική πολλαπλής πρόσβασης διαίρεσης κώδικα (CDMA) η οποία βασίζεται στη χρήση των ίδιων συχνοτήτων μεταξύ πολλαπλών χρηστών για ταυτόχρονη μετάδοση.[32]

Αν και το CDMA προσέφερε πολλά πλεονεκτήματα έναντι του προκατόχου του, όπως η βελτίωση της ποιότητας της φωνής και η καλύτερη ασφάλεια, απαιτούσε την κατασκευή νέας υποδομής καθώς και ένα ακριβό τέλος αδειοδότησης φάσματος για τους παρόχους. Επιπλέον, ο πολλαπλασιασμός νέων συσκευών πρόσβασης και η εισαγωγή νέων υπηρεσιών όπως η ροή βίντεο και τα μέσα κοινωνικής δικτύωσης έθεσαν ακόμη υψηλότερες απαιτήσεις QoS για τους χειριστές, υποχρεώνοντας τους να βελτιώσουν περαιτέρω την ικανότητα των υπάρχοντων κυψελοειδών συστημάτων ώστε να μετακινηθούν από ένα σύστημα βασισμένο στην εξυπηρέτηση φωνής, σε ένα σύστημα βάσει δεδομένων.

Αυτό οδήγησε στην εισαγωγή της τέταρτης γενιάς (4G) κυψελοειδών δικτύων που είναι ένα πραγματικό σύστημα βασισμένο σε IP με ακόμη υψηλότερους ρυθμούς δεδομένων και χωρητικότητας. Ακόμη, πολλές νέες δυνατότητες, όπως η συνάθροιση ζώνης (band aggregation), η

πρόσβαση πολυπλεξίας ορθογωνικής διαίρεσης συχνότητας (OFDMA) ως σχήμα πρόσβασης, οι κεραιές πολλαπλών εισόδων και πολλαπλών εξόδων (MIMO) και η διαμόρφωση δέσμης προστέθηκαν στο πρότυπο 4G για τη βελτίωση των υψηλών ποσοστών δεδομένων και της χωρητικότητας. Επιπλέον, ο αριθμός των συνδεδεμένων συσκευών με τεράστιες απαιτήσεις εύρους ζώνης σε κυψελοειδή δίκτυα αναμένεται να αυξηθεί περαιτέρω λόγω της υιοθέτησης βιομηχανικών τεχνολογιών και της ανάπτυξης συσκευών Internet of Things χαμηλού κόστους. Η εικόνα 1.1 παρουσιάζει ένα χρονοδιάγραμμα εξέλιξης των κυψελωτών συστημάτων.[32][40]



Εικόνα 1.1: Σχηματική αναπαράσταση ιστορικής εξέλιξης κυψελωτών συστημάτων[40]

Για να αντιμετωπιστεί η τεράστια αύξηση της κίνησης δεδομένων κινητής τηλεφωνίας, όπως αναδεικνύουν διάφορες στατιστικές μελέτες και εξαγόμενα στοιχεία, είναι απαραίτητος ο αποτελεσματικός σχεδιασμός του δικτύου μεταβαίνοντας σε μία νέα γενιά, την πέμπτη γενιά που χαρακτηρίζεται ως 5 Generation(5G). Έτσι, το πρότυπο 5G θα καθοδηγήσει τα μελλοντικά κυψελοειδή δίκτυα. Επιπλέον, καταβάλλονται πολλές προσπάθειες τόσο από τη βιομηχανία όσο και από τον ακαδημαϊκό κόσμο για την ικανοποίηση των απαιτήσεων που θέτουν αυτά τα δίκτυα 5G. Τα κυψελοειδή δίκτυα 5G προορίζονται να παρέχουν μέγιστους ρυθμούς δεδομένων έως 10 Gbps, καθυστέρηση έως 1 ms, 1000 × αριθμούς συσκευών, 10 φορές ενεργειακή απόδοση και υψηλή αξιοπιστία, αντίστοιχα, σύμφωνα με στοιχεία του οργανισμού METIS.

Η τεχνολογία 5G αναμένεται να παρέχει συνδεσιμότητα και ανάγκες επικοινωνίας με συγκεκριμένες λύσεις σε κάθετους τομείς όπως η αυτοκινητοβιομηχανία, η υγειονομική περίθαλψη, η κατασκευή, η ψυχαγωγία και άλλους τομείς με οικονομικά αποδοτικό τρόπο. Αξίζει να σημειώσουμε ότι αυτές οι νέες υπηρεσίες έχουν πολύ διαφορετικές απαιτήσεις, επομένως, η ύπαρξη παραδοσιακών λύσεων δικτύων πρόσβασης και βασικής διαχείρισης για κάθε υπηρεσία δεν μπορεί να εγγυηθεί την τελική ποιότητα των υπηρεσιών (Quality of Service, QoS) του χρήστη. Επιπλέον, έχει παρατηρηθεί και κάποια σταδιακή βελτίωση λόγω της εγκατάστασης μικρών κυψελών υπό κάλυψη μακροκυψελών (δηλ. Ετερογενών δικτύων (HetNets)) ειδικά σε περιοχές με συμφόρηση. Η ιδέα του HetNets έχει ήδη εφαρμοστεί σε τρέχοντα δίκτυα. Άλλες πολλά υποσχόμενες προσεγγίσεις για την ενεργοποίηση του μελλοντικού δικτύου πρόσβασης (Access Network, AN) περιλαμβάνουν την

ενεργοποίηση της επικοινωνίας συσκευής σε συσκευή (Device-to-Device, D2D) για τη μείωση της κίνησης δικτύου, την εγκατάσταση αποθήκευσης προσωρινής μνήμης στα δίκτυα πρόσβασης για τη μείωση των καθυστερήσεων, εκτελώντας υπολογισμούς στους τοπικούς σταθμούς βάσης για αναλύσεις σε πραγματικό χρόνο και επιτρέποντας τη χρήση φάσματος χωρίς άδεια όπως το LTE-unlicensed (LTE-U) για την περαιτέρω ενίσχυση της χωρητικότητας του δικτύου [32].

## 1.2 Ανάγκες που μας οδήγησαν στο 5G

Ως αποτέλεσμα των μαζικών τεχνολογικών επαναστάσεων, οι τελικοί χρήστες έχουν αυξηθεί δραστικά. Για να ανταποκριθεί σε τέτοιες δραστικές απαιτήσεις, η ITU έχει ταξινομήσει τις μελλοντικές υπηρεσίες 5G σε τρεις κύριες κατηγορίες που αποτελούνται από εξαιρετικά αξιόπιστη επικοινωνία χαμηλής καθυστέρησης, βελτιωμένη κινητή ευρυζωνική σύνδεση και υπηρεσίες μαζικής επικοινωνίας τύπων μηχανών. Η υπάρχουσα αρχιτεκτονική δικτύου κινητής τηλεφωνίας σχεδιάστηκε για να ικανοποιεί τις απαιτήσεις για υπηρεσίες φωνητικής και συμβατικής ευρυζωνικής κινητής τηλεφωνίας (MBB). Επιπλέον, οι προηγούμενες κυψελοειδής γενιές σχεδιάστηκαν κυρίως για να ικανοποιούν μόνο τις ανθρώπινες επικοινωνιακές απαιτήσεις, όπως φωνή και δεδομένα. Ωστόσο, τα δίκτυα 5G αναμένεται να διευκολύνουν τη βιομηχανική επικοινωνία, προκειμένου να αναπτυχθεί η ψηφιοποίηση της βιομηχανίας. Έτσι, επιτρέπονται καινοτόμες υπηρεσίες και δυνατότητες δικτύωσης για νέους φορείς της βιομηχανίας.[40]

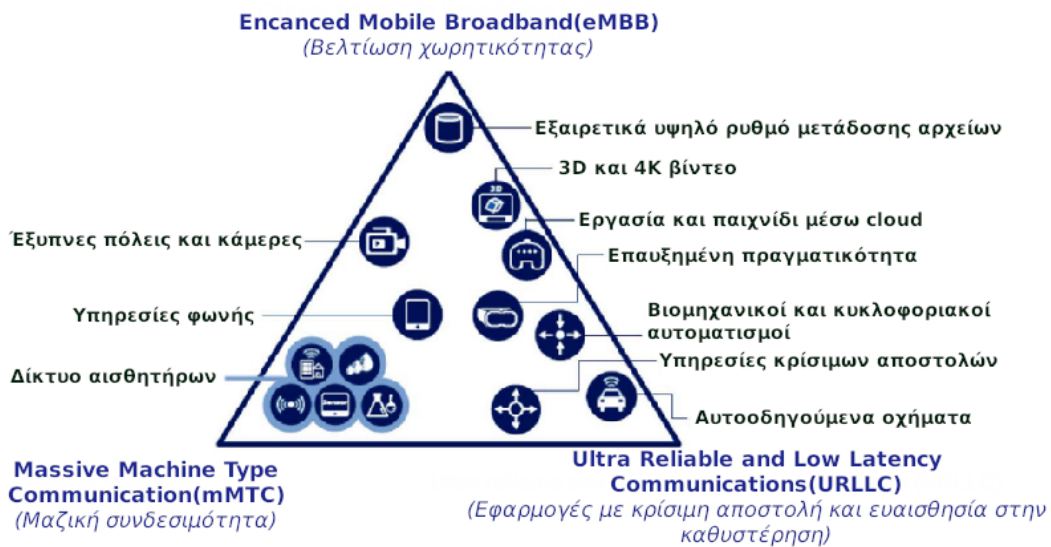
Συνεπώς, η βασική ιδέα για την ανάπτυξη του δικτύου 5g δεν ήταν απλά μια βελτίωση του προηγούμενου 4g αλλά μία διαφορετική φιλοσοφία, που φιλοδοξεί στην επίλυση τριών βασικών προβλημάτων.

Αρχικά, όσον αφορά τις ευρυζωνικές κινητές επικοινωνίες η βελτίωση τους που όπως αναφέραμε ονομάζεται enhanced mobile broadband (eMBB) στοχεύει στην εξυπηρέτηση πιο πυκνοκατοικημένων μητροπολιτικών κέντρων με ταχύτητες κατερχόμενης ζεύξης που πλησιάζουν το 1 Gbps επιτυγχάνοντας παράλληλα βελτίωση στη χωρητικότητα καναλιού.

Δεύτερον, η υπηρεσία Massive Machine Type Communications (mMTC) ενεργοποιεί τεχνολογίες machine-to-machine (M2M) και ικανοποιεί το μεγάλο πλήθος εφαρμογών Internet of Things (IoT) με τέτοιο τρόπο ώστε να λειτουργούν ανεξάρτητα χωρίς επιβαρύνσεις στις άλλες κατηγορίες υπηρεσιών.

Τρίτον το λεγόμενο Ultra-Reliable and Low Latency Communications (URLLC) αντιμετωπίζει τις κρίσιμες ανάγκες επικοινωνιών όπου το εύρος ζώνης δεν είναι τόσο σημαντικό όσο η ταχύτητα και συγκεκριμένα η καθυστέρηση από άκρο σε άκρο η οποία στο 5g αγγίζει τιμές 1 ms ή λιγότερο και υλοποιεί μία αξιόπιστη επικοινωνία κυρίως σε ευαίσθητες ως προς την καθυστέρηση εφαρμογές. [34]

Μια σύνοψη τέτοιων εφαρμογών παρουσιάζει η παρακάτω εικόνα1.2



Εικόνα 1.2: Περιπτώσεις αξιοποίησης 5G τεχνολογίας [34]

### 1.3 Προκλήσεις κατά την πραγματοποίηση του 5G δικτύου

Για την επίτευξη των υπηρεσιών enhanced mobile broadband (eMBB), Massive Machine Type Communications (mMTC) και Ultra-Reliable and Low Latency Communications (URLLC) υπάρχουν ορισμένες προκλήσεις στην υλοποίηση του 5g που πρέπει να ληφθούν υπόψιν.[32]

Αρχικά ένα τέτοιο σύστημα θα πρέπει να βασίζεται στην:

- ▷ *Κλιμάκωση και Αξιοπιστία (Scalability and Reliability).*  
Ο σχεδιασμός ενός επεκτάσιμου δικτύου να μπορεί να στηρίξει τον τεράστιο αριθμό IoT συσκευών. Ο σχεδιασμός αυτός θα πρέπει επίσης να παρέχει αξιόπιστη λειτουργία.[32]
- ▷ *Διασυνδεσιμότητα (Interoperability)*  
Υπάρχουν πολλές ετερογενής IoT διατάξεις που τρέχουν διαφορετικά πρωτόκολλα και μία πρόκληση του 5g είναι να διασυνδέσει αυτές τις διαφορετικές τεχνολογίες οπότε θα πρέπει να υποστηρίξει τη διασυνδεσιμότητα.[32]
- ▷ *Βιωσιμότητα (Sustainability)*  
Η βιώσιμη λειτουργία δικτύου είναι επιτακτική, όσον αφορά τη μείωση του συνολικού κόστους λειτουργίας κάνοντας χρήση ανανεώσιμων πηγών ενέργειας ή χρησιμοποιώντας ενεργειακά αποδοτικό σχεδιασμό.[32]
- ▷ *Ασφάλεια (Security)*  
Επίσης τα δίκτυα 5G σκοπεύουν να αυξήσουν γρήγορα την ανάπτυξη κάθετης βιομηχανίας, η οποία επιβάλλει μεγάλη ποικιλία προκλήσεων ασφαλείας καθώς η βασιζόμενη στο λογισμικό υλοποίηση του εμπεριέχει τρωτά σημεία.[32]

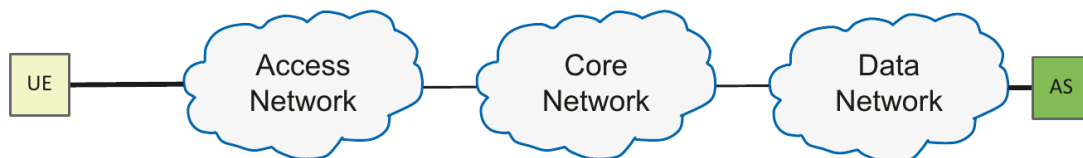
▷ *Τεμαχιζόμενο Δίκτυο (Network Slicing)*

Τέλος μία μεγάλη πρόκληση είναι η κατάτμηση του δικτύου, το network slicing, που εκτός από μία μεμονωμένη τεχνική, τελικά βοηθά γενικότερα και στην επίλυση των παραπάνω θεμάτων.[32]

Στόχος τη μελλοντικής εξέλιξης του 5G δικτύου, όπου οι επόμενες εκδόσεις αποκαλούνται γενικευμένα ως “Beyond”, είναι να αποτελούνται από ένα συνονθύλευμα νέων τεχνολογιών όπως η εικονικοποίηση, αρχιτεκτονικές Cloud, υλοποίηση Containers και μικροπηρεσιών αλλά και αυτοματισμοί. Όλα αυτά, αναλύονται σε επόμενα κεφάλαια. [32]

## 1.4 Επισκόπηση αρχιτεκτονικής και σχεδίασης του δικτύου 5G

Όπως στο 4G (LTE / EPC) και τις προηγούμενες γενιές, το σύστημα 3GPP 5G καθορίζει την αρχιτεκτονική για επικοινωνία μεταξύ εξοπλισμού χρήστη (User Equipment, UE) και τελικού σημείου, όπως διακομιστή εφαρμογών (Application Server, AS) στο δίκτυο δεδομένων (Data Network, DN), ή άλλο UE. Η αλληλεπίδραση μεταξύ του UE και του Δικτύου Δεδομένων γίνεται μέσω του Δικτύου Πρόσβασης (Access Network, AN) και του Δικτύου Πρόσβασης (Core Network, CN) όπως ορίζεται από τα Πρότυπα 3GPP. Το σχήμα 1.3 απεικονίζει μια απλή αναπαράσταση μιας αρχιτεκτονικής από άκρο σε άκρο. Σε αυτή την εργασία στο δεύτερο κεφάλαιο εστιάζουμε στην περιγραφή του 5G Core όπως ορίζεται από τα πρότυπα 3GPP 5G για PLMN και στο κεφάλαιο 3 περιγράφουμε το δίκτυο πρόσβασης που αναφέρεται στο 3GPP ως δίκτυο ράδιο πρόσβασης (RAN).[40]



Εικόνα 1.3: Αναπαράσταση αρχιτεκτονικής σχεδίασης end-to-end [40]

Σε πολύ υψηλό επίπεδο, το Core και το RAN αποτελούνται από πολλές λειτουργίες δικτύου που σχετίζονται με λειτουργίες επιπέδου ελέγχου (Control Plane) και επιπέδου χρήστη (User Plane). Τα πραγματικά δεδομένα (αναφέρονται επίσης ως δεδομένα χρήστη) μεταφέρονται συνήθως μέσω μιας διαδρομής στο επίπεδο χρήστη, ενώ το επίπεδο ελέγχου χρησιμοποιείται για τον καθορισμό της διαδρομής στο επίπεδο χρήστη. Η υπηρεσία σύντομων μηνυμάτων (Short Message Service, SMS) είναι μια εξαίρεση στην οποία τα δεδομένα (σύντομο μήνυμα) κοινοποιούνται μέσω του Control Plane.[40]

Η αρχιτεκτονική του συστήματος 5G (5GS) εκπροσωπείται με δύο τρόπους στα πρότυπα 3GPP. Ο ένας είναι μια αναπαράσταση βάσει υπηρεσίας στην οποία οι λειτουργίες δικτύου επιπέδου ελέγχου έχουν πρόσβαση στις υπηρεσίες του άλλου, και ο άλλος είναι μια αναπαράσταση σημείου αναφοράς στην οποία η αλληλεπίδραση μεταξύ λειτουργιών δικτύου εμφανίζονται με

σημεία αναφοράς από σημείο σε σημείο. Περαιτέρω ανάλυση αυτών στο κεφάλαιο 2. [40]

Η αρχιτεκτονική που βασίζεται στις διαφορετικές υπηρεσίες, είναι η βάση για το δίκτυο πυρήνα του 5G. Αυτό σημαίνει ότι η προδιαγραφή ενός 5g δικτύου εστιάζεται στις υπηρεσίες και τις λειτουργίες που παρέχονται από το βασικό δίκτυο και όχι από εξωτερικούς κόμβους. Με επέκταση αυτών των λειτουργιών σε virtualization/containerization περιβάλλοντα επιτυγχάνουμε το τρίπτυχο uLLC,eMBB,mMTC που αναφέρεται σε ένα δίκτυο που διασυνδέει διαφορετικές διατάξεις κατά ζήτηση μεταξύ τους, με χαμηλή καθυστέρηση και μεγάλο ρυθμό δεδομένων.

### 1.4.1 Αυτόνομη και μη αυτόνομη ανάπτυξη 5G δικτύου

Η αρχική προσεγγιστική υλοποίηση του 5G έγινε με μη αυτόνομο τρόπο, δηλαδή με μία βελτίωση στο δίκτυο πυρήνα του 4G που ονομάζεται Evolved Packet Core(EPC), διαχωρίζοντας υπηρεσίες επιπέδου ελέγχου και επιπέδου χρήστη ώστε να γίνει η εισαγωγή στη φιλοσοφία που θέτει ο αυτόνομος πυρήνας του 5G.

Το EPC βελτιώθηκε με ένα προαιρετικό χαρακτηριστικό που επιτρέπει το διαχωρισμό του επιπέδου ελέγχου και του επιπέδου χρήστη στην έκδοση 14 της 3GPP. Σε αυτήν τη δυνατότητα, το Serving Gateway (SGW) και το Packet Gateway (PGW) χωρίζονται σε ξεχωριστές λειτουργίες επιπέδου ελέγχου και επιπέδου χρήστη (π.χ. SGW-C και SGW-U). Αυτή η προαιρετική δυνατότητα παρέχει περισσότερη ευελιξία και αποδοτικότητα στην ανάπτυξη δικτύου. Στην αρχιτεκτονική 5G, ο διαχωρισμός επιπέδου ελέγχου και επιπέδου χρήστη είναι εγγενής ικανότητα. Η συνάρτηση διαχείρισης συνεδρίας (SMF) χειρίζεται τη λειτουργικότητα του επιπέδου ελέγχου για τη ρύθμιση και τη διαχείριση των περιόδων σύνδεσης, ενώ τα πραγματικά δεδομένα χρήστη δρομολογούνται μέσω της λειτουργίας επιπέδου χρήστη (UPF). Η επιλογή UPF (ή επανεκλογή αυτής) γίνεται από το SMF. Οι επιλογές ανάπτυξης επιτρέπουν το UPF σε κεντρική τοποθεσία ή / και το κατανεμημένο UPF που βρίσκεται κοντά ή μέσα στο Δίκτυο πρόσβασης.[2][40]

Στο EPC, η λειτουργικότητα διαχείρισης κινητικότητας και η λειτουργικότητα διαχείρισης συνεδρίας διαχειρίζονται από το Mobility Management Entity (MME). Στο 5GC, αυτές οι λειτουργίες χειρίζονται ξεχωριστές οντότητες. Η λειτουργία Access and Mobility Management (AMF) χειρίζεται τη διαχείριση και τις διαδικασίες κινητικότητας. Το AMF είναι σημείο τερματισμού για τη σύνδεση επιπέδου ελέγχου του (Ραδιο) Δίκτυο Πρόσβασης ((R) AN) και UE. Η σύνδεση μεταξύ UE και AMF (η οποία διασχίζει το RAN) αναφέρεται ως συστρωμάτωμα μη πρόσβασης (Non-Access Stratum, NAS). Η συνάρτηση διαχείρισης συνόδου (SMF) χειρίζεται τις διαδικασίες διαχείρισης συνόδου. Ο διαχωρισμός της κινητικότητας και οι λειτουργίες διαχείρισης συνεδρίας επιτρέπουν σε ένα AMF να υποστηρίζει διαφορετικά δίκτυα πρόσβασης (3GPP και non-3GPP), ενώ το SMF μπορεί να προσαρμοστεί για συγκεκριμένες προσβάσεις. Μία ανάλυση όλων των αυτών και πολλών ακόμα λειτουργιών παρουσιάζεται στο κεφάλαιο 2.[2][40]

Τελικά, το αποτέλεσμα εργασιών 3GPP για την αρχιτεκτονική δικτύου 5G ήταν ένας αριθμός από επιλέξιμες αρχιτεκτονικές, και με βάση το 3GPP

λήφθηκαν τρεις σημαντικές αποφάσεις:

- Καθορίστηκε ότι το LTE μπορεί να υποστηρίξει τη νέα 5G αρχιτεκτονική
- Καθορίστηκε η υποστήριξη του συνδυασμού LTE και NR στο δίκτυο πρόσβασης
- Καθορίστηκε μία εναλλακτική 5G αρχιτεκτονική βασισμένη στην εξέλιξη του LTE/EPC

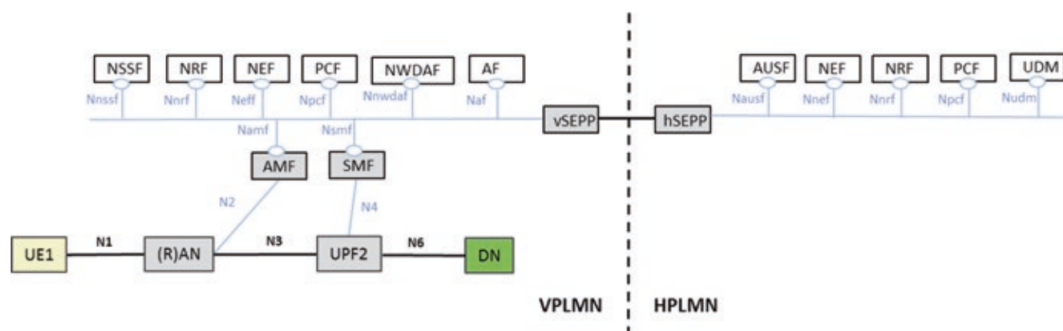
Έτσι, όταν το LTE “συμβάλλει” στην υλοποίηση, τότε το δίκτυο ονομάζεται ως *Μη-αυτόνομο δίκτυο 5G (5G Non-Stand Alone)* ενώ όταν υλοποιείται με αμιγώς δικές του λειτουργίες αναφέρεται ως *Αυτόνομο δίκτυο 5G(5G Stand Alone)*.

Το γεγονός ότι η υποστήριξη πρόσβασης LTE καθορίζεται για τη νέα αρχιτεκτονική 5G σημαίνει ότι ένα δίκτυο πρόσβασης LTE στην πράξη έχει δύο τρόπους σύνδεσης με ένα κεντρικό δίκτυο.[2]

1. Χρήση συνδεσιμότητας S1 σε κεντρικό δίκτυο EPC
2. Χρήση N2 / N3 σε δίκτυο πυρήνα 5GC

### Περιοχή στο 5G

Η εικόνα 1.4 δείχνει μια αρχιτεκτονική περιοχής με τοπικό ξεμπλοκάρισμα στο Επισκεπτόμενο PLMN (VPLMN). Σε αυτό το σενάριο η ενοποιημένη διαχείριση δεδομένων (UDM), η οποία περιλαμβάνει τις πληροφορίες συνδρομής και τη λειτουργία διακομιστή ελέγχου ταυτότητας (AUSF), η οποία περιλαμβάνει τα δεδομένα ελέγχου ταυτότητας / εξουσιοδότησης, βρίσκονται στο οικιακό PLMN (HPLMN). Σημειώνεται, ότι η Υπηρεσία PLMN μπορεί να είναι είτε το HPLMN (δηλαδή, μη περιοχής) είτε ένα VPLMN. Υπάρχει επίσης Security Edge Protection Proxies (SEPP) που προστατεύουν την επικοινωνία μεταξύ του οικιακού και του PLMN που επισκέπτεται. Η UE επικοινωνεί στο Δίκτυο Δεδομένων (DN) μέσω των Λειτουργιών επιπέδου χρήστη (UPF) στο VPLMN. Το AMF και η λειτουργία διαχείρισης συνεδριών (SMF) που χειρίζονται την κινητικότητα και τη διαχείριση συνεδρίας για το UE βρίσκονται επίσης στο VPLMN.[40]



Εικόνα 1.4: Περιοχή 5G συστήματος-Τοπικό σενάριο ξεμπλοκαρίσματος [40]



Εν κατακλείδι, η βασική σχεδιαστική επιλογή, της βασικής αρχιτεκτονικής του 5ης γενιάς κινητών επικοινωνιών διαφέρει στα ακόλουθα:

- Αποτελεί μια ευέλικτη και επεκτάσιμη αρχιτεκτονική δικτύου βάσει υπηρεσιών
- Επιτρέπει διαφορετικές διαμορφώσεις πυρήνα δικτύου σε διαφορετικά τμήματα δικτύου και επιτρέπει απομόνωση πόρων μεταξύ slice δικτύου
- Επιτρέπει σε έναν εξοπλισμό χρήστη(UE) να συνδέεται ταυτόχρονα σε πολλά τμήματα δικτύου (περισσότερα από την περίπτωση των πολλαπλών APN)
- Υποστήριξη ταυτοποίησης και ελέγχου ταυτότητας συνδρομητή με βάση το IMSI, καθώς και ταυτότητας εκτός IMSI, σε ένα ενοποιημένο πλαίσιο ελέγχου ταυτότητας με βάση το EAP
- Διαχωρισμός επιπέδου ελέγχου (CP) και επιπέδου χρήστη (UP) έτσι ώστε:
  - o Να επιτρέπεται η δυνατότητα κλιμάκωσης των λειτουργιών UP και CP ανεξάρτητα
  - o Να επιτρέπεται μια ευέλικτη ανάπτυξη του UP χωριστά από το CP, δηλαδή αποκέντρωση από την κεντρική τοποθεσία ή την κατακεντρωμένη (απομακρυσμένη) τοποθεσία (δηλαδή χωρίς περιορισμό στην τοποθεσία σε σύγκριση με το CP).
- Υποστηρίζει μια γενικότερη λειτουργία user-plane που επιτρέπει τόσο κεντρικές όσο και κατακεντρωμένες αναπτύξεις σε ένα δίκτυο καθώς και και τη δυνατότητα να έχουν διαφορετικά instances της λειτουργίας UP, συγκεντρωμένες και διανεμημένες ταυτόχρονα βελτιώνοντας την ευρυζωνική κινητή τηλεφωνία(eMBB).
- Ενοποιημένο πλαίσιο πολιτικής με επεκτάσεις από το πλαίσιο πολιτικής στο EPC
- Τεμαχισμός των λειτουργιών του τομέα μεταφοράς δικτύου 3GPP για να επιτρέπεται η ανεξάρτητη εξέλιξη και να επιτρέπεται στους παρόχους υπηρεσιών να χρησιμοποιούν διαφορετικές τεχνολογίες μεταφοράς (π.χ. Ethernet, MPLS, μεταφορά βασιζόμενη σε SDN, εικονικοποίηση λειτουργιών) εξοικονομώντας πόρους, πετυχαίνοντας χαμηλή καθυστέρηση(ULLC).
- Ευελιξία ως προς τον διαμοιρασμό και επαναχρησιμοποίηση των λειτουργιών του πυρήνα για προσάρτηση διαφόρων τεχνολογιών(μηχανές, βιομηχανικά εργαλεία, κλπ) (massive machine type communication, mMTC)
- Υποστήριξη σύγκλισης ασύρματης γραμμής και ασύρματης πρόσβασης. Γενικότερα απαιτείται μια αρχιτεκτονική που υποστηρίζει τεχνολογίες παλαιού τύπου και 5G Core. Τα επίπεδα χρήστη υποστηρίζουν πολλαπλές προσβάσεις και βελτιστοποιούνται για υψηλή απόδοση

## 1.5 Έκδοσεις κυκλοφορίας 5G της κοινοπραξίας 3GPP

Το 5G Core περιγράφεται σε ένα σύνολο προδιαγραφών που αναπτύχθηκε από το 3ο Generation Partnership Project (3GPP) και καταγράφηκε στην έκδοση (Release 15, Rel-15) καθώς και σε επόμενες κυκλοφορίες. Το Rel-15 ήταν το πρώτο πλήρες σύνολο προτύπων 5G και κυκλοφόρησε σε διάφορα βήματα μεταξύ Ιουνίου 2018 και στις αρχές του 2019. Το Rel-16 έχει προγραμματιστεί να κυκλοφορήσει στις αρχές του 2020 και ο προγραμματισμός των εργασιών έχει ξεκινήσει την Κυκλοφορία-17 με στόχο να είναι έτοιμες οι προδιαγραφές το 2021 ή το 2022.[2]

### 1.5.1 Έκδοση-15

Η έκδοση 15 περιλαμβάνει προδιαγραφές όπως μη αυτόνομη αρχιτεκτονική (Non-Stand Alone) (NSA), δηλ. New Radio (NR) που χρησιμοποιείται με το LTE και βασικό δίκτυο υποδομής EPC, Αρχιτεκτονική για αυτόνομο δίκτυο (SA), δηλαδή, το NR συνδέεται με το δίκτυο πυρήνα 5G (5GC), 5GC χρησιμοποιώντας μια αρχιτεκτονική βάσει υπηρεσιών (SBA), υποστήριξη εικονικοποιημένης ανάπτυξης, λειτουργίες δικτύου για την παροχή εγγραφής, διαγραφής, εξουσιοδότησης, κινητοποίησης και ασφάλειας, επικοινωνία δεδομένων με δεδομένα IP, υποστήριξη ταυτόχρονης τοπικής και κεντρικής πρόσβασης σε δίκτυο δεδομένων, υποστήριξη για Edge Computing, τεμαχισμός δικτύου, ενοποιημένος έλεγχος πρόσβασης, συγκεντρωτική αρχιτεκτονική για υποστήριξη πρόσβασης non-3GPP, πλαίσιο πολιτικής και υποστήριξη QoS, έκθεση δυνατοτήτων δικτύου, Multi-Operator Core Network, δηλαδή κοινή χρήση του ίδιου NG-RAN από πολλαπλά δίκτυα πυρήνα, υποστήριξη συγκεκριμένων υπηρεσιών, όπως SMS, IMS, Υπηρεσίες τοποθεσίας για έκτακτη ανάγκη, σύστημα δημόσιας προειδοποίησης (Public Warning System, PWS), υπηρεσίες προτεραιότητας πολυμέσων (Multimedia Priority Services, MPS), αποστολή κρίσιμων υπηρεσιών (Mission Critical Services, MCS), απενεργοποίηση δεδομένων PS και τέλος συνεργασία μεταξύ 5G και 4G.[2][42]

### 1.5.2 Έκδοση-16

Η έκδοση 16 έχει οριστεί να περιέχει πολλές προσθήκες, αρκετές από τις οποίες απευθύνονται ειδικά σε διαφορετικούς κλάδους κάθετης βιομηχανίας (V2X), απόκτηση πρόσβασης στην υποστήριξη του συστήματος διεύθυνσης κυκλοφορίας, μεταγωγής και διαχωρισμού στην αρχιτεκτονική του συστήματος 5G (Access Traffic Steering, Switch and Splitting, ATSSS), υποστήριξη και εξέλιξη κυψελοειδούς IoT για το σύστημα 5G (5G CioT), ενεργοποιητές για αυτοματοποίηση δικτύου για 5G (Enablers for Network Automation, eNA), βελτίωση τοπολογίας SMF και UPF σε δίκτυα 5G (Enhancing Topology of SMF and UPF in 5G Networks, ETSUN), βελτίωση στις υπηρεσίες τοποθεσίας 5GC (Enhancement to the 5GC Location Services, 5G eLCS), ενισχυμένη ενοποίηση IMS σε 5GC (Enhanced IMS to

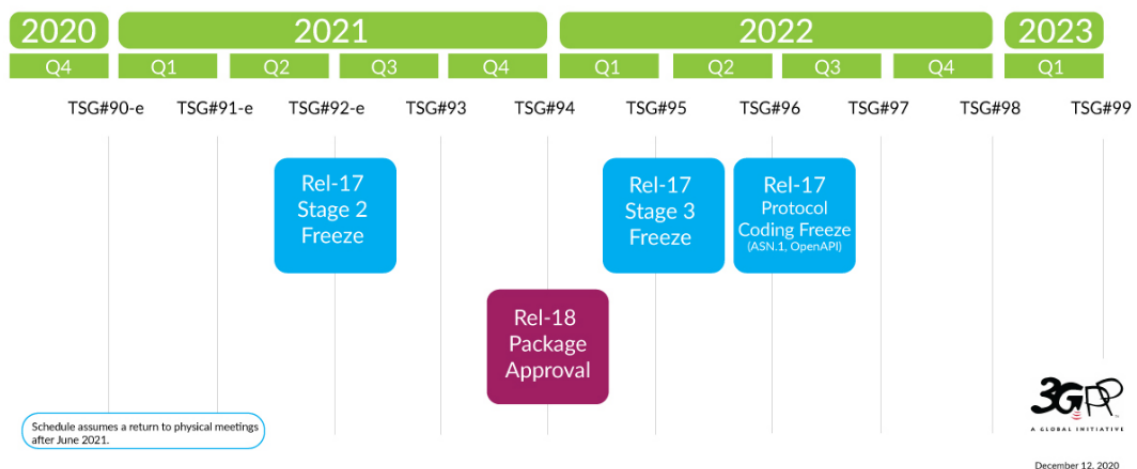
5GC Integration, eIMS5G SBA), 5GS ενισχυμένη υποστήριξη Vertical και LAN Services, βελτιώσεις συστήματος για παροχή πρόσβασης σε περιορισμένες τοπικές υπηρεσίες χειριστή από μη εξουσιοδοτημένα UE (PARLOS) όχι για 5G, βελτιώσεις στην αρχιτεκτονική συστήματος 5G βάσει υπηρεσιών (5G eSBA), βελτίωση υποστήριξης URLLC σε 5GC (5G URLLC), συνεργασία και συνύπαρξη δεδομένων χρήστη (User Data Interworking and Coexistence, UDI-COM), βελτιστοποιήσεις για UE ραδιοφωνική ικανότητα (Radio Capability Signaling RACS) και τέλος υποστήριξη καλωδίων (5WWC). [2][42]

### 1.5.3 Έκδοση-17

Η έκδοση 17 που είναι υπο ανάπτυξη και ορισμένες από τις προδιαγραφές που πρόκειται να περιέχει είναι το NR MIMO, η βελτίωση NR sidelink<sup>1</sup>, 52.6-71 GHz κυματομορφές, βελτίωση δυναμικού διαμοιρασμού φάσματος(DDS), βελτίωση βιομηχανικών IoT και URLLC, NR καθώς και μελέτη IoT πάνω σε μη επίγεια δίκτυα (NTN) και NR eXtended Reality (XR), βελτίωση NR εύρεση θέσης, χαμηλή πολυπλοκότητα NR διατάξεων, εξοικονόμηση ενέργειας, βελτίωση κάλυψης NR και βελτίωση NB-IoT και LTE-MTC. Επίσης, αναπτύσει τις πολλαπλές sim καθώς και ασχολείται περαιτέρω με τεμαχισμό τόσο του δικτύου πρόσβασης όσο και του κορμού, και βελτιώνει τη 5G multicast μετάδοση, το multi-radio DCCA και την ολοκλήρωση της πρόσβασης και του backhaul δικτύου. Τέλος, περιέχει προδιαγραφές για λειτουργίες όπως NR Quality of Experience, διαχωρισμός LTE Control και User επιπέδου, μη δημόσια δίκτυα, εναέριες και δορυφορικές διασυνδέσεις και βελτίωση του UPF για έλεγχο και 5G SBA αρχιτεκτονική.[42]

### 1.5.4 Έκδοση-18

Η έκδοση 18 αναμένεται να εγκριθεί εντός του 2021 και να δημοσιοποιηθούν οι σχετικές προδιαγραφές εργασιών. Στην παρακάτω εικόνα αναπαρίσταται το χρονοδιάγραμμα της 3GPP σχετικά με την χρονική εξέλιξη των εκδόσεων.[42]



Εικόνα 1.5: Χρονοδιάγραμμα εκδόσεων 3GPP για το 5G-NR [42]

<sup>1</sup> Διασύνδεση που ενεργοποιεί την επικοινωνία μεταξύ όμοιων συσκευών (Device-to-Device)

## 1.6 Οργανισμοί ανάπτυξης 5G συστημάτων

### 1.6.1 Περιφερειακή ανάπτυξη / προώθηση του 5G

Ενώ η Διεθνής ένωση Τηλεπικοινωνιών (International Telecommunications Union- Radiocommunication Sector, ITU-R) παίζει τον κεντρικό ρόλο για τον καθορισμό της κατάλληλης τεχνολογίας για κάθε γενιά δικτύου κινητής τηλεφωνίας, η ανάπτυξη της τεχνολογίας διεξάγεται από οργανισμούς τυποποίησης της ανάπτυξης (Standard Development Organizations, SDOs). Το 1998, το έργο εταιρικής σχέσης τρίτης γενιάς (3ο Generation Partnership Project, 3GPP) ξεκίνησε από τους βασικούς παράγοντες της ανάπτυξης του δικτύου κινητής τηλεφωνίας και κέρδισε την υποστήριξη έξι περιφερειακών SDO από την Ευρώπη, την Κίνα, την Ιαπωνία, την Κορέα και την Αμερική. Έτσι, άρχισε να βάζει τα θεμέλια της παγκόσμιας ανάπτυξης για κινητές τεχνολογίες και να προσελκύει τη συμμετοχή μιας ποικιλίας φορέων της βιομηχανίας και της ακαδημαϊκής κοινότητας. Το 3GPP έχει εξελιχθεί σε βασικό οργανισμό προτύπων για την ανάπτυξη τεχνολογίας για δίκτυα κινητής τηλεφωνίας ήδη από το 3G. [40]

Αφού η ITU-R ξεκίνησε τη μελέτη επισκόπησης του 5G το 2012, ιδρύθηκαν αρκετές περιφερειακές ομάδες προώθησης και ερευνητικά φόρουμ στην Κίνα, την Ευρώπη, την Κορέα, την Ιαπωνία και την Αμερική. Αυτές οι περιφερειακές δραστηριότητες περιλαμβάνουν τη μελέτη των απαιτήσεων 5G, τις περιπτώσεις χρήσης και σεναρίων ανάπτυξης, καθώς και διερεύνηση των βασικών τεχνολογιών και της φύσης του φάσματος 5G. Αυτές οι δραστηριότητες συζητούνται εν συντομία σε αυτήν την ενότητα. [40]

### Next Generation Mobile Networks (NGMN)

Το Next Generation Mobile Networks (NGMN) είναι μια συμμαχία με κορυφαίους χειριστές και προμηθευτές παγκοσμίως που στοχεύει στην επέκταση της εμπειρίας επικοινωνίας που θα προσφέρει προσιτές υπηρεσίες ευρυζωνικών κινητών στον τελικό χρήστη. Έχει ιδιαίτερη έμφαση στο 5G, ενώ επιταχύνει την ανάπτυξη του LTE-Advanced και του οικοσυστήματος του. Η NGMN δημοσίευσε τη «Λευκή Βίβλο 5G» (“White Papers 5G”) τον Φεβρουάριο του 2015, η οποία παρείχε μια λίστα απαιτήσεων από την προοπτική του χειριστή σε δίκτυα 5G. Οι απαιτήσεις έδειξαν ότι είναι αναγκαία η ζήτηση για αύξηση χωρητικότητας και ομοιόμορφο ρυθμό δεδομένων εμπειρίας χρήστη σε αστικές έως αγροτικές περιοχές. Αναδεικνύει την ανάγκη επίσης ότι τα δίκτυα 5G θα πρέπει να είναι σε θέση να παρέχουν διαφορετικές υπηρεσίες, συμπεριλαμβανομένου του μαζικού διαδικτύου, όπως δίκτυα αισθητήρων και εξαιρετικά αξιόπιστες επικοινωνίες όπως οι υπηρεσίες ηλεκτρονικής υγείας, υπηρεσίες που πρέπει να παρέχονται σε διαφορετικά σενάρια, συμπεριλαμβανομένων τρένων υψηλής ταχύτητας, κινούμενων σημείων πρόσβασης και αεροσκαφών. [34][40]

### 3rd Generation Partnership Project (3GPP)

Οι ομάδες εργασίας της κοινοπραξίας 3GPP RAN ολοκλήρωσαν τη μελέτη για σενάρια και απαιτήσεις για τεχνολογίες πρόσβασης επόμενης γενιάς (NG) και τη μελέτη για την τεχνολογία πρόσβασης στο νέο ραδιοσύστημα(NR). Τα επόμενα στάδια για τις τεχνικές προδιαγραφές των δικτύων 5G στο 3GPP, συμπεριλαμβανομένου του Next Generation RAN (NG - RAN), βρίσκονται σε εξέλιξη.[34]

Με βάση τις εκτιμήσεις διαφόρων περιπτώσεων χρήσης και ανάπτυξης των σεναρίων 5G, οι σχετικές απαιτήσεις και οι βασικοί δείκτες απόδοσης (Key Performance Indicators, KPIs), καθώς και ένα σύνολο απαιτήσεων για την αρχιτεκτονική NG - RAN και τη μετεγκατάσταση(mitigation) τεχνολογιών ραδιοπρόσβασης NG (Radio Access Technologies, RAT) έχει καθιερωθεί στο 3GPP. Για παράδειγμα, η αρχιτεκτονική NG - RAN υποστηρίζει στενή συνεργασία μεταξύ NG - RAT και (e) LTE, συνδεσιμότητα μέσω πολλαπλών σημείων μετάδοσης, ευέλικτη ανάπτυξη και λειτουργικές επιλογές διαχωρισμού, τεμαχισμός δικτύου και εικονικοποίηση λειτουργίας δικτύου (NFV). Υποστηρίζει περαιτέρω τη διαλειτουργικότητα πολλαπλών προμηθευτών με ανοιχτές διεπαφές μεταξύ RAN και CN και εντός του RAN, και μεταξύ λογικών κόμβων και λειτουργιών του NR και (e) LTE.[34]

Σε γενικές γραμμές, η συμφωνία είναι ότι το 3GPP NG - RAN αποτελείται από NR Gigabit Node - Bs (gNBs), παρέχοντας πρωτόκολλα τερματισμού επιπέδου χρήστη (UP) και επιπέδου ελέγχου (CP) για τις ραδιοεπαφές προς τον εξοπλισμό χρήστη (UE).[34]

### Ομάδα Προώθησης IMT-2020 (5G)

Τον Φεβρουάριο του 2013, ιδρύθηκε στην Κίνα η ομάδα προώθησης IMT-2020 (5G) από τρεις φορείς: το Υπουργείο Βιομηχανίας και Πληροφορικής (MIIT), την Εθνική Επιτροπή Ανάπτυξης και Μεταρρυθμίσεων και το Υπουργείο Επιστήμης και Τεχνολογίας. Είναι η κύρια πλατφόρμα για την προώθηση της έρευνας και ανάπτυξης του 5G στην Κίνα. Η ομάδα προώθησης αποτελείται από κορυφαίους Κινέζους χειριστές, προμηθευτές εξοπλισμού δικτύου, ερευνητικά ιδρύματα και πανεπιστήμια.[34]

Η ομάδα προώθησης IMT-2020 (5G) δημοσίευσε το “White paper 5G” της, το Μάιο του 2014 στο οποίο έδειξε δύο σημαντικές κατηγορίες χρήσης 5G: κινητή ευρυζωνική σύνδεση και Διαδίκτυο πραγμάτων(Internet of Things, IoT).

### Ευρώπη: 5G Public Private Partnership (5G PPP)

Μία άλλη κοινοπραξία είναι αυτή της 5G PPP που έχει εκδώσει τρεις φάσεις με διάφορες εργασίες εντός που ασχολούνται κυρίως με σχεδιαστικές επιλογές της αρχιτεκτονικής του RAN όπως οι παρακάτω περιπτώσεις .

- ▷ *METIS II* όπου έχει αναπτύξει έναν συνολικό σχεδιασμό 5G RAN, εστιάζοντας στην αποτελεσματική ενσωμάτωση των εξελιγμένων παλαιών και νέων AIVs, και στην υποστήριξη τεμαχισμού δικτύου.

- ▷ *NORMA* όπου έχει αναπτύξει μια καινοτόμο, προσαρμοστική και μελλοντική, ανθεκτική αρχιτεκτονική δικτύου 5G, με έμφαση στην υποστήριξη πολλαπλών μισθώσεων και πολλαπλών υπηρεσιών
- ▷ *COHERENT* όπου ανέπτυξε ένα ενοποιημένο προγραμματιζόμενο πλαίσιο ελέγχου για συντονισμό και ευέλικτη διαχείριση φάσματος σε ετερογενή δίκτυα πρόσβασης 5G.
- ▷ *mmMAGIC* όπου ανέπτυξε νέες αρχιτεκτονικές ιδέες RAN για τεχνολογία μικροκυματικής ραδιοπρόσβασης (mmWave), συμπεριλαμβανομένης της ενσωμάτωσης της με ζώνες χαμηλότερης συχνότητας.
- ▷ *5G MonArch* όπου στοχεύει στην επέκταση της υπάρχουσας αρχιτεκτονικής με βασικές καινοτομίες που σχετίζονται με τον έλεγχο μεταξύ τομέων και τη διαχείριση μεταξύ τομέων και μια στοιβία πρωτοκόλλων με δυνατότητα cloud.

Επιπλέον, η 5G PPP Architecture Working Group διευκολύνει τη συζήτηση μεταξύ των έργων 5G PPP που αναπτύσσουν αρχιτεκτονικές έννοιες και στοιχεία, και συλλαμβάνει τα ενοποιημένα ευρήματα σε όλα τα έργα σε ετήσια ενημερωμένη αρχιτεκτονική White Papers.[34][40]

#### **Κορέα: 5G Forum**

Το Φόρουμ 5G ιδρύθηκε από το Υπουργείο Επιστημών και Μελλοντικού Σχεδιασμού και βιομηχανίες κινητής τηλεφωνίας στην Κορέα τον Μάιο του 2013. Τα μέλη του Φόρουμ 5G αποτελούνται από φορείς εκμετάλλευσης κινητών τηλεπικοινωνιών, κατασκευαστές και ακαδημαϊκούς επαγγελματίες. Ο στόχος του Φόρουμ 5G είναι να βοηθήσει στην ανάπτυξη του προτύπου και να συμβάλει στην παγκοσμιοποίηση του.

Πέντε βασικές υπηρεσίες 5G προβλέφθηκαν από το φόρουμ 5G, συμπεριλαμβανομένων των υπηρεσιών κοινωνικής δικτύωσης, τρισδιάστατη απεικόνιση για κινητά, τεχνητή νοημοσύνη, υπηρεσίες υψηλής ταχύτητας, δυνατότητες ανάλυσης υψηλής ευκρίνειας και ολογραφικές τεχνολογίες. Τέτοιες νέες υπηρεσίες θα ενεργοποιηθούν από το δίκτυο 5G με ισχυρές δυνατότητες που θα παρέχουν εξαιρετικά υψηλή χωρητικότητα καναλιού και ρυθμούς δεδομένων. [40]

#### **Ιαπωνία: 5G Mobile Communications Promotion Forum (5GMF)**

Το Φόρουμ Προώθησης Κινητών Επικοινωνιών Πέμπτης Γενιάς (5GMF) ιδρύθηκε τον Σεπτέμβριο του 2014 στην Ιαπωνία. Το 5GMF διεξάγει έρευνα και ανάπτυξη που σχετίζεται με το 5G, συμπεριλαμβανομένης της τυποποίησης, του συντονισμού με σχετικούς οργανισμούς και άλλων δραστηριοτήτων προώθησης.

Η 5GMF δημοσίευσε το White paper «5G Mobile Communications Systems for 2020 and beyond» τον Ιούλιο του 2016, όπου επισημάνθηκαν οι περιπτώσεις χρήσης 5G υπηρεσιών υψηλού ρυθμού δεδομένων, αυτο-οδήγησης, υπηρεσιών βάσει τοποθεσίας κ.λπ. Προέβλεπε ότι το δίκτυο 5G πρέπει να είναι εξαιρετικά ευέλικτο ώστε να ανταποκρίνεται στις απαιτήσεις αυτών των διαφορετικών απαιτήσεων. [40]

### **Βόρεια και Νότια Αμερική: 5G Americas**

Η 5G Americas είναι ένας βιομηχανικός εμπορικός οργανισμός που αποτελείται από κορυφαίους παρόχους και κατασκευαστές υπηρεσιών τηλεπικοινωνιών. Συνεχίστηκε το 2015 από την προηγούμενως γνωστή οντότητα: 4G Americas. Ο οργανισμός στοχεύει να υποστηρίξει και να προωθήσει την πρόοδο και τις πλήρεις δυνατότητες της ασύρματης τεχνολογίας LTE και την εξέλιξή της πέραν των 5G, σε όλα τα δίκτυα, τις υπηρεσίες, τις εφαρμογές και τις ασύρματες συνδεδεμένες συσκευές του οικοσυστήματος στην Αμερική. Η 5G Americas επενδύει στην ανάπτυξη μιας συνδεδεμένης ασύρματης κοινότητας ενώ ταυτόχρονα οδηγεί την ανάπτυξη 5G για την Αμερική.

Η 5G Americas δημοσίευσε White paper για τις υπηρεσίες 5G και τις περιπτώσεις χρήσης τον Νοέμβριο του 2017. Παρέχει μια διορατική έκθεση σχετικά με την τεχνολογία 5G που αντιμετωπίζει νέες τάσεις σε ένα ευρύ φάσμα περιπτώσεων χρήσης και επιχειρηματικών μοντέλων, με τεχνικές απαιτήσεις και αντιστοιχίσεις στις δυνατότητες 5G καθώς αποτελεί και μια συνεχή μελέτη για περιπτώσεις χρήσης 5G για μελλοντικές χρήσεις.[40]

### **Παγκόσμιο 5G Event**

Οι περιφερειακές εξελίξεις 5G απαιτούν έναν παγκόσμιο συντονισμό για τη διαμόρφωση ενός ενοποιημένου προτύπου 5G που να ισχύει παγκοσμίως. Οι περιφερειακοί προγραμματιστές 5G, συμπεριλαμβανομένων των IMT-2020 (5G) PG, 5G PPP, 5G forum, 5GMF, 5G Americas και 5G Brazil, απάντησαν σε αυτό το κάλεσμα δημιουργώντας ένα παγκόσμιο event 5G για να μοιραστούν τις απόψεις και την κατάσταση ανάπτυξης σε κάθε περιοχή. Το γεγονός αυτό βοηθά στην ανοικοδόμηση της παγκόσμιας συναίνεσης για το 5G με συμβαλλόμενους τους παγκόσμιους οργανισμούς προώθησης 5G. Αυτή η σειρά των εκδηλώσεων(events) έχει καταβάλει προσπάθειες για την προώθηση της χρήσης του 5G για διαφορετικές κάθετες βιομηχανίες, οικολογικά συστήματα 5G και καλεί βασικούς φορείς της βιομηχανίας, διοικήσεις και ρυθμιστικές αρχές να συμμετάσχουν στη συζήτηση.

Η πρώτη παγκόσμια εκδήλωση 5G διοργανώθηκε από την IMT-2020 PG στο Πεκίνο, τον Μάιο του 2016, και η εκδήλωση πραγματοποιείται δύο φορές το χρόνο σε εναλλαγή. [40]

### **1.6.2 Ανάπτυξη προτύπων (Standard Development)**

Μαζί με το ITU-R και τις περιφερειακές δραστηριότητες για την ανάπτυξη 5G, οι οργανισμοί τυποποίησης έχουν επίσης επικεντρώσει την προσοχή τους στο 5G από το 2014. Το έργο παγκόσμιας εταιρικής σχέσης, το 3GPP, έχει γίνει ο βασικός τυπικός οργανισμός της ανάπτυξης 5G αλλά και παγκόσμια πρωτοβουλία για κινητά πρότυπα κινητής τηλεφωνίας από την ανάπτυξη του δικτύου 3G. Το τρέχον πρότυπο ευρυζωνικής κινητής τηλεφωνίας 4G, LTE είναι ένα από τα πιο επιτυχημένα πρότυπα κινητής τηλεφωνίας και χρησιμοποιείται παγκοσμίως.

Το 3GPP είναι ένας οργανισμός που ενώνει τους τυπικούς οργανισμούς ανάπτυξης τηλεπικοινωνιών (Standard Development Organizations, SDO) σε όλο τον κόσμο. Αυτοί οι SDO είναι γνωστοί ως συνεργάτες του οργανισμού

(Organization Partners, OP) στην κοινοπραξία 3GPP και επί του παρόντος υπάρχουν επτά: ARIB και TTC από την Ιαπωνία, ATIS από την Αμερική, CCSA από την Κίνα, ETSI από την Ευρώπη, TSDSI από την Ινδία και TTA από την Κορέα. Οι επτά OP παρέχουν στα μέλη σταθερό περιβάλλον για την ανάπτυξη τεχνολογίας 3GPP.[40][41]



Εικόνα 1.6: Λογότυπα και σχέση μεταξύ ITU και 3GPP [41]

Τα μέλη του OP περιλαμβάνουν βασικούς παράγοντες της βιομηχανίας, κορυφαίους χειριστές, προμηθευτές, κατασκευαστές τερματικών χρηστών και προγραμματιστές chipset.

Περιλαμβάνουν επίσης ερευνητικά ινστιτούτα με περιφερειακές επιπτώσεις, ακαδημαϊκοί οργανισμοί και πανεπιστήμια. Επίσης, τα μέλη των OP συμμετέχουν σε μεγάλο βαθμό στην ανάπτυξη τεχνικών προτύπων, τα οποία διασφαλίζουν ότι η τεχνολογία 3GPP αντιμετωπίζει τις ανησυχίες και τα ζητήματα από διαφορετικά μέρη και από διαφορετικές περιοχές. Με βάση τη συναίνεση των μελών από διαφορετικά OP, οι τεχνικές προδιαγραφές που ορίζονται από το 3GPP μεταφέρονται από τα OP στις περιφερειακές τους προδιαγραφές. Με αυτόν τον τρόπο, αναπτύσσονται παγκόσμια πρότυπα για κινητά. Μπορεί να υποστηριχθεί ότι αυτό είναι το βασικό κλειδί για την επιτυχία της τυπικής ανάπτυξης 3GPP.[40][41]

Το LTE είναι ένα πρώιμο παράδειγμα κάτω από αυτό το πνεύμα ανάπτυξης που βασίζεται στη συναίνεση. Η παγκόσμια και ευρεία συμμετοχή έθεσε τα θεμέλια για την επιτυχία της ανάπτυξης, της τυποποίησης και της εφαρμογής του LTE. Λόγω της μεγάλης επιτυχίας του LTE, το 3GPP έχει γίνει το βασικό πρότυπο ανάπτυξης για το 5G. Στα τέλη του 2014, η 3GPP ξεκίνησε μελέτες και ανάπτυξη 5G μαζί με τη σταδιακή ωρίμανση του οράματος 5G.[42]

Στα τέλη του 2015 έως τις αρχές του 2017, όταν το 3GPP βρισκόταν στην 14η έκδοση κυκλοφορίας (γνωστό ως Release-14), πραγματοποιήθηκαν μελέτες 5G σχετικά με τεχνικές απαιτήσεις και σενάρια ανάπτυξης. Αυτές οι μελέτες αποσκοπούσαν στην επίτευξη του οράματος 5G όπως ορίστηκε από τον ITU-R τον Ιούνιο του 2015. Η μελέτη μιας νέας διεπαφής ραδιοφώνου (NR) ξεκίνησε μετά τη μελέτη απαιτήσεων. Τα βασικά τεχνικά στοιχεία εντοπίστηκαν για την ανάπτυξη NR, τα οποία αποτελούν τη βάση των εργασιών προδιαγραφών στην επόμενη έκδοση (δηλαδή, Release-15) που διήρκεσε από τις αρχές του 2017 έως τον Ιούνιο του 2018.[42]

Η πλήρης τεχνολογία 3GPP 5G, συμπεριλαμβανομένων των NR και LTE, αναπτύχθηκαν στην Έκδοση-16 κατά το χρονικό πλαίσιο του 2018 έως το τέλος του 2019. Με αυτήν τη σταδιακή προσέγγιση, το 3GPP έφερε μια λύση 5G στο ITU-R ως IMT-2020 το έτος 2020. Το τελικό χρονοδιάγραμμα που αναφέρει



στο portal της η 3GPP είναι να σταματήσει την ανάπτυξη της έκδοσης 17 στις 10-06-2022 και να συνεχίσει στην έκδοση 18 που άρχισε στις 16-09-2019 και για την οποία δεν έχει αναφερθεί, μέχρι τη συγγραφή αυτής της εργασίας, ημερομηνία περάτωσης.[42]

# Κεφάλαιο 2

## Δίκτυο Κορμού 5G

**Σ**το κεφάλαιο αυτό περιγράφεται το δίκτυο κορμού των κινητών επικοινωνιών που χρησιμοποιείται μέχρι σήμερα αλλά και του 5G που το πεδίο εφαρμογής του δεν περιορίζεται μόνο στις κινητές επικοινωνίες. Αρχικά, δίνεται μία περιγραφή της non-standalone αρχιτεκτονικής δικτύου πυρήνα 5G που έχει προτιμηθεί από τους χειριστές των δικτύων για την αμεσότερη είσοδο στην αγορά της τεχνολογίας 5G. Έπειτα, αναλύεται στα πλαίσια της εργασίας, η αρχιτεκτονική του δικτύου κορμού 5G που πρόκειται να εδραιωθεί μελλοντικά.

### 2.1 Μη αυτόνομο δίκτυο κορμού 5G (Non-Stand Alone)

Στη γενική ιδέα της αρχιτεκτονικής non-Stand-Alone(NSA) ή όπως αλλιώς ονομάζεται E-UTRA New Radio Dual Connectivity(EN-DC) στην τεκμηρίωση της κοινοπραξίας 3GPP χρησιμοποιείται το EPS, σε Διπλή Συνδεσιμότητα, για τη σύνδεση 5G συσκευών με το EPC δίκτυο κορμού μέσω του δικτύου πρόσβασης NR ή/και με τη βοήθεια του LTE για τη διατήρηση της σηματοδότησης.

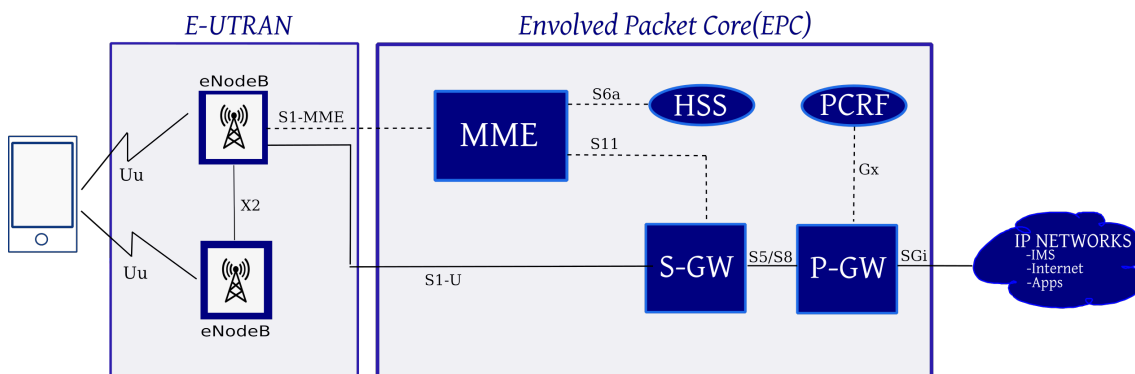
Το εξελιγμένο πακέτο πυρήνα (Evolved Packet Core, EPC) είναι μια αρχιτεκτονική δικτύου που υποστηρίζει διαφόρων τύπων δίκτυα πρόσβασης(GERAN,UTRAN και EUTRAN) αλλά και non-3GPP προσβάσεις όπως ασύρματα τοπικά δίκτυα W-LAN ή ακόμα και ενσύρματα. Το NSA είναι επίσης γνωστό ως "Architecture Option 3". Οι λειτουργίες που περιέχει, και περιγράφονται παρακάτω, με την πάροδο του χρόνου έχουν βελτιωθεί και προσαρμοσθεί στις αυξημένες ανάγκες όπως η συνδεσιμότητα διαφόρων τύπων μηχανών(Machine Type Communication, MTC)καθώς και το κυψελοειδές Internet of Things(CIoT). Με τις βελτιώσεις αυτές υποστηρίζει επίσης υπηρεσίες εγγύτητας για επικοινωνίας συσκευής με συσκευή αλλά και επικοινωνία οχημάτων με άλλες διατάξεις (V2X όπως αναφέρεται,για παράδειγμα V2P-vehicle to Pedestrian).

Δύο ακόμη υπηρεσίες που υποστηρίζει είναι (i) η επιλογή διαφορετικών στιγμιότυπων λειτουργιών δικτύου που εξυπηρετεί την κάθε περίπτωση χωριστά και αναφέρεται ως Dedicated Core Network(DECOR ή DCN) αλλά και (ii) ο διαχωρισμός του gateway του δικτύου σε επίπεδο ελέγχου και επίπεδο

χρήστη ή όπως αναφέρεται Control και User Plane Separation(CUPS).

Τα DECOR και CUPS είναι οι δύο βασικές περιπτώσεις που εφαρμόζονται στο δίκτυο πυρήνα, βελτιώνοντας το EPC για υλοποίηση 5G δικτύου με βάση το EN-DC λόγω της πολύπλευρης διάστασης και της ευελιξίας που παρέχουν στους χειριστές για την ανάπτυξη διαφοροποιημένων πυρήνων δικτύων προς συγκεκριμένους στοχευμένους χρήστες.[2]

### 2.1.1 Βασική Αρχιτεκτονική Evolved Packet Core(EPC)



Εικόνα 2.1: Στοιχειώδης Αρχιτεκτονική δικτύου 4G

Το EPC δίκτυο πρωτοεμφανίστηκε στην εφαρμογή του 4G/LTE και παρακάτω γίνεται μια αναφορά στις βασικές λειτουργίες του, οι οποίες κληρονόμησαν την κεντρική τους ιδέα την απο τις προηγούμενες γενιές.

Το LTE δίκτυο περιλαμβάνει δύο βασικά μέρη. Το Radio Access δίκτυο(E-UTRAN) και το δίκτυο πυρήνα που στην έκδοση του LTE ονομάζεται Evolved Packet Core(EPC).

Το RAN μέρος του LTE περιέχει το eNodeBase(eNB) που είναι υπεύθυνο για τη διαχείριση του συστήματος κεραιών και τη φυσική σύνδεση με τη συσκευή του χρήστη (User Equipment,UE). Παρέχει επίσης και ένα σύνολο λειτουργιών διαχείρισης ραδιο-πόρων (Radio Resource Management, RRM) όπως η δυναμική δέσμευση μνήμη και προγραμματισμός(scheduler), έλεγχος κινητικότητας, ICIC, άδεια ελέγχου ραδιοκύματος(RAC) κλπ.[5]

Παρακάτω αναφερόμαστε, με κάποιες σημαντικές λεπτομέρειες, στις οντότητες που υλοποιούν τον πυρήνα του 4G, όπου στην εικόνα 2.1 αναπαρίσταται οι στοιχειώδης λειτουργίες του 4g δικτύου.

#### Mobility Management Entity (MME)

Το EPC περιλαμβάνει αρχικά την οντότητα διαχείρισης κινητικότητας (Mobility Management Entity,MME). Η MME είναι ο βασικός κόμβος ελέγχου για το δίκτυο πρόσβασης LTE. Είναι υπεύθυνη για τη διαδικασία σελιδοποίησης και επισήμανσης εξοπλισμού χρήστη σε κατάσταση αδράνειας, συμπεριλαμβανομένων της αναμετάδοσης. Συμμετέχει στη διαδικασία ενεργοποίησης / απενεργοποίησης του carrier και είναι επίσης υπεύθυνη για την επιλογή του Serving Gateway για ένα UE στην αρχική σύνδεση και τη στιγμή της παράδοσης εντός του LTE που περιλαμβάνει μετεγκατάσταση κόμβου

δικτύου πυρήνα (Core Network ,CN). Επιπλέον, είναι υπεύθυνη για τον έλεγχο ταυτότητας του χρήστη (μέσω αλληλεπίδρασης με τον διακομιστή οικιακού συνδρομητή). Το σήμα Non Access Stratum (NAS) τερματίζεται στο MME και είναι επίσης υπεύθυνο για τη δημιουργία και την κατανομή προσωρινών ταυτοτήτων στους UE. Ελέγχει την εξουσιοδότηση του UE ώστε να συμμετέχει στο δημόσιο δίκτυο κινητής τηλεφωνίας (PLMN) του παρόχου υπηρεσιών και επιβάλλει περιορισμούς περιαγωγής UE.

Το MME είναι το σημείο τερματισμού του δικτύου για κρυπτογράφηση και προστασία ακεραιότητας για τη σηματοδότηση NAS και χειρίζεται τη διαχείριση κλειδιών ασφαλείας. Η νόμιμη παρακολούθηση της σηματοδότησης υποστηρίζεται επίσης από το MME. Το MME παρέχει επίσης τη λειτουργία επιπέδου ελέγχου για κινητικότητα μεταξύ δικτύων πρόσβασης LTE και 2G / 3G με τη διασύνδεση S3 να τερματίζει στο MME από το SGSN. Τέλος, η λειτουργία MME τερματίζει τη διασύνδεση S6a προς το Home Subscriber Server(HSS) για UE περιαγωγής καθώς επίσης δέχεται και πληροφορίες συνδρομών UE που ο HSS έχει αποθήκευση στη βάση δεδομένων του.[5]

### **Serving Gateway (SGW)**

Το Serving Gateway δρομολογεί και προωθεί πακέτα δεδομένων χρήστη, ενώ ενεργεί επίσης ως άγκυρα κινητικότητας για το επίπεδο χρήστη κατά τη διάρκεια των μεταβάσεων μεταξύ eNodeB καθώς και ως άγκυρα για την κινητικότητα μεταξύ LTE και άλλων τεχνολογιών 3GPP (τερματισμός της διεπαφής S4 και αναμετάδοση της κίνησης μεταξύ 2G / 3G συστήματα και πύλη δικτύου δεδομένων πακέτων). Για UE σε κατάσταση αδράνειας, το Serving Gateway τερματίζει τη διαδρομή δεδομένων κατερχόμενης ζεύξης και ενεργοποιεί την τηλεειδοποίηση κατά την άφιξη δεδομένων κατερχόμενης ζεύξης για τον UE. Διαχειρίζεται και αποθηκεύει περιβάλλοντα UE, όπως για παράδειγμα παράμετροι της υπηρεσίας IP κομιστή και πληροφορίες εσωτερικής δρομολόγησης δικτύου. Εκτελεί επίσης αναπαραγωγή της κίνησης του χρήστη σε περίπτωση νόμιμης παρακολούθησης.[5]

### **Packet Data Network Gateway (PGW)**

Το Packet Data Network Gateway (PDN Gateway, επίσης PGW) παρέχει συνδεσιμότητα του Εξοπλισμού Χρήστη (User Equipment, UE) σε εξωτερικά δίκτυα πακέτων δεδομένων (PDN) ως σημείο εξόδου και εισόδου κίνησης. Ένα κομμάτι του Εξοπλισμού χρήστη μπορεί να έχει ταυτόχρονη συνδεσιμότητα με περισσότερα από ένα Gateway Packet Data Network για πρόσβαση σε πολλαπλά δίκτυα πακέτων δεδομένων. Το PDN Gateway εκτελεί επιβολή πολιτικής, φιλτράρισμα πακέτων για κάθε χρήστη, υποστήριξη φόρτισης, νόμιμη παρακολούθηση και έλεγχο πακέτων. Ένας άλλος βασικός ρόλος του Packet Data Network Gateway είναι να λειτουργεί ως άξονας κινητικότητας μεταξύ τεχνολογιών 3GPP και μη 3GPP, όπως WiMAX και 3GPP2 (CDMA 1X και EvDO).[5]

### Home Subscriber Server (HSS)

Ο οικιακός διακομιστής συνδρομητών (HSS) είναι μια κεντρική βάση δεδομένων που περιέχει αποθηκευμένες πληροφορίες σχετικά με το χρήστη και τις συνδρομές. Οι λειτουργίες του HSS περιλαμβάνουν λειτουργίες όπως διαχείριση κινητικότητας, υποστήριξη εγκατάστασης κλήσεων και συνεδριών, έλεγχο ταυτότητας χρήστη, πληροφορίες αυθεντικοποίησης και εξουσιοδότηση πρόσβασης, προφίλ ποιότητας υπηρεσίας και δυνατότητες προσπέλασης περιαγωγής. Το HSS βασίζεται στο οικιακό μητρώο τοποθεσίας πριν από το Rel-4 (HLR) και στο Κέντρο ελέγχου ταυτότητας (AuC).[5]

### Policy and Charging Rules Function (PCRF)

Η λειτουργία αυτή καθορίζει τους κανόνες πολιτικής και ελέγχου φόρτου καθώς επίσης παρέχει PCC κανόνες για το QoS και για το P-GW. Λαμβάνει αποφάσεις σε πραγματικό χρόνο για κάθε ενεργό χρήστη που κάνει χρήση του δικτύου ελέγχοντας τις ροές δεδομένων.

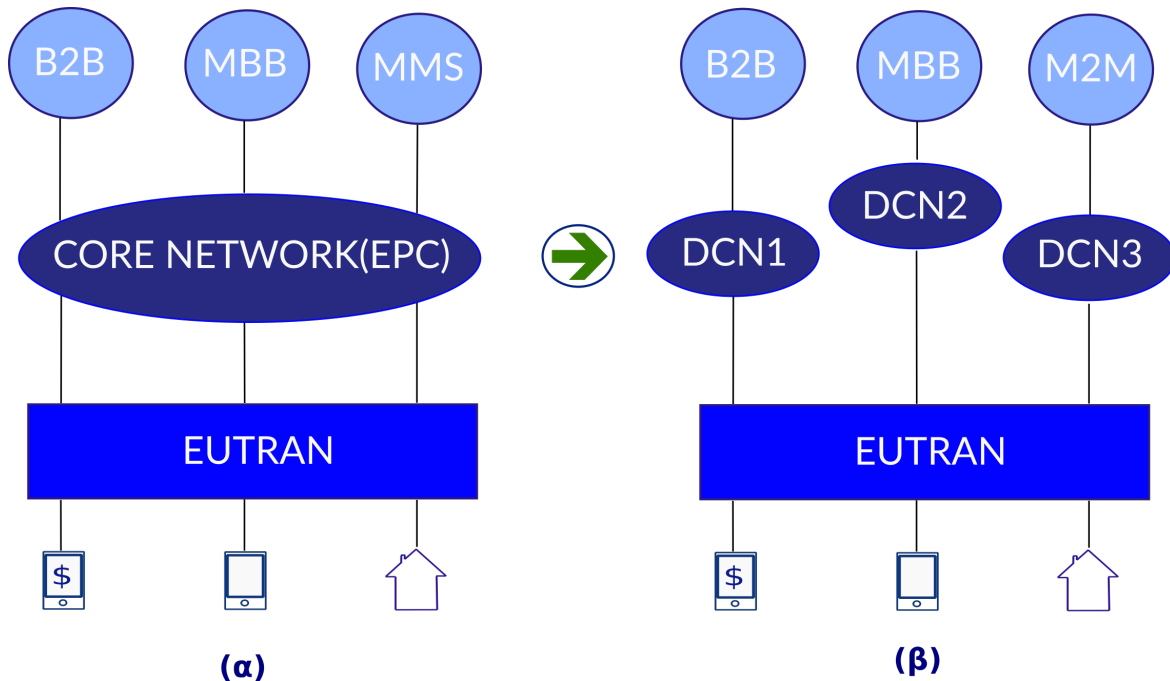
Μεταξύ των λειτουργιών οι διεπαφές χαρακτηρίζονται με το γράμμα S, οι εσωτερικές εξαρτήσεις των λειτουργιών με το G και με το γράμμα X2 οι διεπαφές μεταξύ διαφορετικών nodes(π.χ. για carrier aggregation). Τέλος η διεπαφή UE και E-utran χαρακτηρίζεται ως LTE-Uu.[5]

## 2.1.2 (Enhanced) Dedicated Core Network((e)DECOR ή DCN)

Τα αποκλειστικά δίκτυα κορμού (Dedicated Core Network, DECOR και ενισχυμένο DECOR), επιτρέπουν στους χειριστές (operators) των δικτύων να χωρίσουν τα δικά τους κεντρικά δίκτυα σε ξεχωριστά ειδικά δίκτυα πυρήνα με δυναμικές και κατά αποκλειστικότητα λειτουργίες MME, SGW και PGW που χρησιμοποιούνται για συγκεκριμένους σκοπούς, όπως για παράδειγμα πυρήνας αφιερωμένος για CIoT και MBB. Μαζί με τη λειτουργία διπλής συνδεσιμότητας στο δίκτυο ραδιοπρόσβασης, όπου το RAN μπορεί να αυξήσει την απόδοση του UE προσθέτοντας ένα δευτερεύον RAT χρησιμοποιώντας το ράδιο δίκτυο NR 5G για το UE, ένας χειριστής μπορεί να δημιουργήσει το πρώιμο σύστημα 5G χρησιμοποιώντας EPC. Αυτά τα συνδυασμένα χαρακτηριστικά (δηλαδή DC, (e)DECOR, CUPS) σε EPC με NR ως δευτερεύον RAT αναφέρεται ως EPC για 5G και χρησιμοποιείται σήμερα στη χώρα μας, καθώς ο συνδυασμός αυτής της λειτουργικότητας παρέχει ένα EPC για 5G που επιτρέπει την πρόωρη ανάπτυξη NR, το οποίο συνεχίζει επίσης να υποστηρίζει όλες τις δυνατότητες 4G κάνοντας χρήση υπαρχουσών εγκαταστάσεων των operators.[2]

Στην εικόνα 2.2 παρατηρούμε στην (α) περίπτωση τις διάφορες υπηρεσίες που κάνουν χρήση των δικτύων να εξυπηρετούνται από το ίδιο δίκτυο κορμού δεσμεύοντας όλες τις λειτουργίες που αυτό περιέχει ενώ στην περίπτωση (β) που είναι ένα δίκτυο DECOR, κάθε υπηρεσία έχει το δικό της αποκλειστικό δίκτυο κορμού που εμπεριέχει και αξιοποιεί τις λειτουργίες που χρειάζεται για τη σωστή λειτουργία του και μόνο.

Η τεχνική (e)DECOR εμπνεύστηκε από την επιθυμία των χειριστών δικτύων να αναπτύξουν μέσα σε ένα δίκτυο φορέων εκμετάλλευσης-χειριστών(operators) (που ορίζονται από τα αναγνωριστικά PLMN) πολλαπλά



Εικόνα 2.2: (α)Όλες οι υπηρεσίες μοιράζονται το ίδιο δίκτυο κορμού (β)Χρήση λειτουργιών δικτύου κορμού με βάση τις ανάγκες της κάθε υπηρεσίας

δίκτυα και να κατευθύνουν τους χρήστες προς συγκεκριμένα βασικά δίκτυα κορμού, επιτρέποντας έτσι το διαχωρισμό του δικτύου πλήρους πυρήνα σε πιο συγκεκριμένα τμήματα λειτουργιών, πετυχαίνοντας κλιμάκωση και ευελιξία. Αυτή η δυνατότητα επιτρέπει σε έναν χειριστή να αναπτύξει πολλαπλά Dedicated Core Networks (DCN) εντός ενός PLMN με κάθε DCN να αποτελείται από έναν ή περισσότερους κόμβους δικτύου πυρήνα(CN) ( για παράδειγμα MME μόνο, MME με GWs, MME, GWs και PCRF)και κάθε τέτοιο DCN να μπορεί να είναι αφιερωμένο στην εξυπηρέτηση συγκεκριμένων τύπων συνδρομητών.

Η διαφορά μεταξύ DECOR και (e)DECOR είναι ότι το τελευταίο απαιτεί από το UE να παρέχει συγκεκριμένες πληροφορίες για να διευκολύνει την ταχύτερη και βέλτιστη επιλογή του προτιμώμενου δικτύου πυρήνα.

Το EPS καθιστά ήδη δυνατή την κατεύθυνση των UE σε συγκεκριμένα PLMNs, τα οποία με τη σειρά τους μεταφέρουν το UE στο συγκεκριμένο δίκτυο (συμπεριλαμβανομένου του δικτύου πυρήνα). Η χρήση της έννοιας του ονόματος σημείου πρόσβασης(Access Point Name,APN) επιτρέπει στο PLMN να κατευθύνει τα UE σε συγκεκριμένα διαφοροποιημένα δίκτυα υπηρεσιών, επιλέγοντας διαφορετικές οντότητες επιπέδου χρήστη (δηλ. PDN GWs).

Χωρίς τη βελτιωμένη έκδοση του DECOR (eDECOR), είναι δυνατό για τον χειριστή να ανακατευθύνει τους χρήστες του μεν, αλλά απαιτεί τα PDN GWs να είναι σε θέση, εντός του PLMN, ώστε να μπορούν να χειρίζονται τη συνδεσιμότητα προς τα διαφορετικά δίκτυα υπηρεσιών (π.χ. CIoT, eMBB, VoLTE) για όλους τους χρήστες.[2][3][4]

Επιπλέον, το (e)DECOR επιτρέπει στο EPC να "τεμαχίσει" το βασικό δίκτυο σε στοιχεία που μπορούν να προσαρμοστούν για να εξυπηρετούν συγκεκριμένη ομάδα UE (χρηστών), με βάση τη συνδρομή τους και την επιλεκτική διαμόρφωση τους. Αυτό παρέχει στους χειριστές πρόσθετη ευελιξία

για το διαχωρισμό των χρηστών σε διαφορετικούς τύπους βασικών δικτύων (π.χ. MBB, IoT) ανάλογα με την προβλεπόμενη χρήση. Πριν από την εισαγωγή του DECOR, οι χρήστες (UE) μπορούσαν να έχουν πρόσβαση σε διαφορετικές υπηρεσίες δεδομένων χρησιμοποιώντας έννοιες όπως το Access Point Name (APN), το οποίο οδήγησε στην δυνατότητα επιλογής ενός διαφορετικού άκρου GW στον πυρήνα και σε ένα διαφορετικό δίκτυο δεδομένων ή ακόμα και την επιλογή ενός PLMN, με βάση το υποστηριζόμενο PLMN-ID, που επέτρεπε τη δρομολόγηση των UE σε ένα συγκεκριμένο CN. Το DECOR επιτρέπει στους χειριστές να διαχωρίζουν τους διαφορετικούς τύπους κίνησης-επισκεψιμότητας, σε συγκεκριμένους κόμβους πυρήνα δικτύου και εάν χρειαστεί, τους κλιμακώνει διαφορετικά από το υπόλοιπο δίκτυο πυρήνα για να εξυπηρετήσει τις διαφορετικές απαιτήσεις. Με αυτόν τον τρόπο, ο χειριστής μπορεί επίσης να διαχωρίζει συγκεκριμένους χρήστες πιο αποτελεσματικά και να τους ελέγχει από τα δεδομένα συνδρομής. Με το ενισχυμένο DECOR, το οποίο απαιτεί επίσης ενημέρωση των UE, οι χρήστες μπορούν επίσης να επιλέξουν κατά την εγγραφή στο δίκτυο, ποιος τύπος δικτύου DCN απαιτείται για τη σύνδεση. Για παράδειγμα, ένας χρήστης σε ένα εργοστάσιο, μπορεί να επιλέξει να χρησιμοποιήσει το Dedicated Core Network(DCN) που επιτρέπει τη συνδεσιμότητα ειδικά για το εργοστάσιο που παρέχει πρόσβαση σε συγκεκριμένες υπηρεσίες οι οποίες παρέχονται μόνο σε αυτήν την τοποθεσία. Στο 5G, η υποστήριξη της λειτουργίας “τεμαχισμού” δικτύου (μια πιο περίπλοκη έκδοση του DECOR) ενεργοποιείται εξ αρχής, εξαλείφοντας έτσι τυχόν ζητήματα διαφορετικών τύπων συσκευών που απαιτούν διαφορετική συμπεριφορά δικτύου σχετικά με τον τρόπο ενεργοποίησης του διαχωρισμού του αποκλειστικού πυρήνα δικτύου.[2][3][4]

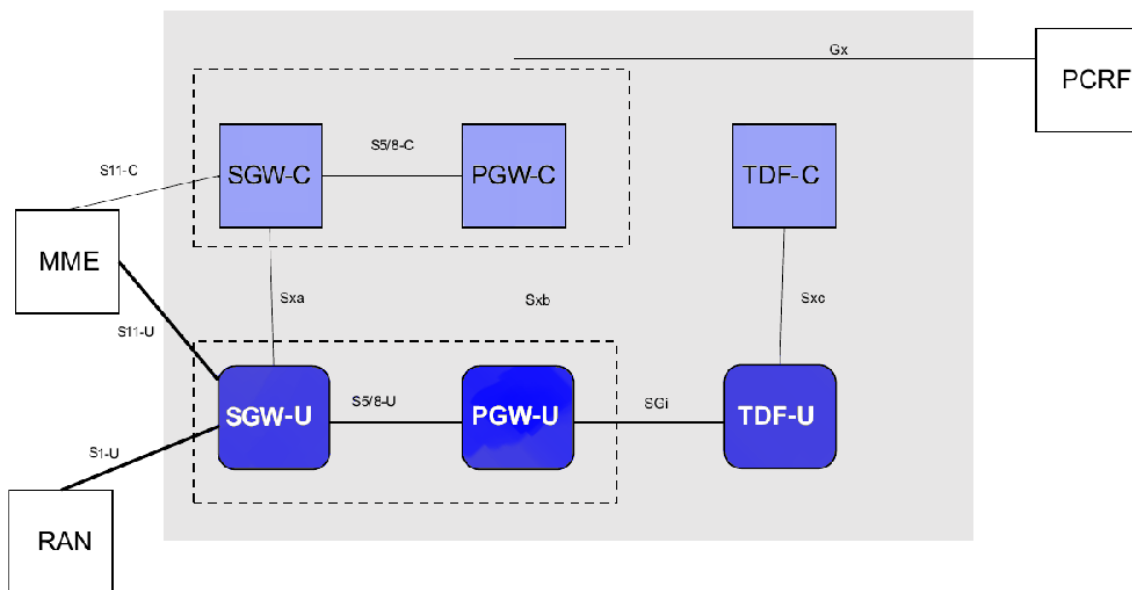
### 2.1.3 Control and User Plane Separation(CUPS)

Το EPC σχεδιάστηκε, σε σύγκριση με το προηγούμενο σύστημα GPRS, για να έχει ξεχωριστές λειτουργίες επιπέδου ελέγχου, αλλά με έμφαση στο διαχωρισμό της διαχείρισης κινητικότητας από τις λειτουργίες διαχείρισης συνεδρίας με τη διαχείριση επιπέδου χρήστη.

Το βασικό EPC παρείχε διαχωρισμό του επιπέδου ελέγχου και επιπέδου χρήστη, ιδίως διαχωρίζοντας τη διαχείριση συνεδρίας, τις λειτουργίες επιπέδου χρήστη και την εξωτερική σύνδεση δεδομένων σε ξεχωριστά GateWay(GW), αλλά αυτά τα GW (για παράδειγμα GW που εξυπηρετούν και PDN GW) διατηρούν ακόμα το επίπεδο ελέγχου διαχείρισης περιόδου λειτουργίας.

Η ανάγκη για τέτοιο διαχωρισμό έγινε καθώς οι φορείς εκμετάλλευσης άρχισαν να εξετάζουν τις επιπτώσεις στο δίκτυό τους από εσωτερικές λειτουργίες όπως το Narrow Band, IoT, MBB, καθώς και την ανάπτυξη υπηρεσιών OTT που βασίζονται στο Διαδίκτυο, όπως ροή βίντεο, κοινή χρήση περιεχομένου και επικοινωνίες κοινωνικών μέσων.[2]

Το CUPS, λοιπόν, επιτρέπει τη λειτουργία Service Gateway(SGW) και Packet Gateway(PGW) να διαχωριστούν ως στοιχεία ελέγχου και επιπέδου χρήστη και δημιουργήθηκε από τις απαιτήσεις των operators για έλεγχο της κλιμάκωσης και την ανεξαρτησία των λειτουργιών επιπέδου χρήστη καθώς και από τη δυνατότητα ανάπτυξης λειτουργιών επιπέδου χρήστη με ευέλικτο τρόπο ανεξαρτητως των λειτουργιών του επιπέδου ελέγχου.



Εικόνα 2.3: Αναπαράσταση πυρήνα δικτύου δομημένου με CUPS [2]

Το αποτέλεσμα επιτρέπει τον διαχωρισμό των λειτουργιών SGW και PGW (καθώς και Traffic Detection Function , TDF) ελέγχου και επιπέδου χρήστη και την ευελιξία να έχει μία λειτουργία επιπέδου ελέγχου για τον έλεγχο πολλαπλών λειτουργιών επιπέδου χρήστη. Αυτή η ικανότητα κλιμάκωσης του επιπέδου ελέγχου και του χρήστη επιτρέπει ανεξάρτητα την αυξημένη χωρητικότητα του επιπέδου χρήστη στο δίκτυο χωρίς να επηρεάζει τα στοιχεία του επιπέδου ελέγχου.

Μετά τον διαχωρισμό των λειτουργιών Control και User Plane σε κάθε κόμβο GW, το επόμενο κρίσιμο σημείο είναι να διασφαλιστεί ότι η επιλογή των λειτουργιών Control Plane GW από το MME λειτουργεί ομαλά όπως συμβαίνει όταν συνδυάζονται οι λειτουργίες CP και UP.

Το MME συνεχίζει να επιλέγει το Serving GW και το PDN GW όπως πριν, αλλά σε μια τεμαχισμένη ανάπτυξη με αυτή την επιλογή να οδηγεί στις οντότητες S-GW-CP και P-GW-CP. Στη συνέχεια, εξαρτάται από το επίπεδο ελέγχου της λειτουργίας GW για να επιλέξει την αντίστοιχη λειτουργία χρήστη του επιπέδου χρήστη. Η οντότητα CP θα παρέχει τα αναγνωριστικά σήραγγας(tunnel) (ή τη σήραγγα GTP-U επιπέδου χρήστη) στο MME σύμφωνα με την προδιαγραφή πριν από το CUPS, αλλά το MME δεν θα γνωρίζει εάν αυτά τα αναγνωριστικά σήραγγας ανήκουν σε αυτόνομη οντότητα SGW-U ή PGW-U ή σε μη διαχωρισμένο SGW ή PGW.[2][3][4]

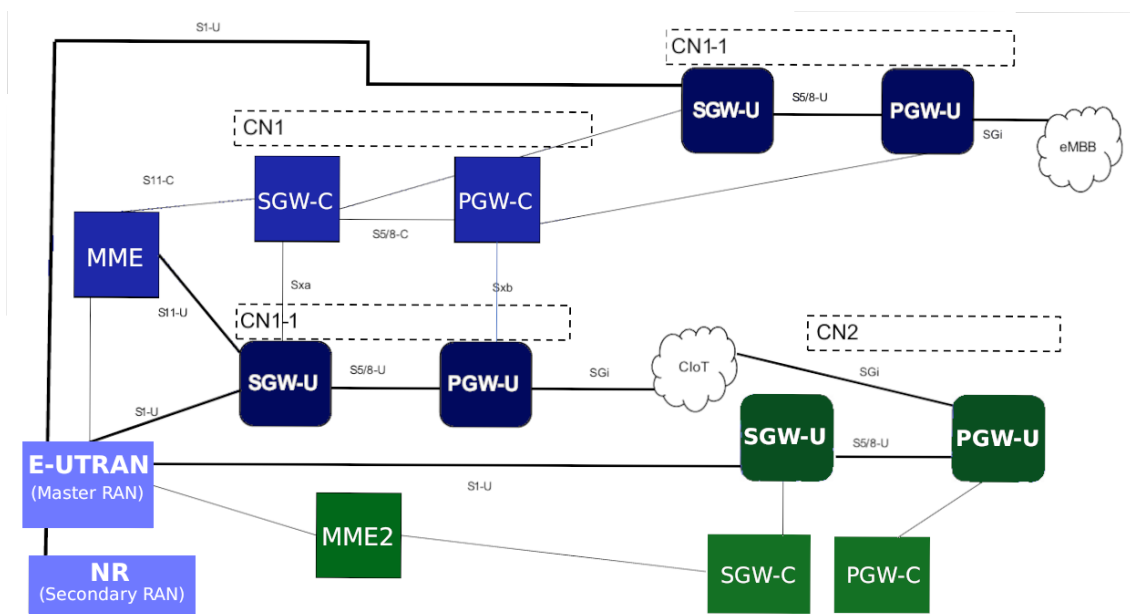
Μπορεί να φαίνεται ως αντίφαση ότι το MME αν και συνδέεται μέσω της διεπαφής S11-C με το SGW-C και με τη διεπαφή S11-U με το SGW-U, εξακολουθεί να μην γνωρίζει εάν το SGW έχει χωρισμένο ή μη διαχωρισμένο CP και UP, αυτό όμως είναι εφικτό δεδομένου ότι το πρωτόκολλο GPRS Tunneling Protocol (GTP) σχεδιάστηκε από την αρχή με ένα εγγενές διαχωρισμό CP-UP, όπου οι διευθύνσεις IP CP και UP και TEID σηματοδοτούνται σε ξεχωριστά αναγνωριστικά εξοπλισμού(IE) ακόμη και για SGW και PGW χωρίς διαχωρισμό. Αυτό κατέστησε δυνατή την εισαγωγή του CUPS στο 3GPP Release 14 ως πρόσθετο χωρίς να επηρεάζεται το MME.



Η λειτουργία CP (SGW-C και PGW-C) πρέπει να λαμβάνει υπόψη διάφορες δυνατότητες για την επιλογή της λειτουργίας UP (SGW-U και PGW-U, αντίστοιχα) που μπορεί να είναι προσαρμοσμένη για τον συγκεκριμένο χρήστη, τον τύπο συνεδρίας / APN, θέση του UE, πληροφορίες σχετικά με το DCN, ανάγκη για την εγγύτητα της λειτουργίας UP στον κόμβο RAN (π.χ., εάν η λειτουργία UP πρέπει να είναι πιο κοντά στην τοποθεσία του UE), διανομή του UP σε σχέση με το CP και τις συνθήκες φόρτωσης, κ.λπ. Οι λεπτομέρειες του τρόπου με τον οποίο γίνεται η επιλογή λειτουργίας UP εξαρτώνται σε μεγάλο βαθμό από την ανάπτυξη του operator και τις συνθήκες χρήσης.[2][3][4]

Όλες αυτές οι δυνατότητες μαζί έχουν επιπτώσεις στις λειτουργίες επιλογής κόμβων δικτύου πυρήνα (π.χ. MME, SGW, PGW) και η επιλογή του Serving και PDN GW μπορεί να βελτιωθεί περαιτέρω για την εξυπηρέτηση αποκλειστικών UE με μεγαλύτερες ανάγκες έτσι ώστε να διατίθεται GW με μεγαλύτερη χωρητικότητα και απόδοση για την υποστήριξη αυξημένης κίνησης δεδομένων. Αυτό είναι επίσης γνωστό ως EUTRA-NR Dual Connectivity (EN-DC) στο σύστημα 3GPP.

Ένα συνολικό παράδειγμα βασικής λειτουργίας επιλογής αυτών των οντοτήτων που περιγράψαμε απεικονίζεται στο παρακάτω σχήμα.



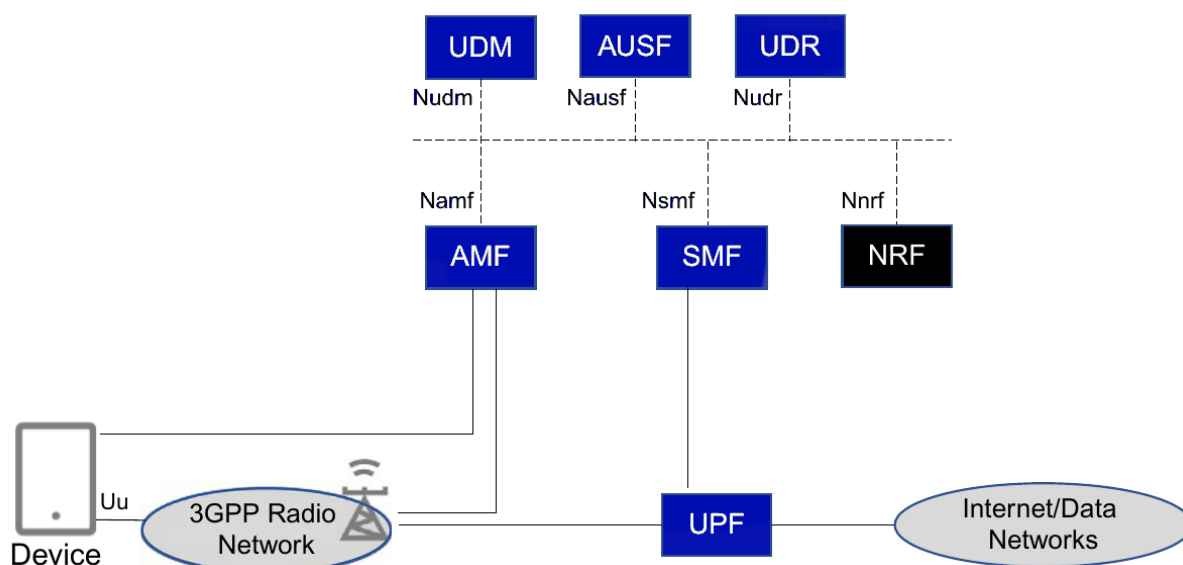
Εικόνα 2.4: Παράδειγμα ανάπτυξης αρχιτεκτονικής δικτύου με DECOR, CUPS και EN-DC [2]

Όπως φαίνεται και από την εικόνα, η χρήση ευέλικτης επιλογής GW επιπέδου χρήστη σε συνδυασμό με αποκλειστικά δίκτυα πυρήνα μέσα σε ένα μόνο PLMN επιτρέπει ορισμένες από τις βασικές λειτουργίες που ισχύουν και στο 5G όπως ο τεμαχισμός, ο πλήρης διαχωρισμός χρήστη και ελέγχου επιπέδου, καθώς και το βελτιωμένο όφελος από τη διπλή συνδεσιμότητα διαφορετικών τύπων RAT. Από την όψη ενός χειριστή που χρησιμοποιεί το non-stand-alone 5G, η (e) DECOR και CUPS με DC επιτρέπει το διαχωρισμό του συστήματος από άκρο σε άκρο του 4G EPS και του δίνει τη δυνατότητα να παρέχει στους πρώτους συνδρομητές του 5G διαφοροποιημένη εμπειρία με τον υπάρχον εξοπλισμό.

Όσον αφορά τον τελικό χρήστη, οι πρώτοι χρήστες 5G μπορούν να απολαύσουν μια βελτιωμένη εμπειρία με μεγαλύτερους ρυθμούς δεδομένων και εξυπηρέτησης μέχρι να εδραιωθεί η πλήρης αρχιτεκτονική του Stand Alone 5G. [2][3]

## 2.2 Αυτόνομο δίκτυο κορμού 5G( Stand Alone)

Στη μελλοντική χρήση του 5G δικτύου, όπως αναφέραμε, πρόκειται να εφαρμοστεί ο αυτόνομος τρόπος λειτουργίας του όπου περιλαμβάνει τις λειτουργίες που περιγράφουμε παρακάτω και στην πιο βασική του μορφή αναπαριστάται στην εικόνα 2.5 που ακολουθεί



Εικόνα 2.5: Βασικά στοιχεία 5G δικτύου [2]

Ακολουθεί μία συνοπτική περιγραφή αυτών των λειτουργιών καθώς και όλων των υπολοίπων όπου αναμένεται η ανάπτυξη τους, σύμφωνα με τα πρότυπα που έχουν δημοσιευθεί.

### 2.2.1 Access και Mobility Management Function (AMF)

Η λειτουργία AMF αποτελεί τη “Λειτουργία Διαχείρισης Πρόσβασης και Κινητικότητας”. Το AMF αλληλεπιδρά με το δίκτυο πρόσβασης μέσω της διεπαφής N2 και με τη συσκευή χρήστη μέσω της διεπαφής N1. Η αλληλεπίδραση με τις άλλες λειτουργίες δικτύου γίνονται μέσω διεπαφών βασισμένες σε υπηρεσίες.

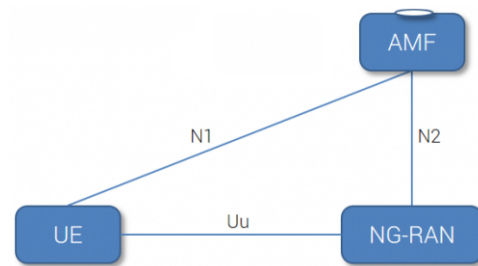
Το AMF εμπλέκεται στις περισσότερες ροές κλήσεων σηματοδότησης στο 5G δίκτυο. Υποστηρίζει κρυπτογραφημένες συνδέσεις σηματοδότησης προς συσκευές, επιτρέποντάς τις την καταχώρηση, τον έλεγχο ταυτότητας και τη μετακίνηση μεταξύ διαφορετικών ραδιοκυψελών στο δίκτυο.

Ειδικότερα, το AMF υποστηρίζει κρυπτογραφημένη εγκαθίδρυση σύνδεσης σηματοδότησης απευθείας στη συσκευή χρήστη (User Equipment, UE) επιτρέποντάς τους να καταχωρηθούν, να πιστοποιηθούν, ελέγχοντας

την ταυτότητα τους καθώς και να μετακινούνται μεταξύ διαφορετικών ραδιοκυφελών του δικτύου. Όταν ένα UE συνδέεται μέσω ενός δικτύου πρόσβασης, π.χ. NG-RAN, υπάρχει ένα μόνο AMF που χειρίζεται όλες τις αλληλεπιδράσεις σηματοδότησης με το UE και μέσω της διεπαφής N1 υποστηρίζει ακόμη και τηλεειδοποίηση συσκευών που βρίσκονται ήδη σε αδράνεια. [2][3][4]

Μια διαφορά με την αρχιτεκτονική EPC είναι ότι το AMF (σε αντίθεση με το MME) δεν χειρίζεται τη διαχείριση συνεδρίας. Αντ' αυτού, το AMF προωθεί όλες τις συνεδρίες και τα μηνύματα σηματοδότησης που σχετίζονται με τη διαχείριση μεταξύ των συσκευών και της λειτουργίας δικτύου SMF που θα δούμε παρακάτω. Μια άλλη διαφορά είναι ότι το AMF (σε αντίθεση με το MME) δεν διενεργεί τον ίδιο τον έλεγχο ταυτότητας της συσκευής, αντ' αυτού το παραγγέλνει ως υπηρεσία από τη λειτουργία δικτύου AUSF. [2][3][4]

Το AMF μεταδίδει επίσης μηνύματα SMS μεταξύ UE και λειτουργίας εξυπηρέτησης σύντομων μηνυμάτων (Short message service function, SMSF) αλλά και μηνύματα υπηρεσιών τοποθεσίας μεταξύ UE και λειτουργίας διαχείρισης τοποθεσίας (Location Management Function, LMF) καθώς και μεταξύ RAN και LMF. Επιπλέον, το AMF μεταδίδει μηνύματα πολιτικής χρήστη μεταξύ της λειτουργίας ελέγχου πολιτικής (Policy control function, PCF) και του UE. Επιπρόσθετα, περιλαμβάνει λειτουργίες ασφαλείας αγκύρωσης υποστηρίζοντας, όπως αναφέραμε, πιστοποίηση και έγκριση των χρηστών (σε συνεργασία με τις λειτουργίες AUSF και UDM). Μετά την επιτυχή έγκριση του χρήστη το AMF αντλεί ξεχωριστά σύνολα κλειδιών για προστασία ακεραιότητας κυρίως για NAS (Non-Access Stratum) σήματα μέσω της διεπαφής N1 μεταξύ UE και AMF, για Radio Resource Control (RRC) σήματα μέσω της διεπαφής N2 μεταξύ UE και NG-RAN αλλά και για κίνηση δεδομένων χρήστη μεταξύ UE και eNB. [2][3][4]



Εικόνα 2.6: Αναπαράσταση συνδεσιμότητας AMF [3]

### Πρόσθεση και διαγραφή AMF

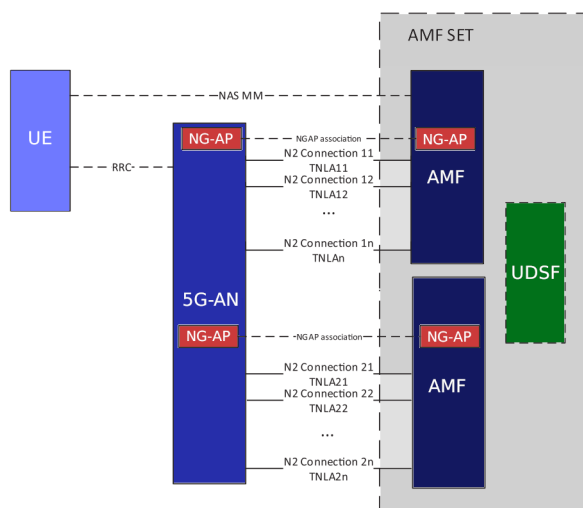
Το δίκτυο κορμού του 5G (5GC), συμπεριλαμβανομένου της διεπαφής N2, υποστηρίζει τη δυνατότητα προσθήκης και αφαίρεσης AMF από ένα σύνολο AMFs (AMFs Set). Μέσα στο 5GC, η λειτουργία αποθετηρίου δικτύου (Network Repository Function, NRF) ενημερώνεται (και το σύστημα DNS για τη συνεργασία με το Evolved Packet System, EPS) όταν προστίθενται νέες λειτουργίες δικτύου (Network Functions, NFs) και το προφίλ NF του AMF περιλαμβάνει ποια παγκόσμια μοναδικά αναγνωριστικά AMF (Globally Unique AMF Identifier, GUAMI) δεσμεύονται από το AMF. [2][3][4]

Για ένα GUAMI μπορεί επίσης να υπάρχει ένα ή περισσότερα εφεδρικά AMF καταχωρημένα στο NRF (π.χ. για χρήση σε περίπτωση αστοχίας ή προγραμματισμένης αφαίρεσης AMF).

Μια προγραμματισμένη αφαίρεση ενός AMF μπορεί να γίνει είτε μέσω του

AMF που καταχωρεί το περιβάλλον των UEs σε μία λειτουργία μη δομημένη αποθήκευσης δεδομένων (Unstructured Data Storage Function, UDSF) ή με το AMF να διαγράφεται από το NRF, οπότε το AMF ειδοποιεί το 5G-AN ότι το AMF δεν θα είναι διαθέσιμο για τη διεργασία μεταφοράς για τα GUAMI που έχουν διαμορφωθεί σε αυτό το AMF. Επιπλέον, το AMF μπορεί αρχικά να μειώσει το φορτίο αλλάζοντας έναν συντελεστή βαρύτητας για το AMF προς το 5G-AN, για παράδειγμα το μηδέν, προκαλώντας το 5G-AN να επιλέξει άλλα AMF μέσα στο AMF Set για νέα UE που εισέρχονται στην περιοχή.[4] Εάν το AMF δηλωθεί ότι δεν είναι διαθέσιμο για τη διεργασία μεταφοράς, τότε το 5G-AN επιλέγει διαφορετικό AMF μέσα στο ίδιο σετ AMF. Εάν αυτό δεν είναι δυνατό, το 5G-AN επιλέγει ένα νέο AMF από άλλο AMF Set.[2]

Εντός του 5GC, αν το NRF ειδοποιήσει το επίπεδο ελέγχου NFs - που έχει εγγραφεί - ότι το AMF αναγνωρίζεται από το GUAMI δεν θα είναι διαθέσιμο για τη διεργασία μεταφοράς. Το CP NF τότε επιλέγει άλλο AMF μέσα στο ίδιο σετ AMF, και το νέο AMF ανακτά το UE από το UDSF και το νέο AMF ενημερώνει το UE με ένα νέο 5G-GUTI και ένα συνδεδεμένο CP NF με τις νέες πληροφορίες διεύθυνσης AMF.[2][4]



Εικόνα 2.7: Επιλογή AMF από ένα σύνολο AMF set [3]

χρήστη μπορεί να αποθηκεύονται σε ένα UDSF ή ανάλογα με τη διαβάθμιση του GUAMI σε άλλα AMFs.[2][3][4]

Η διεπαφή N1 χρησιμοποιείται από ένα UE για τη μετάδοση μη ραδιοφωνικών σημάτων μεταξύ AMF και UE (όπως το NAS) και περιλαμβάνει πληροφορίες σχετικές με τη συνδεσιμότητα, την κινητικότητα και συνεδρίες σχετικά με μηνύματα προς το AMF ώστε να διατηρείται η συνδεσιμότητα και η κινητικότητα του χρήστη προωθώντας παράλληλα πληροφορίες διαχείρισης συνεδρίας στο SMF.[3]

Η διεπαφή N2 υποστηρίζει σηματοδότηση επιπέδου ελέγχου μεταξύ δικτύου πρόσβασης (RAN) και του δικτύου κορμού (5G Core) καλύπτοντας περιπτώσεις σχετικές με διαχείριση στοιχείων UE και συμβάλλει στη διαχείριση συνεδριών/πόρων μονάδας πρωτοκόλλου δεδομένων (Protocol Data Unit, PDU) . Η διεπαφή N2 χρησιμοποιεί Stream Control Transmission Pro-

Εάν δεν έχει αναπτυχθεί UDSF στο σύνολο των AMF τότε γίνεται μία προγραμματισμένη αφαίρεση ενός AMF με τον ίδιο τρόπο όπως το UDSF αλλά με τη διαφορά ότι το AMF τότε προωθεί τα καταχωρημένα στοιχεία του UE σε ένα AMF εντός του συνόλου, αν και συνήθως δημιουργείται ένα backup αρχείο AMF για τα AMF που διαγράφονται. Τέλος μία αφαίρεση ενός AMF μπορεί να είναι και μη προγραμματισμένη όπως για παράδειγμα όταν επίκειται κάποιο σφάλμα. Για την αυτόματη ανάκαμψη σε ένα άλλο AMF τα στοιχεία του

tocon, SCTP (Next Generation Application Protocol, NGAP) μεταξύ δικτύων πρόσβασης και κορμού. [4]

Τέλος, το AMF λαμβάνει αιτήματα και κάνει τις απαραίτητες ενέργειες για τη διαχείριση της σύνδεσης και της κινητικότητας ενώ προωθεί τη διαχείριση συνεδριών μέσω της διεπαφής N11 στη λειτουργία SMF. Το AMF καθορίζει ποιο SMF είναι το πιο κατάλληλο ώστε να χειριστεί τα αιτήματα συνδεσιμότητας που ζητούνται από τη λειτουργία NRF. Το AMF και ένα συγκεκριμένο SMF που ανατίθεται από το NRF χρησιμοποιούν διάυλο μηνυμάτων Service Based Interface (SBI) με τον οποίο συνδέονται όλες οι service-base εφαρμογές.[2][3][4]

### 2.2.2 Session Management Function (SMF)

Η λειτουργία διαχείρισης συνεδρίας (Session Management Function, SMF) του συστήματος 5G, όπως προδίδει και το όνομα της, διαχειρίζεται τελικούς χρήστες (ή στην πραγματικότητα συσκευές). Κατά συνέπεια, είναι υπεύθυνη για τη ρύθμιση της συνδεσιμότητας του UE απευθείας με το δίκτυο δεδομένων καθώς και για τη διαχείριση του επιπέδου χρήστη για αυτή τη συνδεσιμότητα.

Η SMF είναι η λειτουργία που διαχειρίζεται τη συνεδρία χρήστη συμπεριλαμβανομένης της δημιουργίας, της τροποποίησης και της απελευθέρωσης των συνεδριών, και μπορεί να διαθέσει IP διευθύνσεις για τις IP PDU συνεδρίες. Το SMF επικοινωνεί έμμεσα με το UE μέσω του AMF, που μεταδίδει μηνύματα τα οποία σχετίζονται με την περίοδο σύνδεσης μεταξύ των συσκευών και των SMF.[4] Σε σύγκριση με το Evolved Packet System (EPS), η διαχείριση συνεδρίας πρόσθεσε ευελιξία, καθώς υπάρχουν νέες επιλογές για τύπους πρωτοκόλλου τελικού χρήστη, διαφορετικές επιλογές για τον χειρισμό της υπηρεσίας και συνέχεια της συνεδρίας, καθώς και μια ευέλικτη αρχιτεκτονική User Plane.[2]

Ακόμη, το SMF αλληλεπιδρά με άλλες λειτουργίες δικτύου μέσω των service based διεπαφών, επιλέγοντας και ελέγχοντας τις διαφορετικές λειτουργίες δικτύου χρήστη (User Plane Function, UPF) δια μέσου της διεπαφής N4. Επίσης, η SMF αλληλεπιδρά και με τη λειτουργία ελέγχου πολιτικής (Policy Control Function, PCF) για την ανάκτηση πολιτικών που χρησιμοποιούνται από την SMF για τη διαμόρφωση του UPF για τη συνεδρία PDU και επιπλέον περιλαμβάνει τη διαμόρφωση της καθοδήγησης κίνησης στο UPF για μεμονωμένες συνεδρίες. Μία ακόμη αρμοδιότητα της λειτουργίας SMF είναι να συλλέγει δεδομένα φόρτισης και να ελέγχει επίσης τη λειτουργία φόρτισης στο το UPF. Το SMF υποστηρίζει τόσο φόρτιση εκτός σύνδεσης όσο και online.[2][3][4]

Εν κατακλείδι, η SMF αποτελεί βασικό στοιχείο για την 5G Service-Based Αρχιτεκτονική (SBA) καθώς είναι πρωτίστως υπεύθυνη για την αλληλεπίδραση με το αποσυνδεδεμένο επίπεδο δεδομένων, τη δημιουργία ενημερώσεων και την αφαίρεση των συνεδριών της Μονάδας Δεδομένων Πρωτοκόλλου (PDU) αλλά και τη διαχείριση του περιβάλλοντος της περιόδου σύνδεσης με τη Λειτουργία επιπέδου χρήστη (UPF).[3]

### 2.2.3 User plane function(UPF)

Η λειτουργία επιπέδου χρήστη(User Plane Function,UPF) επεξεργάζεται και προωθεί δεδομένα χρήστη. Η λειτουργικότητα της UPF ελέγχεται από τη λειτουργία SMF. Διασυνδέεται με εξωτερικά δίκτυα IP και λειτουργεί ως σημείο αγκύρωσης για τα UEs προς τα εξωτερικά δίκτυα, κρύβοντας την κινητικότητα. Αυτό σημαίνει ότι μια διεύθυνση IP μιας συγκεκριμένης περιόδου λειτουργίας UE PDU μπορεί να δρομολογηθεί στο UPF που εξυπηρετεί αυτήν την συσκευή χρήστη UE και τη συνεδρία.

Το UPF εκτελεί διάφορους τύπους επεξεργασίας των δεδομένων προώθησης. Δημιουργεί αρχεία καταγραφής φόρτου και αναφορές για την κυκλοφορία κατά τη χρήση. Μπορεί επίσης να εφαρμόσει την ανάλυση «πακέτου ελέγχου» ελέγχοντας το περιεχόμενο των πακέτων δεδομένων χρήστη για χρήση είτε ως είσοδος σε αποφάσεις πολιτικής είτε ως βάση για την αναφορά της κίνησης στο δίκτυο. Εκτελείται επίσης πάνω σε διάφορες πολιτικές δικτύου ή χρηστών (για παράδειγμα η επιβολή της πύλης), ανακατεύθυνση της επισκεψιμότητας ή εφαρμογή διαφορετικών περιορισμών ταχύτητας δεδομένων.[2][3][4]

Όταν μια συσκευή βρίσκεται σε κατάσταση αδράνειας και δεν είναι άμεσα προσβάσιμη από το δίκτυο, οποιαδήποτε κίνηση που αποστέλλεται προς αυτήν τη συσκευή αποθηκεύεται προσωρινά από το UPF, που ενεργοποιεί μια σελίδα από το δίκτυο για να αναγκάσει τη συσκευή να επιστρέψει στη συνδεδεμένη κατάσταση και να λάβει τα δεδομένα της.

Το 5G Core UPF μπορεί να αναπτυχθεί σε σειρά, π.χ. ένα UPF κατανέμεται στην άκρη του δικτύου και ένα UPF βρίσκεται σε μια πιο κεντρική τοποθεσία δικτύου. Οι κανόνες δικτύου μπορούν στη συνέχεια να χρησιμοποιηθούν για τον έλεγχο της προώθησης της κυκλοφορίας του κατανεμημένου UPF. Ταξινόμηση πακέτων δεδομένων που προέρχονται από το UE (πακέτα uplink) μπορούν να εφαρμοστούν για να προσδιοριστεί εάν τα δεδομένα θα πρέπει να αποστέλλονται σε ένα τοπικό, κατανεμημένο δίκτυο IP ή εάν τα πακέτα πρόκειται να μεταφερθούν στο κεντρικό UPF.[3]

Το UPF μπορεί επίσης να εφαρμόσει σήμανση ποιότητας πακέτων (Quality-of-Service , QoS) προς το ραδιοδίκτυο ή προς εξωτερικά δίκτυα. Αυτό μπορεί να χρησιμοποιηθεί από το δίκτυο μεταφοράς ώστε να χειριστεί κάθε πακέτο με τη σωστή προτεραιότητα σε περίπτωση συμφόρησης στο δίκτυο.[2][3][4]

### 2.2.4 Network repository function (NRF)

Η λειτουργία Αποθετηρίου Δικτύου (Network repository function, NRF) είναι ένα αποθετήριο απο προφίλ των λειτουργιών δικτύου που είναι διαθέσιμα στο δίκτυο. Σκοπός του NRF είναι το να επιτρέψει στον καταναλωτή υπηρεσιών (για παράδειγμα ένα NF) να ανακαλύψει και να επιλέξει κατάλληλους παραγωγούς υπηρεσιών, δηλαδή NFs και NF υπηρεσίες, χωρίς να χρειάζεται να διαμορφωθεί εκ των προτέρων.

Όταν αναπτύσσεται ή αλλάζει ένα νέο στιγμιότυπο μιας λειτουργίας δικτύου, για παράδειγμα λόγω κλιμάκωσης, το NRF ενημερώνεται με τις νέες πληροφορίες προφίλ. Το προφίλ NRF μπορεί να ενημερωθεί από την ίδια τη λειτουργία δικτύου ή από άλλη οντότητα για λογαριασμό της λειτουργίας

δικτύου. [2]

Υπάρχει επίσης και ένας μηχανισμός διατήρησης ζωντανής λειτουργίας που επιτρέπει στο NRF να διατηρεί το αποθετήριο και να αφαιρεί τα προφίλ των λειτουργιών δικτύου που λείπουν ή είναι αδρανής.

Το προφίλ NF στο NRF περιέχει πληροφορίες όπως ο τύπος του NF, η διεύθυνση, η χωρητικότητα, οι υποστηριζόμενες υπηρεσίες και διευθύνσεις NF για κάθε στιγμιότυπο υπηρεσίας NF. Οι πληροφορίες αυτές παρέχονται στον καταναλωτή υπηρεσιών NF κατά τη διαδικασία αναζήτησης και παρέχει αρκετές πληροφορίες ώστε ο καταναλωτής υπηρεσιών να χρησιμοποιεί τη διεπαφή που βασίζεται στην υπηρεσία των επιλεγμένων NF και των υπηρεσιών NF.

Το προφίλ NRF περιέχει επίσης πληροφορίες εξουσιοδότησης και το προφίλ παρέχεται μόνο σε έναν καταναλωτή που μπορούν να ανακαλύψουν συγκεκριμένη λειτουργία ή υπηρεσία δικτύου.[2][3][4]

### 2.2.5 Unified data management function (UDM)

Η λειτουργία ενοποιημένης διαχείρισης δεδομένων(Unified data management function, UDM) είναι μία διεπαφή(front-end) για τα δεδομένα συνδρομής χρήστη που είναι αποθηκευμένα στο ενοποιημένο αποθετήριο δεδομένων(Unified data repository, UDR).

Η UDM λειτουργία χρησιμοποιεί δεδομένα συνδρομής που μπορεί να αποθηκευτούν στο UDR για την εκτέλεση της λογικών εφαρμογών όπως εξουσιοδότηση πρόσβασης, διαχείριση εγγραφής και δυνατότητα πρόσβασης για τερματισμό ενός συμβάντος όπως για παράδειγμα SMS.

Όταν ένας UE συνδέεται με το σύστημα, το UDM επιτρέπει την πρόσβαση και εκτελεί πολλούς ελέγχους υποστηριζόμενων λειτουργιών, φραγή και περιορισμούς όπως η περιαγωγή.

Επίσης, η UDM παράγει τα διαπιστευτήρια πιστοποίησης όπου η λειτουργία AUSF χρησιμοποιεί με τη σειρά της για να πιστοποιηθεί ένα UE. Επίσης, διαχειρίζεται την μόνιμη απόρρητη ταυτότητα και μπορεί να χρησιμοποιηθεί από άλλες οντότητες για την επίλυση κρυμμένων μόνιμων ταυτοτήτων(SUCI) στην πραγματική πραγματική ταυτότητα(SUPI). Τέλος, μπορούν να χρησιμοποιηθούν για τον ίδιο χρήστη διαφορετικά στιγμιότυπα UDM σε διαφορετικές συναλλαγές και ακόμη το UDM παρακολουθεί ποιο στιγμιότυπο AMF εξυπηρετεί ένα συγκεκριμένο UE και ποια SMF εξυπηρετούν τις συνεδρίες για το PDU του. [2][3][4]

### 2.2.6 Unified Data Repository(UDR)

Το ενοποιημένο αποθετήριο δεδομένων (Unified Data Repository,UDR) είναι μία βάση δεδομένων όπου αποθηκεύονται διάφοροι τύποι δεδομένων. Τα σημαντικότερα δεδομένα που αποθηκεύει είναι τα δεδομένα συνδρομής και τα δεδομένα που ορίζουν διάφορους τύπους πολιτικών δικτύου ή χρηστών. Η αποθήκευση και η πρόσβαση στα δεδομένα προσφέρονται ως υπηρεσίες σε άλλες λειτουργίες δικτύου, και συγκεκριμένα στις UDM, PCF και NEF.[2]

### 2.2.7 Unstructured data storage function( UDSF)

Η λειτουργία μη δομημένης αποθήκευσης δεδομένων (Unstructured data storage function, UDSF) είναι μια προαιρετική λειτουργία που επιτρέπει σε άλλα NF να αποθηκεύουν δυναμικά δεδομένα έξω από το ίδιο το NF. Αυτό μερικές φορές αναφέρεται ως «stateless» εφαρμογή.

Τα μη δομημένα δεδομένα αναφέρονται σε δεδομένα για τα οποία η δομή δεν ορίζεται στις προδιαγραφές που έχει προτείνει η κοινοπραξία 3GPP. Κάθε προμηθευτής που χρησιμοποιεί UDSF μπορεί να επιβάλει τη δική του συγκεκριμένη δομή των αποθηκευμένων δεδομένων στο UDSF και δεν αναμένεται να μπορεί να διαβάσει, αλλά και να κατανοήσει τον τύπο, αυτών των αποθηκευμένων δεδομένων ένα NF από διαφορετικούς προμηθευτές.[2][3]

### 2.2.8 AUthentication Server Function (AUSF)

Η λειτουργία πιστοποίησης εξυπηρετητή(AUthentication Server Function , AUSF) παρέχει τρεις υπηρεσίες και βρίσκεται μέσα στο οικιακό δίκτυο του συνδρομητή. Είναι υπεύθυνη για τον έλεγχο ταυτότητας στο οικιακό δίκτυο, βάσει πληροφοριών που ελήφθησαν από το UE και πληροφορίες που ανακτήθηκαν από το UDM. Παρέχει παραμέτρους ασφαλείας για την προστασία του “Steering of Roaming”, δηλαδή της διεύθυνσης περιαγωγής μεταξύ των διαφορετικών V-PLMN και παρέχει επίσης παραμέτρους ασφαλείας για την προστασία πληροφοριών στη διαδικασία ενημέρωσης των UE. [2]

### 2.2.9 5G equipment identity registry(5G-EIR)

Η καταχώρηση αναγνωριστικού εξοπλισμού 5G (5G equipment identity registry, 5G-EIR) είναι μια λειτουργία δικτύου που μπορεί να ελέγξει αν το αναγνωριστικό του μόνιμου εξοπλισμού (ένα αναγνωριστικό του πραγματικού υλικού της συσκευής) έχει συμπεριληφθεί στη μαύρη λίστα ή όχι. Αυτό μπορεί για παράδειγμα να χρησιμοποιηθεί από φορείς εκμετάλλευσης έτσι ώστε να αποκλείσουν την πρόσβαση στο δίκτυο σε μία συσκευή ή οποία έχει κλαπεί και έχει καταχωρηθεί στη μαύρη λίστα.[2][3]

### 2.2.10 Policy control function (PCF)

Η λειτουργία ελέγχου πολιτικής(Policy control function, PCF) παρέχει έλεγχο πολιτικής για λειτουργίες που σχετίζονται με τη διαχείριση συνεδριών, για πρόσβαση και λειτουργικότητα σχετική με την κινητικότητα, για επιλογή πρόσβασης UE και επιλογή PDU Session σχετικά με τη λειτουργικότητα και υποστηρίζει τη διαπραγμάτευση μελλοντικής μεταφοράς του ιστορικού των δεδομένων.[2][3]

Για πολιτικές σχετικές με τη διαχείριση συνεδριών, το PCF αλληλεπιδρά με λειτουργίες εφαρμογών και το SMF παρέχει εξουσιοδοτημένο QoS και έλεγχο φόρτου για ροές δεδομένων υπηρεσίας, για έλεγχο πολιτικής σχετικά με την περίοδο σύνδεσης PDU και αναφορά συμβάντων για συνεδρίες PDU.



Το PCF αλληλεπιδρά επίσης με το AMF για τον έλεγχο πολιτικής πρόσβασης και κινητικότητας που περιλαμβάνουν τη διαχείριση των περιορισμών περιοχής εξυπηρέτησης και τη διαχείριση της επιλογής κατά προτεραιότητας ραδιοσυχνότητας ( Radio Frequency Selection Priority, RFSP), μια παράμετρος που χρησιμοποιείται από το NG-RAN για τη διαφοροποίηση της επεξεργασίας διαφορετικών UE. Επιπλέον, το PCF παρέχει επίσης πληροφορίες πολιτικής στο UE (μέσω του AMF). Αυτές οι πολιτικές περιλαμβάνουν πολιτικές ανακάλυψης(discover) και επιλογής(selection) για δίκτυα εκτός 3GPP, πολιτική επιλογής τρόπου συνέχισης συνεδρίας, πολιτική επιλογής slice δικτύου, πολιτική επιλογής ονόματος δικτύου δεδομένων κι άλλα.[2][3]

### 2.2.11 Network slice selection function(NSSF )

Η λειτουργία επιλογής τεμαχίου δικτύου(Network slice selection function,NSSF ) επιλέγει το (σύνολο) στιγμιότυπων slice δικτύου για το UE και το σύνολο των AMF που πρέπει να εξυπηρετεί το UE. Το AMF μπορεί να είναι αφιερωμένο σε ένα ή ένα σύνολο slice δικτύου και το NSSF που γνωρίζει όλα τα slices του δικτύου βοηθά το AMF να επιλέξει για τη λειτουργικότητα. Ο τεμαχισμός δικτύου περιγράφεται στο κεφάλαιο 4.[2]

### 2.2.12 Network exposure function(NEF)

Η λειτουργία έκθεσης δικτύου (Network exposure function, NEF) έχει παρόμοιο ρόλο με το SCEF στο EPS και υποστηρίζει την έκθεση συμβάντων και δυνατοτήτων από το σύστημα 5G σε εφαρμογές και λειτουργίες δικτύου εντός και εκτός του δικτύου του χειριστή.

Η NEF μπορεί να υποστηρίζει την παρακολούθηση(monitoring) συγκεκριμένων συμβάντων στο σύστημα 5G και να καταστήσει αυτά τα συμβάντα διαθέσιμα σε εξουσιοδοτημένες εφαρμογές και λειτουργίες δικτύου. Παραδείγματα συμβάντων που είναι διαθέσιμα στην έκδοση 3GPP Release 15 είναι η τοποθεσία UE, η δυνατότητα πρόσβασης, η κατάσταση περιαγωγής και η απώλεια σύνδεσης.

Υποστηρίζει επίσης την παροχή προβλεπόμενων πληροφοριών συμπεριφοράς UE, αυτές οι πληροφορίες μπορούν να χρησιμοποιηθούν περαιτέρω π.χ. στο AMF για συντονισμό της συμπεριφοράς του συστήματος και της UE. Επιπλέον,η NEF υποστηρίζει εξωτερικές εφαρμογές για τη διαχείριση συγκεκριμένων QoS ή / και φόρτισης. Μπορεί να χρησιμοποιηθεί από εξουσιοδοτημένες εφαρμογές(για παράδειγμα API) για να ζητήσει συγκεκριμένη διαχείριση QoS / προτεραιότητας για μια συνεδρία, και για τον καθορισμό ισχύοντος χρεώσεων ή της τιμής χρέωσης. Ένα μόνο στιγμιότυπο της λειτουργίας NEF μπορεί να υποστηρίζει ένα υποσύνολο των λειτουργιών και σε ένα δίκτυο μπορεί να υπάρχουν NEF με διαφορετικές δυνατότητες.[2][3]

### 2.2.13 Network data analytics function(NWDAF)

Η λειτουργία ανάλυσης δεδομένων δικτύου(Network data analytics function, NWDAF) είναι μια λειτουργία του δικτύου 5G που μπορεί να συλλέγει δεδομένα, να εκτελεί στοιχεία ανάλυσης και να παρέχει αποτελέσματα σε άλλες λειτουργίες του δικτύου.

Οι λειτουργίες δικτύου ενδέχεται να προσαρμόζουν της συμπεριφορά τους βάσει αυτών των αναφερόμενων αποτελεσμάτων απο τη NWDAF. Στην έκδοση 15 της κοινοπραξίας 3GPP η λειτουργία είναι κάπως περιορισμένη και παρέχει μόνο ανάλυση δεδομένων τεμαχισμένου (slice) δικτύου (όπως ανάλυση πληροφοριών επιπέδου φόρτωσης του slice). Οι λειτουργίες PCF και NSSF που περιγράφηκαν προηγουμένως είναι δύο λειτουργίες που μπορούν να αξιοποιήσουν αναλυτικά στοιχεία της λειτουργίας NWDAF. Για παράδειγμα το NSSF επιλέγει ένα slice με μειωμένο επίπεδο φόρτωσης βάσει αυτών των πληροφοριών. [2][3]

### 2.2.14 Security edge protection proxy(SEPP)

Ο διακομιστής μεσολάβησης προστασίας για τη ασφάλεια στα άκρα του δικτύου(Security edge protection proxy, SEPP) είναι ένας μη διαφανής διακομιστής μεσολάβησης που χρησιμοποιείται για την προστασία της σηματοδότησης μεταξύ των χειριστών σε περιπτώσεις περιαγωγής. Το SEPP λειτουργεί ως ένας “διακόπτης-ρελέ” μεταξύ του Παραγωγού Υπηρεσιών και του Καταναλωτή Υπηρεσιών και αποκρύπτει την τοπολογία του δικτύου από άλλους χειριστές, υποστηρίζοντας παράλληλα φιλτράρισμα μηνυμάτων και παρακολούθηση ασφαλείας.[2][3]

### 2.2.15 Non-3GPP inter working function(N3IWF)

Η λειτουργία διαλειτουργικότητας εκτός 3GPP (N3IWF) τεχνολογιών χρησιμοποιείται για την ενσωμάτωση τύπων προσβάσεων εκτός 3GPP με τον πυρήνα 5G, όπως για παράδειγμα το WiFi.

Το N3IWF τεματίζει τα πρωτόκολλα IKEv2 και Ipsec, και περιγράφονται σε επόμενο κεφάλαιο, που χρησιμοποιούνται προς το UE μέσω NWu και μεταδίδει τις πληροφορίες που απαιτούνται για τον έλεγχο ταυτότητας του εξοπλισμού χρήστη και την εξουσιοδότηση πρόσβασης στον πυρήνα 5G μέσω της διεπαφής N2. Συνδέεται στον πυρήνα 5G μέσω των N2 και N3 διεπαφών για τα επίπεδα ελέγχου και χρήστη, αντίστοιχα.[2][3]

### 2.2.16 Application function(AF)

Η λειτουργία εφαρμογών (Application Function, AF) είναι μια απεικόνιση 3GPP εφαρμογών εντός του δικτύου του φορέα που αλληλεπιδρά με το 3GPP δίκτυο πυρήνα . Οι εφαρμογές μπορεί να αλληλεπιδρούν και να επηρεάζουν ορισμένες πτυχές του πυρήνα 5G και ενδέχεται να επηρεάζουν τη δρομολόγηση της κυκλοφορίας στο δίκτυο (παράδειγμα μια εφαρμογή υπολογιστικών άκρων), ή ακόμα μπορεί να έχουν πρόσβαση στη λειτουργία έκθεσης που αλληλεπιδρά με τον PCF για να επηρεάζουν τις πολιτικές QoS και φόρτισης.

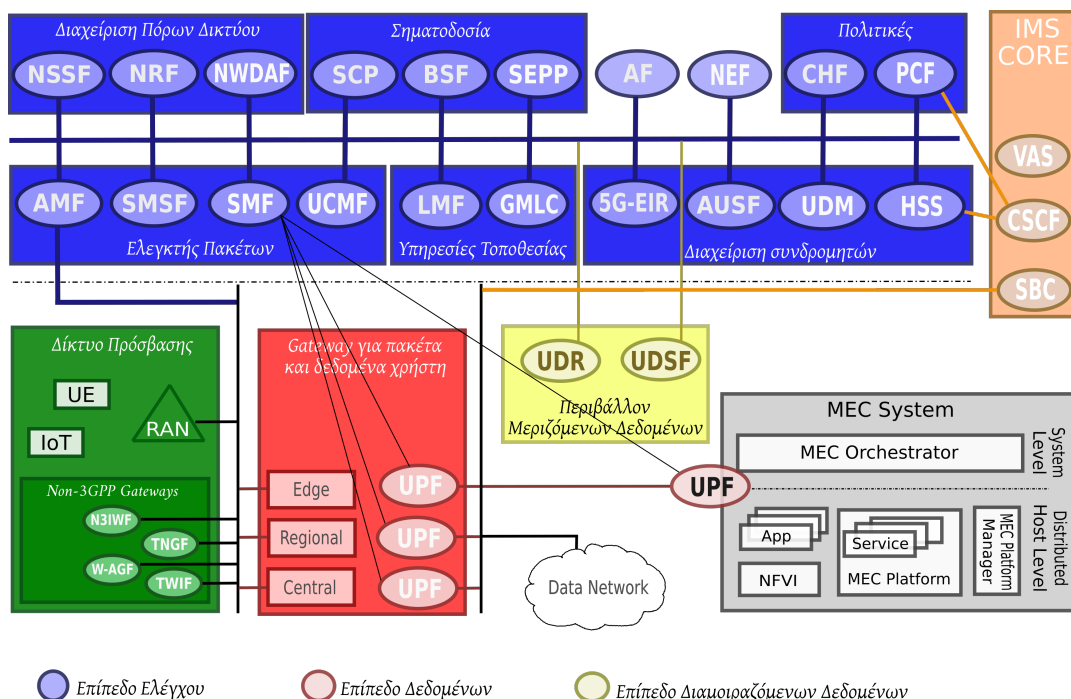
Εφαρμογές που θεωρούνται αξιόπιστες από έναν χειριστή ενδέχεται να επιτρέπεται να αλληλεπιδρούν απευθείας με σχετικές λειτουργίες δικτύου ενώ άλλες εφαρμογές ενδέχεται να χρησιμοποιούν ένα πλαίσιο εξωτερικής έκθεσης μέσω του NEF για να αλληλεπιδρούν με σχετικές λειτουργίες δικτύου.[2]

### 2.2.17 Short message service function(SMSF)

Η λειτουργία εξυπηρέτησης σύντομων μηνυμάτων (Short message service function, SMSF) υποστηρίζει την παράδοση SMS μεταξύ του UE και του 5G Core (μέσω του AMF). Η SMSF είναι υπεύθυνη για τον έλεγχο της συνδρομής και τον τερματισμό πρωτόκολλων SMS (SM-RP / SM-CP) που χρησιμοποιούνται για επικοινωνία με το UE. Η AMF παρέχει πρόσβαση στη σύνδεση NAS στο UE ως υπηρεσία στο SMSF πάνω από το οποίο το μεταφέρονται μηνύματα SM-RP / SM-CP.[2][3]

### 2.2.18 Location management function (LMF)

Η λειτουργία διαχείρισης τοποθεσίας Location management function, LMF) παρέχει λειτουργικότητα για τον προσδιορισμό της θέσης ενός UE. Η LMF μπορεί να ανακτήσει την τοποθεσία που εκτιμάται από το UE καθώς και μετρήσεις τοποθεσίας και άλλα δεδομένα από το NG-RAN. Με βάση τα ανακτημένα δεδομένα, τους ελέγχους συνδρομής και απορρήτου, το LMF μπορεί να καθορίσει και να παρέχει τη θέση των UE σε άλλα NF. Για να φτάσει στο UE και στο NG-RAN, το LMF χρησιμοποιεί υπηρεσίες από το AMF για πρόσβαση στη σύνδεση NAS στο UE και στη σύνδεση N2 NG-RAN αντίστοιχα.[2][3]



Εικόνα 2.8: Σύνολο λειτουργιών με εφαρμογή IMS Core και MEC συστήματος [43]

Η επιλογή του δικτύου κορμού γίνεται απο τους χειριστές των δικτύων και μπορεί να υπάρχει μεμονωμένη χρήση των δύο περιπτώσεων που περιγράφονται παραπάνω ή ακόμα και συνδυασμός αυτών. Σε κάθε περίπτωση όμως η λειτουργικότητα, το κόστος και η ωριμότητα της κάθε τεχνολογίας αποτελούν καταλυτικά χαρακτηριστικά επιλογής για την επίτευξη ενός ολοκληρωμένου και λειτουργικού συστήματος.

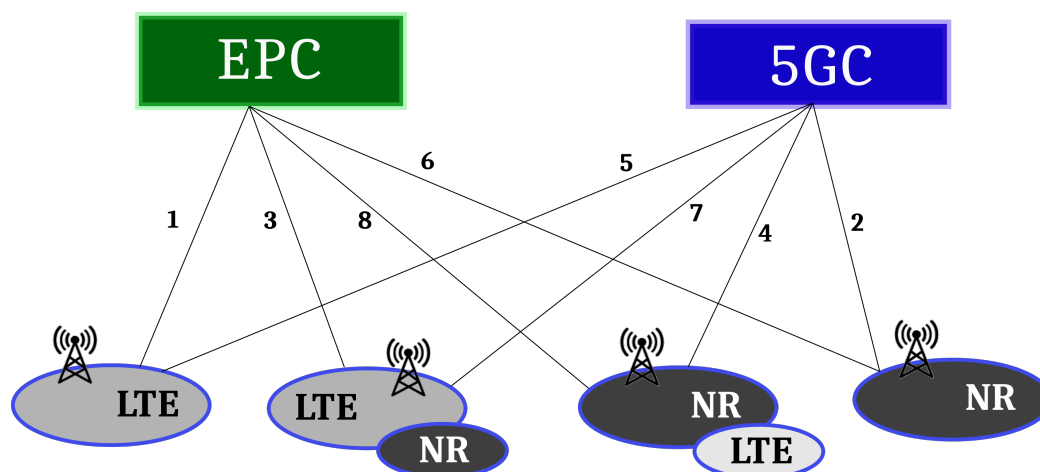
Στην εικόνα 2.8 αναπαριστάται μία πλήρως δομημένη αρχιτεκτονική αυτόνομου 5g συστήματος πυρήνα που συνδέεται με ένα δίκτυο πρόσβασης και ανταλλάσσει δεδομένα αρχικά με ένα πυρήνα IP Multimedia Core Network Subsystem που δέχεται πακέτα πολυμέσων και εξυπηρετείται άμεσα απο τη λειτουργία HSS καθώς ακολουθεί τις πολιτικές του PCF. Επίσης, συμμετέχει στη διακίνηση των δεδομένων που εξυπηρετεί το Gateway.

Επιπλέον, παρατηρούμε και ένα Multi-Access Edge Computing(MEC) που εξυπηρετείται απο το UPF και απο το SMF που κάνει έναρξη μιας νέας συνεδρίας για να διακινήσει τα δεδομένα του.[43]

Σύμφωνα με τις διαφορετικές δομές του δικτύου γίνεται κατανοητό ότι μπορούμε να κάνουμε μεμονωμένη χρήση ενός εξ' αυτών αλλά και ένα σύνολο συνδυασμών που μας επιτρέπουν να υλοποιούμε ένα σύστημα επικοινωνίας τερματικών με επιτυχία. Ο παρακάτω πίνακας αναφέρει ορισμένες επιλογές που είναι διαθέσιμες για την ανάπτυξη ενός τέτοιου ολοκληρωμένου συστήματος επικοινωνίας.

Access Network:	Μόνο LTE	Μόνο NR	LTE με NR μόνο για τα δεδομένα	NR με LTE μόνο για τα δεδομένα
EPC Δίκτυο Κορμού	Επιλογή 1 (=4G)	Επιλογή 6 (Αγνοήθηκε)	Επιλογή 3	Επιλογή 8 (Αγνοήθηκε)
5GC Δίκτυο Κορμού	Επιλογή 5	Επιλογή 2	Επιλογή 7	Επιλογή 4

Πίνακας 2.1: Αναπαράσταση διαφορετικών υλοποιήσεων συνδυαστικών επιλογών [2]



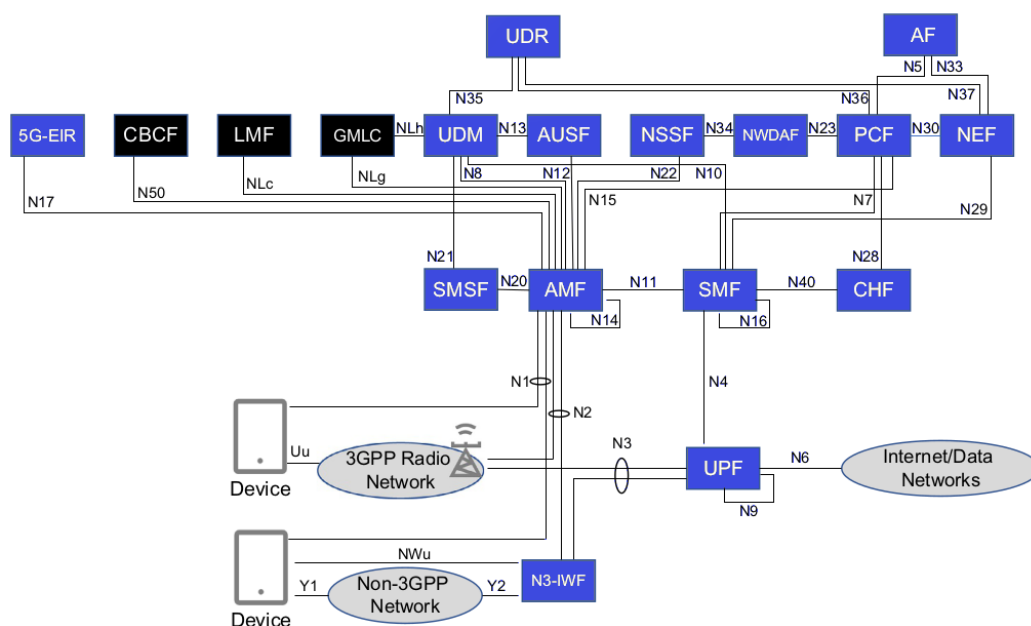
Εικόνα 2.9: Διαφορετικοί συνδυασμοί επιλογών χρήσης δικτύου κορμού[2]

## 2.3 Μοντέλα αρχιτεκτονικής δικτύου κορμού 5G

Σε σύγκριση με την υπάρχουσα αρχιτεκτονική EPC, η αρχιτεκτονική πυρήνα 5GC είναι ταυτόχρονα πολύ παρόμοια και πολύ διαφορετική. Τα μέρη επεξεργασίας δεδομένων χρήστη, καθώς και η ενσωμάτωση με δίκτυα ραδιοπρόσβασης 3GPP, βρίσκουν ομοιότητες μεταξύ του νέου 5GC και της παραδοσιακής αρχιτεκτονικής δικτύου EPC, που ορίστηκε αρχικά για 4G / LTE. Το τμήμα του δικτύου που περιέχει λειτουργικότητα μόνο για σηματοδότηση, είναι από την άλλη πλευρά πολύ διαφορετικό. Μια άλλη διαφορά μεταξύ της αρχιτεκτονικής EPC που χρησιμοποιείται για 4G και 5G NSA είναι ότι η αρχιτεκτονική του 5G Core μπορεί να απεικονιστεί και να περιγραφεί με δύο διαφορετικούς τρόπους. Στις δύο παραγράφους που ακολουθούν περιγράφονται οι δύο αυτές περιπτώσεις που συναντάμε.[2]

### 2.3.1 Αρχιτεκτονική σημείου αναφοράς (Reference Point Architecture)

Η οπτικοποίηση της αρχιτεκτονικής του δικτύου πυρήνα 5G, δείχνει πώς οι λειτουργίες δικτύου αλληλεπιδρούν με άλλες λειτουργίες δικτύου, με τις παραδοσιακές διασυνδέσεις από σημείο σε σημείο. Οι διεπαφές αυτές μπορεί να είναι χρήσιμες για να δείξουν ποιες από τις λειτουργίες δικτύου χρησιμοποιούν ή καταναλώνουν, τις υπηρεσίες από τις οποίες λειτουργούν άλλα δίκτυα. Ακόμα κι αν όλες οι λειτουργίες του δικτύου θεωρητικά θα μπορούσαν να συνδεθούν σε ένα πλήρες πλέγμα σύνδεσης, οι πραγματικές ροές κλήσεων καθορίζουν τους συνδυασμούς υπηρεσιών που ισχύουν σε πραγματικές λειτουργίες. Αυτοί οι συνδυασμοί απεικονίζονται ως λογικές διεπαφές, ή πιο σωστά - σημεία αναφοράς, στην εικόνα που φαίνεται παρακάτω, σε μία αναπαράσταση σημείο προς σημείο.[2]



Εικόνα 2.10: Οπτικοποίηση Αρχιτεκτονικής διεπαφών σημείο-προς-σημείο [2]

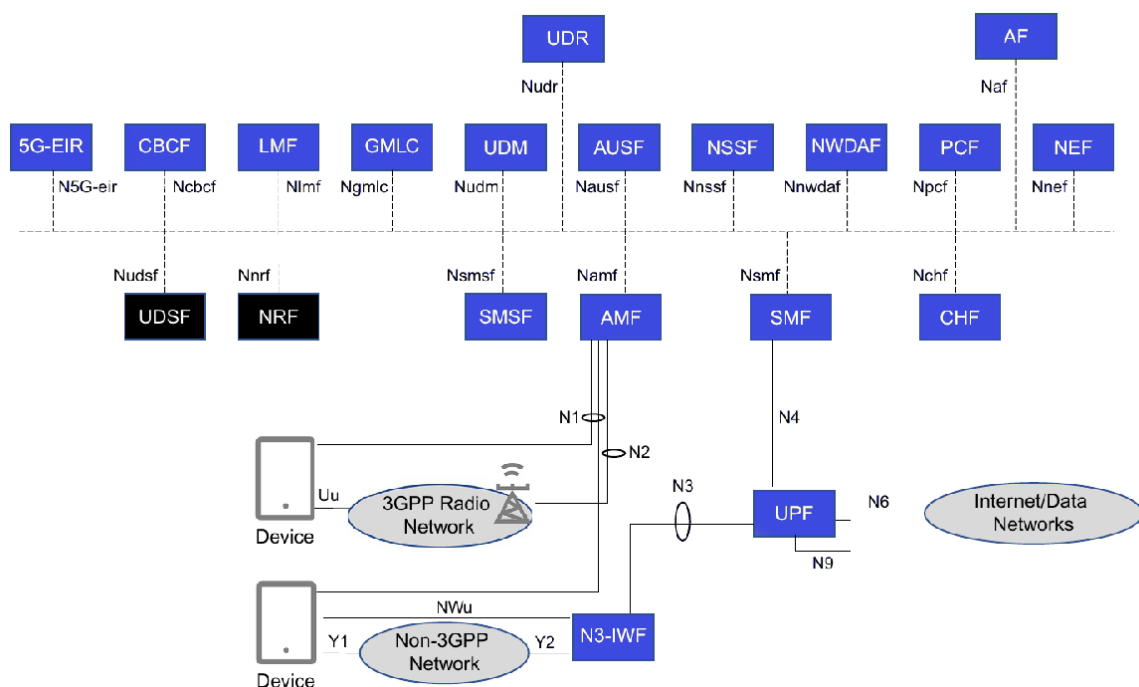
- N1: Σημείο αναφοράς μεταξύ του UE και του AMF.  
N2: Σημείο αναφοράς μεταξύ του (R)AN και του AMF.  
N3: Σημείο αναφοράς μεταξύ του (R)AN και του UPF.  
N4: Σημείο αναφοράς μεταξύ του SMF και του UPF.  
N6: Σημείο αναφοράς μεταξύ του UPF και ενός δικτύου δεδομένων.  
N9: Σημείο αναφοράς μεταξύ δύο UPFs.  
N5: Σημείο αναφοράς μεταξύ του PCF και ενός AF.  
N7: Σημείο αναφοράς μεταξύ του SMF και του PCF.  
N8: Σημείο αναφοράς μεταξύ του UDM και του AMF.  
N10: Σημείο αναφοράς μεταξύ του UDM και του SMF.  
N11: Σημείο αναφοράς μεταξύ του AMF και του SMF.  
N12: Σημείο αναφοράς μεταξύ AMF και AUSF.  
N13: Σημείο αναφοράς μεταξύ του UDM και AUSF.  
N14: Σημείο αναφοράς μεταξύ δύο AMFs.  
N15: Σημείο αναφοράς μεταξύ του PCF και του AMF.  
N16: Σημείο αναφοράς μεταξύ δύο SMFs.  
N16a: Σημείο αναφοράς μεταξύ SMF και I-SMF.  
N17: Σημείο αναφοράς μεταξύ AMF και 5G-EIR.  
N18: Σημείο αναφοράς μεταξύ οποιουδήποτε NF και UDSF.  
N19: Σημείο αναφοράς μεταξύ δύο PSA UPFs για 5G LAN-type υπηρεσίες.  
N22: Σημείο αναφοράς μεταξύ AMF και NSSF.  
N23: Σημείο αναφοράς μεταξύ PCF και NWDAF.  
N24: Σημείο αναφοράς μεταξύ του PCF ενός δικτύου επισκέπτη και του PCF στο οικιακό δίκτυο.  
N26: Σημείο αναφοράς μεταξύ AMF και MME.  
N27: Σημείο αναφοράς μεταξύ NRF του δικτύου επισκέπτη και του NRF στο οικιακό δίκτυο.  
N28: Σημείο αναφοράς μεταξύ PCF και CHF.  
N29: Σημείο αναφοράς μεταξύ NEF και SMF.  
N30: Σημείο αναφοράς μεταξύ PCF και NEF.  
N31: Σημείο αναφοράς μεταξύ του NSSF σε ένα ed network και του NSSF στο οικιακό δίκτυο.  
N32: Σημείο αναφοράς μεταξύ SEPP του δικτύου επισκέπτη και του SEPP στο οικιακό δίκτυο.  
N33: Σημείο αναφοράς μεταξύ NEF και AF.  
N34: Σημείο αναφοράς μεταξύ NSSF και NWDAF.  
N35: Σημείο αναφοράς μεταξύ UDM και UDR.  
N36: Σημείο αναφοράς μεταξύ PCF και UDR.  
N37: Σημείο αναφοράς μεταξύ NEF και UDR.  
N38: Σημείο αναφοράς μεταξύ I-SMFs.  
N40: Σημείο αναφοράς μεταξύ SMF και του CHF.  
N50: Σημείο αναφοράς μεταξύ AMF και του CBCF.  
N51: Σημείο αναφοράς μεταξύ AMF και NEF.  
N52: Σημείο αναφοράς μεταξύ NEF και UDM.  
N55: Σημείο αναφοράς μεταξύ AMF και του UCMF.  
N56: Σημείο αναφοράς μεταξύ NEF και του UCMF.  
N57: Σημείο αναφοράς μεταξύ AF και του UCMF.  
N58: Σημείο αναφοράς μεταξύ AMF και του NSSAAF.

N59: Σημείο αναφοράς μεταξύ UDM και του NSSAAF.

Αξίζει να σημειωθεί ότι τα σημεία αναφοράς που αριθμούνται από N40 έως N49 έχουν δεσμευθεί για μελλοντική χρήση.[7]

### 2.3.2 Αρχιτεκτονική βασιζόμενη στις υπηρεσίες (Service-Based Architecture, SBA)

Η δεύτερη οπτικοποίηση δείχνει τον τρόπο σύνδεσης διαφορετικών λειτουργιών δικτύου. Η κύρια διαφορά σε σύγκριση με προηγούμενες αρχιτεκτονικές 3GPP σε αυτήν την οπτικοποίηση είναι η έννοια των διεπαφών που βασίζονται σε υπηρεσίες. Αυτό σημαίνει ότι οι λειτουργίες του δικτύου που περιλαμβάνουν λογικές μεθόδους και λειτουργίες για την επεξεργασία ροών σηματοδότησης δεν διασυνδέονται μέσω διεπαφών από σημείο σε σημείο, αλλά αντ' αυτού εκθέτουν και καθιστούν διαθέσιμες υπηρεσίες στις άλλες λειτουργίες δικτύου. [2] Για κάθε αλληλεπίδραση μεταξύ λειτουργιών δικτύου, μία από αυτές λειτουργεί ως «Καταναλωτής υπηρεσίας» και ο άλλος ως «Παραγωγός υπηρεσιών». Η αναπαράσταση αυτής της αρχιτεκτονικής φαίνεται στο παρακάτω σχήμα



Εικόνα 2.11: Οπτικοποίηση Αρχιτεκτονικής διεπαφών βασισμένες στις υπηρεσίες(SBA) [2]

Μια σημαντική διαφορά στον πυρήνα 5G σε σύγκριση με προηγούμενες γενιές παραδοσιακών αρχιτεκτονικών δικτύου που εκπροσωπούνται από "κόμβους" ή "στοιχεία δικτύου" που συνδέονται με διεπαφές, είναι η χρήση αλληλεπιδράσεων που βασίζονται σε υπηρεσίες μεταξύ λειτουργιών δικτύου. Αυτό σημαίνει ότι κάθε λειτουργία δικτύου προσφέρει μία ή περισσότερες υπηρεσίες σε άλλες λειτουργίες δικτύου στο δίκτυο. Στην αρχιτεκτονική 5GC,

αυτές οι υπηρεσίες διατίθενται μέσω διασυνδέσεων λειτουργιών δικτύου που συνδέονται με την κοινή αρχιτεκτονική βάσει υπηρεσίας (SBA). Στην πράξη αυτό σημαίνει ότι η λειτουργικότητα υποστηρίζεται σε μία συγκεκριμένη εργασία λειτουργίας και είναι διαθέσιμη και προσβάσιμη μέσω API (Διεπαφή προγραμματισμού εφαρμογών). Θα πρέπει να σημειωθεί ότι αυτή η αρχιτεκτονική ισχύει μόνο για τη λειτουργία σηματοδότησης και όχι για τη μεταφορά δεδομένων χρήστη.

Παρακάτω αναφέρονται οι τεχνικές και οι τεχνολογίες που υποστηρίζουν την αρχιτεκτονική που βασίζεται στις υπηρεσίες(SBA)[6][7]

### HTTP REST διεπαφές

Η μέθοδος επικοινωνίας που ορίζεται για το 5G Core βασίζεται στο ευρέως χρησιμοποιούμενο “HTTP REST paradigm” που είναι ένα σύνολο κανόνων ή οδηγιών που καθορίζουν τον τρόπο όπου ένας ιστός τεχνολογιών επικοινωνίας αποκτά πρόσβαση σε υπηρεσίες από κατανεμημένες εφαρμογές χρησιμοποιώντας Διεπαφή Προγραμματισμού Εφαρμογών(Application Programming Interface, API). Η Μεταφορά αναπαραστατικής κατάστασης(Representational State Transfer,REST) ορίζει ένα σύνολο κανόνων σχεδιασμού για τον τρόπο εφαρμογής της επικοινωνίας μεταξύ διαφορετικών ενοτήτων λογισμικού σε μία δικτυακή αρχιτεκτονική.[2]

Αυτός είναι και ο τυπικός τρόπος σχεδιασμού εφαρμογών δικτύωσης IT σήμερα, και επιλέχθηκε από την 3GPP ως μέσο που επιτρέπει την αυστηρότερη ενσωμάτωση μεταξύ έργων κινητού δικτύου και περιβαλλόντων IT συστημάτων (πληροφορικής), καθώς και για προσπάθειες ανάπτυξης μικρότερων και απλουστευμένων υπηρεσιών.

Η προσδοκία είναι ότι οι δυνατότητες του δικτύου θα είναι ευκολότερο να επεκταθούν κατά τη χρήση σχετικά πιο “ελαφρών” υπηρεσιών βάσει διεπαφής (Service-Based Interface, SBI), παρά εάν χρησιμοποιείτε μια πιο παραδοσιακή αρχιτεκτονική από σημείο σε σημείο που βασίζεται σε λεπτομερής και εκτεταμένες προσπάθειες καθορισμού πρωτοκόλλου.[2][6]

Η χρήση SBI και API μπορεί επίσης να θεωρηθεί ως λογική επιλογή από το 3GPP κατά τον καθορισμό του 5G δικτύου πυρήνα, καθώς οι εφαρμογές λογισμικού 5GC που υλοποιούν τις λειτουργίες δικτύου θεωρείται ότι εκτελούνται σε ένα IT-like ή ακόμη και κοινόχρηστο περιβάλλον IT,συνήθως σε ένα κέντρο δεδομένων cloud.

Μια εναρμόνιση τόσο των τεχνολογιών λογισμικού όσο και της IT αρχιτεκτονικής σε ολόκληρη τη κατασκευή του δικτύου κινητής τηλεφωνίας και την υποστήριξη εφαρμογών IT είναι σε κάποιο βαθμό δυνατή με αυτήν την προσέγγιση.

Το HTTP REST χρησιμοποιεί σύνταξη μηνυμάτων από το ευρέως χρησιμοποιούμενο πρωτόκολλο ιστού HTTP και βασίζεται στην έννοια της μοντελοποίησης πόρων, που σημαίνει ότι μια κατανεμημένη εφαρμογή λογισμικού μπορεί να αντιμετωπιστεί μέσω Uniform Resource Identifiers (URIs), όπου στην πράξη είναι μια διεύθυνση ιστού που δείχνει έναν πόρο ή σύνολο πόρων. Επιπλέον, χρησιμοποιείται ένα πολύ απλό σύνολο εντολών, οι τυπικές «μέθοδοι» HTTP. Οι πιο σημαντικές εντολές του πρωτοκόλλου αναφέρονται παρακάτω.[6]



- GET - χρησιμοποιείται για τη λήψη δεδομένων από έναν διακομιστή και δεν αλλάζει τα δεδομένα.
- POST - χρησιμοποιείται για την αποστολή δεδομένων σε διακομιστή.
- PUT - χρησιμοποιείται επίσης για την αποστολή δεδομένων σε διακομιστή, αλλά αντικαθιστά τα υπάρχοντα δεδομένα.
- DELETE - χρησιμοποιείται για την αφαίρεση δεδομένων από έναν διακομιστή.

Μια σημαντική πτυχή του REST είναι ότι κάθε επικοινωνία πρέπει να περιλαμβάνει το πλήρες σύνολο πληροφοριών που απαιτείται για μια συγκεκριμένη ενέργεια επεξεργασίας. Δεν πρέπει να βασίζεται σε προηγούμενα μηνύματα και ως εκ τούτου μπορεί να θεωρηθεί ως stateless. Η χρήση αυτής της αρχής για το σχεδιασμό λογισμικού επιτρέπει εξαιρετικές δυνατότητες κλιμάκωσης και κατανομής του συστήματος. [6]

### Εγγραφή και ανακάλυψη υπηρεσίας (Service registration and discovery)

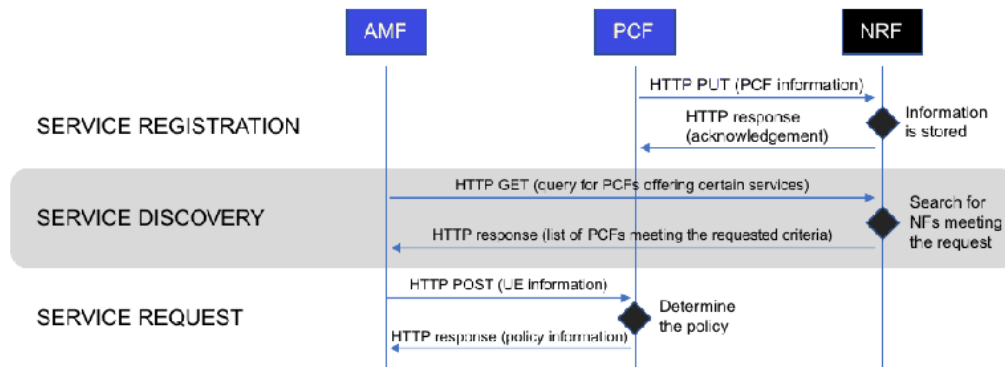
Όταν δύο λειτουργίες δικτύου επικοινωνούν μέσω της αρχιτεκτονικής 3GPP SBA, αναλαμβάνουν δύο διαφορετικούς ρόλους. Η συνάρτηση δικτύου που αποστέλλει το αίτημα έχει το ρόλο ενός καταναλωτή υπηρεσίας, ενώ η συνάρτηση δικτύου που προσφέρει μια υπηρεσία και ενεργοποιεί κάποια ενέργεια βάσει του αιτήματος έχει το ρόλο ενός παραγωγού υπηρεσιών. Με την ολοκλήρωση της ζητούμενης ενέργειας, ο Παραγωγός υπηρεσιών ανταποκρίνεται στον Καταναλωτή της Υπηρεσίας.[2]

Ένα κρίσιμο σημείο κατά τη διαδικασία αυτή, είναι ο μηχανισμός με τον οποίο ο καταναλωτής υπηρεσιών μπορεί να εντοπίσει και να επικοινωνήσει με έναν παραγωγό υπηρεσιών που μπορεί να παρέχει την ζητούμενη υπηρεσία. Η λύση βασίζεται στην έννοια του Service Discovery.

Το Service Discovery βασίζεται στο ότι μια γνωστή λειτουργία στο δίκτυο παρακολουθεί όλους τους διαθέσιμους παραγωγούς υπηρεσιών και τις υπηρεσίες που προσφέρουν. Αυτό επιτυγχάνεται μέσω του ότι κάθε Παραγωγός Υπηρεσιών, για παράδειγμα μια Λειτουργία Δικτύου 3GPP όπως το PCF, καταγράφει ότι οι υπηρεσίες του είναι διαθέσιμες. Στην αρχιτεκτονική 5GC, αυτή η εγγραφή γίνεται σε μια αποκλειστική λειτουργία δικτύου που αναφερθήκαμε προηγουμένως και ονομάζεται λειτουργία αποθετηρίου δικτύου (NRF). Αυτό επιτρέπει στο NRF να παρακολουθεί όλα διαθέσιμες υπηρεσίες όλων των λειτουργιών δικτύου στο δίκτυο. Επίσης κάθε μεμονωμένη λειτουργία δικτύου πρέπει να παρέχεται ή να διαμορφώνεται με τη διεύθυνση ενός ή περισσότερων NRF, αλλά δεν χρειάζεται να έχει διευθύνσεις σε όλες τις άλλες λειτουργίες δικτύου που έχουν διαμορφωθεί.[6]

Ένα πρακτικό παράδειγμα που περιλαμβάνει τρεις πραγματικές λειτουργίες δικτύου PCF, AMF και NRF αναπαρίσταται στο παρακάτω σχήμα υποθέτοντας ότι όλες οι λειτουργίες δικτύου που πρέπει να αλληλεπιδράσουν είναι μέρος μιας συγκεκριμένης ροής κλήσεων.[2]

Όπως παρατηρούμε από την εικόνα, η ροή ξεκινά με το PCF να κάνει εγγραφή υπηρεσίας. Κατά τη διάρκεια της εγγραφής, το PCF ενεργεί ως



Εικόνα 2.12: Ενοποιημένη ροή κλησεων[2]

Καταναλωτής Υπηρεσίας και το NRF ως Παραγωγός Υπηρεσιών, προσφέροντας την υπηρεσία «Εγγραφή Πόρων Δικτύου» στο PCF.

Έπειτα, το PCF εγγράφεται στο NRF χρησιμοποιώντας ένα μήνυμα HTTP PUT που περιλαμβάνει πληροφορίες σχετικά με το PCF, όπως διαθέσιμες υπηρεσίες, διεύθυνση δικτύου και ταυτότητα. Το NRF επαληθεύει ότι το αίτημα είναι έγκυρο, αποθηκεύει τα δεδομένα που σχετίζονται με την εγγραφή PCF και αναγνωρίζει την εγγραφή PCF με απόκριση πίσω στο PCF. Τώρα οι υπηρεσίες PCF είναι διαθέσιμες σε άλλες λειτουργίες δικτύου μέσω ερωτήματος του NRF.[6][7]

Στην επόμενη φάση, μια άλλη λειτουργία δικτύου όπως το AMF θέλει να χρησιμοποιήσει τις υπηρεσίες ενός PCF. Αυτό επιτυγχάνεται μέσω του πρώτου ερωτήματος του NRF για μια λίστα PCF που προσφέρουν αυτές τις υπηρεσίες. Αυτή η φάση ονομάζεται Service Discovery. Σε αυτήν την περίπτωση, το AMF είναι ο καταναλωτής υπηρεσιών και το NRF είναι ο παραγωγός υπηρεσιών. Το AMF στέλνει ένα ερώτημα στο NRF, δηλώνοντας τι είδους λειτουργία δικτύου ζητά και ποιες υπηρεσίες θα υποστηρίξει αυτό το NF. Αυτό γίνεται χρησιμοποιώντας ένα μήνυμα HTTP GET. Το NRF φιλτράρει όλες τις λειτουργίες δικτύου που είναι καταχωρημένες και παρέχουν τις ζητούμενες υπηρεσίες και, στη συνέχεια, ανταποκρίνεται στο AMF.

Όταν ολοκληρωθεί αυτό το βήμα, το AMF μπορεί να κάνει μια επιλογή PCF που πληροί τις απαιτήσεις υπηρεσίας και, στη συνέχεια, να επικοινωνήσει με τον επιλεγμένο PCF με ένα αίτημα εξυπηρέτησης. Σε αυτό το βήμα, το AMF είναι και πάλι ο καταναλωτής υπηρεσιών, ενώ ο PCF είναι ο παραγωγός υπηρεσιών. Αυτό γίνεται χρησιμοποιώντας ένα μήνυμα HTTP POST.

Σε αυτό το σημείο τονίζεται ότι θα πρέπει να λαμβάνεται υπόψη ότι το αίτημα υπηρεσίας που αναφέρεται εδώ δεν αναμιγνύεται με το Αίτημα Υπηρεσίας που αποστέλλει μια κινητή συσκευή στο δίκτυο όταν πρόκειται να μετακινηθεί από κατάσταση αδράνειας σε λειτουργία σύνδεσης. Με την παραλαβή αυτού του αιτήματος υπηρεσίας, το PCF καθορίζει την ισχύουσα πολιτική που ζητείται από το AMF και ανταποκρίνεται στο με μια απόκριση HTTP.

Τέλος, αξίζει να σημειώσουμε ότι αυτά τα τρία μέρη δεν συμβαίνουν συνήθως κατα ανάγκη σε σειρά. Μια λειτουργία δικτύου συνήθως καταγράφεται στο NRF όταν τίθεται σε λειτουργία, ενώ τα αιτήματα ανακάλυψης και υπηρεσίας ενδέχεται, για παράδειγμα, να πραγματοποιούνται

όταν μια συσκευή συνδέεται στο δίκτυο.[2][6][7]

Η υπόλοιπη ροή κλήσεων και η επακόλουθη αλληλεπίδραση μεταξύ των λειτουργιών δικτύου είναι πέρα από τα πλαίσια αυτής της εργασίας, αλλά η ιδέα παραμένει η ίδια σε κάθε βήμα και για όλες τις άλλες ροές κλήσεων μεταξύ λειτουργιών δικτύου που αλληλεπιδρούν με HTTP εντός της αρχιτεκτονικής που βασίζεται στην υπηρεσία(SBA). Η λειτουργία ενός δικτύου λειτουργεί ως παραγωγός υπηρεσιών, όπως αναφερθήκαμε, και μια άλλη ως ο καταναλωτής υπηρεσιών. Και όλη η επικοινωνία γίνεται χρησιμοποιώντας το πρωτόκολλο HTTP.[2]

Υπάρχει και ένας άλλος τρόπος αλληλεπίδρασης μεταξύ ενός παραγωγού υπηρεσιών και ενός ή πολλών καταναλωτών υπηρεσιών που βασίζεται στο γεγονός ότι μία ή περισσότερες λειτουργίες δικτύου μπορούν να εγγραφούν σε μια υπηρεσία από άλλη λειτουργία δικτύου. Η Λειτουργία Δικτύου που ενεργεί ως Παραγωγός Υπηρεσιών αποστέλλει ειδοποιήσεις σε όλους τους Καταναλωτές Υπηρεσιών όταν πληρούνται ορισμένα συγκεκριμένα κριτήρια, για παράδειγμα όταν έχουν αλλάξει ορισμένες πληροφορίες. Η έννοια της εγγραφής και ειδοποίησης καταργεί την ανάγκη για τους καταναλωτές υπηρεσιών να ζητούν συχνά πληροφορίες από τον παραγωγό υπηρεσιών, αντί να τους επιτρέπει να περιμένουν να ειδοποιηθεί ο παραγωγός υπηρεσιών όταν κάτι συνέβη.[2][6]

Παρατηρώντας τις δύο παραπάνω αρχιτεκτονικές, μια άλλη διαφορά μεταξύ των δύο τρόπων αναπαράστασης της αρχιτεκτονικής, εκτός από τις διαφορετικές συνδέσεις διεπαφών, είναι ότι ορισμένες λειτουργίες δικτύου εφαρμόζονται μόνο σε μία από τις αναπαραστάσεις αυτές σε κάθε περίπτωση.[6] Στην αναπαράσταση βάσει υπηρεσιών, όπως φαίνεται στην εικόνα 2.11, οι δύο λειτουργίες δικτύου NRF και UDSF είναι ορατές (επισημαίνονται με μαύρο χρώμα) και ισχύουν μόνο για την αναπαράσταση της αρχιτεκτονικής με βάση την υπηρεσία. Το UDSF έχει μία διασύνδεση από σημείο σε σημείο (N18) αλλά είναι λιγότερο χρήσιμο να αναπαρασταθεί καθώς μπορεί να συνδεθεί με οποιαδήποτε άλλη λειτουργία δικτύου.[6]

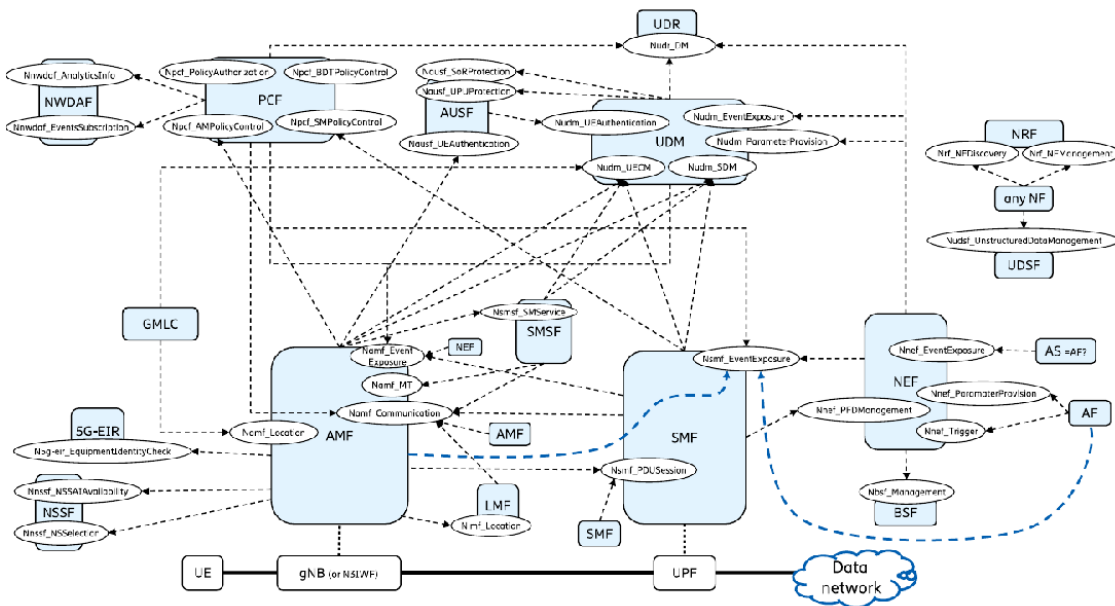
## 2.4 Υπηρεσίες και λειτουργίες υπηρεσιών

Η παράγραφος αυτή αναλύει περαιτέρω το μοντέλο αρχιτεκτονικής βασισμένης στις υπηρεσίες και εμβαθύνει, όπως προδίδει και ο τίτλος, στο πλήθος των υπηρεσιών εκείνων που στοιχειοθετούν την εν λόγω αρχιτεκτονική αλλά και πως οι εκάστοτε λειτουργίες του δικτύου πυρήνα 5G τις αξιοποιεί.

Οι λειτουργίες του 5GCN προσφέρουν τις δυνατότητές τους σε άλλες λειτουργίες δικτύου 5GCN ως υπηρεσίες NF, στις οποίες υπάρχει πρόσβαση μέσω διεπαφών που βασίζονται σε υπηρεσίες. Το επίκεντρο των προδιαγραφών είναι να καθορίσει τη συμπεριφορά των παραγωγών υπηρεσιών και να αφήσει την ευελιξία για τους καταναλωτές υπηρεσιών προκειμένου να επιτρέψει την επαναχρησιμοποίηση των υπηρεσιών όταν αυτό είναι σχετικό και δυνατό.[2]

Στην παρακάτω εικόνα αναπαρίστανται όλες οι υπηρεσίες για κάθε

περίπτωση αλλά και η τοπολογία συνδεσιμότητας μεταξύ των λειτουργιών.



Εικόνα 2.13: Απλή επισκόπηση υπηρεσιών 5G δικτύου [2]

Όπως δείχνει και η εικόνα κάθε βασική λειτουργία του 5GCN περιλαμβάνει έναν αριθμό από τέτοιες υπηρεσίες που εξυπηρετούν τους λόγους και την αρχιτεκτονική βασισμένη στις υπηρεσίες που περιγράψαμε παραπάνω, απλοποιώντας έτσι την επικοινωνία μεταξύ τους αλλά και με τους χρήστες του δικτύου.[2]

Παρακάτω συνοψίζονται οι διεπαφές αυτές, βασιζόμενες στις υπηρεσίες, και γίνεται μία απλή αναφορά στη χρήση τους. [2][6][7][8]

### 2.4.1 Υπηρεσίες της AMF

Το AMF ενεργεί ως παραγωγός υπηρεσιών για τέσσερις υπηρεσίες Namf\_Communication, Namf\_EventExposure, Namf\_MT και Namf\_Location. Η υπηρεσία Namf\_Communication είναι η κύρια υπηρεσία του AMF και έχει ένα πλήθος λειτουργίες Υπηρεσίας όπως το να επιτρέπει σε άλλους Nfs, όπως το SMF και το PCF, να επικοινωνούν με το UE ή / και το NG-RAN μέσω του AMF. Επίσης, επιτρέπει στα νέα AMF να ανακτούν το περιβάλλον UE σε περιπτώσεις κινητικότητας. Επιτρέπει ακόμη τη συνδρομή σε αλλαγές κατάστασης και έχει μια λειτουργία που επιτρέπει στο SMF να ζητήσει αναγνωριστικά του φορέα.[2][4]

#### Υπηρεσία Namf\_Communication

Η υπηρεσία Namf\_Communication επιτρέπει στην υπηρεσία NF να επικοινωνεί με τα UE μέσω μηνυμάτων N1 NAS ή να επικοινωνεί με το NG-RAN ή με άλλα δίκτυα πρόσβασης.[2][4]

### Υπηρεσία Namf\_EventExposure

Η υπηρεσία Namf\_EventExposure επιτρέπει στις NFs να εγγραφούν και να λαμβάνουν ειδοποιήσεις σχετικά με τις εκδηλώσεις του AMF. Η υπηρεσία Namf\_EventExposure έχει τρεις λειτουργίες υπηρεσίας Namf\_EventExposure\_Subscribe, Namf\_EventExposure\_UnSubscribe και Namf\_EventExposure\_Notify.

Το AMF μπορεί να εκθέσει πληροφορίες σχετικά με εκδηλώσεις που σχετίζονται με UE όπως:

- Αλλαγές τοποθεσίας
- Αλλαγές ζώνης ώρας
- Αλλαγές τύπου πρόσβασης
- Αλλαγές κατάστασης εγγραφής
- Αλλαγές στην κατάσταση συνδεσιμότητας
- Απώλεια επικοινωνίας UE
- Κατάσταση προσβασιμότητας UE

Ένα φίλτρο συμβάντων μπορεί να χρησιμοποιηθεί από τη αιτηθείσα NF για να περιορίσει το συγκεκριμένο συμβάν ενδιαφέροντος. Για παράδειγμα, εάν μία υπηρεσία NF ενδιαφέρεται να μάθει πότε ένα UE μετακινείται μέσα και έξω από μια συγκεκριμένη περιοχή παρακολούθησης, μπορεί να εγγραφεί στο συμβάν τοποθεσίας και να καθορίσει ένα φίλτρο συμβάντος για την περιοχή παρακολούθησης παραμέτρων και μια συγκεκριμένη τιμή αναγνωριστικού περιοχής παρακολούθησης.[2][4]

### Υπηρεσία Namf\_MT

Η υπηρεσία Namf\_MT επιτρέπει σε μια υπηρεσία NF να βεβαιωθεί ότι η UE είναι προσβάσιμη για αποστολή (για παράδειγμα MT SMS σε UE). Η υπηρεσία Namf\_MT διαθέτει επίσης μια λειτουργία υπηρεσίας που επιτρέπει σε μία NF να ανακτήσει πληροφορίες για να βοηθήσει στον τερματισμό της επιλογής τομέα για υπηρεσίες φωνής IMS.[2][4]

### Υπηρεσία Namf\_Location

Αυτή η υπηρεσία Namf\_Location επιτρέπει σε μία υπηρεσία NF να ζητά πληροφορίες τοποθεσίας για ένα συγκεκριμένο UE. Οι βασικές λειτουργίες αυτής της υπηρεσίας NF είναι:

- Να επιτρέπεται στις NF να ζητούν την τρέχουσα γεωδαιτική και προαιρετικά χωρική θέση ενός στόχου UE.
- Να επιτρέπεται στις NF να ειδοποιούνται για πληροφορίες συμβάντων που σχετίζονται με συνεδρίες έκτακτης ανάγκης.
- Να επιτρέπεται στις NF να ζητούν πληροφορίες τοποθεσίας που παρέχονται από το δίκτυο (NPLD) ή / και τοπική ζώνη ώρας που αντιστοιχεί στην τοποθεσία ενός συγκεκριμένου UE.[2][4]

## 2.4.2 Υπηρεσίες της SMF

Η λειτουργία SMF παρέχει δύο υπηρεσίες, την υπηρεσία Nsmf\_PDUSession και την υπηρεσία Nsmf\_EventExposure. Η υπηρεσία Nsmf\_PDUSession παρέχει τη

δυνατότητα διαχείρισης συνεδριών PDU και η υπηρεσία Namf\_EventExposure παρέχει τη δυνατότητα έκθεσης συμβάντων από το SMF.

Η υπηρεσία Nsmf\_EventExposure επιτρέπει στα NF να εγγραφούν και να λαμβάνουν ειδοποιήσεις για συμβάντα που σχετίζονται με συνεδρίες PDU και έχει τρεις λειτουργίες υπηρεσίας, τις Nsmf\_EventExposure\_Subscribe, Nsmf\_EventExposure\_UnSubscribe και Nsmf\_EventExposure\_Notify. Το SMF μπορεί να εκθέσει πληροφορίες σχετικά με εκδηλώσεις που σχετίζονται με την περίοδο σύνδεσης PDU όπως:

- UE διεύθυνση IP ή αλλαγή προθέματος.
- Έναρξη συνεδρίας PDU.
- Αλλαγή διαδρομής UP.
- Αλλαγή του τύπου πρόσβασης.
- Αλλαγή PLMN.

Το φίλτρο συμβάντων μπορεί να χρησιμοποιηθεί από το αιτούν NF για να περιορίσει το συγκεκριμένο συμβάν ενδιαφέροντος. Τα φίλτρα συμβάντων καθορίζουν τις προϋποθέσεις που πρέπει να πληρούνται για την ενεργοποίηση της ειδοποίησης και μπορούν να περιλαμβάνουν μία ή περισσότερες παραμέτρους καθώς και τις τιμές που κάθε παράμετρος πρέπει να ταιριάζει για να ενεργοποιήσει μια γνωστοποίηση.

Ο στόχος της αναφοράς συμβάντων SMF, μπορεί να αντιστοιχεί σε ένα μοναδικό αναγνωριστικό περιόδου σύνδεσης PDU, ένα αναγνωριστικό UE και ένα εσωτερικό αναγνωριστικό ομάδας ή γενικότερα όλα τα UE σε ένα συγκεκριμένο DNN.[2][4]

### 2.4.3 Υπηρεσίες της PCF

Το PCF λειτουργεί ως παραγωγός υπηρεσιών για έξι υπηρεσίες Npcf\_AMPolicyControl, Npcf\_Authorization Policy, Npcf\_SMPolicyControl, Npcf\_BDTPolicyControl, Npcf\_UEPolicyControl και Npcf\_EventExposure. Η υπηρεσία Npcf\_AMPolicyControl παρέχει πολιτικές ελέγχου πρόσβασης, επιλογής δικτύου και διαχείρισης κινητικότητας και πολιτικές επιλογής διαδρομών UE στο AMF.

Η εξουσιοδότηση Npcf\_Policy εξουσιοδοτεί και δημιουργεί πολιτικές κατόπιν αιτήματος από μια AF που σχετίζεται με την περίοδο σύνδεσης PDU στην οποία δεσμεύεται η περίοδος AF.

Το Npcf\_SMPolicyControl παρέχει πολιτικές σχετικά με την περίοδο σύνδεσης PDU στο SMF.

Η υπηρεσία Npcf\_BDTPolicyControl, PCF παρέχει την πολιτική μεταφοράς δεδομένων στο NEF.

Τέλος, η υπηρεσία του PCF που παρέχει τη διαχείριση των πολιτικών συσχέτισης του UE στους καταναλωτές NF είναι η Npcf\_UEPolicyControl.[2][4]

### 2.4.4 Υπηρεσίες της UDM

Το UDM ενεργεί ως παραγωγός υπηρεσιών για πέντε υπηρεσίες. Οι υπηρεσίες UDM χρησιμοποιούνται από τα AMF, SMF, SMSF, NEF, GMLC και AUSF μέσω της διεπαφής που βασίζεται στις υπηρεσίες Nudm.

Εάν το UDM είναι stateless και αποθηκεύει πληροφορίες εξωτερικά σε ένα UDR, χρησιμοποιεί τις υπηρεσίες Nudr. Η υπηρεσία Nudm\_UEContextManagement χρησιμοποιείται για τη διαχείριση περιβάλλοντος UE και επιτρέπει σε NF όπως το AMF, το SMF και το SMSF να εγγραφούν και να καταργήσουν την εγγραφή στο UDM και μπορούν να παρέχουν στους NFs πληροφορίες που σχετίζονται με το UE. Το NRF και οι υπηρεσίες του είναι βασικοί παράγοντες για την αρχιτεκτονική που βασίζεται σε υπηρεσίες, καθώς συγκεντρώνει και αυτοματοποιεί τη διαμόρφωση που απαιτείται για τις υπηρεσίες NF / NF για την ανακάλυψη, την επιλογή και τη σύνδεση σε ομότιμες υπηρεσίες NF / NF με τις σωστές δυνατότητες τα οποία επιτυγχάνονται μέσω των τριών αντίστοιχων υπηρεσιών που παρέχει το NRF ήτοι Nnrf\_NFManagement, Nnrf\_NFDiscovery και Nnrf\_AccessToken. [2][4]

### 2.4.5 Υπηρεσίες της AUSF

Το AUSF παρέχει στους καταναλωτές υπηρεσιών NF τις ακόλουθες υπηρεσίες:

- Nausf\_UEA Έλεγχος ταυτότητας, έλεγχος ταυτότητας του UE και παροχή βασικού υλικού (AMF)
- Nausf\_SoRProtection, προστατεύει τη Λίστα πληροφοριών διεύθυνσης για τον αιτούντα NF (UDM)
- Nausf\_UPUProtection (UDM)

Τα AMF και UDM, όπως αναφέραμε και παραπάνω, είναι τα NF που χρησιμοποιούν το AUSF.

### 2.4.6 Υπηρεσίες της SMSF

Το SMSF παρέχει την υπηρεσία Nsmsf\_SMS, που επιτρέπει την ενεργοποίηση και απενεργοποίηση της υπηρεσίας SM και την αποστολή μηνυμάτων SMS ανερχόμενης ζεύξης.

### 2.4.7 Υπηρεσίες της UDR

Η υπηρεσία Nudr\_DataManagement (ονομάζεται επίσης Nudr\_DM), επιτρέπει στους καταναλωτές NF να υποβάλλουν ερωτήματα, να δημιουργούν, να ενημερώνουν, να εγγραφούν για ειδοποιήσεις αλλαγών, να διαγραφούν για ειδοποιήσεις αλλαγής και να διαγράφουν δεδομένα που είναι αποθηκευμένα στο UDR, με βάση το σύνολο των δεδομένων που ισχύουν για τον καταναλωτή.

Αρχικά έχουν καθοριστεί σύνολα δεδομένων και αναγνωριστικά συνόλων δεδομένων για: Δεδομένα συνδρομής, Δεδομένα πολιτικής, Δεδομένα εφαρμογής και Δεδομένα για έκθεση. Τα σύνολα δεδομένων και τα αναγνωριστικά συνόλου δεδομένων προορίζονται να είναι επεκτάσιμα έτσι ώστε να καλύψουν πρόσθετα νέα αναγνωριστικά καθώς και για συγκεκριμένα αναγνωριστικά χειριστή και σχετικά δεδομένα.[2][4]

### 2.4.8 Υπηρεσίες 5G-EIR

Το 5G-EIR παρέχει μια λειτουργία υπηρεσίας, την N5g-eir\_EquipmentIdentityCheck, που χρησιμοποιείται από την AMF για να

ελέγξει αν το μόνιμο αναγνωριστικό εξοπλισμού (PEI) βρίσκεται στη μαύρη λίστα ή όχι. [2][4]

### 2.4.9 Υπηρεσίες της NWDAF

Το NWDAF παρέχει δύο υπηρεσίες Nnwda\_EventsSubscription και Nnwda\_AnalyticsInfo. Η υπηρεσία Nnwda\_EventsSubscription επιτρέπει στους καταναλωτές της υπηρεσίας NF να εγγραφούν / διαγραφούν για διαφορετικούς τύπους πληροφοριών από το NWDAF. Η υπηρεσία Nnwda\_AnalyticsInfo επιτρέπει στους καταναλωτές υπηρεσιών NF να ζητούν πληροφορίες διαφορετικών τύπων από το NWDAF.

Στην έκδοση 3GPP 15, το NDWAF περιορίζεται σε συμβάντα επιπέδου φόρτωσης σε μία ή περισσότερες παρουσίες Slice δικτύου και ορίων επιπέδου φόρτωσης. Σε μεταγενέστερες εκδόσεις αναμένεται ότι το NWDAF θα υποστηρίξει επιπλέον συμβάντα και φίλτρα συμβάντων. [2][4]

### 2.4.10 Υπηρεσίες της UDSF

Οι υπηρεσίες UDSF ορίστηκαν μόνο στο δεύτερο στάδιο της έκδοσης 15 της 3GPP. Δεν καθορίστηκε κάποια λύση του πρωτοκόλλου στο στάδιο 3, αλλά αναμένεται ότι οι μεταγενέστερες εκδόσεις θα μελετήσουν κατάλληλες λύσεις πρωτοκόλλου που μπορούν να υποστηρίξουν τις απαιτήσεις απόδοσης σε δυναμική πρόσβαση δεδομένων που απαιτείται από τα NF's χρησιμοποιώντας το UDSF.[2][4]

### 2.4.11 Υπηρεσίες της NSSF

Το NSSF παράγει δύο υπηρεσίες Nnssf\_NSSelection και Nnssf\_NSSAIAvailability. Η υπηρεσία Nnssf\_NSSelection παρέχει τις πληροφορίες για το Slice δικτύου στον Αιτούντα και η υπηρεσία Nnssf\_NSSAI διαθεσιμότητας παρέχει τη διαθεσιμότητα των S-NSSAI σε κάθε βάση ανά TA.[2][4]

### 2.4.12 Υπηρεσίες της LMF

Η συγκεκριμένη λειτουργία LMF υποστηρίζει μία υπηρεσία, Nlmf\_Location. Η υπηρεσία Nlmf\_Location επιτρέπει στο AMF να ζητά προσδιορισμό τοποθεσίας για έναν στόχο UE. Επιτρέπει στο AMF να ζητήσει την τρέχουσα γεωδαιτική και προαιρετικά πολιτική θέση ενός στόχου UE. Η υπηρεσία Nlmf\_Location έχει μία λειτουργία υπηρεσίας, τη λειτουργία Nlmf\_Location\_DetermineLocation.[2][4]

### 2.4.13 Υπηρεσίες της NEF

Το NEF υποστηρίζει οκτώ υπηρεσίες οι οποίες παρατίθενται παρακάτω:

- Nnef\_EventExposure, παρέχει υποστήριξη για έκθεση σε συμβάντα
- To Nnef\_PFD Management, παρέχει υποστήριξη για τη διαχείριση PFD
- Nnef\_ParameterProvision, παρέχει υποστήριξη για την παροχή πληροφοριών



που μπορούν να χρησιμοποιηθούν για το UE στο 5GS

- Nnef\_Trigger, παρέχει υποστήριξη για ενεργοποίηση συσκευών
- Nnef\_BDTPNegotiation, παρέχει υποστήριξη για διαπραγμάτευση σχετικά με τις πολιτικές μεταφοράς για τη μελλοντική μεταφορά δεδομένων στο παρασκήνιο
- Nnef\_TrafficInfluence, παρέχει τη δυνατότητα να επηρεάζει τη δρομολόγηση της κυκλοφορίας
- Nnef\_ChargeableParty, χειρίζεται το χρεώσιμο μέρος για μια συνεδρία δεδομένων για ένα UE
- Nnef\_AFsessionWithQoS, ζητά από το δίκτυο να παρέχει ένα συγκεκριμένο QoS για μια περίοδο λειτουργίας AS[2][4]

## Κεφάλαιο 3

# Δίκτυο Πρόσβασης 5G

**Π**αράλληλα με τις εργασίες για την νέα τεχνολογία ραδιοπρόσβασης NR (New Radio) στο 3GPP, οι γενικές αρχιτεκτονικές του συστήματος τόσο του δικτύου ραδιοπρόσβασης (RAN) όσο και του του Core Network (CN) επανεξετάστηκε, συμπεριλαμβανομένου του διαχωρισμού λειτουργικότητας μεταξύ των δύο δικτύων.

Το δίκτυο πρόσβασης (Radio Access Network, RAN) είναι υπεύθυνο για όλες τις λειτουργίες που σχετίζονται με το ραδιόσύστημα του συνολικού δικτύου που περιλαμβάνει, για παράδειγμα, προγραμματισμό, χειρισμό ραδιο-πόρων, πρωτόκολλα αναμετάδοσης, κωδικοποίηση και διάφορα σχήματα πολλαπλών κεραιών. Είναι δηλαδή το σύστημα με το οποίο οι τελικοί χρήστες συνδέονται με την υποδομή του δικτύου κορμού και εξυπηρετούνται από το backhaul δίκτυο. Αν και στις προηγούμενες γενιές δικτύου η πρόσβαση απευθυνόταν κυρίως σε κινητές συσκευές χρήστη, στο 5G η ραδιο-πρόσβαση είναι απλά μία περίπτωση, καθώς η νέα αυτή τεχνολογία απευθύνεται σε ένα μεγάλος εύρος πελατών (για παράδειγμα βιομηχανία) λόγω ότι το 5G επιλύει σημαντικά προβλήματα και παρέχει βελτιώσεις που αναφέρονται παρακάτω. Για το λόγο αυτό το δίκτυο πρόσβασης σημειώνεται ως (R)AN.[11]

Συγκριτικά, λοιπόν, με το LTE, το NR παρέχει πολλά οφέλη. Μερικά από αυτά είναι:

- εκμετάλλευση ζωνών πολύ υψηλότερης συχνότητας, ως μέσο για την απόκτηση πρόσθετων φασμάτων, για την υποστήριξη πολύ μεγάλου εύρους ζώνης μετάδοσης και σχετικά υψηλούς ρυθμούς δεδομένων
- εξαιρετικά λιτός σχεδιασμός ενισχύοντας την ενεργειακή απόδοση του δικτύου καθώς και τη μείωση παρεμβολών
- προώθηση συμβατότητας προετοιμάζοντας για μελλοντικές, αλλά άγνωστες, περιπτώσεις χρήσης και τεχνολογίες
- χαμηλή καθυστέρηση για βελτίωση της απόδοσης και ενεργοποίηση νέων περιπτώσεων χρήσης
- κεντροποιημένος σχεδιασμός που επιτρέπει την εκτεταμένη χρήση της διαμόρφωσης δέσμης και τεράστιος αριθμός στοιχείων κεραιάς όχι μόνο για μετάδοση δεδομένων (σε κάποιο βαθμό είναι δυνατή στο LTE) αλλά και για διαδικασίες ελέγχου-επιπέδου όπως αρχική πρόσβαση.

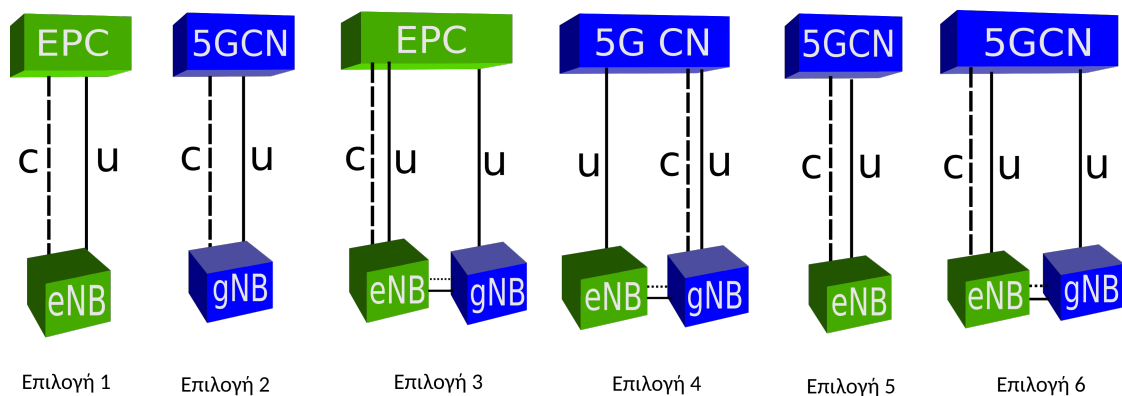
Ο κόμβος που ικανοποιεί τα παραπάνω και χρησιμοποιείται τόσο στο 5G όσο και στις τεχνολογίες διπλής συνδεσιμότητας ονομάζεται επόμενη γενιάς κόμβος-B (next generation Node-B, ή εν συντομία gNB).[10][11][12]

## 3.1 Συνδεσμολογίες 5G RAN

### 3.1.1 Επιλογές συνδεσιμότητας 5G CN και 5G RAN

Οι επιλογές για τη συνδεσιμότητα στο 5G ποικίλουν και παράλληλα με την τεχνολογία ραδιο πρόσβασης NR μπορούμε να χειριστούμε ταυτόχρονα σε ένα ραδιο σύστημα NR και LTE σημεία πρόσβασης. Ωστόσο, για να επιτρέψει την έγκαιρη εισαγωγή του NR σε υπάρχοντα δίκτυα, είναι επίσης δυνατή η σύνδεση NR με το EPC, το βασικό δίκτυο LTE. Αυτό απεικονίζεται ως "επιλογή 3" στο σχήμα 3.1 και είναι επίσης γνωστή ως "μη αυτόνομη λειτουργία" ή λειτουργία "non-stand alone" με το LTE να χρησιμοποιείται για τη λειτουργία ελέγχου-επιπέδου όπως η αρχική πρόσβαση, η τηλεειδοποίηση και η κινητικότητα.[3]

Την αυτόνομη και μη αυτόνομη δομή του δικτύου πυρήνα τη συζητήσαμε στο προηγούμενο κεφάλαιο. Εδώ συμπληρώνουμε αυτή τη γνώση με ένα ολοκληρωμένο σύστημα 5G που εκτός από τους διαφορετικούς τύπους του δικτύου κορμού έχουμε και διαφορετικές συνδεσμολογίες με το το δίκτυο πρόσβασης και συγκεκριμένα με το δίκτυο ραδιοπρόσβασης. Έτσι, διακρίνουμε τη αυτόνομη λειτουργία και τη μη αυτόνομη λειτουργία ενός συστήματος 5G.



Εικόνα 3.1: Διαφορετικοί συνδυασμοί CN και RAN[10]

Το eNB και το gNB μπορούν να θεωρηθούν ως σταθμοί βάσης για LTE και NR, αντίστοιχα. Στην επιλογή 3, το κεντρικό δίκτυο EPC είναι συνδεδεμένο στο eNB. Όλες οι λειτουργίες του επιπέδου ελέγχου, χειρίζονται από το LTE και το NR χρησιμοποιείται μόνο για τα δεδομένα του επιπέδου χρήστη. Το gNB συνδέεται με το eNB και τα δεδομένα επιπέδου χρήστη από το EPC μπορούν να προωθηθούν, από το eNB στο gNB.[3]

Υπάρχουν επίσης παραλλαγές αυτού όπως η επιλογή 3α και η επιλογή 3x. Στην επιλογή 3α, τα μέρη του επιπέδου χρήστη τόσο του eNB όσο και του gNB συνδέονται με το EPC. Στην επιλογή 3x, μόνο το επίπεδο χρήστη gNB είναι συνδεδεμένο στο EPC και τα δεδομένα επιπέδου χρήστη στο eNB δρομολογούνται μέσω του gNB.[3]

Για αυτόνομη λειτουργία(stand alone), το gNB συνδέεται απευθείας στον πυρήνα 5G όπως φαίνεται στην επιλογή 2. Οι λειτουργίες επιπέδου χρήστη και επιπέδου ελέγχου διαχειρίζονται από το gNB. Οι επιλογές 4, 5 και 7 δείχνουν διάφορες δυνατότητες για τη σύνδεση ενός LTE eNB στο 5GCN.[2]

### ■ Πλεονεκτήματα μη αυτόνομης λειτουργίας 5g (Non-Stand Alone, NSA)

Τα πλεονεκτήματα χρήσης της μη αυτόνομης λειτουργίας είναι δύο:

- ▶ Μεγάλη ταχύτητα συνδεσιμότητας με τους πελάτες που έχουν προμηθευτεί 5G συσκευές
- ▶ Αξιοποίηση υπάρχουσας τεχνολογίας και εξοπλισμού διαχειριστών(operator) του δικτύου πυρήνα και μεταφοράς

### ■ Πλεονεκτήματα αυτόνομης λειτουργίας 5g (Stand Alone, SA)

Η χρήση ενός αυτόνομου δικτύου 5G πλεονεκτεί καθώς:

- ▶ Οι διαχειριστές των δικτύων μπορούν πλέον να ενσωματώσουν στο δίκτυο τους και νέες υπηρεσίες όπως έξυπνες πόλεις και εργοστάσια
- ▶ Είναι πλήρως εικονικοποιημένη, αρχιτεκτονική εγγενούς νέφους (CNA), η οποία εισάγει νέους τρόπους ανάπτυξης και διαχείρισης υπηρεσιών
- ▶ Η αρχιτεκτονική επιτρέπει τον από άκρο σε άκρο λογικό διαχωρισμό υπηρεσιών
- ▶ Ο αυτοματισμός αυξάνει την αποτελεσματικότητα ενώ μειώνει το κόστος λειτουργίας των δικτύων.
- ▶ Με την τυποποίηση, που σε μια προσέγγιση που βασίζεται στο cloud, οι MNO μπορούν επίσης να βασίζονται στην καλύτερη καινοτομία αναπαραγωγής τόσο από τους προμηθευτές όσο και από τις κοινότητες ανοιχτού κώδικα
- ▶ Επιλέγοντας μια αρχιτεκτονική βασισμένη σε cloud υπηρεσίες μικροϋπολογιστών, οι MNO μπορούν επίσης να αποφασίσουν για μια γκάμα μοντέλων ανάπτυξης, όπως ιδιωτικό cloud, δημόσιο cloud ή υβριδικό για την επίτευξη των επιχειρηματικών τους στόχων

## 3.1.2 Ραδιοπρόσβαση

Το δίκτυο ραδιο-πρόσβασης μπορεί να έχει δύο τύπους κόμβων που συνδέονται με το δίκτυο πυρήνα του 5G:

1. Ένα gNB, που εξυπηρετεί συσκευές NR χρησιμοποιώντας το επίπεδο χρήστη NR και πρωτόκολλα του επιπέδου ελέγχου προς το UE ή
2. Ένα ng-eNB, που εξυπηρετεί συσκευές LTE (E-UTRA) χρησιμοποιώντας το επίπεδο χρήστη LTE και πρωτόκολλα επιπέδου ελέγχου προς το UE

*Ένα δίκτυο ραδιοπρόσβασης που αποτελείται από δύο ng-eNBs για ασύρματη πρόσβαση LTE και τα gNB για ραδιοεπικοινωνία NR είναι γνωστά ως NG-RAN.*

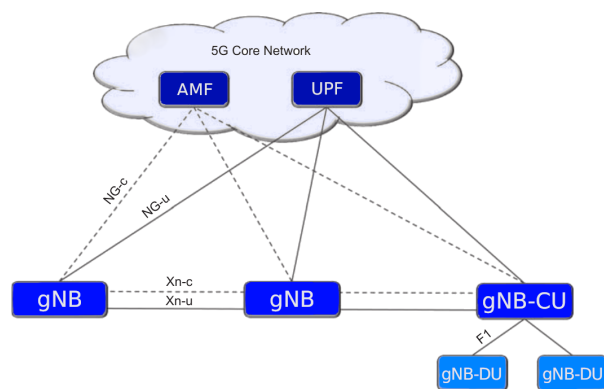
Το gNB (ή ng-eNB) είναι υπεύθυνο για όλες τις λειτουργίες που σχετίζονται με το ραδιόσύστημα σε ένα ή διάφορα κελιά, για παράδειγμα,

διαχείριση πόρων ραδιοσυστήματος, έλεγχος εισαγωγής, εγκαθίδρυση σύνδεσης, δρομολόγηση δεδομένων επιπέδου χρήστη στο UPF και επίπεδο ελέγχου, πληροφορίες για τη διαχείριση ροής AMF και QoS. Είναι σημαντικό να σημειωθεί ότι ένα gNB είναι ένας λογικός κόμβος και όχι μια φυσική εφαρμογή. [17]

Μια κοινή εφαρμογή ενός gNB είναι ένας ιστός τριπλού τομέα, όπου ένας σταθμός βάσης χειρίζεται μεταδόσεις σε τρεις κυψέλες, αν και μπορούν να βρεθούν και άλλες υλοποιήσεις, όπως μια μονάδα επεξεργασίας βασικής ζώνης στην οποία βρίσκονται πολλές απομακρυσμένες ραδιοκεφαλές συνδεδεμένες. Παραδείγματα των τελευταίων είναι ένας μεγάλος αριθμός εσωτερικών κυψελών ή αρκετών κυψελών κατα μήκος, που ανήκουν στο ίδιο gNB.[17]

Το gNB και το ng-eNB φιλοξενούν διάφορες λειτουργίες που περιγράφουμε σε αυτήν την παράγραφο. Τέτοιες λειτουργίες είναι η διαχείριση ραδιοπόρων(Radio Resource Management, RRM) όπως ο έλεγχος ραδιο φορέων(radio bearers) έλεγχος αποδοχής ραδιοσυστήματος, συνδέσεις, έλεγχος κινητικότητας, δυναμική κατανομή πόρων για τα UE's για την ανερχόμενη και κατερχόμενη ζεύξη (προγραμματισμός, scheduling). Επίσης, περιέχει

λειτουργίες συμπίεσης IP κεφαλίδας, κρυπτογράφηση και προστασία ακεραιότητας δεδομένων. Επιλέγει, ένα AMF προς επισύναψη του UE όταν δεν μπορεί να προσδιοριστεί δρομολόγηση σε AMF από τις πληροφορίες που παρέχονται από το UE. Ακόμη, δρομολογεί δεδομένα επιπέδου χρήστη προς τα UPFs καθώς και πληροφορίες επιπέδου ελεγχου προς το AMF. Η ρύθμιση και αποδέσμευση συνδέσεων είναι λειτουργίες των gNB και ng-eNB, όπως και ο προγραμματισμός(scheduling) και μετάδοση μηνυμάτων τηλεειδοποίησης και πληροφοριών εκπομπής συστήματος(προέρχονται απο το AMF ή OAM). Επιπρόσθετα, φιλοξενεί λειτουργίες όπως η διαμόρφωση μέτρησης και αναφορά μέτρησης για κινητικότητα και προγραμματισμό, η σήμανση πακέτου επιπέδου μεταφοράς στην ανερχόμενη ζεύξη, η διαχείριση συνεδρίας, υποστήριξη του Network Slicing, διαχείριση ροής QoS και αντιστοίχιση σε ραδιοφορείς δεδομένων και υποστήριξη UE σε κατάσταση RRC\_INACTIVE. Τέλος, περιλαμβάνει λειτουργία διανομής για μηνύματα NAS και κοινή χρήση δικτύου πρόσβασης,λειτουργία για διπλή συνδεσιμότητα καθώς και στενή συνεργασία μεταξύ NR και E-UTRA.[17]



Εικόνα 3.2: Διεπαφές Δικτύου ραδιο-πρόσβασης [10]

### 3.1.3 Βασική διασύνδεση δικτύου πρόσβασης

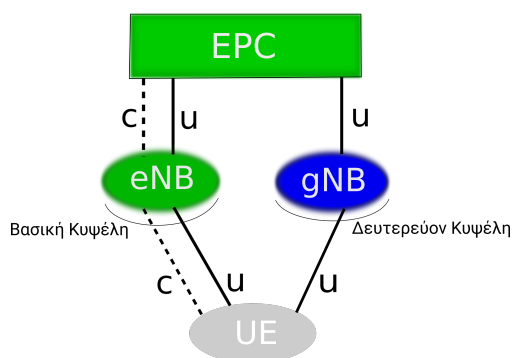
Όπως φαίνεται και στην εικόνα, το gNB είναι συνδεδεμένο στο δίκτυο πυρήνα 5G μέσω της διασύνδεσης NG, πιο συγκεκριμένα στο UPF μέσω του NG τμήμα

επιπέδου χρήστη (NG-u) και στο AMF μέσω του τμήματος επιπέδου ελέγχου NG (NG-c).[10]

Ένα gNB μπορεί να συνδεθεί σε πολλά UPF / AMF για τους σκοπούς του διαμοιρασμού φόρτωσης (load sharing) και πλεονασμού (redundancy). Η διασύνδεση Xn, που συνδέει τα gNB μεταξύ τους, χρησιμοποιείται κυρίως για την υποστήριξη της λειτουργίας κινητικότητας και της διπλής συνδεσιμότητας. Αυτή η διεπαφή μπορεί επίσης να χρησιμοποιηθεί για πολλαπλές λειτουργίες διαχείρισης ραδιοπόρων (Radio Resource Management, RRM). Η διασύνδεση Xn χρησιμοποιείται επίσης για την υποστήριξη κινητικότητας χωρίς απώλειες μεταξύ γειτονικών κυψελών όσον αφορά την προώθηση πακέτων.[10]

Υπάρχει επίσης ένας τυποποιημένος τρόπος ώστε να χωρίζεται το gNB σε δύο μέρη, δηλαδή σε μια κεντρική μονάδα (gNB-CU) και μία ή περισσότερες καταναμημένες μονάδες (gNB Distributed Unit, gNB-DU) χρησιμοποιώντας τη διεπαφή F1. Στην περίπτωση ενός διαχωρισμένου gNB, τα πρωτόκολλα RRC, PDCP και SDAP, που περιγράφονται παρακάτω, διατίθενται στο gNB-CU και οι υπόλοιπες οντότητες πρωτοκόλλου (RLC, MAC, PHY) στο gNB-DU. Η διεπαφή μεταξύ του gNB (ή του gNB-DU) και της συσκευής είναι γνωστή ως η διεπαφή Uu.[10]

Για να επικοινωνήσει μια συσκευή, απαιτείται τουλάχιστον μία σύνδεση μεταξύ της συσκευής και του δικτύου. Η συσκευή συνδέεται σε μία κυψέλη που χειρίζεται όλες τις μεταδόσεις uplink καθώς και downlink. Όλες οι ροές δεδομένων, τα δεδομένα χρήστη καθώς και η RRC σηματοδότηση, αντιμετωπίζονται από αυτή την κυψέλη κάτι που αποτελεί μία προσέγγιση κατάλληλη για ένα ευρύ φάσμα εφαρμογών. Ωστόσο, επιτρέποντας τη συσκευή να συνδέεται στο δίκτυο μέσω πολλαπλών κυψελών μπορεί να είναι επωφελής σε ορισμένα σενάρια.[10]



Εικόνα 3.3: Διπλή συνδεσιμότητα LTE-NR με χρήση της επιλογής 3. [10]

Η διπλή συνδεσιμότητα μεταξύ LTE και NR έχει ιδιαίτερη σημασία καθώς είναι η βάση για μη αυτόνομη λειτουργία (non stand alone) χρησιμοποιώντας την επιλογή 3 όπως απεικονίζεται στο σχήμα 3.3. Η κύρια κυψέλη που βασίζεται στο LTE χειρίζεται το σήμα επιπέδου ελέγχου και (δυστυχώς) η δευτερεύον κυψέλη που βασίζεται στο NR χειρίζεται μόνο το επίπεδο χρήστη, ενισχύοντας ουσιαστικά το ρυθμό μετάδοσης δεδομένων.

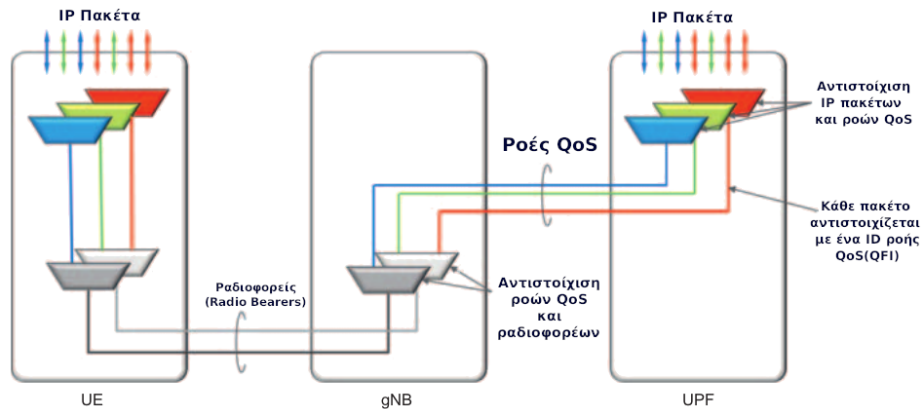
Η διπλή συνδεσιμότητα μεταξύ NR και NR είναι μέρος της σχεδίασης 3GPP στις επόμενες εκδόσεις.

Ένα παράδειγμα είναι η συγκέντρωση επιπέδου χρήστη (user-plane aggregation), όπου οι ροές από πολλά κελιά συγκεντρώνονται προκειμένου να αυξηθεί ο ρυθμός δεδομένων. Ένα άλλο παράδειγμα είναι ο διαχωρισμός του επιπέδου ελέγχου και επιπέδου χρήστη όπου η επικοινωνία επιπέδου ελέγχου γίνεται από έναν κόμβο και το επίπεδο χρήστη από άλλο. Το σενάριο μιας συσκευής συνδεδεμένης σε δύο κυψέλες είναι γνωστή ως διπλή συνδεσιμότητα.[10]

## 3.2 Χειρισμός διαφορετικών QoS

Ο χειρισμός διαφορετικών απαιτήσεων ποιότητας υπηρεσίας (QoS) είναι εφικτός ήδη από το LTE και στο οποίο βασίζεται το NR ενισχύοντας αυτό το πλαίσιο. Οι βασικές αρχές του LTE διατηρούνται, δηλαδή ότι το δίκτυο είναι υπεύθυνο για τον έλεγχο QoS και ότι το δίκτυο πυρήνα 5G και όχι το δίκτυο ραδιοπρόσβασης γνωρίζει αυτή την υπηρεσία.[10]

Ο χειρισμός του QoS είναι απαραίτητος για την πραγματοποίηση του τεμαχισμού του δικτύου. Για κάθε συνδεδεμένη συσκευή, υπάρχει μία ή περισσότερες συνεδρίες PDU, καθεμία με μία ή περισσότερες ροές QoS και ραδιοφορέων (bearer) δεδομένων. Τα πακέτα IP αντιστοιχίζονται στις QoS ροές σύμφωνα με τις απαιτήσεις QoS, για παράδειγμα σε όρους καθυστέρησης ή απαιτούμενους ρυθμούς δεδομένων, ως μέρος της λειτουργίας UDF στο δίκτυο. Κορμού Κάθε πακέτο μπορεί να επισημανθεί με ένα QoS Flow Identifier (QFI) για να βοηθήσει τον χειρισμό του QoS. Το δεύτερο βήμα, η χαρτογράφηση των ροών QoS σε ραδιοφορείες δεδομένων, γίνεται στο δίκτυο ραδιοπρόσβασης. Έτσι, το δίκτυο κορμού γνωρίζει τις απαιτούμενες υπηρεσίες ενώ το δίκτυο ραδιοπρόσβασης χαρτογραφεί μόνο τις ροές QoS στους ραδιοφορείς (radio-bearers). Η χαρτογράφηση QoS-flow-to-radio-bearer δεν είναι απαραίτητα μία αντιστοίχιση one-to-one αλλά πολλαπλές ροές QoS μπορούν να χαρτογραφηθούν στον ίδιο φορέα ραδιοφώνου δεδομένων (Εικ. 3.4).[10]



Εικόνα 3.4: Ροές QoS και Radio Beares σε μια PDU συνεδρία[10]

Υπάρχουν δύο τρόποι ελέγχου της χαρτογράφησης από ροές QoS σε ραδιοφορείς δεδομένων στην ανερχόμενη ζεύξη: ανακλαστική χαρτογράφηση και ρητή διαμόρφωση.

Στην περίπτωση της ανακλαστικής χαρτογράφησης, η οποία είναι ένα νέο χαρακτηριστικό στο NR όταν συνδέεται με το δίκτυο πυρήνα 5G, η συσκευή παρατηρεί το QFI στα πακέτα downlink για τη συνεδρία PDU. Αυτό παρέχει στη συσκευή γνώση σχετικά με το ποιες ροές IP χαρτογραφούνται σε ποια ροή QoS και ποιο ραδιοφορέα. Στη συνέχεια, η συσκευή χρησιμοποιεί την ίδια αντιστοίχιση για την επισκεψιμότητα ανερχόμενης ζεύξης.

Στην περίπτωση της ρητής χαρτογράφησης, η ροή QoS προς την αντιστοίχιση τους ραδιοφορείς δεδομένων διαμορφώνεται στη συσκευή με χρήση σηματοδότησης RRC.[10]

### 3.2.1 Hybrid Automatic Repeat reQuest(HARQ)

Η υβριδική αυτόματη αίτηση επανάληψης (Hybrid Automatic Repeat re-Quest, HARQ) είναι ένα εργαλείο που έχει εφαρμοστεί σε πολλά συστήματα επικοινωνίας για να αυξήσει την αξιοπιστία σε μια απλή μετάδοση αλλά και για τη γενικότερη φασματική απόδοση. Σε ένα σύστημα που εφαρμόζεται αυτός ο μηχανισμός, οποιαδήποτε μετάδοση δεδομένων αναγνωρίζεται από τον αντίστοιχο παραλήπτη, όπως για παράδειγμα η κατερχόμενη ζεύξη από τη συσκευή και η ανερχόμενη ζεύξη από τον σταθμό βάσης.[19]

Με βάση κάποιο δωθέν κριτήριο απόφασης(για παράδειγμα έλεγχος με κυκλικούς κώδικες- CRC), ελέγχεται η ακεραιότητα των ληφθέντων πακέτων. Εάν από τον έλεγχο δε εγκριθεί, ένα αντίστοιχο μήνυμα ανάδρασης αρνητικής αναγνώρισης “negative acknowledged”(NACK) αποστέλλεται για να ζητηθεί η αναμετάδοση του πακέτου, ή σε αντίθετη περίπτωση, η επιτυχημένη λήψη του πακέτου χαρακτηρίζεται ως αναγνωρισμένη “acknowledged”(ACK). Στην πρώτη περίπτωση, το πρωτότυπο μήνυμα ή μία πλεονάζουσα έκδοση αναμεταδίδεται. Ο δέκτης τελικά συνδυάζει και το πρωτότυπο μήνυμα και το αναμεταδιδόμενο πακέτο ώστε να ανιχνεύσει το πρωτότυπο. [19]

Έτσι, το HARQ είναι ένα εργαλείο που αυξάνει την αξιοπιστία κάνοντας χρήση χρονικής και συχνοτικής ποικιλομορφίας (αναλόγως των μεταβλητών), ενέργειας και του κέρδους της κωδικοποίησης.[19]

### 3.2.2 Forward Error Correction(FEC)

Τα συστήματα 5G που υλοποιούνται περιλαμβάνουν επίσης προηγμένες τεχνολογίες διόρθωσης σφαλμάτων προς τα εμπρός (Forward Error Correction, FEC), όπως προηγμένοι κώδικες Turbo, Low-Density Parity Check (LDPC) κώδικες καθώς και Polar κώδικες. Από την πλευρά του αποκωδικοποιητή, οι FEC κώδικες συνήθως αποκωδικοποιούνται κάνοντας χρήση επαναληπτικών στρατηγικών αποκωδικοποίησης. Η 3GPP επέλεξε ως πιο πιθανά σχήματα κωδικοποίησης για το eMBB τις LDPC και Polar κωδικοποιήσεις για τα σήματα δεδομένων και ελέγχου αντίστοιχα. Επειδή οι ρυθμοί δεδομένων στο 5G είναι πολύ υψηλοί ακόμη και στην πλευρά των τερματικών, είναι αναγκαία η ανάπτυξη υψηλής ταχύτητας αποκωδικοποιητών καναλιών, οι οποίοι θα είναι συνάμα και ενεργειακά αποδοτικοί. Ωστόσο, για την συμβατότητα με το προηγούμενης γενιάς LTE αποκτά ιδιαίτερο ενδιαφέρον η έρευνα σε ευέλικτες αρχιτεκτονικές αποκωδικοποιήσεις, ικανές να αντιμετωπίσουν τις Polar, LDPC και Turbo κωδικοποιήσεις.[19]

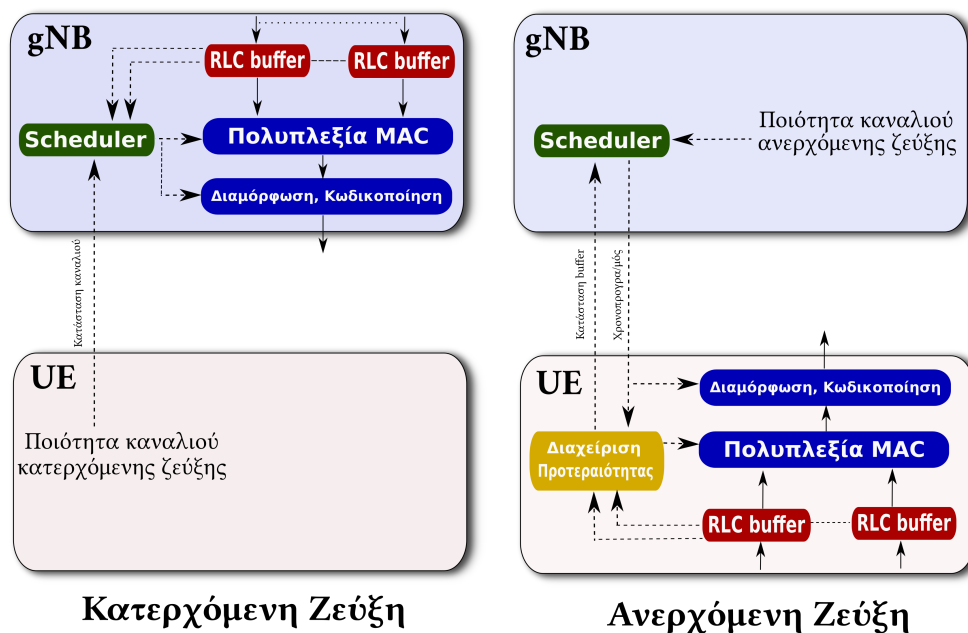
### 3.2.3 Χρονοπρογραμματισμός (Scheduling)

Μία από τις βασικές αρχές του NR δικτύου πρόσβασης είναι ο διαμοιρασμός του καναλιού μετάδοσης όπου χρονικοί-συχνοτικοί πόροι διαμοιράζονται δυναμικά μεταξύ των χρηστών. Ο προγραμματιστής (scheduler) είναι ένα μέρος του MAC επιπέδου (αν και συνήθως αποτελεί ξεχωριστή οντότητα) και ελέγχει τις αναθέσεις των πόρων στην ανερχόμενη και κατερχόμενη ζεύξη σε όρους όπου ονομάζονται μπλοκ πόρων(resource blocks) στο πεδίο συχνοτήτων και OFDM σύμβολα και θυρίδες(slots) στο πεδίο του χρόνου.[19]



Η βασική λειτουργία του προγραμματιστή είναι ο δυναμικός προγραμματισμός, όπου το gNB λαμβάνει μια απόφαση προγραμματισμού, συνήθως μία φορά ανά θυρίδα, και στέλνει πληροφορίες προγραμματισμού στο επιλεγμένο σύνολο συσκευών. Παρόλο που ο προγραμματισμός ανά θυρίδα είναι μια κοινή περίπτωση, ούτε οι αποφάσεις προγραμματισμού ούτε η πραγματική μετάδοση δεδομένων περιορίζονται από την έναρξη ή το τέλος των ορίων των θυρίδων. Αυτό είναι χρήσιμο για την υποστήριξη λειτουργίας χαμηλής καθυστέρησης καθώς και μελλοντικών επεκτάσεων σε λειτουργία μη αδειοδοτούμενου φάσματος.[19]

Ο προγραμματισμός uplink και downlink είναι διαχωρισμένος στο NR, και οι αποφάσεις προγραμματισμού uplink και downlink μπορούν να ληφθούν ανεξάρτητα το ένα από το άλλο (εντός των ορίων που θέτει η περίπτωση duplex στην περίπτωση λειτουργίας half-duplex) Ο προγραμματιστής κατερχόμενης ζεύξης είναι υπεύθυνος για τον (δυναμικό) έλεγχο όσον αφορά σε ποιες συσκευές μεταδίδει και, για καθεμία από αυτές τις συσκευές, το σύνολο μπλοκ πόρων πάνω στο οποίο πρέπει να μεταδίδεται το DL-SCH της συσκευής. Η επιλογή μορφής μεταφοράς (επιλογή μεγέθους μπλοκ μεταφοράς, σχήμα διαμόρφωσης και αντιστοίχιση κεραίας) και η πολυπλεξία λογικού καναλιού για μεταδόσεις κατερχόμενης ζεύξης, ελέγχονται από το gNB, όπως απεικονίζεται στο αριστερό μέρος του σχήματος 3.5.[11][19]



Εικόνα 3.5: Μορφή Μεταφοράς για κατερχόμενη και ανερχόμενη ζεύξη[10]

Ο προγραμματιστής ανερχόμενης ζεύξης εξυπηρετεί έναν παρόμοιο σκοπό, δηλαδή να ελέγχει (δυναμικά) ποιες συσκευές πρόκειται να μεταδώσουν στο αντίστοιχο UL-SCH τους και σε ποιον πόρο συχνότητας-χρόνου (συμπεριλαμβανομένου του φορέα). Παρά το γεγονός ότι ο προγραμματιστής gNB καθορίζει τη μορφή μεταφοράς για τη συσκευή, είναι σημαντικό να επισημανθεί ότι η απόφαση προγραμματισμού ανερχόμενης ζεύξης δεν προγραμματίζει ρητά ένα ορισμένο λογικό κανάλι αλλά τη συσκευή ως έχει.[11][19]

Ο προγραμματισμός που εξαρτάται από το κανάλι κατερχόμενη ζεύξης υποστηρίζεται μέσω πληροφοριών κατάστασης καναλιού (CSI), που αναφέρονται από τη συσκευή στο gNB και αντικατοπτρίζουν την στιγμιαία ποιότητα καναλιού downlink στους τομείς χρόνου και συχνότητας καθώς και πληροφορίες απαραίτητες για τον προσδιορισμό της κατάλληλης επεξεργασίας στην κεραία στην περίπτωση χωρικής πολυπλεξίας. Στο uplink, οι πληροφορίες κατάστασης καναλιού που είναι απαραίτητες για τον προγραμματισμό που εξαρτάται από το κανάλι uplink μπορούν να βασίζονται σε ένα σήμα αναφοράς sound που μεταδίδεται από κάθε συσκευή για την οποία το gNB θέλει να εκτιμήσει την ποιότητα του καναλιού ανερχόμενη ζεύξης. Για να βοηθήσει τον προγραμματιστή ανερχόμενη ζεύξης στις αποφάσεις του, η συσκευή μπορεί να μεταδώσει πληροφορίες κατάστασης buffer και κεφαλής ισχύος στο gNB χρησιμοποιώντας στοιχεία ελέγχου MAC. Αυτές οι πληροφορίες μπορούν να μεταδοθούν μόνο εάν η συσκευή έχει λάβει έγκυρη επιχορήγηση προγραμματισμού. Για καταστάσεις όπου δεν συμβαίνει αυτό, παρέχεται ένδειξη ότι η συσκευή χρειάζεται πόρους ανερχόμενη ζεύξης και παρέχεται ως μέρος της δομής ελέγχου-σηματοδότησης L1 / L2.[11][19]

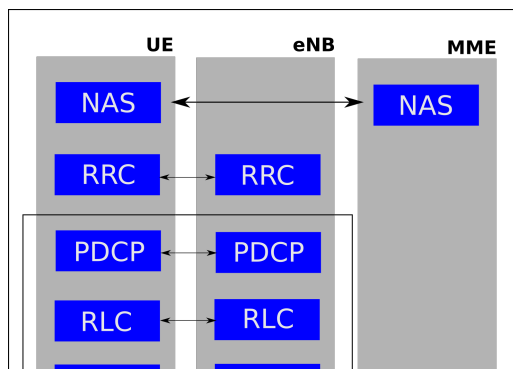
### 3.3 Αρχιτεκτονική Ραδιοπρωτοκόλλων

Αρχικά θα περιγράψουμε τη στοίβα πρωτοκόλλων όπως αυτή έχει διαμορφωθεί από την συνδεσιμότητα του non stand alone δικτύου πυρήνα με τη βοήθεια του eNB στο δίκτυο πρόσβασης και έπειτα θα αναφερθούμε στις διαφοροποιήσεις πρωτοκόλλων που εισήγηγαγε η εφαρμογή του gNB.

Οι στοίβες πρωτοκόλλων, από την έναρξη του GPRS, χωρίζεται σε δύο επίπεδα: το επίπεδο χρήστη ( User Plane ή επίπεδο μετάδοσης) και το επίπεδο ελέγχου(Control Plane ή επίπεδο σηματοδοσίας). Το επίπεδο χρήστη παρέχει τους τρόπους και τις διαδικασίες μετάδοσης των δεδομένων του χρήστη ανάμεσα στο κινητό σταθμό και σε ένα εξωτερικό δίκτυο πακέτων δεδομένων. Το επίπεδο ελέγχου υποστηρίζει και ελέγχει τις λειτουργίες σηματοδοσίας και μετάδοσης μέσα στο δίκτυο.[10]

Οι λειτουργίες του επιπέδου χρήστη( συμπίεση επικεφαλίδας πακέτων, κρυπτογράφηση, ARQ και HARQ) υλοποιούνται μέσω διασύνδεσης του εξοπλισμού χρήστη (UE) με το eNB, στο φυσικό επίπεδο (PHY), στο επίπεδο ελέγχου πρόσβασης (MAC), στο επίπεδο ελέγχου ραδιοζεύξης (RLC) και στο επίπεδο πρωτοκόλλου ελέγχου πακέτων δεδομένων (PDCP), που περιλαμβάνουν τις λειτουργίες συμπίεσης επικεφαλίδας και κρυπτογράφησης(encryption) του επιπέδου χρήστη όπως φαίνεται και στο σχήμα. Στο ίδιο σχήμα απεικονίζεται και η στοίβα πρωτοκόλλων για το επίπεδο ελέγχου. [14]

Λαμβάνοντας υπόψη τη συνολική αρχιτεκτονική δικτύου, μπορεί να συζητηθεί η αρχιτεκτονική πρωτοκόλλου RAN για τα επίπεδα χρήστη και ελέγχου, όπως αναφερθήκαμε παραπάνω για non stand alone επιλογές, αλλά



και για Stand Alone(αυτόνομα 5G συστήματα). Το παρακάτω σχήμα τώρα απεικονίζει την αρχιτεκτονική πρωτοκόλλου RAN σε συνδεσμολογία με το AMF το οποίο δεν αποτελεί μέρος του RAN αλλά περιλαμβάνεται στο σχήμα για πληρότητα και επίδειξη της Stand Alone επιλογής.

Όπως φαίνεται στο σχήμα δεν υπάρχουν μεγάλες διαφορές μεταξύ των δύο επιλογών(NSA και SA) και πολλές οντότητες πρωτοκόλλων είναι κοινές στα επίπεδα χρήστη και ελέγχου και ως εκ τούτου τα PDCP, RLC, MAC και PHY θα περιγραφούν μόνο στην ενότητα επιπέδου χρήστη.[12]

Στη συνέχεια, ακολουθεί μία ενότητα που αναφέρεται στα πρωτόκολλα επιπέδου χρήστη, ακολουθούμενη από την ενότητα που αναλύει τα πρωτόκολλα του επιπέδου ελέγχου.

### 3.3.1 Πρωτόκολλα Επιπέδου Χρήστη(User Plane)

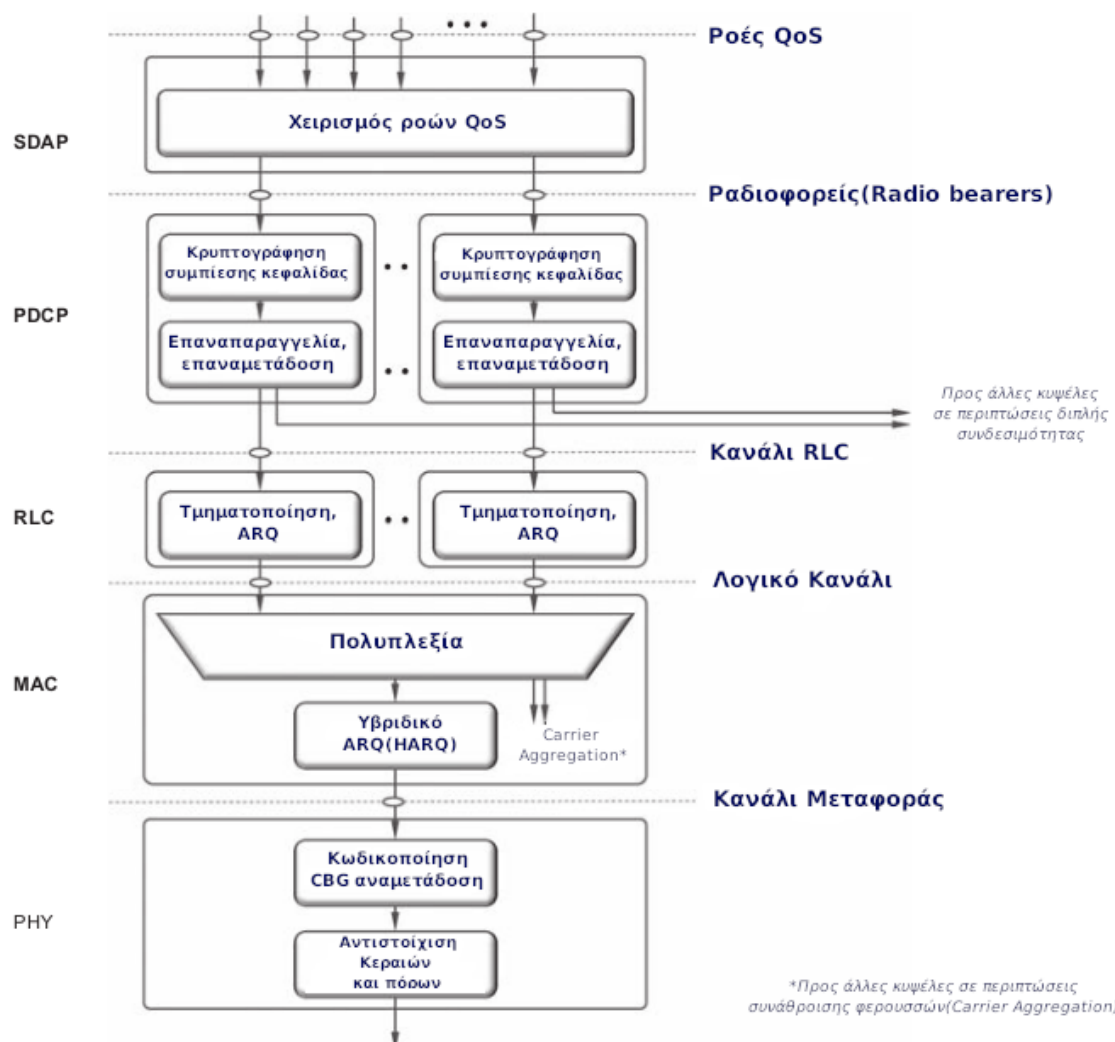
Μια γενική επισκόπηση της αρχιτεκτονικής πρωτοκόλλου επιπέδου χρήστη NR για την κατερχόμενη ζεύξη παρουσιάζεται στο σχήμα παρακάτω. Πολλά από τα επίπεδα πρωτοκόλλου είναι παρόμοια με αυτά του LTE, αν και υπάρχουν και κάποιες διαφορές. Μία από τις διαφορές είναι ο χειρισμός ποιότητας υπηρεσίας(QoS) σε NR όταν συνδέεται σε δίκτυο πυρήνα 5G, όπου το στρώμα πρωτοκόλλου SDAP δέχεται μία ή περισσότερες ροές QoS που μεταφέρουν πακέτα IP σύμφωνα με τις απαιτήσεις του QoS. Στην περίπτωση του επιπέδου χρήστη NR συνδεδεμένο στο EPC, το SDAP δεν χρησιμοποιείται.[12]

Όπως θα καταστεί σαφές παρακάτω, δεν ισχύουν όλες οι οντότητες που απεικονίζονται στο σχήμα 3.6 σε όλες τις περιπτώσεις. Για παράδειγμα, η κρυπτογράφηση δεν χρησιμοποιείται για μετάδοση των βασικών πληροφοριών συστήματος. Η δομή πρωτοκόλλου ανερχόμενης ζεύξης είναι παρόμοια με τη δομή κατερχόμενης ζεύξης στο σχήμα 3.7, αν και υπάρχουν κάποιες διαφορές, για παράδειγμα η επιλογή μορφής μεταφοράς και ο έλεγχος της πολυπλεξίας λογικών καναλιών.

Οι διαφορετικές οντότητες πρωτοκόλλου του δικτύου ραδιοπρόσβασης συνοψίζονται παρακάτω, σε ένα παράδειγμα κατερχόμενης NR ζεύξης επιπέδου χρήστη όπως φαίνεται από τη συσκευή.

#### Service Data Adaptation Protocol (SDAP)

Το πρωτόκολλο προσαρμογής δεδομένων υπηρεσίας (Service Data Adaptation Protocol, SDPA) είναι υπεύθυνο για την αντιστοίχιση μιας ροής QoS από το δίκτυο κορμού 5G και ενός ραδιοφορέα(bearer) δεδομένων, καθώς και για την επισήμανση του αναγνωριστικού ροής QoS (QFI) σε πακέτα ανερχόμενης και κατερχόμενης ζεύξης. Ο λόγος για την εισαγωγή του SDAP στο NR είναι η λειτουργία ένας νέου χειρισμού QoS συγκριτικά με το LTE όταν συνδέεται με



Εικόνα 3.7: Αρχιτεκτονική πρωτοκόλλου κατερχόμενης ζεύξης NR επιπέδου χρήστη όπως φαίνεται από τη συσκευή[10]

τον πυρήνα 5G. Όταν το gNB είναι συνδεδεμένο στο EPC, όπως συμβαίνει για τη μη αυτόνομη λειτουργία, το SDAP δεν χρησιμοποιείται και επίσης αυτό το πρωτόκολλο υπάρχει μόνο στο επίπεδο χρήστη.[10]

### Packet Data Convergence Protocol (PDCP)

Το στρώμα PDCP που από την πλευρά του δικτύου τερματίζεται στο eNB στο C-Plane επεξεργάζεται και μεταφέρει τις πληροφορίες του στρώματος RRC ενώ στο U-Plane χειρίζεται πακέτα δεδομένων IP και εκτελεί συμπίεση κεφαλίδας IP για να μειώσει τον αριθμό των bit για μετάδοση μέσω της διεπαφής ραδιοσυστήματος. Ο μηχανισμός συμπίεσης κεφαλίδας βασίζεται στο πλαίσιο συμπίεσης κεφαλίδας Robust Header Compression (ROHC), ένα σύνολο τυποποιημένων αλγορίθμων συμπίεσης κεφαλίδας που χρησιμοποιούνται επίσης για πολλές άλλες τεχνολογίες κινητής επικοινωνίας. Ακόμη, υλοποιεί τις λειτουργίες της κρυπτογράφησης και της προστασίας της ακεραιότητας των δεδομένων, την προστασία από υποκλοπές και, για το επίπεδο ελέγχου, την προστασία ακεραιότητας για να διασφαλίσει ότι τα μηνύματα ελέγχου

προέρχονται από τη σωστή πηγή. Στην πλευρά του δέκτη, το PDCP εκτελεί τις αντίστοιχες λειτουργίες αποκρυπτογράφησης και αποσυμπίεσης. Τέλος, υλοποιεί τις διαδικασίες επαναμετάδοσης κατά την πραγματοποίηση μεταπομπής.[14]

Το PDCP είναι επίσης υπεύθυνο για την προώθηση πακέτων δεδομένων που δεν έχουν παραδοθεί κατά τη μετάβαση από ένα gNB σε ένα άλλο. Η οντότητα PDCP στη συσκευή θα χειριστεί επίσης την αναμετάδοση όλων των πακέτων ανερχόμενης ζεύξης που δεν έχουν παραδοθεί ακόμη στο gNB καθώς η προσωρινή μνήμη των υβριδικών-ARQ(HARQ) αδειάζουν κατά την παράδοση. Ός Hybrid automatic repeat request (hybrid ARQ ή HARQ) είναι ένας συνδυασμός ελέγχου σφάλματος, υψηλής ταχύτητας προώθησης σφαλμάτων (FEC) και αυτόματου αιτήματος επανάληψης (ARQ).[11]

Σε αυτήν την περίπτωση, ορισμένα PDU ενδέχεται να ληφθούν εις διπλούν, τόσο μέσω της σύνδεσης με το παλιό gNB όσο και με το νέο gNB. Το PDCP σε αυτήν την περίπτωση θα αφαιρέσει τυχόν διπλότυπα και μπορεί επίσης να διαμορφωθεί ώστε να εκτελεί αναδιάταξη ώστε να διασφαλίζεται η παράδοση των SDU με σειρά, σε πρωτόκολλα υψηλότερου επιπέδου, εάν είναι επιθυμητό.[11]

Το στρώμα PDCP μπορεί επίσης να χρησιμοποιήσει αυτή τη διπλοτυπία για πολυπλεξία δηλαδή να διπλασιάζει τα πακέτα και να τα μεταδίδει σε πολλαπλές κυψέλες, επιτυγχάνοντας χωρική πολυπλεξία αυξάνοντας την ευρωστία και την αξιοπιστία του συστήματος καθώς το ίδιο πακέτο αποστέλλεται από διαφορετικές κυψέλες μα αποτέλεσμα να αυξάνεται η πιθανότητα να παραδοθεί. [11]

### Radio Link Control (RLC)

Τα στρώματα RLC και MAC επίσης τερματίζονται, από την πλευρά του δικτύου, στο eNB. Η κύρια λειτουργία του RLC είναι η οργάνωση πακέτων δεδομένων ανωτέρων στρωμάτων σε μέγεθος κατάλληλο για μετάδοση μέσω της ραδιοεπαφής του LTE, παρέχοντας αξιοπιστία στη ραδιοεπαφή και μπορεί να ανιχνεύσει μια εσφαλμένη μετάδοση πακέτων μετά την άφιξη στον δέκτη. Συνεπώς, στο επίπεδο RLC ανακτώνται και τα πακέτα που έχουν χαθεί κατά τη μετάδοση, ενώ αναδιατάσσονται και τα πακέτα που φτάνουν στον δέκτη σε λάθος διάταξη. [14]

Το πρωτόκολλο RLC είναι υπεύθυνο για την κατάτμηση των RLC Service Data Units(SDUs) από το PDCP σε RLC Packet Data Units (PDUs) κατάλληλου μεγέθους. Διαχειρίζεται επίσης την αναμετάδοση λανθασμένων λαμβανόμενων PDU, καθώς και την αφαίρεση διπλών PDU. Ανάλογα με τον τύπο της υπηρεσίας, το RLC μπορεί να διαμορφωθεί σε μία από τις τρεις λειτουργίες για εκτέλεση ορισμένων ή όλων των λειτουργιών:

- διαφανή λειτουργία, που όπως υποδηλώνει το όνομα, διαφανής και δεν προστίθενται κεφαλίδες
- λειτουργία χωρίς αναγνώριση που υποστηρίζει τμηματοποίηση και διπλή ανίχνευση
- λειτουργία αναγνώρισης που υποστηρίζει επιπλέον την αναμετάδοση λανθασμένων πακέτων

Μία σημαντική διαφορά σε σύγκριση με το LTE είναι ότι το RLC δεν διασφαλίζει μεταγενέστερη παράδοση SDU σε ανώτερα επίπεδα. Η κατάργηση της παράδοσης σε σειρά από το RLC μειώνει τη συνολική καθυστέρηση καθώς τα μεταγενέστερα πακέτα δεν χρειάζεται να περιμένουν για την αναμετάδοση ενός παλιότερου πακέτου που λείπει πριν παραδοθούν σε υψηλότερα επίπεδα αλλά μπορούν να προωθηθούν αμέσως. [12]

Η τμηματοποίηση είναι μία από τις κύριες λειτουργίες RLC όπως επίσης και συνένωση(concatenation) που υποστηρίζεται και στο LTE. Ανάλογα με την απόφαση του προγραμματιστή, επιλέγεται μια συγκεκριμένη ποσότητα δεδομένων, δηλαδή ένα συγκεκριμένο μέγεθος μεταφοράς-μπλοκ. Ως μέρος του συνολικού σχεδιασμού χαμηλής καθυστέρησης του NR, είναι η απόφαση προγραμματισμού σε περίπτωση μετάδοσης uplink η οποία γίνεται γνωστή στη συσκευή λίγο πριν από τη μετάδοση, με τη σειρά μερικών συμβόλων OFDM πριν. Στην περίπτωση της συνένωσης στο LTE, το RLC PDU δεν μπορεί να συναρμολογηθεί έως ότου γίνει γνωστή η απόφαση προγραμματισμού, η οποία οδηγεί σε μια επιπλέον καθυστέρηση μέχρι την μετάδοση ανερχόμενης ζεύξης και δεν μπορεί να ανταποκριθεί στην απαίτηση χαμηλής καθυστέρησης του NR. Αφαιρώντας τη συνένωση από το RLC, τα RLC PDUs μπορούν να συναρμολογηθούν εκ των προτέρων και μετά τη λήψη της απόφασης προγραμματισμού, η συσκευή πρέπει να προωθήσει μόνο έναν κατάλληλο αριθμό RLC PDUs στο στρώμα MAC, ο αριθμός των οποίων ποικίλει ανάλογα με το προγραμματισμένο μέγεθος μπλοκ μεταφοράς. Για να γεμίσει πλήρως το μέγεθος του μπλοκ μεταφοράς, το τελευταίο RLC PDU μπορεί να περιέχει ένα τμήμα ενός SDU. Η λειτουργία τμηματοποίησης είναι απλή καθώς κατά τη λήψη του προγραμματισμού, η συσκευή περιλαμβάνει τον αριθμό των δεδομένων που απαιτούνται για τη συμπλήρωση του μπλοκ μεταφοράς και ενημερώνουν την κεφαλίδα για να υποδείξει ότι είναι ένα τμήμα SDU.[11]

Ο RLC μηχανισμός αναμετάδοσης είναι επίσης υπεύθυνος ώστε να παραδίδει τα δεδομένα στα ανώτερα επίπεδα απαλλαγμένα από σφάλματα. Για να το πετύχει αυτό, ένα πρωτόκολλο αναμετάδοσης λειτουργεί ανάμεσα στις RLC οντότητες στον πομπό και στον δέκτη.

Παρακολουθώντας τους αριθμούς ακολουθίας που υποδεικνύονται στις επικεφαλίδες των εισερχόμενων PDUs, το RLC λήψης μπορεί να αναγνωρίσει ελλείπουσες PDU (ο αριθμός ακολουθίας RLC είναι ανεξάρτητος από τον αριθμό ακολουθίας PDCP). Οι αναφορές κατάστασης επιστρέφονται στην οντότητα RLC που μεταδίδει, ζητώντας την αναμετάδοση εκλειπόμενων PDU. Με βάση την ληφθείσα αναφορά κατάστασης, η οντότητα RLC στον πομπό μπορεί να προβεί στην κατάλληλη ενέργεια και να εκπέμψει εκ νέου τα PDU που λείπουν, εάν χρειαστεί.

Αν και το RLC είναι ικανό να χειριστεί σφάλματα μετάδοσης λόγω θορύβου, απρόβλεπτων παραλλαγών καναλιών κ.λ.π., η παράδοση χωρίς σφάλματα αντιμετωπίζεται στις περισσότερες περιπτώσεις από το πρωτόκολλο υβριδικού ARQ(HARQ) που βασίζεται στο επίπεδο MAC. Η χρήση ενός μηχανισμού αναμετάδοσης στο RLC μπορεί επομένως να φαίνεται περιττή στην αρχή, ωστόσο αυτό δεν συμβαίνει καθώς και η χρήση και των δύο μηχανισμών αναμετάδοσης που βασίζονται σε RLC και MAC υποκινούνται στην πραγματικά στις διαφορές στη σηματοδότηση ανάδρασης.[10]

### Medium Access Control (MAC)

Το πρωτόκολλο MAC ελέγχει την απόδοση των πόρων και τη σηματοδότηση των επιβεβαιώσεων στη ραδιοεπαφή. Είναι υπεύθυνο για την πολυπλεξία και απο-πολυπλεξία δεδομένων μεταξύ φυσικού στρώματος και στρώματος RLC κυρίως κατά τη συνάθροιση φερουσών. Επικοινωνεί με το στρώμα RLC μέσω λογικών καναλιών και με το φυσικό στρώμα, μέσω καναλιών μεταφοράς. Χειρίζεται επίσης την πολυπλεξία λογικών καναλιών και τις HARQ αναμεταδόσεις. Οι κύριες λειτουργίες του MAC είναι: ο χρονοπρογραμματισμός των ραδιο-πόρων (scheduling) μεταξύ των Ues, η υλοποίηση των διαδικασιών τυχαίας πρόσβασης και η χρονική ευθυγράμμιση (timing alignment) στην άνω ζεύξη.[14]

Στην επόμενη ενότητα περιγράφονται τα κανάλια μετάδοσης που χρησιμοποιεί το MAC επίπεδο.

### Physical Layer (PHY)

Το φυσικό επίπεδο (PHY) περιλαμβάνει την επεξεργασία των καναλιών μεταφοράς (transport channels) που υλοποιούν τις διαδικασίες ελέγχου σφαλμάτων, την επεξεργασία των φυσικών καναλιών (physical channels) που υλοποιούν τις τεχνικές OFDMA, SC-FDMA και MIMO και το αναλογικό τμήμα (μείκτες, κεραίες κλπ.). Η επικοινωνία του PHY με το MAC γίνεται μέσω καναλιών μεταφοράς, ενώ τα διάφορα τμήματα του PHY επικοινωνούν μεταξύ τους μέσω φυσικών καναλιών.[16]

Το φυσικό επίπεδο επίσης, είναι υπεύθυνο για την κωδικοποίηση, τη διεργασία HARQ φυσικού επιπέδου, τη διαμόρφωση, τη διεργασία πολλαπλών κεραιών και την αντιστοιχία του σήματος με τους κατάλληλους πόρους χρόνου και συχνότητας. Επίσης, χειρίζεται την αντιστοιχία των καναλιών μετάδοσης με τα φυσικά κανάλια. [16]

Το φυσικό επίπεδο γενικότερα παρέχει υπηρεσίες στο MAC επίπεδο στο πρότυπο των καναλιών μεταφοράς. Στην επόμενη ενότητα περιγράφονται τα κανάλια μετάδοσης που χρησιμοποιεί το PHY επίπεδο.

## 3.3.2 Πρωτόκολλα επιπέδου ελέγχου

Το επίπεδο χρήστη αποτελείται στο LTE από τα παραπάνω επίπεδα ενώ στο επίπεδο ελέγχου προστίθενται και το στρώμα Radio Resource Control (RRC) καθώς και το πρωτόκολλο ελέγχου του συστήματος μη πρόσβασης (Non-Access Stratum, NAS).

### Radio Resource Control (RRC)

Το στρώμα RRC υπάρχει, όπως αναφέραμε, μόνο στο C-Plane και αυτό από την πλευρά του δικτύου τερματίζεται στο eNB. Υλοποιεί τις λειτουργίες ευρυεκπομπής, της τηλε-ειδοποίησης, της διαχείρισης συνδέσεων RRC, τις λειτουργίες κινητικότητας, τον έλεγχο και την αναφορά των μετρήσεων του εξοπλισμού χρήστη και τον έλεγχο του ραδιο-κομιστή (Radio Bearer control). Τέλος, μεταφέρει τις πληροφορίες του NAS είτε αυτές προορίζονται για κάποιο

συγκεκριμένο συνδρομητή (dedicated) ή για όλους τους συνδρομητές του δικτύου(common).[14]

### Non-Access Stratum(NAS)

Το πρωτόκολλο ελέγχου του συστρώματος μή πρόσβασης(Non-Access Stratum,NAS) τερματίζεται, απο την πλευρά του δικτύου, στη μονάδα MME και μεταξύ άλλων πραγματοποιεί τη διαχείριση του κομιστή EPS(Enolved Packet System), τις διαδικασίες επαλήθευσης ταυτότητας, το χειρισμό της κινητικότητας και την ενεργοποίηση της τηλε-ειδοποίησης στην άεργη κατάσταση του ECM(EPS Connection Management) και τους ελέγχους ασφαλείας του συστήματος. Η λειτουργία αυτή διαφοροποιείται απο το Access Stratum(AS) όπου χειρίζεται τη λειτουργία μεταξύ της συσκευής και του δικτύου ραδιοπρόσβασης.[10][14]

## 3.4 Κανάλια μετάδοσης

Στα δίκτυα LTE και NR οι πληροφορίες είτε πρόκειται για δεδομένα είτε μηνύματα δικτύου(σηματοδοσία, μηνύματα ελέγχου κλπ) διακινούνται μέσω καναλιών, τα οποία διαφοροποιούνται και διακρίνονται σε υποκατηγορίες ανάλογα με το είδος της πληροφορίας που μεταφέρουν, την κατεύθυνση της ζεύξης όπου λειτουργούν και τη χρησιμότητα τους.[14]

Τα κανάλια όπου μεταφέρεται η πληροφορία εντοπίζονται στο επίπεδο MAC και στο φυσικό επίπεδο(PHY) και με βάση αυτά μπορούμε να τα διαχωρίσουμε περαιτέρω ανάλογα με το ρόλο που έχουν να διατελέσουν καθώς και με το είδος της μεταδιδόμενης πληροφορίας αντίστοιχα. Όπως αναφερθήκαμε και παραπάνω, στο MAC επίπεδο μπορούμε να κατατάξουμε τα κανάλια μετάδοσης. Για μία πιο ουσιαστική ανάλυση εισήχθη αυτή η ξεχωριστή ενότητα όπου αναπτύσσονται οι διάφορες περιπτώσεις των καναλιών αυτών. Το επίπεδο MAC χειρίζεται τη λογική-πολυπλεξία καναλιών, τις λειτουργίες αναμετάδοσης HARQ, καθώς και τις συναρτήσεις προγραμματισμού. Είναι επίσης υπεύθυνο για την πολυπλεξία / αποπολυπλεξία δεδομένων σε πολλαπλούς φορείς όταν χρησιμοποιείται η συνάρθρωση φερουσών.[11]

Η ενότητα αυτή ουσιαστικά είναι συνέχεια των πρωτοκόλλων επιπέδου χρήστη καθόσον τα στρώματα MAC και PHY ανήκουν σε αυτό. Λόγο της μεγάλης σημασίας του όμως και του όγκου συγγράφεται σε ξεχωριστή ενότητα.

### 3.4.1 Κανάλια επιπέδου MAC

Στην περίπτωση των καναλιών επιπέδου MAC μπορούμε να διακρίνουμε δύο κατηγορίες καναλιών. Τα λογικά κανάλια και τα κανάλια μεταφοράς.

#### ► Λογικά Κανάλια

Το MAC επίπεδο παρέχει υπηρεσίες στο RLC με τη μορφή λογικών καναλιών. Ένα λογικό κανάλι(logical channel) ορίζεται από τον τύπο και το είδος των πληροφοριών που μεταφέρει αλλά και ποιοι είναι οι αποδέκτες των



πληροφοριών αυτών. Γενικά, ταξινομείται ως λογικό κανάλι ελέγχου(logical control channel), όταν χρησιμοποιείται για τη μετάδοση πληροφοριών ελέγχου, σηματοδότησης και διαμόρφωσης που είναι απαραίτητες για τη λειτουργία ενός συστήματος NR, ή ως κανάλι κίνησης(logical traffic channel), που χρησιμοποιείται για τη διακίνηση δεδομένων χρήστη.[10][14]

Επίσης, υπάρχουν λογικά κανάλια που είναι εκχωρημένα σε ένα UE αποκλειστικά(dedicated logical channels) και άλλα που χρησιμοποιούνται από περισσότερα UEs(common logical channels)

Το σύνολο των τύπων λογικών καναλιών που καθορίζονται για το NR περιλαμβάνει:

- ▷ Το **Κανάλι ελέγχου εκπομπής (Broadcast Control Channel, BCCH)**, χρησιμοποιείται για τη μετάδοση πληροφοριών συστήματος από το δίκτυο σε όλες τις συσκευές σε μία κυψέλη. Το BCCH μεταφέρει μηνύματα πληροφοριών του επιπέδου RRC που εκπέμπει ο κόμβος eNB προς όλους τους κόμβους της κυψέλης. Πριν από την πρόσβαση στο σύστημα, μια συσκευή πρέπει να αποκτήσει τις πληροφορίες συστήματος για να μάθει πώς διαμορφώνεται το σύστημα και, γενικά, πώς να συμπεριφέρεται σωστά μέσα σε μία κυψέλη. Κατά την αρχική σύνδεση της UE στο δίκτυο, το UE λαμβάνει βασικές ρυθμίσεις του δικτύου για να μπορέσει να προσαρμόσει ανάλογα τις δικές του λειτουργικές παραμέτρους. Οι πληροφορίες που μεταφέρει το BCCH χωρίζονται σε δύο ομάδες: οι πιο σημαντικές από αυτές, όπως για παράδειγμα το εύρος ζώνης, περιέχονται στο Master Information Block(MIB) και οι υπόλοιπες στο System Information Block(SIB).[10][14]

Αξίζει να σημειώσουμε ότι, στην περίπτωση μη αυτόνομης λειτουργίας(Non Stand Alone), οι πληροφορίες συστήματος παρέχονται από το σύστημα LTE και δεν υπάρχει BCCH.[10][14]

- ▷ Το **κανάλι ελέγχου τηλεειδοποίησης (Paging Control Channel, PCCH)**, χρησιμοποιείται για τηλεειδοποίηση συσκευών των οποίων η θέση, σε επίπεδο κυψέλης, δεν είναι γνωστή στο δίκτυο. Επομένως, το μήνυμα τηλεειδοποίησης πρέπει να μεταδοθεί και σε γειτονικές κυψέλες. Στην περίπτωση μη αυτόνομης λειτουργίας, η τηλεειδοποίηση παρέχεται από το σύστημα LTE και δεν υπάρχει PCCH.[10][14]
- ▷ Το **κοινό κανάλι ελέγχου (Common Control Channel, CCCH)**, χρησιμοποιείται για τη μετάδοση πληροφοριών ελέγχου σε συνδυασμό με τυχαία πρόσβαση.[10]
- ▷ Το **αφιερωμένο στον έλεγχο κανάλι (Dedicated Control Channel, DCCH)**, χρησιμοποιείται για τη μετάδοση πληροφοριών ελέγχου από και προς μια συσκευή. Αυτό το κανάλι χρησιμοποιείται για μεμονωμένη διαμόρφωση συσκευών όπως η ρύθμιση διαφόρων παραμέτρων σε συσκευές.[10]
- ▷ Το **αφιερωμένο στην κίνηση δεδομένων κανάλι (Dedicated Traffic Channel, DTCH)**, χρησιμοποιείται για τη μετάδοση δεδομένων χρήστη προς και από μια συσκευή. Αυτός είναι ο λογικός τύπος καναλιού που

χρησιμοποιείται για τη μετάδοση όλων των δεδομένων χρήστη uplink και downlink unicast.[15]

Τα παραπάνω λογικά κανάλια υπάρχουν γενικά και σε ένα σύστημα LTE και χρησιμοποιούνται για παρόμοια λειτουργικότητα. Ωστόσο, το LTE παρέχει επιπλέον λογικά κανάλια για δυνατότητες που δεν υποστηρίζονται ακόμη από το NR (αλλά πιθανότατα θα παρουσιαστούν στις προσεχής μελλοντικές κυκλοφορίες).[15]

Συνοφίζουμε τα παραπάνω κανάλια στον παρακάτω πίνακα

Λογικό Κανάλι		Είδος Πληροφορίας	Κατεύθυνση Ζεύξης
DTCH	Dedicated Traffic CHannel	Δεδομένα επιπέδου χρήστη	UL , DL
DCCCH	Dedicated Control CHannel	Σηματοδοσία	UL , DL
CCCH	Common Control CHannel	Σηματοδοσία	UL , DL
PCCH	Paging Control CHannel	Μηνύματα ελέγχου Τηλεειδοποίησης	DL
BCCH	Broadcast Control CHannel	Μηνύματα ελέγχου ευρυεκπομπής	DL

Πίνακας 3.1: Είδη Λογικών καναλιών [14]

### ► Κανάλια Μεταφοράς

Από το φυσικό επίπεδο, το στρώμα MAC χρησιμοποιεί υπηρεσίες με τη μορφή καναλιών μεταφοράς. Ένα κανάλι μεταφοράς καθορίζεται από το πώς και με ποια χαρακτηριστικά μεταδίδονται οι πληροφορίες μέσω της διεπαφής του δικτύου πρόσβασης. Τα δεδομένα σε ένα κανάλι μεταφοράς οργανώνονται σε μπλοκ μεταφοράς. Σε κάθε χρονικό διάστημα μετάδοσης (Transmission Time Interval, TTI), το πολύ ένα μπλοκ μεταφοράς δυναμικού μεγέθους μεταφέρεται πάνω σε μία διεπαφή του ραδιοσυστήματος απο και προς μιας συσκευής(στην περίπτωση της χωρικής πολυπλεξίας άνω των τεσσάρων στρωμάτων, υπάρχουν δύο μπλοκ ανά TTI).

Η σύνδεση τώρα με κάθε μπλοκ μεταφοράς είναι μια μορφή μεταφοράς (Transport Format , TF), η οποία καθορίζει τον τρόπο μετάδοσης του μπλοκ μεταφοράς μέσω της ραδιοεπαφής. Η μορφή μεταφοράς περιλαμβάνει πληροφορίες σχετικά με το μέγεθος του μπλοκ μεταφοράς, το σχήμα διαμόρφωσης και κωδικοποίησης και την αντιστοίχιση της κεραιάς. Μεταβάλλοντας τη μορφή μεταφοράς, το στρώμα MAC μπορεί έτσι να πραγματοποιήσει διαφορετικούς ρυθμούς δεδομένων, μια διαδικασία γνωστή ως επιλογή μορφής μεταφοράς ( transport-format selection).[10][14][15]

Οι τύποι καναλιών μεταφοράς που καθορίστηκαν για το NR είναι:

- ▷ Το **κανάλι μετάδοσης (Broadcast Channel, BCH)** έχει μια σταθερή μορφή μεταφοράς, που παρέχεται από τις προδιαγραφές. Χρησιμοποιείται για τη μετάδοση τμημάτων πληροφοριών του λογικού καναλιού BCCH, ειδικότερα του λεγόμενου Master Information Block (MIB) που είναι μπλοκ που περιέχουν βασικές πληροφορίες όπως αναφέραμε και παραπάνω, ενώ οι υπόλοιπες μεταφέρονται μέσω του DL-SCH.[10][14][15]
- ▷ Το **κανάλι τηλεειδοποίησης (Paging Channel, PCH)** χρησιμοποιείται για να μεταδώσει πληροφορίες τηλεειδοποίησης(μηνύματα paging) απο

ένα PCCH λογικό κανάλι ελέγχου μηνυμάτων. Το PCH υποστηρίζει ασυνεχή λήψη (Discontinuous Reception, DRX) για να επιτρέψει στη συσκευή να εξοικονομήσει ενέργεια μπαταρίας “ξυπνώντας” τη για να λάβει το PCH μόνο σε προκαθορισμένες χρονικές στιγμές.[10][14][15]

- ▷ Το **κοινόχρηστο κανάλι κατερχόμενης ζεύξης (Downlink Shared Channel, DL-SCH)** είναι το κύριο κανάλι μεταφοράς που χρησιμοποιείται για τη μετάδοση δεδομένων κατερχόμενης ζεύξης στο NR. Υποστηρίζει βασικά χαρακτηριστικά NR, όπως δυναμική προσαρμογή ρυθμού και προγραμματισμό που εξαρτάται από το κανάλι στους τομείς χρόνου και συχνότητας, υβριδικό ARQ με soft combination και χωρική πολυπλεξία. Υποστηρίζει επίσης DRX για τη μείωση της κατανάλωσης ενέργειας της συσκευής παρέχοντας μία συνεχώς ενεργή εμπειρία. Το DL-SCH χρησιμοποιείται επίσης για τη μετάδοση των τμημάτων πληροφοριών συστήματος BCCH που δεν έχουν αντιστοιχηθεί στο BCH. Κάθε συσκευή διαθέτει DL-SCH ανά κυψέλη με το οποίο είναι συνδεδεμένη. Σε υποδοχές(slots) όπου λαμβάνονται πληροφορίες συστήματος υπάρχει ένα επιπλέον DL-SCH από τη μεριά της συσκευής.[15]

- ▷ Το **κοινό κανάλι ανερχόμενης ζεύξης (Uplink Shared Channel, UL-SCH)** είναι το αντίστοιχο uplink στο DL-SCH, δηλαδή το κανάλι μεταφοράς uplink που χρησιμοποιείται για τη μετάδοση δεδομένων ανερχόμενης ζεύξης.[15]

*Το μεγαλύτερο ποσοστό των μεριζόμενων δεδομένων(δεδομένα χρήστη και μηνύματα σηματοδότησης) διακινείται μέσω των κοινόχρηστων(ή μεριζόμενων) καναλιών άνω και κάτω ζεύξης (UL-SCH και DL-SCH), που για το λόγο αυτό είναι και τα σημαντικότερα κανάλια μεταφοράς.[10][14][15]*

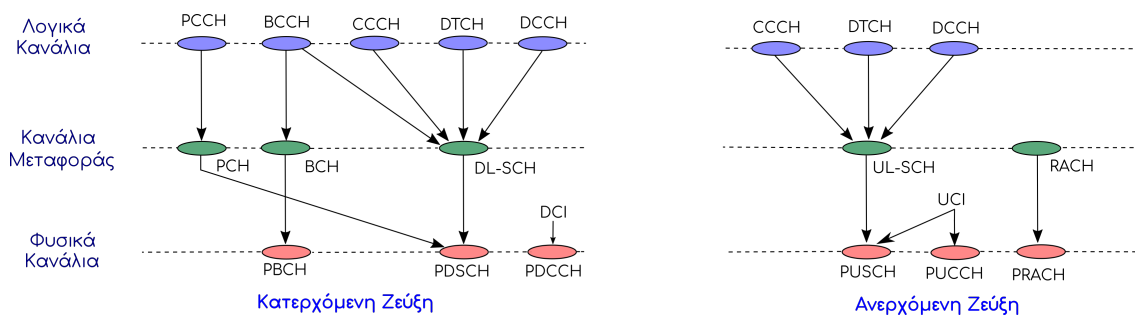
- ▷ Το **Κανάλι μεταφοράς τυχαίας πρόσβασης(Random-Access Channel , RACH)** είναι συνήθης διαδικασία με την οποία το UE προγραμματίζει τις εκπομπές του είναι με βάση τα δικαιώματα χρήσης ραδιο-πόρων(χρονο-σχιμές και υπο-διάυλοι) που του εκχωρεί ο κόμβος eNB/gNB. Κατ’εξάιρεση στο MAC στρώμα ενός UE μπορεί να δημιουργηθούν εκπομπές τυχαίας πρόσβασης(random acces) οι οποίες να αποστέλλονται στο δίκτυο απ’ευθείας, χωρίς να έχει προηγηθεί εκχώρηση ραδιο-πόρων απο τον κόμβο eNB/gNB. Ειδικά για αυτού του είδους τις εκπομπές χρησιμοποιείται το κανάλι μεταφοράς τυχαίας πρόσβασης(Random-Access Channel , RACH) που κατατάσσεται στα κανάλια μεταφοράς αν και δεν μεταδίδει μπλόκ μεταφοράς. [15]

Εκτός απο το είδος των πληροφοριών που μεταφέρουν, τα κανάλια μεταφοράς διαφέρουν και στον τρόπο πρόληψης και αντιμετώπισης των σφαλμάτων. Συγκεκριμένα, στις μεταδόσεις των καναλιών UL-SCH και DL-SCH εφαρμόζονται τεχνικές ARQ και HARQ, ενώ επιπλέον ο ρυθμός κωδικοποίησης προσαρμόζεται στις συνθήκες του διαύλου (SINR). Αντίθετα, στα υπόλοιπα κανάλια μεταφοράς εφαρμόζονται απλά τεχνικές διόρθωσης σφάλματος (Forward Error Correction, FEC) με σταθερό ρυθμό κωδικοποίησης.

Κανάλι μεταφοράς		Είδος Πληροφορίας	Κατεύθυνση Ζεύξης
UL-SCH	UpLink Shared CHannel	Δεδομένα και σηματοδosis για την άνω ζεύξη	UL
RACH	RANdom Access CHannel	Αιτήματα για τυχαία πρόσβαση	UL
DL-SCH	DownLink Shared CHannel	Δεδομένα και σηματοδosis για την κάτω ζεύξη	DL
PCH	Paging CHannel	Μηνύματα Τηλεειδοποίησης	DL
BCH	Broadcast CHannel	Μηνύματα ευρυεκπομπής (MIB)	DL

Πίνακας 3.2: Είδη καναλιών μεταφοράς[14]

Μέρος της λειτουργικότητας του στρώματος MAC είναι επίσης και η πολυπλεξία διαφορετικών λογικών καναλιών καθώς και η αντιστοιχία των λογικών καναλιών στα κατάλληλα κανάλια μεταφοράς. Η αντιστοίχιση μεταξύ τύπων λογικών καναλιών και τύπων καναλιών μεταφοράς δίνεται στην εικόνα 3.8.



Εικόνα 3.8: Αντιστοίχιση μεταξύ λογικών, μεταφοράς και φυσικού καναλιού[10]

Το σχήμα αυτό αναδεικνύει πλην των άλλων πως τα DL-SCH και UL-SCH είναι τα κύρια κανάλια μεταφοράς κατερχόμενης και ανερχόμενης ζεύξης αντίστοιχα. Στο σχήμα, περιλαμβάνονται επίσης τα αντίστοιχα φυσικά κανάλια, που περιγράφονται παρακάτω και απεικονίζεται η αντιστοιχία μεταξύ καναλιών μεταφοράς και φυσικών καναλιών.

Το στρώμα MAC μπορεί να πολυπλέξει σε ένα κανάλι μεταφοράς πολλαπλά λογικά κανάλια, όπου κάθε λογικό κανάλι έχει τη δική του οντότητα RLC.

Στον δέκτη, το στρώμα MAC χειρίζεται την αντίστοιχη αποπολυπλεξία και προωθεί τα RLC PDUs στην αντίστοιχη οντότητα RLC, όπου για να υποστηρίξει την αποπολυπλεξία στον δέκτη, χρησιμοποιείται μια κεφαλίδα MAC. Η τοποθέτηση των κεφαλίδων MAC έχει βελτιωθεί σε σύγκριση με το LTE, με πρώτο μέλημα την ελαχιστοποίηση της καθυστέρησης. Δηλαδή αντί να εντοπίζει όλες τις πληροφορίες κεφαλίδας MAC στην αρχή ενός MAC PDU, (πράγμα που σημαίνει ότι η σύνθεση του MAC PDU (Packet Data Unit) δεν μπορεί να ξεκινήσει έως ότου είναι διαθέσιμη η απόφαση προγραμματισμού), η υποκεφαλίδα που αντιστοιχεί σε μια συγκεκριμένη MAC SDU (Service Data Unit) τοποθετείται αμέσως πριν από το SDU. Αυτό επιτρέπει την προεπεξεργασία των PDU πριν ληφθεί η απόφαση προγραμματισμού (scheduling). [10][11]

Η υποκεφαλίδα περιέχει την ταυτότητα του λογικού καναλιού (LCID), από το οποίο προήλθε το RLC PDU, καθώς και το μήκος του PDU σε byte. Περιέχει επίσης και μια σημαία που δείχνει το μέγεθος το μήκος του δείκτη, καθώς και

ένα δεσμευμένο κομμάτι για μελλοντική χρήση. Εκτός από την πολυπλεξία διαφορετικών λογικών καναλιών, το στρώμα MAC μπορεί επίσης να εισαγάγει στοιχεία ελέγχου MAC στα μπλοκ μεταφοράς που θα μεταδοθούν μέσω των καναλιών μεταφοράς. Ένα στοιχείο ελέγχου MAC χρησιμοποιείται και για τη σηματοδότηση ελέγχου ζώνης και αναγνωρίζεται με δεσμευμένες τιμές στο πεδίο LCID, όπου η τιμή LCID δείχνει τον τύπο πληροφοριών ελέγχου. Για μεταδόσεις κατερχόμενης ζεύξης, τα στοιχεία ελέγχου MAC βρίσκονται στην αρχή του MAC PDU, ενώ για τις μεταδόσεις ανερχόμενης ζεύξης τα στοιχεία ελέγχου MAC βρίσκονται στο τέλος. Και πάλι, η τοποθέτηση επιλέγεται προκειμένου να διευκολυνθεί η λειτουργία χαμηλής καθυστέρησης στη συσκευή.[10][11]

#### ◆ Στοιχεία ελέγχου MAC

Τα στοιχεία ελέγχου MAC (MAC control elements), χρησιμοποιούνται για σηματοδότηση ελέγχου ζώνης. Παρέχουν έναν γρηγορότερο τρόπο αποστολής σηματοδότησης ελέγχου από το RLC, χωρίς να χρειάζεται να καταφύγουμε σε περιορισμούς που αφορούν τα μεγέθη ωφέλιμου φορτίου και την αξιοπιστία που προσφέρει το φυσικό επίπεδο ελέγχου L1 / L2 (PDCCH ή PUCCH).[10][11]

#### ◆ Συνάθροιση Φερουσών και Διπλή Συνδεσιμότητα(Carrier Aggregation και Dual conectivity)

Η οντότητα MAC είναι επίσης υπεύθυνη για τη διανομή δεδομένων από κάθε ροή μεταξύ των διαφορετικών φορέων ή κυψελών, στην περίπτωση συνάθροισης φερουσών (carrier aggregation). Η βασική αρχή για τη συνάθροιση φερουσών είναι η ανεξάρτητη επεξεργασία των συστατικών φορέων στο φυσικό στρώμα, συμπεριλαμβανομένης της σηματοδότησης ελέγχου, του προγραμματισμού και της αναμετάδοσης υβριδικών-ARQ, ενώ η συνάθροιση φερουσών είναι “αόρατη” πάνω από το στρώμα MAC.[10][11]

Συνεπώς, κατά τη συναθροισή φερουσών στο στρώμα MAC, λογικά κανάλια, συμπεριλαμβανομένων οποιονδήποτε στοιχείων ελέγχου MAC, πολυπλέκονται για να σχηματίσουν μπλοκ μεταφοράς ανά συστατικό φορέα, όπου με τη σειρά του ο κάθε φορέας έχει τη δική του οντότητα υβριδικού-ARQ.[10][11]

Τόσο η συνάθροιση φερουσών όσο και η διπλή συνδεσιμότητα έχουν ως αποτέλεσμα τη σύνδεση της συσκευής σε περισσότερες από μία κυψέλες. Παρά αυτήν την ομοιότητα, υπάρχουν θεμελιώδεις διαφορές μεταξύ τους, που σχετίζονται κυρίως με το πόσο στενά συντονίζονται οι διαφορετικές κυψέλες και αν βρίσκονται στα ίδια ή σε διαφορετικά gNBs.[10][11]

Η συνάθροιση φερουσών (carrier aggregation) συνεπάγεται πολύ στενό συντονισμό, με όλες τις κυψέλες να ανήκουν στο ίδιο gNB. Οι αποφάσεις προγραμματισμού λαμβάνονται από κοινού για όλες τις κυψέλες στις οποίες είναι συνδεδεμένη η συσκευή από έναν κοινό προγραμματιστή(scheduler).[10][11]

Η διπλή συνδεσιμότητα, από την άλλη πλευρά, επιτρέπει πολύ χαλαρότερο συντονισμό μεταξύ των κυψελών. Οι κυψέλες μπορούν να ανήκουν σε διαφορετικά gNB, και μπορεί ακόμη και να ανήκουν σε διαφορετικές

τεχνολογίες ραδιοπρόσβασης, όπως συμβαίνει με τη διπλή συνδεσιμότητα NR-LTE σε περίπτωση μη αυτόνομης λειτουργίας (Non Stand Alone).[10][11]

Συνάθροιση φερουσών και διπλή συνδεσιμότητα μπορούν επίσης να συνδυαστούν. Αυτός είναι ο λόγος που υφίστανται και οι όροι κύρια ομάδα κυψελλών και δευτερεύουσα ομάδα κυψελλών. Σε καθεμία από τις ομάδες κυψελλών, μπορεί να χρησιμοποιηθεί συνάθροιση φερουσών.[10][11]

### 3.4.2 Κανάλια επιπέδου PHY

Τα μεταδιδόμενα δεδομένα στην κατερχόμενη και ανερχόμενη ζεύξη χρησιμοποιούν τους τύπους DL-SCH (DownLink Schedule) και UL-SCH (UpLink Schedule) του καναλιού μεταφοράς. Υπάρχει το πολύ ένα μπλοκ μεταφοράς σε μία μόνο συσκευή ανά χρονικό διάστημα μετάδοσης (Transmission Time Interval, TTI) σε DL-SCH ή UL-SCH. Στην περίπτωση συνάθροισης φορέα, υπάρχει ένα DL-SCH (ή UL-SCH) ανά φορέα στοιχείου που φαίνεται από τη συσκευή.

Ένα φυσικό κανάλι αντιστοιχεί στο σύνολο των πόρων χρόνου / συχνότητας που χρησιμοποιούνται για τη μετάδοση ενός συγκεκριμένου καναλιού μεταφοράς και κάθε κανάλι μεταφοράς αντιστοιχίζεται σε ένα φυσικό κανάλι, όπως φαίνεται στο σχήμα 3.8.

Ο διαχωρισμός ελέγχου και δεδομένων υποστηρίζεται και στα φυσικά κανάλια. Στη συνέχεια περιγράφεται αυτός ο διαχωρισμός καθώς γίνεται και μια αναφορά στα σήματα και τις πληροφορίες που εφαρμόζονται.

#### ► Φυσικά κανάλια δεδομένων

Οι ακόλουθοι τύποι καναλιού φυσικού επιπέδου που ορίζονται για το NR, και αφορούν τη διακίνηση δεδομένων είναι οι εξής:

- ▷ Το **φυσικό κοινόχρηστο κανάλι κατερχόμενης ζεύξης (Physical Downlink Shared Channel, PDSCH)** είναι το κύριο φυσικό κανάλι που χρησιμοποιείται για τη μετάδοση δεδομένων unicast, αλλά και για τη μετάδοση, για παράδειγμα, πληροφοριών σελιδοποίησης, μηνυμάτων απόκρισης τυχαίας πρόσβασης και παράδοσης τμημάτων των πληροφοριών του συστήματος.[10][16]
- ▷ Το **φυσικό κανάλι μετάδοσης (Physical Broadcast Channel, PBCH)** μεταφέρει μέρος των πληροφοριών συστήματος, που απαιτούνται από τη συσκευή για πρόσβαση στο δίκτυο.[10]
- ▷ Το **φυσικό κοινόχρηστο κανάλι ανερχόμενης ζεύξης (Physical Uplink Shared Channel, PUSCH)** είναι ο αντίστοιχος ανερχόμενος σύνδεσμος του PDSCH. Υπάρχει το πολύ ένα PUSCH ανά στοιχείο ανερχόμενου φορέα ανά συσκευή.[10]
- ▷ Το **φυσικό κανάλι τυχαίας πρόσβασης (Physical Random-Access Channel, PRACH)** χρησιμοποιείται για την τυχαία πρόσβαση.[16]

Σημειώνεται ότι ορισμένα από τα φυσικά κανάλια, και πιο συγκεκριμένα τα κανάλια που χρησιμοποιούνται για πληροφορίες ελέγχου κατερχόμενης ζεύξης και ανερχόμενης ζεύξης (PDCCH και PUCCH) δεν ανταποκρίνονται σε αντίστοιχα κανάλια μεταφοράς.[16]

### ► Φυσικά κανάλια ελέγχου

Τα σήματα ελέγχου σε φυσικό επίπεδο τα διαχειρίζονται κυρίως τα εξής κανάλια:

- ▷ Το **φυσικό κανάλι ελέγχου κατερχόμενης ζεύξης (Physical Downlink Control Channel, PDCCH)** χρησιμοποιείται για πληροφορίες ελέγχου κατερχόμενης ζεύξης, κυρίως αποφάσεις προγραμματισμού, που απαιτούνται για λήψη PDSCH, και για προγραμματισμό παραχωρήσεων που επιτρέπουν τη μετάδοση στο PUSCH. Οι πληροφορίες που μεταφέρει το PDCCH προορίζονται αποκλειστικά για το UE.[12]
- ▷ Το **φυσικό ανερχόμενο κανάλι ελέγχου (Physical Uplink Control Channel, PUCCH)** χρησιμοποιείται από τη συσκευή για την αποστολή υβριδικών-ARQ επιβεβαιώσεων, υποδεικνύοντας στο gNB εάν το μπλοκ μεταφοράς κατερχόμενης ζεύξης λήφθηκε επιτυχώς ή όχι, για να στείλει αναφορές κατάστασης καναλιού που βοηθούν τον προγραμματισμό που εξαρτάται από το κανάλι ζεύξης, αλλά και για αιτήματα πόρων για τη μετάδοση δεδομένων uplink. Στην ανερχόμενη ζεύξη, αν το UE εκπέμπει μόνο πληροφορίες ελέγχου, τότε αυτές μεταφέρονται από το PUCCH. Εάν όμως ταυτόχρονα εκπέμπει και δεδομένα, τότε τόσο τα δεδομένα όσο και οι πληροφορίες ελέγχου μεταφέρονται από το μεριζόμενο φυσικό κανάλι δεδομένων άνω ζεύξης(PUSCH), το οποίο χρησιμοποιεί διαφορετική ομάδα υπο-διαύλων από το PUCCH.[16]

Ενώ στο LTE το πλήθος των OFDM συμβόλων που χρησιμοποιούνται για τη μετάδοση του PDCCH καθορίζεται από το κανάλι Physical Control Format Indicator Channel(PCFICH) στο NR καθώς το μέγεθος των συνόλων πόρων ελέγχου δεν ποικίλει δυναμικά και η επαναχρησιμοποίηση πόρων ελέγχου για δεδομένα αντιμετωπίζεται με διαφορετικό τρόπο από ό, τι στο LTE. Επίσης, το Physical Hybrid ARQ Indicator Channel (PHICH) χρησιμοποιείται στο LTE για τον χειρισμό των αναμεταδόσεων ανερχόμενης ζεύξης και συνδέεται στενά με τη χρήση ενός συγχρονισμένου πρωτοκόλλου υβριδικού-ARQ, αλλά δεδομένου ότι το πρωτόκολλο NR υβριδικού-ARQ είναι ασύγχρονο τόσο στην ανερχόμενη ζεύξη όσο και στην κατερχόμενη ζεύξη, το PHICH δεν απαιτείται στο NR.[12][16]

Συνεπώς, το PDCCH είναι ο μόνος τύπος για τα επίπεδα L1/L2 καναλιού ελέγχου στο 5G NR.

### ◆ Πληροφορίες ελέγχου

Εκτός από τα φυσικά κανάλια με ένα αντίστοιχο κανάλι μεταφοράς, υπάρχουν επίσης φυσικά κανάλια χωρίς αντίστοιχο κανάλι μεταφοράς. Αυτά τα κανάλια, γνωστά ως κανάλια ελέγχου L1 / L2, χρησιμοποιούνται για πληροφορίες ελέγχου κατερχόμενης ζεύξης (Downlink Control Information, DCI), παρέχοντας στη συσκευή τις απαραίτητες πληροφορίες για σωστή λήψη και αποκωδικοποίηση της μετάδοσης δεδομένων κατερχόμενης ζεύξης και πληροφορίες ελέγχου ανερχόμενης ζεύξης (Uplink Control Information, UCI) που χρησιμοποιούνται για την παροχή του προγραμματισμού και

του πρωτοκόλλου HARQ με πληροφορίες σχετικά με την κατάσταση στη συσκευή.[16]

Οι πληροφορίες ελέγχου είναι ουσιαστικά μηνύματα που χρησιμοποιούνται για να υποστηριχθούν βασικές διαδικασίες του φυσικού στρώματος. Οι πληροφορίες ελέγχου άνω ζεύξης (UCI) μπορεί να περιλαμβάνουν διάφορα μηνύματα, όπως:

- μηνύματα με τα οποία το UE επιβεβαιώνει τη λήψη των δεδομένων του κόμβου(eNB/gNB), μέσω του καναλιού DL- SCH(HARQ Acknowledgements)
- πληροφορίες για την ποιότητα του διαύλου (CQI) που είναι ουσιαστικά η μεταβολή του λόγου σήματος προς θόρυβο παρεμβολών (Signal Interference Noise Ratio, SINR) συναρτήσεως της συχνότητας
- δείκτες που αξιοποιούνται κατά την εφαρμογή τεχνικών χωρικής πολυπλεξίας(PMI και RI και γενικότερα του δείκτη κατάστασης του διαύλου(Channel State Information, CSI)
- αίτημα του UE να του εκχωρηθούν ραδιο- πόροι προκειμένου να μεταφέρει δεδομένα μέσω του PUSCH, στην άνω ζεύξη(SR)[16]

#### ◆ Φυσικά σήματα

Τα φυσικά σήματα χρησιμοποιούνται για την υποστήριξη των βασικών λειτουργιών του φυσικού στρώματος. Στην ανερχόμενη ζεύξη(UL) υπάρχουν δύο σήματα αναφοράς, το Demodulation Reference Signal(DRS) και το Sounding Reference Signal(SRS). Τα σήματα αναφοράς DRS εκπέμπονται ταυτόχρονα με τα PUSCH και PUCCH και χρησιμοποιούνται ως αναφορά φάσης για την εκτίμηση του διαύλου. Τα σήματα αναφοράς DRS και SRS πολυπλέκονται χρονικά με τα δεδομένα στο UL. Με τη γνώση του DRS το eNB γνωρίζει το δίαυλο στα υποκανάλια που χρησιμοποιεί το UE. Δε γνωρίζει όμως τι συμβαίνει σε άλλες συχνότητες. Αυτό επιλύεται με το SRS. Οι εκπομπές των SRS γίνονται σε χρονικές στιγμές που καθορίζει το eNB/gNB και χρησιμοποιούνται για εκτίμηση της ποιότητας διαύλου σε εκτεταμένες ζώνες συχνοτήτων που καλύπτουν τουλάχιστον 4 μπλοκ πόρων(Resource Blocks, RBs) ή πολλαπλάσια των 4 RBs.[14]

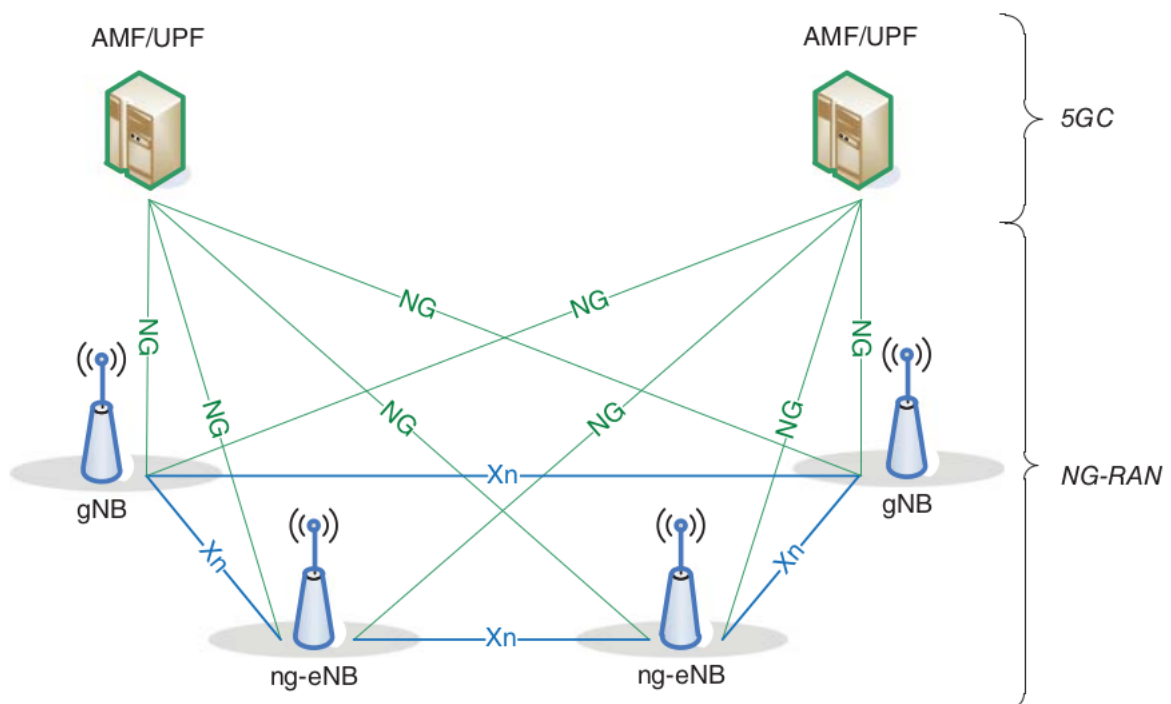
Τα φυσικά σήματα στην κατερχόμενη ζεύξη (DL) περιλαμβάνουν τα σήματα συγχρονισμού και τα σήματα αναφοράς. Τα πρωτεύοντα και δευτερεύοντα σήματα συγχρονισμού (Primary Synchronization Signal,PSS και Secondary Synchronization Signal, SSS) αξιοποιούνται απο το UE κατά τη φάση της αρχικής σύνδεσης του UE στο δίκτυο, προκειμένου να αναγνωρίσει τον κόμβο(eNB/gNB) της κυψέλης και να συνδεθεί σε αυτό. Τα σήματα αναφοράς της κατερχόμενης ζεύξης χρησιμοποιούνται για την εκτίμηση του διαύλου και την αποδιαμόρφωση απο τα τερματικά και τοποθετούνται σε συγκεκριμένες θέσεις στο χρόνο και στη συχνότητα. Εκπέμπεται δηλαδή ένα σήμα αναφοράς απο κάθε θύρα κεραίας ώστε να είναι εφικτή η εκτίμηση σε διαφορετικές θέσεις. Τα σήματα που είναι αποκλειστικά για την κυψέλη (Cell-specific Reference Signal) εκπέμπονται σε κάθε υπο-πλαίσιο(subframe) της κατερχόμενης ζεύξης και σε κάθε RB στη συχνότητα, ώστε να καλύπτεται όλο το εύρος ζώνης κυψέλης. Τα σήματα αυτά χρησιμοποιούνται για απο τα τερματικά για την επιλογή της κυψέλης στην οποία θα συνδεθούν καθώς και για τη διαδικασία της μεταπομπής. Τα σήματα αναφοράς ποτ απευθύνονται αποκλειστικά σε ένα



UE, εκπέμπονται μόνο στα RBs που προορίζονται για το συγκεκριμένο UE και χρησιμοποιούνται για την εκτίμηση διαύλου και προκειμένου να υποστηριχθεί η λειτουργία της αποκλειστικής διαμόρφωσης δέσμης (beamforming). [16]

### 3.5 Διεπαφές δικτύου πρόσβασης

Στα τηλεπικοινωνιακά συστήματα, κυρίως τα κυψελωτά, επιβάλλεται σε ορισμένες περιπτώσεις να υπάρχει επικοινωνία μεταξύ των κόμβων ώστε να εξυπηρετεί τεχνικές όπως η διπλή συνδεσιμότητα, η συνάθροιση φερουσών, η κατασκευή μη αυτόνομου 5G συστήματος (non-stand alone) καθώς και οποιαδήποτε εφαρμογή απαιτεί τη μεταξύ τους συνδεσιμότητα. Διακρίνουμε δύο κύριες κατηγορίες διεπαφών την Xn που είναι η συνδεσιμότητα μεταξύ των διαφορετικών κόμβων eNB και gNB αλλά και η διεπαφή NG που διασυνδέει το δίκτυο πρόσβασης με το δίκτυο κορμού. Επιπρόσθετα έχουν προταθεί και οι διεπαφές F1 και E1 στις οποίες θα γίνει μία μικρή αναφορά. Οι Xn διεπαφές αφορούν τόσο το επίπεδο χρήστη όσο και το επίπεδο ελέγχου όπως αναλύεται παρακάτω.[17]



Εικόνα 3.9: Διεπαφές για τη διασύνδεση 5G-Core και 5G-RAN [17]

#### 3.5.1 Η διεπαφή Xn

##### ► Διεπαφή Xn επιπέδου χρήστη (Xn-U)

Η διεπαφή Xn επιπέδου χρήστη (Xn-U) ορίζεται μεταξύ δύο NG-RAN κόμβων. Η στοίβα πρωτοκόλλου του επιπέδου χρήστη στη Xn διεπαφή αναπαρίσταται στην διπλανή εικόνα. Το επίπεδο δικτύου μεταφοράς βασίζεται στη μεταφορά

IP διευθύνσεων ενώ το GTP-U χρησιμοποιείται πάνω από το UDP / IP για τη μεταφορά PDUs επιπέδου χρήστη.[17]

Η Xn-U διεπαφή παρέχει μη-εγγυημένη παράδοση των PDUs επιπέδου χρήστη και υποστηρίζει προώθηση δεδομένων και έλεγχο ροής. Ακόμη, υποστηρίζει τρεις διαφορετικούς τύπους ωφέλιμου φορτίου(payload), το PDCP Service Data Units (SDUs) (για παράδειγμα στην περίπτωση DRB-level προώθησης δεδομένων για μεταπομπή), το Service Data Adaptation Protocol (SDAP) SDUs (στην περίπτωση του PDU session-level προώθησης δεδομένων για μεταπομπή) ή PDCP PDUs (όπως στην περίπτωση διπλής συνδεσιμότητας). [20]

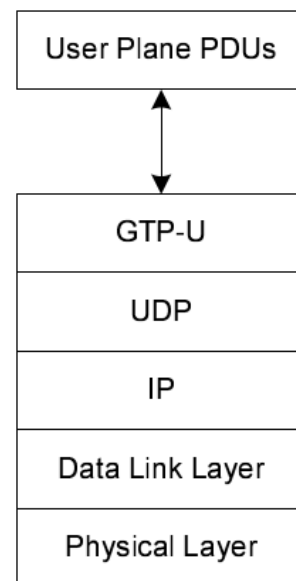
Για τη διπλή συνδεσιμότητα το Xn-U χρησιμοποιεί ένα NR επίπεδο χρήστη (NR-U) πρωτόκολλο. Δηλαδή, το περιεχόμενο του GTP-U container που χρησιμοποιεί και η λειτουργικότητα που υποστηρίζει είναι διαφορετική από εκείνη του NG-U. Όπως αναφέρθηκε παραπάνω, αυτό το πρωτόκολλο επιπέδου χρήστη είναι κοινό για τα Xn και F1.

Σε αντίθεση με το πρωτόκολλο επιπέδου χρήστη συνεδρίας PDU (3GPP TS 38.415) που ορίζεται για τη διεπαφή NG-U, στο πρωτόκολλο NR-U οι σήραγγες GTP-U αντιστοιχίζονται σε φορείς NG-RAN (που αντιστοιχούν στα DRB) και όχι σε συνεδρίες PDU. Αυτό συμβαίνει επειδή παρόλο που το 5GC σταμάτησε να χρησιμοποιεί την έννοια φορέων, αυτά εξακολουθούν να υπάρχουν μεταξύ των UE και NG-RAN.[17][20]

Ένας επιπλέον λόγος για τον ορισμό των βελτιώσεων επιπέδου χρήστη για διασυνδέσεις δικτύου Xn και F1 είναι ότι αυτές οι διεπαφές θεωρούνται κάπως λιγότερο αξιόπιστες, σε σύγκριση με τις διεπαφές πυρήνα δικτύου. Επιπλέον, ορισμένοι κόμβοι δικτύου NG-RAN ενδέχεται να έχουν μικρότερα buffer. Όλα αυτά μπορεί να οδηγήσουν σε συμφόρηση στις διασυνδέσεις δικτύου και απώλεια πακέτων, γι' αυτό πρέπει να καθοριστούν μηχανισμοί ελέγχου ροής και παράδοσης σε σειρά, κάτι που είναι πολύ σημαντικό ειδικότερα όταν υπάρχουν απώλειες πακέτων μέσω της εναέριας διασύνδεσης.[17][20]

Οι βασικές λειτουργίες του NR-U είναι:

- Μεταφορά δεδομένων: μεταφορά δεδομένων μεταξύ NG- RAN κόμβων ώστε να υποστηρίξει διπλή συνδεσιμότητα ή ανάπτυξη διαχωρισμού CU/DU.
- Έλεγχος ροής: ενεργοποιώντας έναν NG- RAN κόμβο για να παρέχει πληροφορίες αντροφοδότησης που συσχετίζονται με τη ροή δεδομένων που λαμβάνονται από έναν δεύτερο NG- RAN κόμβο.
- Αναμεταδόσεις: επιτρέποντας τις αναμεταδόσεις μέσω του ιδίου κόμβου,



Εικόνα 3.10: Xn-U στοίβα πρωτοκόλλων. [17]

για τα δεδομένα που προωθήθηκαν σε αυτόν, ή μέσω διαφορετικού κόμβου.

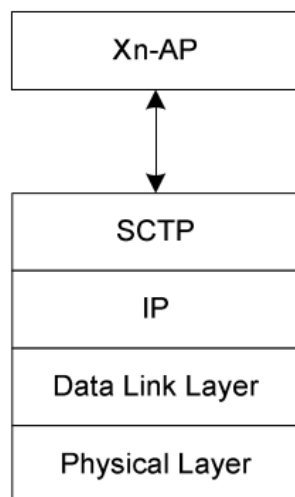
- **Μεταβίβαση πληροφοριών βοήθειας:** μεταφορά πληροφοριών βοήθειας σχετικά με το ραδιοσύστημα όταν το επίπεδο ραδιοεπικοινωνίας δεν επιδέχεται διαχείριση στον ίδιο κόμβο με τον έλεγχο δεδομένων. Η μεταφορά δεδομένων χρησιμοποιείται επίσης κατά τη λειτουργία κινητικότητας, αν και σε αυτήν την περίπτωση τα δεδομένα μεταφέρονται χωρίς την επέκταση NR-U, επομένως δεν είναι διαθέσιμες όλες οι λειτουργίες NR-U. Η μεταφορά δεδομένων χρησιμοποιείται επίσης κατά τη λειτουργία κινητικότητας, αν και σε αυτήν την περίπτωση τα δεδομένα μεταφέρονται χωρίς την επέκταση NR-U, επομένως όλες οι συναρτήσεις NR-U δεν είναι διαθέσιμες.[20]

Οι λειτουργίες NR-U υλοποιούνται ως ένα σύνολο πρόσθετων μηνυμάτων που μεταφέρονται μέσα στο NR container σε μια κεφαλίδα επέκτασης GTP-U ενός GTP-U PDU. Τα μηνύματα περιλαμβάνουν:

- Δεδομένα χρήστη κατερχόμενης ζεύξης
- Κατάσταση παράδοσης δεδομένων κατερχόμενης ζεύξης (*Downlink Data Delivery Status, DDDS*)
- Δεδομένα βοηθητικών λειτουργιών [20]

#### ►Διεπαφή Xn επιπέδου ελέγχου (Xn-C)

Η διεπαφή Xn επιπέδου ελέγχου(Xn- C) ορίζεται επίσης μεταξύ δύο NG- RAN κόμβων.



Εικόνα 3.11: Xn-C στοίβα πρωτοκόλλων. [17]

Η στοίβα πρωτοκόλλων επιπέδου ελέγχου για τη Xn διεπαφή φαίνεται στην διπλανή εικόνα. Το επίπεδο δικτύου μεταφοράς είναι ενσωματωμένο σε ένα πρωτόκολλο Stream Control Transmission Protocol (SCTP) πάνω από το IP επίπεδο. Το πρωτόκολλο σηματοδότησης επιπέδου εφαρμογής αναφέρεται ως XnAP (Xn Application Protocol). Το επίπεδο SCTP παρέχει την εγγυημένη παράδοση των μηνυμάτων επιπέδου εφαρμογής. Στο επίπεδο μεταφοράς IP, η μετάδοση από σημείο σε σημείο χρησιμοποιείται για την παράδοση της PDU σηματοδότησης.[17]

Η διεπαφή Xn-C υποστηρίζει λειτουργίες όπως η διαχείριση Xn διεπαφής, η διαχείριση κινητικότητας UE, συμπεριλαμβανομένης της μεταφοράς του περιβάλλοντος και της τηλεειδοποίησης του RAN και διπλή συνδεσιμότητα. [20]

Η στοίβα πρωτοκόλλων Xn- C (3GPP TS 38.423) είναι παρόμοια με αυτή για τη διεπαφή NG- C (3GPP TS 38.413) και υποστηρίζει επίσης πολλαπλή

SCTP λειτουργικότητα σύνδεσης διευκολύνοντας τις εικονικοποιημένες αναπτύξεις.

Ο σκοπός και η γενική δομή των διαδικασιών διαχείρισης διασύνδεσης Xn είναι οι ίδιες με αυτές του NG. Οι διαδικασίες είναι [20]:

- Xn Αίτημα εγκατάστασης / Απόκριση / Αποτυχίας
- NG-RAN Κόμβος Ενημέρωση διαμόρφωσης / Ενημέρωση Αναγνώρισης / Αποτυχία ενημέρωσης
- Αίτημα ενεργοποίησης κυψέλης / Απόκριση / Αποτυχία
- Επαναφορά αιτήματος / απόκριση και ένδειξη σφάλματος
- Xn Αίτημα κατάργησης / Απόκριση / Αποτυχίας.

### 3.5.2 Η διεπαφή NG

Το NG-RAN τοποθετείται στο επίπεδο ραδιο-δικτύου (Radio Network Layer, RNL) και επιπέδου δικτύου μεταφοράς (Transport Network Layer, TNL). Η αρχιτεκτονική NG-RAN, δηλαδή οι λογικοί κόμβοι NG-RAN και οι διεπαφές μεταξύ τους, ορίζονται ως μέρος του RNL.

Η αρχιτεκτονική NG-RAN αποτελείται από ένα σύνολο gNB και ng-eNB που συνδέονται με το 5GC μέσω της διασύνδεσης NG, η οποία είναι μία λογική επαφή και καθορίζεται στην έκδοση του ETSI, TS 38.300. [21]

Το NG-RAN μπορεί να έχει πολλά σημεία πρόσβασης NG προς το 5GC και κάθε σημείο πρόσβασης NG (σε NG-RAN ή 5GC) πληροί ανεξάρτητα τις απαιτήσεις των σχετικών προδιαγραφών NG (σειρά 3GPP 38.41x).[21]

Μπορεί ακόμη να υπάρχουν πολλές λογικές διεπαφές NG-C προς το 5GC από οποιονδήποτε κόμβο NG-RAN. Η επιλογή της διασύνδεσης NG-C καθορίζεται στη συνέχεια από τη λειτουργία NAS Node Selection. Επίσης, μπορεί να υπάρχουν και πολλές λογικές διεπαφές NG-U προς το 5GC από οποιονδήποτε κόμβο NG-RAN. Η επιλογή της διεπαφής NG-U γίνεται εντός του 5GC και σηματοδοτείται στον κόμβο NG-RAN από το AMF.[21]

Οι γενικές αρχές για τον προσδιορισμό της διασύνδεσης NG είναι ότι η διεπαφή NG είναι ανοιχτή και υποστηρίζει την ανταλλαγή πληροφοριών σηματοδότησης μεταξύ του NG-RAN και του 5GC.

Από λογική άποψη, το NG είναι διασύνδεση σημείων μεταξύ κόμβου NG-RAN και κόμβου 5GC και η λογική διασύνδεση από σημείο σε σημείο είναι εφικτή ακόμη και αν δεν υπάρχει φυσική άμεση σύνδεση μεταξύ του NG-RAN και 5GC. Επιπρόσθετα, η διασύνδεση NG υποστηρίζει διαχωρισμό επιπέδου ελέγχου και επιπέδου χρήστη και διαχωρίζει το επίπεδο ραδιοδικτύου και το επίπεδο δικτύου μεταφοράς καθώς επίσης αποτελεί και μια μελλοντική απόδειξη για την εκπλήρωση διαφορετικών νέων απαιτήσεων και υποστήριξης νέων υπηρεσιών και νέων λειτουργιών επιτρέποντας παράλληλα βελτιστοποίηση και αποδοτικότητα κωδικοποίησης / αποκωδικοποίησης.[21]

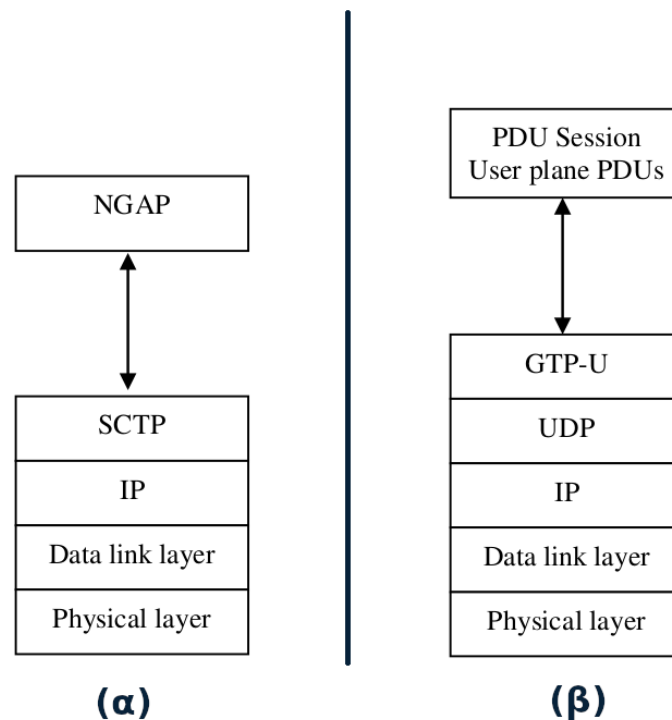
Ως προς τις δυνατότητες της, η διεπαφή NG υποστηρίζει διεργασίες για τον καθορισμό, τη συντήρηση και την απελευθέρωση μέρος των συνεδριών PDU του NG-RAN αλλά και για διεργασίες για την εκτέλεση μεταπομπής εντός του RAT και της μεταπομπής μεταξύ RAT. Τέλος, υπο την ευθύνη του είναι και ο ο διαχωρισμός κάθε UE σε επίπεδο πρωτοκόλλου για διαχείριση σηματοδότησης συγκεκριμένου χρήστη.[21]

► **NG επιπέδου ελέγχου(NG-C)**

Η στοίβα πρωτοκόλλου επιπέδου ελέγχου της διασύνδεσης NG φαίνεται στο διπλανό σχήμα. Το επίπεδο δικτύου μεταφοράς βασίζεται σε IP μεταφορά. Για την αξιόπιστη μεταφορά μηνυμάτων σηματοδότησης, προστίθεται SCTP πάνω από το IP. Το πρωτόκολλο σηματοδότησης επιπέδου εφαρμογής αναφέρεται ως NGAP (NG Application Protocol).[21]

► **NG επιπέδου χρήστη(NG-U)**

Η διεπαφή επιπέδου χρήστη NG (NG-U) ορίζεται μεταξύ ενός κόμβου NG-RAN και ενός UPF. Η διασύνδεση NG-U παρέχει μη εγγυημένη παράδοση για τη συνεδρία PDU των PDU επιπέδου χρήστη μεταξύ του NG-RAN. Η στοίβα πρωτοκόλλων για τη διεπαφή NG-U φαίνεται στην αντίστοιχη εικόνα.[21]



Εικόνα 3.12: Στοίβα πρωτοκόλλων διεπαφής NG (α) Επιπέδου ελέγχου και (β) Επιπέδου χρήστη [17]

### 3.5.3 Η διεπαφή F1

Οι γενικές αρχές που διέπουν τη διεπαφή F1, ορίζουν τη διεπαφή F1 ως ανοιχτή και προϋποθέτει αυτή να υποστηρίζει την ανταλλαγή πληροφοριών σηματοδότησης μεταξύ των τελικών σημείων και επιπλέον, η διεπαφή να υποστηρίζει τη μετάδοση δεδομένων στα αντίστοιχα τελικά σημεία. Από λογική άποψη, η F1 είναι η απο σημείο-σε-σημείο διασύνδεση μεταξύ δύο τελικών σημείων.

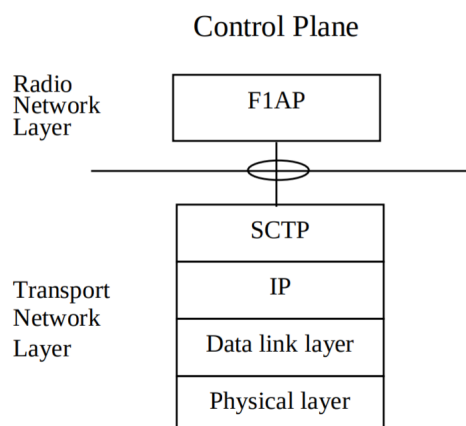
**ΣΗΜΕΙΩΣΗ:** Μια λογική διασύνδεση από σημείο σε σημείο πρέπει να είναι

εφικτή ακόμη και αν δεν υπάρχει φυσική άμεση σύνδεση μεταξύ των τελικών σημείων.

Επίσης, η διεπαφή F1 υποστηρίζει διαχωρισμό επιπέδου ελέγχου και επιπέδου χρήστη και διαχωρίζει το επίπεδο ραδιοδικτύου και του επιπέδου δικτύου μεταφοράς. Ακόμη, επιτρέπει την ανταλλαγή πληροφοριών που σχετίζονται με UE αλλά και πληροφορίες που δεν σχετίζονται με UE και έχει σχεδιαστεί με προοπτική ώστε να υποστηρίζει νέες υπηρεσίες και νέες λειτουργίες. Αξίζει να σημειωθεί ότι ένα gNB-CU και ένα σύνολο gNB-DUs είναι ορατά σε άλλους λογικούς κόμβους ως gNB ή en-gNB όπου το gNB τερματίζει τις διεπαφές Xn και NG και το en-gNB τερματίζει τη X2 και τη S1-U διεπαφές. (Το gNB-CU μπορεί να διαχωριστεί στο επίπεδο ελέγχου (CP) και στο επίπεδο χρήστη (UP) και επιπλέον, οι προδιαγραφές διασύνδεσης F1 διευκολύνουν τη διασύνδεση ενός gNB-CU και ενός gNB-DU που παρέχονται από διαφορετικούς κατασκευαστές.[21]

Η διεπαφή F1 υποστηρίζει διεργασίες για τη δημιουργία, τη συντήρηση και την απελευθέρωση ραδιο-φορέων για το τμήμα NG-RAN των συνεδριών PDU και για τους φορείς πρόσβασης ραδιοεπικοινωνίας EUTRAN καθώς και διεργασίες για τη δημιουργία, συντήρηση και απελευθέρωση καναλιών BH RLC. Ο διαχωρισμός κάθε UE σε επίπεδο πρωτοκόλλου για συγκεκριμένη διαχείριση σηματοδότησης χρήστη και ο διαχωρισμός κάθε IAB-MT σε επίπεδο πρωτοκόλλου για διαχείριση σηματοδότησης ειδικά για IAB-MT είναι λειτουργίες που εξυπηρετεί η διεπαφή F1, όπως επίσης εξυπηρετεί τη μεταφορά μηνυμάτων σηματοδότησης RRC μεταξύ του UE και του gNB-CU.[22]

### ► F1 πρωτόκολλο επιπέδου Ελέγχου (F1-C)



Εικόνα 3.13: Στοίβα πρωτοκόλλων διεπαφής F1 επιπέδου ελέγχου [22]

Το σχήμα 3.13 δείχνει τη δομή πρωτοκόλλου για F1-C. Το TNL βασίζεται σε μεταφορά IP, που περιλαμβάνει το SCTP πάνω από IP. Το πρωτόκολλο σηματοδότησης επιπέδου εφαρμογής αναφέρεται ως F1AP (F1 Application Protocol).[22]

Παρακάτω παρουσιάζουμε συνοπικά τις λειτουργίες της διεπαφής F1 για το σήματα του επιπέδου ελέγχου.

- **Λειτουργία διαχείρισης διασύνδεσης F1**

Μία βασική λειτουργία της διεπαφής F1- C είναι η λειτουργία διαχείρισης διασύνδεσης F1. Αυτή περιλαμβάνει τη λειτουργία ένδειξης σφάλματος που χρησιμοποιείται από το gNB-DU ή gNB-CU για να υποδείξει στο gNB-CU ή gNB-DU ότι έχει προκύψει σφάλμα, η λειτουργία επαναφοράς που χρησιμοποιείται για την αρχικοποίηση της ομότιμης οντότητας μετά τη ρύθμιση του κόμβου και μετά από ένα συμβάν αποτυχίας (αυτή η διαδικασία μπορεί να χρησιμοποιηθεί τόσο από το gNB-DU όσο και από το gNB-CU), η λειτουργία ρύθμισης F1 που επιτρέπει την ανταλλαγή δεδομένων επιπέδου εφαρμογής που απαιτούνται για να λειτουργούν σωστά τα gNB-DU και gNB-CU στη διεπαφή F1 και να ανταλλάσσεται η προβλεπόμενη διαμόρφωση TDD DL-UL που προέρχεται από το gNB-DU ή προορίζεται για το gNB-DU και η λειτουργία εγκατάστασης του F1 που ξεκινά από το gNB-DU.[22]

- **Λειτουργία διαχείρισης πληροφοριών συστήματος**

Ο προγραμματισμός των πληροφοριών εκπομπής συστήματος πραγματοποιείται στο gNB-DU. Το gNB-DU είναι υπεύθυνο για τη μετάδοση των πληροφοριών συστήματος σύμφωνα με τις διαθέσιμες παραμέτρους προγραμματισμού.[22]

- **Λειτουργία διαχείρισης πληροφοριών συστήματος**

Ο προγραμματισμός εκπομπής των πληροφοριών συστήματος πραγματοποιείται στο gNB-DU. Το gNB-DU είναι υπεύθυνο για τη μετάδοση των πληροφοριών συστήματος σύμφωνα με τις διαθέσιμες παραμέτρους προγραμματισμού.[22]

- **Λειτουργία διαχείρισης περιβάλλοντος F1 UE**

Η λειτουργία διαχείρισης περιβάλλοντος F1 UE υποστηρίζει τη δημιουργία και τροποποίηση του απαραίτητου συνολικού περιβάλλοντος UE.[22]

- **Λειτουργία μεταφοράς μηνυμάτων RRC**

Αυτή η λειτουργία επιτρέπει τη μεταφορά μηνυμάτων RRC μεταξύ gNB-CU και gNB-DU. Τα μηνύματα RRC μεταφέρονται πάνω από τη διεπαφή F1- C.[22]

- **Λειτουργία τηλεειδοποίησης**

Το gNB-DU είναι υπεύθυνο για τη μετάδοση πληροφοριών τηλεειδοποιήσεων σύμφωνα με τις παρεχόμενες παραμέτρους προγραμματισμού.[22]

- **Λειτουργία μετάδοσης πληροφοριών μηνυμάτων προειδοποίησης**

Αυτή η λειτουργία επιτρέπει τη συνεργασία με τις διαδικασίες μετάδοσης προειδοποιητικών μηνυμάτων μέσω της διεπαφής NG.[22]

- **Λειτουργία μηνυμάτων Απομακρυσμένης Διαχείρισης Παρεμβολών (Remote Interference Management, RIM)**

Αυτή η λειτουργία επιτρέπει τη μεταφορά μηνυμάτων απομακρυσμένης διαχείρισης παρεμβολών (RIM) μεταξύ του gNB-CU και του gNB-DU. Τα μηνύματα RIM μεταφέρονται μέσω F1-C.[22]

- **Λειτουργία ιχνηλάτησης(Trace)**

Η λειτουργία ιχνηλάτησης παρέχει μέσα για τον έλεγχο περιόδων παρακολούθησης για μια διεπαφή UE μέσω F1.[22]

- **Λειτουργία διαχείρισης φορτίου**

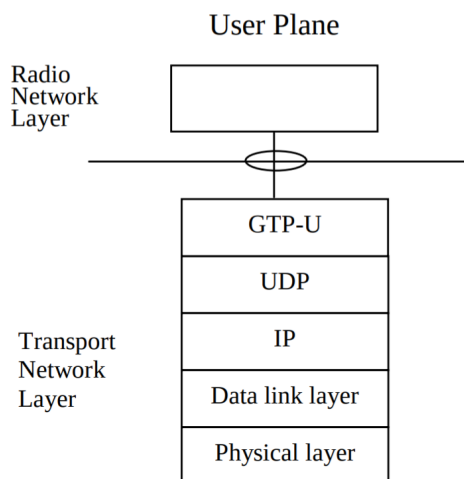
Η λειτουργία διαχείρισης φορτίου επιτρέπει σε ένα gNB-CU να ζητά την αναφορά των μετρήσεων φορτίου στο gNB-DU και χρησιμοποιείται από το gNB-DU για την αναφορά του αποτελέσματος των μετρήσεων που επιδέχεται το gNB-DU.[22]

- **Λειτουργία υποστήριξης αυτο-βελτιστοποίησης**

Αυτή η λειτουργία επιτρέπει στο gNB-CU να παρέχει πληροφορίες στο gNB-DU προκειμένου να υποστηρίξει τη λειτουργία αυτο-βελτιστοποίησης.[22]

► **F1 Επίπεδο χρήστη Πρωτόκολλο (F1 User Plane Protocol, F1-U)**

Η εικόνα παρακάτω δείχνει τη δομή πρωτοκόλλων για το F1-U. Το TNL βασίζεται σε μεταφορά IP, που περιλαμβάνει το UDP και το GTP-U πάνω από το IP.



Εικόνα 3.14: Στοιβά πρωτοκόλλων διεπαφής F1 επιπέδου χρήστη [22]

Οι λειτουργίες του F1-U είναι κυρίως δύο. Η πρώτη αφορά τη μετάδοση των δεδομένων χρήστη μεταξύ των gNB-CU και gNB-DU, και η δεύτερη λειτουργία αφορά τον έλεγχο ροής, επιτρέποντας τον έλεγχο της ροής δεδομένων χρήστη κατερχόμενης ζεύξης προς το gNB-DU.[22]



### 3.5.4 Η διεπαφή E1

Οι γενικές αρχές για τον προσδιορισμό της διεπαφής E1 είναι ότι η διεπαφή E1 είναι ανοιχτή και υποστηρίζει την ανταλλαγή πληροφοριών σηματοδότησης μεταξύ των τελικών σημείων ενώ από λογική άποψη, το E1 είναι διεπαφή μεταξύ σημείων μεταξύ gNB-CU-CP και gNB-CU-UP. Σημειώνουμε και εδώ ότι μια λογική διασύνδεση από σημείο σε σημείο πρέπει να είναι εφικτή ακόμη και αν δεν υπάρχει φυσική άμεση σύνδεση μεταξύ των τελικών σημείων. Η διεπαφή E1 διαχωρίζει το επίπεδο ραδιοδικτύου και το επίπεδο δικτύου μεταφορών και επιτρέπει την ανταλλαγή πληροφοριών σχετικών με UE αλλά και πληροφοριών που δεν σχετίζονται με UE. Αξίζει επίσης να τονίσουμε ότι η διεπαφή E1 είναι μια διεπαφή ελέγχου και δεν χρησιμοποιείται για την προώθηση δεδομένων χρήστη. Οι προδιαγραφές της διεπαφής E1 διευκολύνουν τη διασύνδεση ενός gNB-CU-CP και ενός gNB-CU-UP που παρέχονται από διαφορετικούς κατασκευαστές.[23]

Η διεπαφή E1 υποστηρίζει τις παρακάτω λειτουργίες όπως:

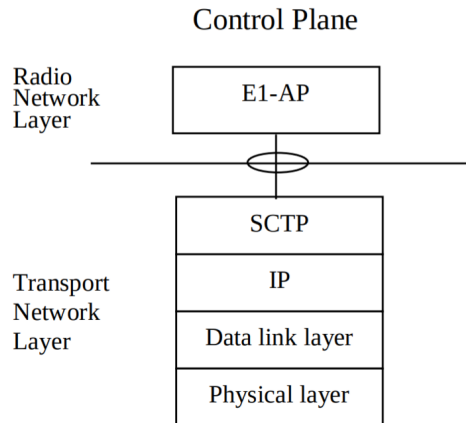
- **Λειτουργία διαχείρισης E1 διεπαφής**

Η λειτουργία διαχείρισης της E1 διεπαφής περιλαμβάνει ένα πλήθος συναρησεων που εξυπηρετούν διαφορετικό σκοπό. Η συνάρτηση ένδειξης σφάλματος χρησιμοποιείται από το gNB-CU-UP ή gNB-CU-CP για να υποδείξει στο gNB-CU-CP ή gNB-CU-UP ότι έχει προκύψει σφάλμα. Η συνάρτηση επαναφοράς χρησιμοποιείται για την αρχικοποίηση της ομότιμης οντότητας μετά τη ρύθμιση κόμβου και μετά από ένα συμβάν αποτυχίας. Αυτή η διαδικασία μπορεί να χρησιμοποιηθεί τόσο από το gNB-CU-UP όσο και από το gNB-CU-CP. Η λειτουργία ρύθμισης E1 επιτρέπει την ανταλλαγή δεδομένων επιπέδου εφαρμογής που απαιτούνται για τα gNB-CU-UP και gNB-CU-CP για σωστή λειτουργία στη διεπαφή E1. Η ρύθμιση E1 ξεκινά τόσο από το gNB-CU-UP όσο και από το gNB-CU-CP. Οι συναρτήσεις gNB-CU-UP Update και gNB-CU-CP Configuration Update επιτρέπουν την ενημέρωση των δεδομένων διαμόρφωσης επιπέδου εφαρμογής που απαιτούνται μεταξύ του gNB-CU-CP και του gNB-CU-UP για σωστή λειτουργία μέσω της διεπαφής E1. Οι λειτουργίες E1 setup και gNB-CU-UP Update Configuration Update επιτρέπουν την ενημέρωση NR CGI (s), S-NSSAI (s), PLMN-ID (s) και QoS πληροφοριών που υποστηρίζονται από το gNB-CU-UP.[23]

- **Λειτουργία διαχείρισης περιβάλλοντος κομιστή-φορέα(bearer) E1**

Η εγκαθίδρυση του περιβάλλοντος του E1 φορέα ξεκινά από το gNB-CU-CP και γίνεται αποδεκτό ή απορρίπτεται από το gNB-CU-UP βάσει κριτηρίων ελέγχου εισόδου (π.χ. αν ο πόρος δεν είναι διαθέσιμος). Η τροποποίηση του περιβάλλοντος φορέα του E1 μπορεί να ξεκινήσει είτε από gNB-CU-CP είτε από gNB-CU-UP. Ο κόμβος λήψης μπορεί να αποδεχτεί ή να απορρίψει την τροποποίηση. Η συνάρτηση διαχείρισης περιβάλλοντος φορέων E1 υποστηρίζει επίσης την απελευθέρωση του περιβάλλοντος κομιστή που είχε προηγουμένως καθοριστεί στο gNB-CU-UP. Η απελευθέρωση του πλαισίου κομιστή ενεργοποιείται από το gNB-CU-CP είτε άμεσα είτε μετά από αίτημα που ελήφθη από το gNB-CU-UP.

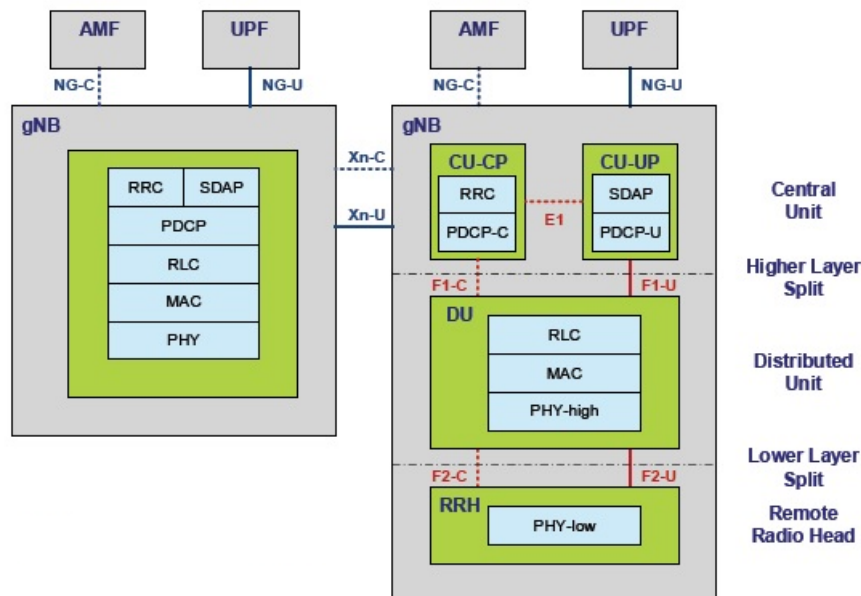
Αυτή η λειτουργία χρησιμοποιείται για τη ρύθμιση και την τροποποίηση της διαμόρφωσης αντιστοίχισης ροής QoS σε DRB. [23]



Εικόνα 3.15: Στοιβά πρωτοκόλλων διεπαφής E1 [23]

Η εικόνα δείχνει τη δομή πρωτοκόλλου E1. Το TNL βασίζεται σε μεταφορά IP, που περιλαμβάνει το Sctp πάνω από IP. Το πρωτόκολλο σηματοδότησης επιπέδου εφαρμογής αναφέρεται ως E1AP (E1 Application Protocol).

Εν κατακλείδι, μπορούμε να συνοψίσουμε σε μία εικόνα όλες τις διεπαφές τις οποίες αναφέραμε παραπάνω, εφαρμοζόμενες σε ένα σύστημα 5G που είναι και το αντικείμενο της εργασίας.



Εικόνα 3.16: Συνολική επισκόπηση των διαφόρων τύπων διεπαφών για το gNB του 5G NR [24]

## 3.6 Τεχνικές Διαμόρφωσης 5G συστημάτων

### 3.6.1 Orthogonal Frequency-Division Multiplexing(OFDM)

Απο την απαρχή χρήσης του LTE ήδη χρησιμοποιείται η τεχνική πολλαπλής πρόσβασης με Ορθογώνια διαμόρφωση συχνότητας(OFDM) για δεδομένα κατερχόμενης ζεύξης και SC-FDMA για μετάδοση στην ανερχόμενη ζεύξη.

Η μέθοδος Orthogonal Frequency-Division Multiplexing(OFDM) είναι μια μέθοδος μετάδοσης μέσω πολλαπλών καναλιών. Το φάσμα των υποφερουσών αλληλοεπικαλύπτεται προκειμένου να έχουμε ένα αποδοτικό εύρος ζώνης, και επίσης δεν χρησιμοποιούνται ξεχωριστά ζωνοπερατά φίλτρα και ταλαντωτές για κάθε υποκανάλι.

Τα πολλαπλά ορθογώνια σήματα των υποφερουσών, τα οποία αλληλοεπικαλύπτονται στο φάσμα, μπορούν να παραχθούν γενικεύοντας το κριτήριο του Nyquist από μονής φέρουσας σε πολλαπλής.[11]

Για την εφαρμογή της ορθογωνιότητας, χρησιμοποιείται ο διακριτός μετασχηματισμός Fourier (DFT) και ο αντίστροφος (IDFT), και συγκεκριμένα ο γρήγορος μετασχηματισμός Fourier (FFT/IFFT). Προκειμένου να επιτευχθεί η ζητούμενη φασματική απόδοση και να εξασφαλισθεί η απουσία της διακαναλικής παρεμβολής (ICI) θα πρέπει τα σήματα που αποστέλλονται μέσω του κάθε καναλιού να είναι ορθογώνια μεταξύ τους, δηλαδή όταν η στιγμιαία τιμή του σήματος ενός υποκαναλιού βρίσκεται στο μέγιστό της, όλα τα υπόλοιπα θα πρέπει να είναι μηδενικά.[11]

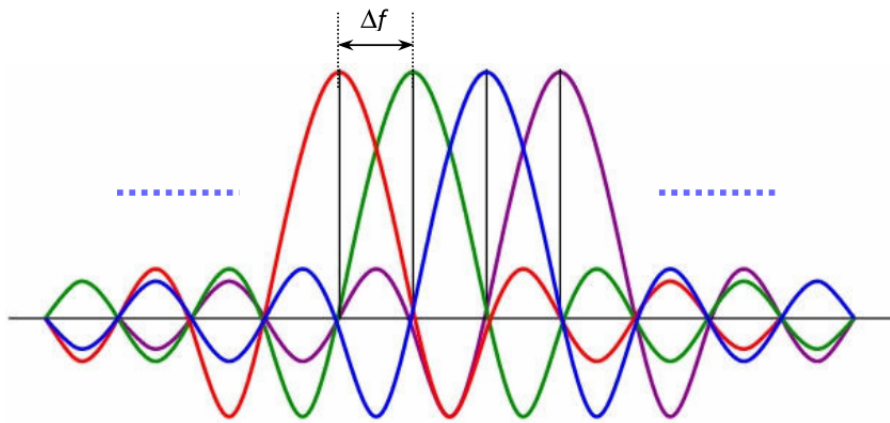
Στην έκδοση LTE-Advanced έγινε χρήση της βελτιωμένης OFDM Access που αποτελεί την πλέον χρήσιμη προσέγγιση για κυψελοειδή συστήματα κινητών επικοινωνιών. Έτσι, αντί να επιλέγεται ένας χρήστης που χρησιμοποιεί όλες τις υποφέρουσες κάποια χρονική στιγμή, είναι πιο αποδοτικό να επιτρέπεται σε πολλαπλούς χρήστες να επιλέγουν το δικό τους υποσύνολο υποφερουσών που φέρουν καλύτερες συνθήκες καναλιού, καθώς ο κάθε χρήστης εντός μιας κυψέλης ενδέχεται να έχει διαφορετικό SNIR (signal-to-noise and interference ratios).[11]

Το ποσό των φυσικών πόρων που ανατίθεται σε κάθε χρήστη εξαρτάται τόσο από το απαιτούμενο data-rate του καθ' ενός, όσο και από την ενίσχυση ποικιλομορφίας πολλαπλών χρηστών.

### 3.6.2 Single Carrier- FDMA(SC-FDMA)

Το SC-FDMA αποτελεί εναλλακτική λύση για το OFDMA, ειδικά στις επικοινωνίες ανερχόμενης ζεύξης όπου ο χαμηλότερος λόγος μέγιστης προς μέση ισχύ (PAPR) ωφελεί σημαντικά το κινητό τερματικό όσον αφορά την απόδοση ισχύος μετάδοσης και το μειωμένο κόστος του ενισχυτή ισχύος. Έχει υιοθετηθεί ήδη ως σχήμα πολλαπλής πρόσβασης uplink στο 3GPP Long Term Evolution (LTE), ή Evolved UTRA (E-UTRA).[14]

Αν και η διαφορά στην απόδοση είναι μικρή, το πλεονέκτημα του SC-FDMA για χαμηλό PAPR το καθιστά επιθυμητό για ασύρματη μετάδοση ζεύξης σε συστήματα κινητής επικοινωνίας, όπου η απόδοση ισχύος του πομπού είναι ύψιστης σημασίας.[11]



Εικόνα 3.17: OFDM υποφέρουσες συχνότητες [12]

Η επεξεργασία μετάδοσης του SC-FDMA είναι παρόμοια με αυτή του OFDMA. Για κάθε χρήστη, η ακολουθία των bit που μεταδίδονται χαρτογραφείται σε έναν σύνθετο αστερισμό συμβόλων (BPSK, QPSK ή διαμόρφωση πλάτους M-Quadrature). Στη συνέχεια, στους διαφορετικούς πομπούς (χρήστες) εκχωρούνται διαφορετικοί συντελεστές Fourier. Αυτή η ανάθεση χρησιμοποιείται για την χαρτογράφηση και αποχαρτογράφηση. Η πλευρά του δέκτη περιλαμβάνει ένα μπλοκ αποχαρτογράφησης, ένα μπλοκ IDFT και ένα μπλοκ ανίχνευσης για κάθε σήμα χρήστη που θα ληφθεί. Ακριβώς όπως στο OFDM, εισάγονται διαστήματα φύλαξης (που ονομάζονται κυκλικά προθέματα) με κυκλική επανάληψη μεταξύ μπλοκ συμβόλων με σκοπό την αποτελεσματική εξάλειψη παρεμβολών μεταξύ συμβόλων από την εξάπλωση του χρόνου (που προκαλείται από διάδοση πολλαπλών διαδρομών) μεταξύ των μπλοκ.[14]

### Πλεονεκτήματα χρήσης FDMA τεχνικών

Ένα από τα βασικά πλεονεκτήματα στα συστήματα OFDM (συμπεριλαμβανομένου του SC-FDMA) είναι η ικανότητα προστασίας από την εξάπλωση καθυστέρησης πολλαπλών διαδρομών. Τα μακρά σύμβολα OFDM επιτρέπουν την εισαγωγή μιας περιόδου προστασίας μεταξύ κάθε συμβόλου για την εξάλειψη των παρεμβολών μεταξύ συμβόλων λόγω της εξάπλωσης καθυστέρησης πολλαπλών διαδρομών. Εάν η περίοδος προστασίας είναι μεγαλύτερη από την καθυστέρηση που εξαπλώνεται στο ραδιοφωνικό κανάλι και εάν κάθε σύμβολο OFDM επεκτείνεται κυκλικά στην περίοδο προστασίας (αντιγράφοντας το τέλος του συμβόλου στην αρχή για τη δημιουργία του κυκλικού προθέματος), τότε για το ενδιαμέσο σύμβολο οι παρεμβολές μπορούν να εξαλειφθούν πλήρως.[11][12][14]

Υπάρχουν αρκετά πλεονεκτήματα από τη χρήση του OFDM σε ένα σύστημα πρόσβασης κινητών.

- Τα μεγάλης χρονικής διάρκειας σύμβολα και τα διαστήματα ασφαλείας εξασφαλίζουν ευρωστία στην πολυδιάδοση και περιορίζουν τη διασυμβολική παρεμβολή

- Εξαλείφει την ανάγκη για ενδοκυβελική ακύρωση παρεμβολών
- Επιτρέπει την ευέλικτη χρήση του φάσματος συχνοτήτων.
- Αυξάνει τη φασματική απόδοση λόγω ορθογωνικότητας μεταξύ των υποφερουσών.
- Επιτρέπει τη βελτιστοποίηση του ρυθμού μετάδοσης δεδομένων για όλους τους χρήστες σε μια κυψέλη, μεταδίδοντας τις καλύτερες (για παράδειγμα χωρίς διαλείψεις) υποφέρουσες για κάθε χρήστη. Αυτό το τελευταίο χαρακτηριστικό είναι η θεμελιώδης πτυχή του OFDMA: η χρήση της τεχνολογίας OFDM για την πολυπλεξία της κυκλοφορίας, εκχωρώντας συγκεκριμένα μοτίβα υπο-μεταφορέων στο χώρο συχνοτήτων-χρόνου σε διαφορετικούς χρήστες.
- Το OFDM μπορεί εύκολα να κλιμακωθεί σε ευρεία κανάλια που είναι πιο ανθεκτικά σε διαλείψεις. Οι ισοσταθμιστές καναλιών OFDM είναι πολύ απλούστεροι στην εφαρμογή από ό,τι οι ισοσταθμιστές CDMA, καθώς το σήμα OFDM αντιπροσωπεύεται στον τομέα συχνότητας παρά στον τομέα χρόνου.
- Το OFDM μπορεί να γίνει εντελώς ανθεκτικό στην εξάπλωση καθυστέρησης πολλαπλών διαδρομών. Αυτό είναι εφικτό επειδή τα μακρά σύμβολα που χρησιμοποιούνται για το OFDM μπορούν να διαχωριστούν με ένα διάστημα προστασίας που είναι γνωστό ως κυκλικό πρόθεμα (CP). Το CP είναι ένα αντίγραφο του τέλους ενός συμβόλου που έχει εισαχθεί στην αρχή. Με τη δειγματοληψία του λαμβανόμενου σήματος στον βέλτιστο χρόνο, ο δέκτης μπορεί να αφαιρέσει την παρεμβολή περιοχής χρόνου μεταξύ γειτονικών συμβόλων που προκαλούνται από την εξάπλωση καθυστέρησης πολλαπλών διαδρομών στο ραδιοφωνικό κανάλι. Για το λόγο αυτό πολλές φορές η τεχνική διαμόρφωσης ονομάζεται CP- OFDM.
- Το OFDM εφαρμόζεται καλύτερα σε τεχνολογίες MIMO. Η αναπαράσταση του πεδίου συχνοτήτων του σήματος επιτρέπει την εύκολη κωδικοποίηση ώστε να ταιριάζει με το σήμα με τα χαρακτηριστικά συχνότητας και φάσης του καναλιού πολλαπλών διαδρομών.[11][12][14]

Αν και οι τεχνικές διαμόρφωσης συμβάλλουν σε μια πιο αξιόπιστη επικοινωνία, οι μηχανισμοί Forward Error Correction(FEC) και Hybrid Automatic Repeat ReQuest(HARQ) είναι οι πιο παραγωγικοί για την ελαχιστοποίηση σφαλμάτων.

### 3.6.3 Non-Orthogonal Multiple Access(NOMA)

Το NR χρησιμοποιεί κυρίως τις ορθογώνιες τεχνικές πολλαπλής πρόσβασης που αναφέραμε παραπάνω ώστε να διαχωρίσει τις διάφορες συσκευές που συνδέονται στο δίκτυο στα στα πεδία του χρόνου ή/και της συχνότητας. Ωστόσο, τεχνικές μη-ορθογώνιας πρόσβασης μπορούν να αυξήσουν την χωρητικότητα σε μερικές περιπτώσεις. Κατά τη διάρκεια των

πρώιμων σταδίων ανάπτυξης του NR, η μη-ορθογώνια τεχνική πολλαπλής πρόσβασης (non-orthogonal multiple access, NOMA) μπορεί να μελετήθηκε εν συντομία όμως στην έκδοση 15 και μετά, απέκτησε αρκετό ενδιαφέρον για μελλοντική χρήση.[11]

## 3.7 Το φάσμα συχνοτήτων του 5G

Κλείνοντας το κεφάλαιο για το ραδιοδίκτυο πρόσβασης του 5G θα πρέπει να αναφερθούμε και στο φάσμα συχνοτήτων που αυτό χρησιμοποιεί.

### 3.7.1 Παγκόσμια κατάσταση φάσματος 5G

Νέες ζώνες ορίζονται συνεχώς από το 3GPP, για τις προδιαγραφές LTE, αλλά για τις νέες προδιαγραφές NR αν και πολλές νέες ζώνες ορίζονται μόνο για λειτουργία NR. Και τα δύο ζεύγη ζωνών, όπως έχουν διαχωριστεί τα εύρη συχνοτήτων για ανερχόμενη και κατερχόμενη ζεύξη, περιλαμβάνονται στις προδιαγραφές NR.

Οι συζευγμένες ζώνες χρησιμοποιούνται για τη λειτουργία Frequency Division Duplex (FDD), ενώ οι μη συζευγμένες ζώνες χρησιμοποιούνται για τη λειτουργία Time Division Duplex (TDD). Ορισμένες μη συζευγμένες ζώνες ορίζονται ως Συμπληρωματικές ζώνες ζεύξης (SDL) ή Συμπληρωματικές ζώνες ανόδου (SDL). Αυτές οι ζώνες συνδυάζονται με την ανερχόμενη ή κατερχόμενη ζεύξη άλλων ζωνών μέσω της συνάθροισης φορέα.[2][10]

Υπάρχει ένα μεγάλο ενδιαφέρον παγκοσμίως για τη διάθεση του φάσματος για υλοποιήσεις 5G. Αυτό καθοδηγείται από φορείς εκμετάλλευσης και βιομηχανικούς οργανισμούς όπως η Παγκόσμια Ένωση Προμηθευτών Κινητών και η “DIGITALEUROPE”, αλλά υποστηρίζεται επίσης από ρυθμιστικούς φορείς σε διάφορες χώρες και περιοχές. Το φάσμα ενδιαφέροντος μπορεί να χωριστεί σε ζώνες χαμηλών, μεσαίων και υψηλών συχνοτήτων στις οποίες αναφερόμαστε στη συνέχεια:

1. Οι ζώνες χαμηλής συχνότητας αντιστοιχούν σε υπάρχουσες ζώνες LTE κάτω των 2 GHz, οι οποίες είναι κατάλληλες ως στρώμα κάλυψης, παρέχοντας ευρεία και βαθιά κάλυψη, συμπεριλαμβανομένης της εσωτερικής. Οι ζώνες με υψηλότερο ενδιαφέρον εδώ είναι οι ζώνες 600 και 700 MHz, οι οποίες αντιστοιχούν στις ζώνες 3GPP NR n71 και n28. Δεδομένου ότι οι ζώνες δεν είναι πολύ μεγάλες, αναμένεται μέγιστο εύρος ζώνης καναλιού 20 MHz στις ζώνες χαμηλής συχνότητας.[10] Για πρόωρη ανάπτυξη, η ζώνη των 600 MHz έχει δεσμευθεί για το NR στις ΗΠΑ, ενώ η ζώνη των 700 MHz ορίζεται ως μία από τις λεγόμενες πρωτοποριακές ζώνες για την Ευρώπη. Επιπλέον, ένας αριθμός πρόσθετων ζωνών LTE στο εύρος κάτω των 3 GHz αναγνωρίζονται για πιθανή δέσμευση και έχουν εκχωρηθεί αριθμοί ζώνης NR. Δεδομένου ότι οι ζώνες έχουν ήδη αναπτυχθεί με το LTE, το NR αναμένεται να αναπτυχθεί σταδιακά σε μεταγενέστερο στάδιο.[10]
2. Οι ζώνες μεσαίας συχνότητας βρίσκονται στην περιοχή 3-6 GHz και μπορούν να παρέχουν κάλυψη, χωρητικότητα, καθώς και υψηλούς

ρυθμούς δεδομένων μέσω του ευρύτερου εύρους ζώνης καναλιού. Το υψηλότερο ενδιαφέρον παγκοσμίως είναι στην περιοχή 3300-4200 MHz, όπου το 3GPP έχει ορίσει τις ζώνες NR n77 και n78. Λόγω των ευρύτερων ζωνών, υπάρχει η δυνατότητα για χρήση εύρους ζώνης καναλιού έως 100 MHz. Μπορούν επίσης να εκχωρηθούν έως και 200 MHz ανά χειριστή σε αυτό το εύρος συχνοτήτων μακροπρόθεσμα, μέσω της τεχνικής συνάθροισης φερουσών.[10] Επιπρόσθετα, το εύρος 3300-4200 MHz είναι παγκόσμιου ενδιαφέροντος, με ορισμένες παραλλαγές να εμφανίζονται σε τοπικό επίπεδο και ειδικότερα το εύρος 3400-3800 MHz είναι μια πρωτοποριακή ζώνη στην Ευρώπη, ενώ η Κίνα και η Ινδία προγραμματίζουν συχνότητες 3300-600 MHz και στην Ιαπωνία εξετάζονται 3600-4200 MHz. Παρόμοια εύρη συχνοτήτων λαμβάνονται υπόψη στη Βόρεια Αμερική (3550-3700 MHz και αρχικές συζητήσεις περίπου 3700-4200 MHz), Λατινική Αμερική, Μέση Ανατολή, Αφρική, Ινδία, Αυστραλία κ.λπ. Συνολικά 45 χώρες υπέγραψαν την αναγνώριση του IMT για τη ζώνη 3300-3400 MHz στο WRC-15. Υπάρχει επίσης ένα μεγάλο ενδιαφέρον για υψηλότερη ζώνη στην Κίνα (κυρίως 4800-5000 MHz) και την Ιαπωνία (4400-4900 MHz). Επιπλέον, υπάρχει μια σειρά πιθανών ζωνών επαναπροσδιορισμού LTE στην περιοχή 2-6 GHz που έχουν αναγνωριστεί ως ζώνες NR.[10]

3. Οι ζώνες υψηλής συχνότητας βρίσκονται στην περιοχή των μικροκυμάτων(mm-Wave) δηλαδή άνω των 24 GHz. Ταιριάζουν καλύτερα σε κάλυψη τοπικών hotspot με πολύ υψηλή χωρητικότητα και μπορούν να παρέχουν πολύ υψηλούς ρυθμούς δεδομένων. Το υψηλότερο ενδιαφέρον είναι στην περιοχή 24,25-29,5 GHz, με τις ζώνες της 3GPP NR n257 και n258. Το εύρος ζώνης καναλιού που καθορίζεται για αυτές τις ζώνες αναμένεται έως 400 MHz, ενώ ακόμη υψηλότερα εύρη ζώνης δύναται να αξιοποιηθούν μέσω της τεχνικής συνάθροισης φορέων.[10]

Το εύρος συχνοτήτων mmWave είναι μια νέα ανάπτυξη IMT και η ζώνη 27,5-28,35 ταυτοποιήθηκε σε πρώιμο στάδιο στις ΗΠΑ, ενώ τα 24,25-27,5 GHz, που ονομάζονται επίσης "ζώνη 26 GHz", είναι μια πρωτοποριακή μπάντα για την Ευρώπη, σημειώνοντας ότι ενδέχεται να μην διατίθενται όλες οι συχνότητες για 5G. Διαφορετικά μέρη του μεγαλύτερου εύρους 24,25- 29,5 GHz εξετάζονται παγκοσμίως. Το εύρος 27,5-29,5 GHz είναι το πρώτο εύρος που σχεδιάζεται για την Ιαπωνία ενώ το εύρος 26,5-29,5 GHz στην Κορέα. Το εύρος 37-40 GHz έχει επίσης σχεδιαστεί για τις ΗΠΑ και παρόμοιες περιοχές περίπου 40 GHz λαμβάνονται υπόψη και σε πολλές άλλες περιοχές, συμπεριλαμβανομένης της Κίνας.[10]

### 3.7.2 Ζώνες συχνοτήτων για το NR

Το NR μπορεί να αναπτυχθεί τόσο σε υπάρχουσες ζώνες IMT όσο και σε μελλοντικές ζώνες που μπορεί να αναγνωριστούν στο WRC ή σε περιφερειακούς φορείς. Η δυνατότητα λειτουργίας μιας τεχνολογίας ραδιοπρόσβασης σε διαφορετικές ζώνες συχνοτήτων αποτελεί θεμελιώδη πτυχή των παγκόσμιων κινητών υπηρεσιών. Οι περισσότερες συσκευές 2G, 3G και 4G έχουν δυνατότητα πολλαπλών ζωνών, καλύπτοντας ζώνες

που χρησιμοποιούνται σε διάφορες περιοχές του κόσμου για την παροχή παγκόσμιας περιαγωγής. Δεδομένου ότι το NR εκτείνεται σε ένα τόσο μεγάλο εύρος συχνοτήτων, υπάρχουν ορισμένες διατάξεις που προορίζονται μόνο για συγκεκριμένες περιοχές συχνοτήτων. Αυτό περιλαμβάνει τον τρόπο με τον οποίο μπορούν να εφαρμοστούν οι διαφορετικές αριθμολογίες NR.[10][12]

Πολλές απαιτήσεις RF καθορίζονται με διαφορετικές απαιτήσεις σε όλες τις ζώνες. Αυτό ισχύει σίγουρα για το NR, αλλά και για τις προηγούμενες γενιές. Παραδείγματα απαιτήσεων RF για συγκεκριμένη ζώνη είναι η επιτρεπόμενη μέγιστη ισχύς εκπομπής, απαιτήσεις / όρια στα επίπεδα εκπομπής εκτός ζώνης (OOB) και στα επίπεδα αποκλεισμού δέκτη.[10][12]

Οι διαφορετικοί εξωτερικοί περιορισμοί, που συχνά επιβάλλονται από ρυθμιστικούς φορείς, και περιπτώσεις διαφοροποιήσεων στο λειτουργικό περιβάλλον που λαμβάνονται υπόψη κατά την τυποποίηση είναι λόγοι για τις διαφορετικές συχνότητες ενώ οι διαφορές αυτές μεταξύ των ζωνών είναι πιο έντονες για το NR λόγω του πολύ μεγάλου εύρους των ζωνών συχνοτήτων. Για τη λειτουργία NR στις νέες ζώνες mm-Wave άνω των 24 GHz, τόσο οι συσκευές όσο και οι σταθμοί βάσης θα εφαρμοστούν με εν μέρει νέα τεχνολογία και θα υπάρξει μια ευρύτερη χρήση μαζικού MIMO, σχηματισμού δέσμης και προηγμένων συστημάτων κεραιών. Αυτό δημιουργεί διαφορές στον τρόπο καθορισμού των απαιτήσεων ραδιοσυχνοτήτων, του τρόπου με τον οποίο μετρούνται για την αξιολόγηση της απόδοσης και τελικά, του τι καθορίζεται για τα όρια και τις απαιτήσεις.[]

Οι ζώνες συχνοτήτων εντός του πεδίου εφαρμογής της παρούσας έκδοσης(έκδοση 15) στο 3GPP χωρίζονται για αυτόν τον λόγο σε δύο περιοχές συχνοτήτων:

- ▶ **Πεδίο συχνοτήτων 1 (Frequency range 1, FR1) περιλαμβάνοντας τις υπάρχουσες αλλά και νέες ζώνες κάτω των 6 GHz.**
- ▶ **Πεδίο συχνοτήτων 2 (Frequency range 2 (FR2) περιλαμβάνει νέες ζώνες συχνοτήτων στο εύρος 24.25-52.6 GHz.**

Αυτές οι ζώνες συχνοτήτων ενδέχεται να επεκταθούν ή να συμπληρωθούν με άλλες ζώνες συχνοτήτων σε επόμενες εκδόσεις της κοινοπραξίας 3GPP, όπως η FR3 η οποία έχει ήδη εμφανισθεί με συχνότητες που ξεκινούν από 60 GHz. Σε κάθε περίπτωση όμως η ανώτερη επιτευχθείσα συχνότητα είναι τα 300 GHz. Οι υψηλότερες συχνότητες από το FR3 και έπειτα αναφέρονται και ως μη αδειοδοτούμενες συχνότητες καθόσον δεν έχουν λάβει την απαραίτητα άδεια χρήσης από τους αρμόδιους φορείς.

Σε μη συζευγμένα φάσματα, η ασυμμετρία στην επικοινωνία των συσκευών μπορεί να παρέχεται μέσω της χρήσης άνισων κύκλων λειτουργίας στον τομέα χρόνου για ανερχόμενη και κατερχόμενη ζεύξη. Σε συζευγμένα φάσματα, η ασυμμετρία είναι επίσης δυνατή μέσω της ανάπτυξης άνισου εύρους ζώνης για uplink και downlink. Ο όρος «αμφίδρομη»(duplex) αναφέρεται σε αμφίδρομη επικοινωνία μεταξύ δύο συσκευών και διακρίνεται από την απλή περίπτωση. Στην αμφίδρομη περίπτωση, οι μεταδόσεις μέσω του συνδέσμου σε κάθε κατεύθυνση μπορούν να πραγματοποιούνται ταυτόχρονα «πλήρες - duplex» ή σε αμοιβαία αποκλειστικούς χρόνους «half-duplex». Έτσι, διακρίνονται περιπτώσεις Time Division Duplex (TDD) και Frequency Division Duplex (FDD) downlink ή uplink. [10][12]



Γενικότερα, οι ζώνες συχνοτήτων όπου θα λειτουργεί το NR θα είναι σε συζευγμένα (paired) αλλά και μη συζευγμένα φάσματα, απαιτώντας ευελιξία σε περιπτώσεις duplex. Για το λόγο αυτό, το NR υποστηρίζει λειτουργία FDD και TDD. Ορισμένες περιοχές καθορίζονται επίσης για SDL ή SUL. Το 3GPP ορίζει ζώνες λειτουργίας, όπου κάθε ζώνη λειτουργίας είναι ένα εύρος συχνοτήτων για uplink και / ή downlink που καθορίζεται με ένα συγκεκριμένο σύνολο απαιτήσεων RF. Κάθε ζώνη λειτουργίας έχει έναν αριθμό, όπου οι ζώνες NR αριθμούνται n1, n2, n3, κ.λπ. Όταν το ίδιο εύρος συχνοτήτων ορίζεται ως ζώνη λειτουργίας για διαφορετικές τεχνολογίες ραδιοπρόσβασης, χρησιμοποιείται ο ίδιος αριθμός, αλλά γράφεται με διαφορετικός τρόπος. Οι ζώνες 4G LTE γράφονται με αριθμούς (1, 2, 3, κ.λπ.), ενώ οι ζώνες 3G UTRA γράφονται με λατινικούς αριθμούς (I, II, III κ.λπ.). Οι ζώνες λειτουργίας LTE που χρησιμοποιούνται με την ίδια ρύθμιση για NR αναφέρονται συχνά ως «ζώνες δέσμευσης LTE».[10][12]

Η έκδοση 15 των προδιαγραφών 3GPP για NR περιλαμβάνει 26 ζώνες λειτουργίας στο εύρος συχνοτήτων 1 και τρεις στο εύρος συχνοτήτων 2. Οι ζώνες για NR έχουν ένα σχήμα αρίθμησης με εκχωρημένους αριθμούς από n1 έως n512 χρησιμοποιώντας τους ακόλουθους κανόνες:

1. Για NR σε ζώνες δεσμευμένες από το LTE, οι αριθμοί ζώνης LTE επαναχρησιμοποιούνται για το NR, προσθέτοντας απλά ένα «n».
2. Σε νέες ζώνες για το NR εκχωρούνται οι ακόλουθοι αριθμοί:
  - Το εύρος n65 έως n256 προορίζεται για ζώνες NR στο εύρος συχνοτήτων 1 (μερικές από αυτές τις ζώνες μπορούν να χρησιμοποιηθούν και για LTE).
  - Η περιοχή n257 έως n512 προορίζεται για νέες ζώνες NR στο εύρος συχνοτήτων 2. Το σχήμα "διατηρεί" αριθμούς ζώνης και είναι συμβατό με LTE (και UTRA) και δεν οδηγεί σε νέους αριθμούς LTE άνω των 256, που είναι το μέγιστο δυνατό σήμερα. Οποιοσδήποτε νέες ζώνες για το LTE μπορούν επίσης να εκχωρηθούν σε αχρησιμοποίητους αριθμούς κάτω των 65. Στην έκδοση 15, οι ζώνες λειτουργίας στο εύρος συχνοτήτων 1 βρίσκονται στην περιοχή n1 έως n84 όπως φαίνεται στον πίνακα 3.4. Οι ζώνες στο εύρος συχνοτήτων 2 κυμαίνονται από n257 έως n260, όπως φαίνεται στον πίνακα 4.1.

Μπάντα NR	Εύρος Uplink και Downlink(MHz)	Επιλογή Duplex	Περιοχές λειτουργίας
n257	26500-29500	TDD	ΑΣΙΑ,ΑΜΕΡΙΚΗ(GLOBAL)
n258	24250-27500	TDD	ΕΥΡΩΠΗ,ΑΣΙΑ(GLOBAL)
n259	37000-40000	TDD	ΑΜΕΡΙΚΗ(GLOBAL)

Πίνακας 3.3: Εύρος Συχνοτήτων 2 (Frequency Range 2, FR2)[10]

Μπάντα NR	Εύρος Uplink(MHz)	Εύρος Downlink(MHz)	Επιλογή Duplex	Βασικές περιοχές λειτουργίας
n1	1920-1980	2110-2170	FDD	ΕΥΡΩΠΗ,ΑΣΙΑ
n2	1850-1910	1930-1990	FDD	ΑΜΕΡΙΚΗ,ΑΣΙΑ
n3	1710-1785	1805-1880	FDD	ΕΥΡΩΠΗ,ΑΣΙΑ,ΑΜΕΡΙΚΗ
n5	824-849	869-894	FDD	ΑΜΕΡΙΚΗ,ΑΣΙΑ
n7	2500-2570	2620-2690	FDD	ΕΥΡΩΠΗ,ΑΣΙΑ
n8	880-915	925-960	FDD	ΕΥΡΩΠΗ,ΑΣΙΑ
n20	832-862	791-821	FDD	ΕΥΡΩΠΗ
n28	703-748	758-803	FDD	ΑΣΙΑ/ΕΙΡΗΝΙΚΟΣ
n38	2570-2620	2570-2620	TDD	ΕΥΡΩΠΗ
n41	2496-2690	2496-2690	TDD	ΗΠΑ,ΚΙΝΑ
n50	1432-1517	1432-1517	TDD	-
n51	1427-1432	1427-1432	TDD	-
n66	1710-1780	2110-2200	FDD	ΑΜΕΡΙΚΗ
n70	1695-1710	1995-2020	FDD	-
n71	663-698	617-652	FDD	ΑΜΕΡΙΚΗ
n74	1427-1470	1475-1518	FDD	ΙΑΠΩΝΙΑ
n75	Μη Διαθέσιμο	1432-1517	SDL	ΕΥΡΩΠΗ
n76	Μη Διαθέσιμο	1427-1432	SDL	ΕΥΡΩΠΗ
n77	3300-4200	3300-4200	TDD	ΕΥΡΩΠΗ,ΑΣΙΑ
n78	3300-3800	3300-3800	TDD	ΕΥΡΩΠΗ,ΑΣΙΑ
n79	4400-5500	4400-5500	TDD	ΑΣΙΑ
n80	1710-1785	Μη Διαθέσιμο	SUL	-
n81	880-915	Μη Διαθέσιμο	SUL	-
n82	832-862	Μη Διαθέσιμο	SUL	-
n83	703-748	Μη Διαθέσιμο	SUL	-
n84	1920-1980	Μη Διαθέσιμο	SUL	-

Πίνακας 3.4: Εύρος Συχνότητων 1 (Frequency Range 1, FR1)[10]

Αν και η επιλογή συχνότητας αποτελεί μία σημαντική προδιαγραφή για ένα τηλεπικοινωνιακό σύστημα, το πως το 5G διαχειρίζεται τη ραδιοκυματική δέσμη είναι ακόμα πιο ενδιαφέρον και αναλύεται στο επόμενο κεφάλαιο που συνοψίζονται ορισμένα νέα χαρακτηριστικά που εισάγει η αρχιτεκτονική του 5G.



# Κεφάλαιο 4

## Καινοτόμες προσεγγίσεις στο 5G

**Η** τεχνολογία 5G όπως αναφέραμε θεωρείται μια επανάσταση στα τηλεπικοινωνιακά δίκτυα αλλά και στα εφαρμοζόμενα δίκτυα σε πολλούς τομείς όπως η ιατρική, η βιομηχανία κ.α.. Και αυτό είναι αποτέλεσμα εφαρμογής υπαρχόντων καινοτόμων τεχνικών και μεθόδων αλλά και νέων χαρακτηριστικών. Στο κεφάλαιο αυτό αναλύονται ορισμένα νέα χαρακτηριστικά και νέες τεχνικές και τεχνολογίες που εισήχθησαν για πρώτη φορά σε τηλεπικοινωνιακό σύστημα και αποτελούν τους βασικούς άξονες λειτουργίας και εξέλιξης των συστημάτων 5G και Beyond.

### 4.1 Πρωτόκολλα επικοινωνίας στο 5G

Αυτή η παράγραφος περιγράφει τα κύρια πρωτόκολλα που χρησιμοποιούνται στο 5GS, με στόχο την επισκόπηση αυτών των πρωτοκόλλων στα διάφορα επίπεδα καθώς και την αναφορά στις βασικές τους ιδιότητες.

#### 4.1.1 5G στρώμα μη-πρόσβασης(5G Non-Access Stratum, 5G NAS)

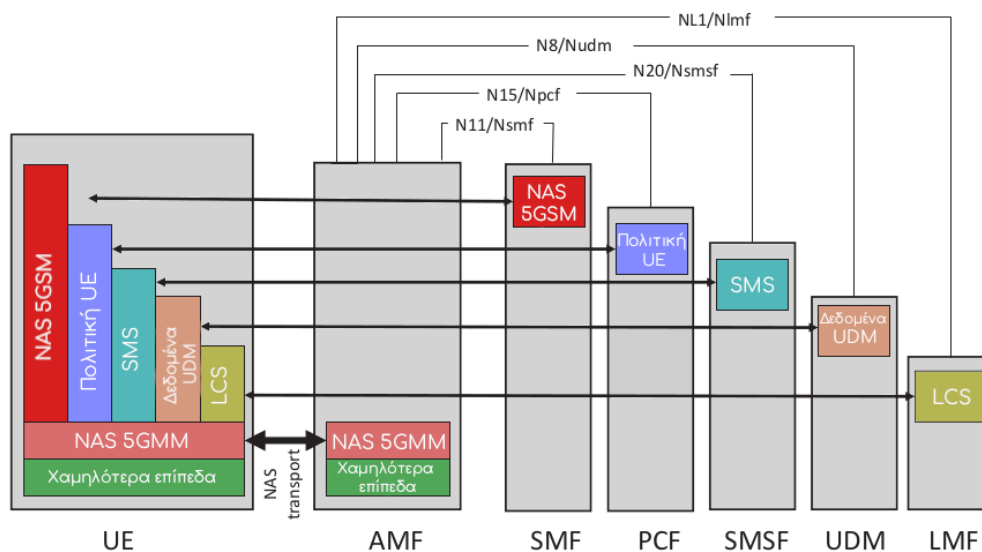
Το NAS δηλώνει τα κύρια πρωτόκολλα επιπέδου ελέγχου μεταξύ του UE και του κεντρικού δικτύου. Οι κύριες λειτουργίες της NAS είναι:

- Χειρισμός εγγραφής και κινητικότητας UE, συμπεριλαμβανομένης γενικής λειτουργικότητας για έλεγχο πρόσβασης, όπως διαχείριση σύνδεσης, έλεγχος ταυτότητας, χειρισμός ασφάλειας NAS, αναγνώριση UE και διαμόρφωση UE
- Υποστήριξη διαδικασιών διαχείρισης συνεδρίας για τη δημιουργία και τη διατήρηση της σύνδεσης PDU και του QoS για το επίπεδο χρήστη μεταξύ του UE και του DN
- Γενική μεταφορά NAS μεταξύ UE και AMF για μεταφορά άλλων τύπων μηνυμάτων που δεν ορίζονται ως μέρος του πρωτοκόλλου NAS ως έχει. Αυτό περιλαμβάνει, π.χ. μεταφορά SMS, πρωτόκολλο LPP για υπηρεσίες τοποθεσίας, δεδομένα UDM όπως μηνύματα Steering of Roaming (SOR), καθώς και πολιτικές UE (URSP).[25]

Το NAS αποτελείται από δύο βασικά πρωτόκολλα για την υποστήριξη της παραπάνω λειτουργικότητας. Το πρωτόκολλο 5GS Mobility Management

(5GMM) και το πρωτόκολλο 5GS Session Management (5GSM).[2][25]

Το πρωτόκολλο 5GMM εκτελείται μεταξύ του UE και του AMF και είναι το βασικό πρωτόκολλο NAS που χρησιμοποιείται για τον χειρισμό εγγραφών UE, κινητικότητας, ασφάλειας και μεταφοράς του πρωτοκόλλου 5GSM καθώς και της γενικής μεταφοράς NAS άλλων τύπων μηνυμάτων. Το 5GSM πρωτόκολλο τρέχει μεταξύ UE και SMF (μέσω του AMF) και υποστηρίζει τη διαχείριση της σύνδεσης PDU. Μεταφέρεται πάνω από το πρωτόκολλο 5GMM όπως φαίνεται στο σχήμα παρακάτω. Το πρωτόκολλο 5GMM χρησιμοποιείται επίσης για τη μεταφορά πληροφοριών μεταξύ UE και PCF, UE και SMSF, κ.λ.π. . Στο 5G, το πρωτόκολλο NAS χρησιμοποιείται τόσο μέσω πρόσβασης 3GPP όσο και εκτός 3GPP. Αυτή είναι μια βασική διαφορά σε σύγκριση με το EPS / 4G, όπου το NAS ήταν ειδικά σχεδιασμένο για πρόσβαση 3GPP (E-UTRAN) μόνο.[2][25]



Εικόνα 4.1: Στοιβά Πρωτοκόλλου NAS[2]

Τα μηνύματα NAS μεταφέρονται μέσω NGAP (χρησιμοποιείται στο σημείο αναφοράς N2) μεταξύ AMF και (R) AN και με ειδικά μέσα πρόσβασης μεταξύ (R)AN και UE. Το NGAP περιγράφεται παρακάτω.

Τα πρωτόκολλα 5G NAS ορίζονται ως νέα πρωτόκολλα στο 5G αλλά έχουν πολλές ομοιότητες με τα πρωτόκολλα NAS που χρησιμοποιούνται για 4G / EPS και επίσης τα πρωτόκολλα NAS που ορίζονται για 2G / 3G / GPRS.[2]

### 5G Διαχείριση Κινητικότητας (5G Mobility Management)

Οι διεργασίες 5GMM χρησιμοποιούνται για να παρακολουθούν την τοποθεσία του UE, για τον έλεγχο ταυτότητας του UE και τον έλεγχο της προστασίας της ακεραιότητας και της κρυπτογράφησης. Ακόμη, οι διεργασίες 5GMM επιτρέπουν επίσης στο δίκτυο να εκχωρεί νέες προσωρινές ταυτότητες στο UE (5G-GUTI) και επίσης να ζητά πληροφορίες ταυτότητας (SUCI και PEI) από το UE. Επιπλέον, παρέχουν τις πληροφορίες δυνατοτήτων του UE στο δίκτυο και το δίκτυο μπορεί επίσης να ενημερώσει το UE για πληροφορίες σχετικά με συγκεκριμένες υπηρεσίες στο δίκτυο. Το πρωτόκολλο 5GMM λειτουργεί έτσι σε επίπεδο UE (ανά τύπο πρόσβασης) σε αντίθεση με το πρωτόκολλο 5GSM

που βρίσκεται σε επίπεδο περιόδου λειτουργίας ανά PDU. Η σηματοδότηση 5GMM NAS πραγματοποιείται μεταξύ του UE και του AMF. [25]

Οι βασικές διαδικασίες 5GMM είναι:

- Εγγραφή
- Διαγραφή
- Αυθεντικοποίηση
- Έλεγχος λειτουργίας ασφαλείας
- Αίτηση υπηρεσίας
- Γνωστοποίηση
- Μεταφορά NAS ανερχόμενης ζεύξης
- Μεταφορά NAS κατερχόμενης ζεύξης
- Ενημέρωση διαμόρφωσης UE (π.χ. για ανακατανομή 5G-GUTI, ενημέρωση λίστας TAI κ.λπ.)
- Αίτημα ταυτότητας UE

Οι διεργασίες 5GMM μπορούν να εκτελεστούν μόνο εάν έχει δημιουργηθεί σύνδεση σηματοδότησης NAS μεταξύ του UE και του AMF. Εάν δεν υπάρχει ενεργή σύνδεση σηματοδότησης, το επίπεδο 5GMM πρέπει να ξεκινήσει τη δημιουργία μιας σύνδεσης σηματοδότησης NAS. Η σύνδεση σηματοδότησης NAS πραγματοποιείται με διαδικασία εγγραφής ή αίτησης υπηρεσίας από το UE. Για τη σηματοδότηση NAS κάτω ζεύξης, εάν δεν υπάρχει ενεργή σύνδεση σηματοδότησης, το AMF ξεκινά πρώτα μια διαδικασία τηλεειδοποίησης που ενεργοποιεί το UE να εκτελέσει τη διαδικασία αιτήματος υπηρεσίας.[25]

Οι διεργασίες 5GMM βασίζονται με τη σειρά τους σε υπηρεσίες από το υποκείμενο πρωτόκολλο NGAP μεταξύ του (R) AN και του AMF (δηλ. N2) και της ειδικής πρόσβασης σηματοδότησης μεταξύ UE και (R) AN όπως το RRC για πρόσβαση 3GPP για τη δημιουργία συνδεσιμότητας.[25]

### 5G Διαχείριση Συνεδριών (5G Session Sanagement)

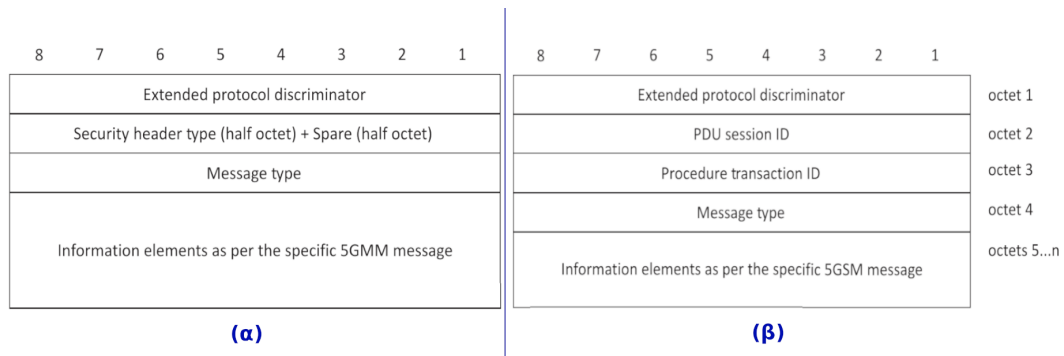
Οι διαδικασίες 5GSM χρησιμοποιούνται για τη διαχείριση των συνεδριών PDU και του QoS για το επίπεδο χρήστη. Αυτό περιλαμβάνει διαδικασίες για τη δημιουργία και την απελευθέρωση των συνεδριών PDU καθώς και την τροποποίηση των περιόδων σύνδεσης PDU, για προσθήκη, κατάργηση ή τροποποίηση των κανόνων QoS. Οι διαδικασίες 5GSM χρησιμοποιούνται επίσης για τη διεξαγωγή του δευτερεύοντος ελέγχου ταυτότητας για μια συνεδρία PDU. Το πρωτόκολλο 5GSM λειτουργεί σε επίπεδο συνεδρίας PDU σε αντίθεση με το πρωτόκολλο 5GMM που λειτουργεί σε επίπεδο UE.[25]

Οι βασικές 5GSM διεργασίες είναι:

- Εγκαθίδρυση συνεδρίας PDU
- Έκδοση συνεδρίας PDU
- Τροποποίηση συνεδρίας PDU
- Έλεγχος ταυτότητας και εξουσιοδότηση περιόδου σύνδεσης PDU
- Κατάσταση 5GSM (για ανταλλαγή πληροφοριών κατάστασης περιόδου σύνδεσης PDU)

## Μηνύματα NAS

Κάθε μήνυμα NAS περιέχει έναν "Διευκρινιστή πρωτοκόλλου(Protocol Discriminator)" και ένα τύπο μηνύματος. Στις παρακάτω εικόνες αναπαρίσταται η δομή των μηνυμάτων NAS.



Εικόνα 4.2: Δομή πλαισίου(frame) μηνυμάτων NAS για (α) 5GMM και (β) 5GSM[2]

Το Protocol Discriminator είναι μια τιμή που δείχνει το πρωτόκολλο που χρησιμοποιείται, δηλαδή, για μηνύματα 5G NAS είναι είτε 5GMM είτε 5GSM (για την ακρίβεια, στο 5G, ορίζεται ένα Extended Protocol Discriminator). Ο τύπος μηνύματος υποδεικνύει το συγκεκριμένο μήνυμα που αποστέλλεται, π.χ. αίτημα εγγραφής, αποδοχή εγγραφής ή αίτημα τροποποίησης περιόδου σύνδεσης PDU.

Τα μηνύματα NAS 5GMM περιέχουν επίσης μια κεφαλίδα ασφαλείας που υποδεικνύει εάν το μήνυμα προστατεύεται από ακεραιότητα ή / και κρυπτογραφείται. Τα μηνύματα 5GSM περιέχουν μια ταυτότητα περιόδου σύνδεσης PDU που προσδιορίζει σε ποια συνεδρία PDU αναφέρεται το μήνυμα 5GSM. Τα υπόλοιπα στοιχεία πληροφοριών στα μηνύματα 5GMM και 5GSM είναι προσαρμοσμένα για κάθε συγκεκριμένο μήνυμα NAS.[2][14][25]

### 4.1.2 NG Πρωτόκολλο εφαρμογών (NG Application Protocol, NGAP)

Το πρωτόκολλο NGAP έχει σχεδιαστεί για χρήση στη διεπαφή N2 μεταξύ του (R)AN και του AMF. Αξίζει να σημειωθεί ότι οι ομάδες 3GPP RAN έχουν δώσει το όνομα NG στη διεπαφή RAN-AMF που στη συνολική αρχιτεκτονική του συστήματος ονομάζεται N2. Το όνομα πρωτοκόλλου NGAP προέρχεται έτσι από το όνομα διασύνδεσης NG με την προσθήκη του AP (Application Protocol), το οποίο είναι ένας όρος που έχει χρησιμοποιηθεί πολλές φορές από το 3GPP για να υποδηλώσει ένα πρωτόκολλο σηματοδότησης μεταξύ δύο λειτουργιών δικτύου.[2][28]

Το NGAP υποστηρίζει όλους τους απαραίτητους μηχανισμούς για τον χειρισμό των διαδικασιών μεταξύ AMF και (R) AN και υποστηρίζει επίσης διαφανή μεταφορά για διεργασίες που εκτελούνται μεταξύ του UE και του AMF ή άλλων βασικών λειτουργιών δικτύου. Το NGAP ισχύει τόσο για πρόσβαση 3GPP όσο και για πρόσβαση εκτός 3GPP που είναι ενσωματωμένη στο 5GC. Αυτή είναι μια βασική διαφορά για το EPC όπου το S1AP σχεδιάστηκε

για χρήση μόνο με πρόσβαση 3GPP (E-UTRAN) και όχι με πρόσβαση εκτός 3GPP. Ωστόσο, παρόλο που το NGAP είναι εφαρμόσιμο σε οποιαδήποτε πρόσβαση, ο σχεδιασμός του στοχεύει κυρίως σε προσβάσεις 3GPP (NG-RAN), οι οποίες μπορούν επίσης να παρατηρηθούν στις προδιαγραφές πρωτοκόλλου που ορίζονται στο 3GPP TS 38.413. Στο πρωτόκολλο αυτό έχει προστεθεί υποστήριξη για συγκεκριμένες παραμέτρους που σχετίζονται με πρόσβαση εκτός 3GPP.[2][28]

Οι αλληλεπιδράσεις NGAP μεταξύ AMF και (R)AN χωρίζονται σε δύο ομάδες:

- i **Υπηρεσίες που δεν σχετίζονται με UE:** Αυτές οι υπηρεσίες NGAP σχετίζονται με ολόκληρη την παρούσα διασύνδεση NG μεταξύ του κόμβου (R) AN και του AMF. Χρησιμοποιούνται, για παράδειγμα, για τη δημιουργία της σύνδεσης σηματοδότησης NGAP μεταξύ AMF και (R) AN, για χειρισμό ορισμένων καταστάσεων υπερφόρτωσης και για την ανταλλαγή δεδομένων διαμόρφωσης RAN και AMF.
- ii **Υπηρεσίες που σχετίζονται με UE:** Αυτές οι υπηρεσίες NGAP σχετίζονται με ένα UE. Αυτή η σηματοδότηση NGAP σχετίζεται επομένως με διεργασίες στις οποίες εμπλέκεται ένα UE, π.χ. κατά την εγγραφή, την εγκατάσταση συνεδρίας PDU κ.λπ.

Το πρωτόκολλο NGAP υποστηρίζει τις ακόλουθες λειτουργίες:

- Λειτουργίες διαχείρισης διασύνδεσης NG (δηλ. N2), όπως για παράδειγμα αρχική ρύθμιση διασύνδεσης NG καθώς και Επαναφορά, Ένδειξη σφάλματος, Ένδειξη υπερφόρτωσης και Εξισορρόπηση φορτίου.
- Αρχικοποίηση χαρακτηριστικών ρυθμίσεων UE για τη δημιουργία ενός αρχικού περιβάλλοντος UE στον κόμβο (R)AN.
- Παροχή πληροφοριών δυνατοτήτων UE στο AMF (όταν λαμβάνεται από το UE).
- Λειτουργίες φορητότητας για UE προκειμένου να επιτρέπεται η παράδοση στο NG-RAN, π.χ. αίτημα εναλλαγής διαδρομής.
- Ρύθμιση, τροποποίηση και απελευθέρωση πόρων περιόδου λειτουργίας PDU (πόροι User Plane)
- Τηλεειδοποίηση, παρέχοντας τη λειτουργικότητα για το 5GC ώστε να ειδοποιεί το UE.
- Λειτουργία μεταφοράς σηματοδότησης NAS μεταξύ του UE και του AMF
- Διαχείριση της δέσμευσης μεταξύ ενός συνδέσμου NGAP UE και ενός συγκεκριμένου συνδέσμου επιπέδου δικτύου μεταφοράς για ένα δεδομένο UE
- Λειτουργία μεταφοράς κατάστασης (μεταφέρει πληροφορίες κατάστασης αριθμού ακολουθίας PDCP από τον κόμβο NG-RAN προέλευσης σε κόμβο NG-RAN στόχου (μέσω AMF) για την υποστήριξη παράδοσης σε σειρά και αποφυγής επανάληψης για παράδοση).
- Ίχνος ενεργών UE.
- Υποστήριξη αναφορών θέσης UE και πρωτοκόλλου τοποθέτησης.
- Μετάδοση μηνυμάτων προειδοποίησης.

Τέλος, το NGAP αποτελείται και από στοιχειώδεις διεργασίες. Μια στοιχειώδης διεργασία είναι μια μονάδα αλληλεπίδρασης μεταξύ του (R) AN (π.χ. κόμβος NG-RAN) και του AMF. Αυτές οι στοιχειώδεις διεργασίες



καθορίζονται ξεχωριστά και προορίζονται να χρησιμοποιηθούν για τη δημιουργία πλήρων ακολουθιών με ευέλικτο τρόπο.[2][28]

### 4.1.3 Πρωτόκολλο μεταφοράς υπερκειμένου (Hypertext transfer protocol, HTTP)

Αν και στο πρωτόκολλο HTTP αναφερθήκαμε και στο κεφάλαιο 2, είναι ήδη γνωστό και διαδεδομένο καθώς αποτελεί και το πιο οικείο πρωτόκολλο σήμερα, κατά τη χρήση του διαδικτύου(internet) δίνοντας πρόσβαση στις ιστοσελίδες όπου υπερσύνδεσμοι οδηγούν σε άλλους πόρους με αποτέλεσμα να είναι προσβάσιμοι από έναν χρήστη με μεγάλη ευκολία.

Την ίδια στιγμή, το HTTP θεωρείται μια νέα εισαγωγή στην οικογένεια των πρωτοκόλλων στα βασικά δίκτυα 3GPP, τουλάχιστον από τη σκοπιά των διεπαφών του Control Plane. Ενώ το επίπεδο ελέγχου 2G / 3G / 4G βασίστηκε σε μεγάλο βαθμό στα GTP-C, MAP και Diameter στο κεντρικό δίκτυο, το 5GC Control Plane βασίζεται σχεδόν αποκλειστικά σε HTTP.

Το HTTP ορίστηκε ως πρωτόκολλο εφαρμογής για τη διανομή και την πρόσβαση σε πληροφορίες υπερμέσων με την αρχική ανάπτυξη του να λαμβάνει χώρα στις πρώτες μέρες του World Wide Web στα τέλη της δεκαετίας του 1980 με την έκδοση v0.9. Η νεότερη αναθεώρηση του, η HTTP / 2, τυποποιήθηκε το 2015 στο IETF RFC 7540 και αυτή είναι η έκδοση που χρησιμοποιεί το 3GPP για το 5GC Control Plane. [2]

Ο κύριος στόχος του HTTP / 2 ήταν να βελτιώσει την απόδοση προκειμένου να προσφέρει καλύτερη εμπειρία στους χρήστες του διαδικτύου. Τα βασικά οφέλη του HTTP / 2 σε σύγκριση με το HTTP 1.1 είναι η υποστήριξη για πλήρη πολυπλεξία αιτημάτων και απαντήσεων, υποστήριξη για συμπίεση πεδίων κεφαλίδας HTTP για ελαχιστοποίηση των γενικών πρωτοκόλλων και υποστήριξη για προτεραιότητα αιτήσεων και ώθηση διακομιστή. [26]

Αυτό που κάνει ουσιαστικά το HTTP/2 είναι ότι αλλάζει (βελτιώνοντας) τον τρόπο μορφοποίησης και μεταφοράς των πληροφοριών στα μηνύματα μεταξύ του πελάτη και του διακομιστή. Ωστόσο, αυτή η μορφοποίηση δεν είναι ορατή στο επίπεδο εφαρμογής.[26]

Το HTTP είναι ένα πρωτόκολλο απόκρισης αιτήματος που εκτελείται μεταξύ πελάτη και διακομιστή. Το Εικόνα 4.3: Στοίβα πρωτοκόλλου πρωτόκολλο μεταφέρεται μέσω TCP για HTTP.[2] να εξασφαλιστεί αξιόπιστη μετάδοση.

Το HTTP 1.1 θα μπορούσε επίσης να μεταφερθεί σε άλλα πρωτόκολλα μεταφοράς, αλλά το HTTP/2 ορίζεται ότι μεταφέρεται μόνο μέσω TCP.[26]

Το 3GPP έχει συζητήσει για τη χρήση HTTP με μεταφορά QUIC (το HTTP μέσω του QUIC αναφέρεται επίσης ως HTTP/3), αλλά έμεινε εκτός λειτουργίας επειδή δεν ήταν αρκετά ώριμο για εφαρμογή στην έκδοση 15 της 3GPP. Ωστόσο, μελετάται η χρήση του HTTP μέσω QUIC και πιθανότατα θα καθοριστεί σε μια μελλοντική έκδοση 3GPP.[26]

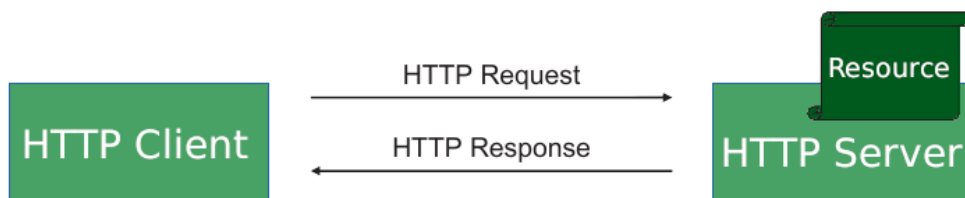
HTTP
(TLS)
TCP
IP
L2/L1

Η στοίβα πρωτοκόλλου για HTTP φαίνεται στο διπλανό σχήμα. Το Transport Layer Security (TLS) (αναλύεται παρακάτω) χρησιμοποιείται προαιρετικά για την προστασία της κίνησης HTTP μεταξύ πελάτη και διακομιστή και σε αυτή την περίπτωση, HTTP μέσω TLS δηλαδή, αναφέρεται επίσης ως HTTPS.[26]

Όταν ένας πελάτης HTTP θέλει να επικοινωνήσει με έναν διακομιστή δημιουργεί πρώτα μια σύνδεση TCP προς μια συγκεκριμένη θύρα του διακομιστή. Η προεπιλεγμένη θύρα για HTTP είναι η 80, ενώ η προεπιλεγμένη θύρα για HTTPS είναι η 443. Με το 5GC, ένα NF που παράγει μια υπηρεσία (δηλαδή, ενεργεί ως διακομιστής HTTP) μπορεί να καταχωρίσει τη διεύθυνση FQDN ή / και τη διεύθυνση IP και τη θύρα για την υπηρεσία σε RF.[2]

Ο καταναλωτής NF (δηλαδή, η οντότητα που ενεργεί ως πελάτης HTTP) μπορεί στη συνέχεια να ανακαλύψει από το NRF το διακομιστή FQDN ή τη διεύθυνση IP και προαιρετικά τον αριθμό θύρας, για σύνδεση με μια συγκεκριμένη υπηρεσία NF. Εάν ένας παραγωγός NF δεν καταχωρίσει κανένα αριθμό θύρας στο NRF, θα χρησιμοποιηθούν οι προεπιλεγμένοι αριθμοί θύρας για HTTP και HTTPS. Μόλις δημιουργηθεί η σύνδεση TCP, ο πελάτης μπορεί να στείλει ένα αίτημα HTTP στον διακομιστή μέσω αυτής της σύνδεσης TCP. Πολλές εκκρεμείς αιτήσεις HTTP μπορούν να σταλούν σε μία σύνδεση TCP. Αυτό είναι ένα από τα βασικά πλεονεκτήματα με το HTTP/2 καθώς βελτιώνει τη δυνατότητα πολλαπλών ζεύγη αιτημάτων / απαντήσεων HTTP μέσω μιας σύνδεσης TCP, επιτρέποντας τη χρήση λιγότερου αριθμού συνδέσεων TCP σε σύγκριση με το HTTP 1.1. Μπορεί να αναφερθεί ότι το HTTP 1.1 περιλαμβάνει ένα χαρακτηριστικό που ονομάζεται “pipelining” που επιτρέπει κάποιο επίπεδο πολυπλεξίας, αλλά έχει σοβαρούς περιορισμούς και δεν είναι τόσο ικανό όσο το HTTP/2.[2]

Όπως αναφέρθηκε παραπάνω, το HTTP είναι ένα πρωτόκολλο απόκρισης αιτήματος. Ο πελάτης δηλαδή, στέλνει αιτήματα στον διακομιστή και ο διακομιστής στέλνει απαντήσεις. Σε μια κοινή περίπτωση χρήσης στο Διαδίκτυο σήμερα, ο πελάτης είναι πρόγραμμα περιήγησης ιστού και ο διακομιστής είναι διακομιστής ιστού που εκτελείται σε υπολογιστή σε ένα κέντρο δεδομένων(data center). Κατά τη ρύθμιση στο 5GC, ο πελάτης και ο διακομιστής είναι NF. Το σχήμα 4.4 απεικονίζει μια απλή ανταλλαγή HTTP.



Εικόνα 4.4: Απλή συναλλαγή HTTP [26]

Ο στόχος ενός αιτήματος HTTP ονομάζεται «πόρος». Ένας πόρος αντιπροσωπεύει κάτι που παρέχεται από το διακομιστή. Μπορεί να αντιπροσωπεύει πολλά πράγματα και δεν καθορίζεται με περισσότερες λεπτομέρειες από το πρωτόκολλο HTTP. Όταν πρόκειται για περιήγηση στον ιστό, ένας πόρος μπορεί, π.χ., να είναι ιστοσελίδα, έγγραφο ή φωτογραφία. Στο 3GPP 5GC, ένας πόρος μπορεί, για παράδειγμα, να είναι μια συνεδρία

PDU (για υπηρεσίες που παράγονται από SMF), μια σύνοδος πολιτικής (για υπηρεσίες που παράγονται από PCF) ή δεδομένα συνδρομής (για υπηρεσίες που παράγονται από την UDM). Κάθε πόρος προσδιορίζεται από ένα Uniform Resource Identifier (URI). Μια πολύ συνηθισμένη μορφή του URI είναι το Uniform Resource Locator (URL), το οποίο είναι ένας ειδικός τύπος URI που αναγνωρίζει έναν πόρο και παρέχει επίσης πληροφορίες σχετικά με τον τρόπο πρόσβασης σε αυτούς τους πόρους, π.χ. χρησιμοποιώντας ένα πρωτόκολλο όπως το HTTP.[2][26]

Στο 5GC, το URI στο μήνυμα αίτησης προσδιορίζει μοναδικά τον πόρο στον παραγωγό NF. Ένα απόλυτο URI για μια διεπαφή βάσει υπηρεσιών στο 5GC έχει την ακόλουθη δομή:

`{apiRoot}/{apiName}/{apiVersion}/{apiSpecificResourceUriPart}`

Θα περιγράψουμε εν συντομία κάθε μέρος του URI και θα δώσουμε ένα παράδειγμα για το 5G.

Το "apiRoot" είναι μια συνένωση πολλών τμημάτων:

- σχήμα ("http" ή "https")
- μια σταθερή συμβολοσειρά ": //"
- κεντρικός υπολογιστής και προαιρετική θύρα (η λεγόμενη «αρχή»)
- μια προαιρετική συμβολοσειρά ειδικά για ανάπτυξη (πρόθεμα API) που ξεκινά με χαρακτήρα "/"

Το "apiName" καθορίζει το όνομα του API και το "apiVersion" υποδεικνύει την έκδοση του API. Το "apiRoot", "apiName" και "apiVersion" ορίζουν μαζί το βασικό URI του API και έπειτα κάθε "apiSpecificResourceUriPart" καθορίζει ένα URI πόρου σε σχέση με αυτό το βασικό URI. Η δομή και το περιεχόμενο του apiSpecificResourceUriPart "διαφέρει ανάλογα με την υπηρεσία τύπου. Για παράδειγμα στο UDM, ο πελάτης NF στέλνει αιτήματα για "παρεχόμενους" πόρους, όπως δεδομένα συνδρομής, με ένα URI που περιλαμβάνει, π.χ., SUPI. Ένα παράδειγμα θα μπορούσε να μοιάζει με "https://udm1.operatorX.com/nudmsdm/v1/imsi-1234567890 / sm-data ", όπου το IMSI(ο μοναδικός αριθμός UE) σε αυτό το παράδειγμα είναι 1234567890".[2]

Αντίθετα, οι πόροι SMF και AMF δημιουργούνται δυναμικά κατά το χρόνο εκτέλεσης, π.χ. όταν δημιουργούνται οι καταχωρητές UE ή μια περίοδο σύνδεσης PDU. Συνεπώς, το URI δεν μπορεί να είναι τόσο στατικό όσο στο παράδειγμα UDM. Αντ' αυτού, ο παραγωγός NF (διακομιστής) επιστρέφει μια αναφορά πόρου στον καταναλωτή NF (πελάτης) στο πρώτο μήνυμα απάντησης. Επομένως, όταν ο καταναλωτής θέλει να αντιμετωπίσει αυτόν τον συγκεκριμένο πόρο (π.χ. PDU Session in SMF), χρησιμοποιείται ένα URI που περιλαμβάνει αυτήν την αναφορά πόρου. Ένα παράδειγμα θα μπορούσε να είναι "https://smf3.operatorY.com/nsmf- pdusession / v1 / sm-kontekss / 347c3edf-129a-276e-e4c7-c48e7b515605 ", όπου το τελευταίο μέρος είναι η αναφορά πόρου.[2]

Μετά τη λήψη ενός αιτήματος HTTP, ο διακομιστής, ο οποίος έχει πρόσβαση στον πόρο, αναλύει το αίτημα και ενδέχεται να εκτελεί λειτουργίες εκ μέρους του πελάτη και, στη συνέχεια, επιστρέφει ένα μήνυμα απόκρισης στον πελάτη. Η απάντηση περιλαμβάνει πληροφορίες κατάστασης για τη συναλλαγή και συνήθως περιέχει το ζητούμενο περιεχόμενο (αναπαράσταση του πόρου που ζητήθηκε).[2][26]

## Σχεδιασμός RESTful

Το 3GPP έχει ως στόχο να καθορίσει όλες τις υπηρεσίες στο 5GC σύμφωνα με το «πρότυπο» REST. Το “REST” (συντομογραφία για το “Representational State Transfer”) είναι ένα αρχιτεκτονικό “στυλ”(paradigm) λογισμικού που εισήγαγε ο Roy T. Fielding στη διατριβή του το 2000. Καθορίζει ένα σύνολο κανόνων σχεδιασμού λογισμικού για τον τρόπο σχεδίασης της διαλειτουργικότητας των συστημάτων υπολογιστών στο διαδίκτυο.

Οι υπηρεσίες RESTful web χρησιμοποιούν ένα ομοιόμορφο και προκαθορισμένο σύνολο “stateless”(που δεν λαμβάνει πληροφορίες κατάστασης διακομιστή) λειτουργιών για να επιτρέπουν στα συστήματα να έχουν πρόσβαση και να χειρίζονται τις αναπαραστάσεις κειμένου των πόρων που βασίζονται στον ιστό.[2][26]

Οι αρχές του RESTful design συνοψίζονται στην παρακάτω αρίθμηση, προσαρμοσμένη από τη μελέτη 3GPP που έγινε στο 3GPP TS 29.891. Στην πράξη, τα υπάρχοντα API που ισχυρίζονται ότι είναι RESTful ακολουθούν αυτές τις αρχές σε διαφορετικούς βαθμούς. Το ίδιο ισχύει και στο 3GPP. Μερικές από αυτές τις αρχές είναι:[26]

1. **Client/Server:** Αυτή αναφέρεται στον καταμερισμό ευθυνών μεταξύ πελάτη και διακομιστή όπου ένας πελάτης στέλνει ένα αίτημα σε έναν διακομιστή που επεξεργάζεται το αίτημα και επιστρέφει μια απάντηση
2. **Stateless:** Κάθε αίτημα από πελάτη σε διακομιστή πρέπει να περιέχει όλες τις απαραίτητες πληροφορίες για την κατανόηση του αιτήματος. Συνεπώς, η κατάσταση συνεδρίας διατηρείται αποκλειστικά στον πελάτη. Για παράδειγμα, ένα SMF θα έχει κατάσταση σχετικά με τις συνεδρίες PDU, το AMF θα έχει κατάσταση σχετικά με την κινητικότητα UE πλαίσιο, το PCF θα έχει κατάσταση σχετικά με ενεργές συνεδρίες πολιτικής κ.λπ.
3. **Cacheable:** Εάν μια απάντηση είναι προσωρινά αποθηκευμένη (cacheable), ο πελάτης μπορεί να αποθηκεύσει προσωρινά μια απόκριση και να χρησιμοποιήσει ξανά αυτά τα δεδομένα απόκρισης αργότερα, για ισοδύναμα αιτήματα.
4. **Uniform interface:** Μια διεπαφή βασισμένη σε REST στηρίζεται στην αναγνώριση πόρων και επιτρέπει τη χειραγώγηση πόρων μέσω αναπαραστάσεων αυτών των πόρων.
5. **Layered system:** Το σύστημα με επίπεδα αποτελείται από ιεραρχικά στρώματα με περιορισμό στη συμπεριφορά των συστατικών έτσι ώστε κάθε στοιχείο να μην μπορεί να “δει” πέρα από το άμεσο επίπεδο με το οποίο αλληλεπιδρούν.
6. **Code on Demand (optional):** Το REST επιτρέπει την επέκταση της λειτουργικότητας του πελάτη με τη λήψη και εκτέλεση κώδικα με τη μορφή μικροεφαρμογών ή σεναρίων.

### Γλώσσα ορισμού διεπαφής (Interface definition language, IDL)

Όταν ορίζονται HTTP APIs, είναι συνηθισμένο τα API να περιγράφονται χρησιμοποιώντας Interface Definition Language (IDL). Ένα IDL είναι μια γλώσσα προδιαγραφών που επιτρέπει την περιγραφή ενός API χρησιμοποιώντας τυπικούς κανόνες προκειμένου να έχει μια σαφή περιγραφή των πόρων, των λειτουργιών, των στοιχείων πληροφοριών, των δομών δεδομένων, των μορφών δεδομένων κ.λπ.[28]

Χρησιμοποιώντας ένα IDL για την επίσημη περιγραφή ενός API, συμβάλλει στην αποφυγή κάθε ασάφειας που μπορεί να προκύψει εάν τα αιτήματα και οι απαντήσεις HTTP θα περιγραφούν χρησιμοποιώντας απλά αγγλικά με λιγότερο τυπικούς κανόνες. Το όφελος με ένα IDL είναι επομένως ότι μπορούν να αποφευχθούν προβλήματα διαλειτουργικότητας, που προκαλούνται από διαφορετικούς προμηθευτές που ερμηνεύουν διαφορετικά το τυπικό κείμενο.[28]

Το IDL είναι ανεξάρτητο από τον προμηθευτή και τη γλώσσα προγραμματισμού υπολογιστών που χρησιμοποιείται για την εφαρμογή του API σε λογισμικό στα πραγματικά προϊόντα. Αυτό το καθιστά κατάλληλο για τον ορισμό ενός API και τις αλληλεπιδράσεις μεταξύ λογισμικού που έχουν γραφτεί από διαφορετικούς προμηθευτές και σε διαφορετικές γλώσσες προγραμματισμού. Δεδομένου ότι είναι μια επίσημη γλώσσα με συγκεκριμένες δομές, μπορεί επίσης να είναι ένα εργαλείο για την ανάπτυξη λογισμικού και στην πραγματικότητα χρησιμοποιείται για τη δημιουργία τμημάτων του κώδικα.[2][28]

Η προδιαγραφή OpenAPI είναι μια προδιαγραφή για τον τρόπο καθορισμού ενός API που είναι γραμμένο σε ένα αρχείο κειμένου αναγνώσιμο από τον άνθρωπο. Μπορεί να χρησιμοποιεί JSON ή YAML τύπους αρχείων για να εκφράσει τις προδιαγραφές API. Το 3GPP επέλεξε το YAML για τις προδιαγραφές των διεπαφών που βασίζονται στις υπηρεσίες, κυρίως επειδή το YAML είναι πιο εύκολο για έναν άνθρωπο να διαβάζει και να γράφει από ότι το JSON. Ωστόσο, οι προδιαγραφές OpenAPI σε YAML και JSON είναι ως επί το πλείστον ισοδύναμες.[28]

Η περιγραφή YAML μιας υπηρεσίας NF περιλαμβάνεται ως παράρτημα σε κάθε αντίστοιχο TS (π.χ. 3GPP TS 29.518 για υπηρεσίες AMF), καθώς και ένα ξεχωριστό αρχείο YAML που διανέμεται μαζί με το TS.[28]

Η χρήση REST μεθόδων θα βρεί σημαντική εφαρμογή στον τεμαχισμό δικτύου που αναμένεται να βοηθήσει κυρίως τους βιομηχανικούς πελάτες να ρυθμίζουν και να προσαρμόζουν το δίκτυο 5G που χρησιμοποιούν, ανάλογα με τις ανάγκες τους. Δηλαδή να έχουν απομακρυσμένο έλεγχο αλλά και κατά ζήτηση (on demand) των λειτουργιών που εκμεταλλεύονται από τους operators.[2]

### Ασφάλεια επιπέδου μεταφοράς (Transport layer security, TLS)

Το Transport Layer Security (TLS) είναι ένα κρυπτογραφικό πρωτόκολλο που στοχεύει στην παροχή ασφαλούς επικοινωνίας μέσω ενός δικτύου IP. Είναι ένα πολύ κοινό πρωτόκολλο σήμερα, δεδομένου ότι χρησιμοποιείται για την προστασία της επικοινωνίας HTTP μεταξύ προγραμμάτων περιήγησης και

διακομιστών ιστού. Όταν το HTTP προστατεύεται χρησιμοποιώντας το TLS, συνήθως αναφέρεται ως HTTPS (HTTP Secure).[26]

Το πρωτόκολλο TLS μπορεί να παρέχει κρυπτογράφηση και ακεραιότητα δεδομένων μεταξύ δύο επικοινωνιακών οντοτήτων και επίσης αμοιβαίο έλεγχο ταυτότητας των δύο τελικών σημείων. Είναι ανεξάρτητο πρωτόκολλο εφαρμογής, ώστε τα πρωτόκολλα υψηλότερου επιπέδου να μπορούν να εκτελούνται με διαφάνεια πάνω από το TLS.[26]

Το TLS καθορίζεται από το IETF και έχουν οριστεί πολλές αναθεωρήσεις του TLS. Η πρώτη έκδοση TLS 1.0 ορίστηκε το 1999 και βασίστηκε σε προηγούμενες εργασίες για το Secure Socket Layer (SSL). Το TLS 1.1 κυκλοφόρησε τότε το 2006. Μια κοινή έκδοση TLS που χρησιμοποιείται στο Διαδίκτυο σήμερα είναι το TLS 1.2 (ορίζεται στο IETF RFC 5246 από το 2008), αλλά η υποστήριξη για το TLS 1.3 (ορίζεται στο IETF RFC 8446 από το 2018) αρχίζει να γίνεται πιο συνηθισμένο. Το TLS που χρησιμοποιείται στο 5G για την προστασία των διεπαφών βασίζονται σε HTTP.[26]

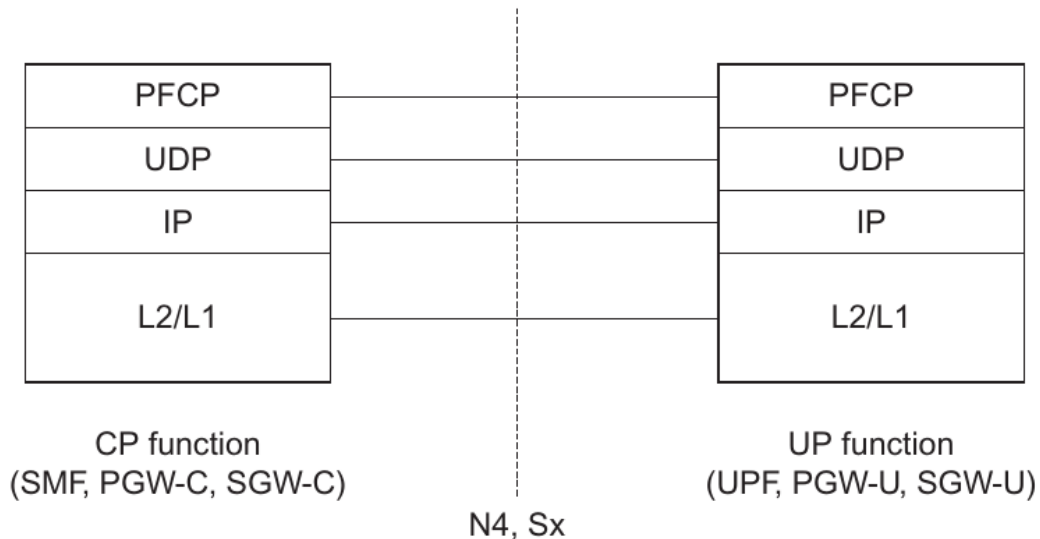
Το 3GPP επιτρέπει τη χρήση των TLS 1.1, TLS 1.2 και TLS 1.3, παρόλο που δεν συνιστάται η χρήση του TLS 1.1. Το TLS αποτελείται από δύο κύρια συστατικά:

- Ένα πρωτόκολλο χειραφίας TLS που επικυρώνει τα δύο τελικά σημεία. Αυτό το στοιχείο διαπραγματεύεται επίσης κρυπτογραφικές παραμέτρους και δημιουργεί το βασικό υλικό. Το πρωτόκολλο χειραφίας έχει σχεδιαστεί για να είναι ανθεκτικό σε επιθέσεις, δηλαδή, ένας εισβολέας δεν πρέπει να μπορεί να επηρεάσει τη διαπραγμάτευση ασφάλειας μεταξύ των δύο τελικών σημείων.[2][26]
- Ένα πρωτόκολλο εγγραφής TLS που χρησιμοποιεί τις παραμέτρους που καθορίζονται από το πρωτόκολλο χειραφίας για την προστασία της κίνησης μεταξύ των τελικών σημείων. Το πρωτόκολλο εγγραφής χωρίζει την κίνηση δεδομένων σε μια σειρά εγγραφών. Καθεμία από αυτές τις εγγραφές προστατεύεται στη συνέχεια χρησιμοποιώντας τα κλειδιά που έχουν δημιουργηθεί κατά τη φάση χειραφίας.[2][26]

#### 4.1.4 Πρωτόκολλο ελέγχου προώθησης πακέτων (Packet forwarding control protocol, PFCP)

Το πρωτόκολλο ελέγχου προώθησης πακέτων (PFCP) χρησιμοποιείται πάνω από το σημείο αναφοράς N4 μεταξύ SMF και UPF για τον έλεγχο του UPF. Το PFCP ορίστηκε για το EPC όταν ο διαχωρισμός CP-UP του SGW και PGW εισήχθη στην έκδοση 14 της 3GPP και στην περίπτωση αυτή το σημείο αναφοράς μεταξύ SGW-C / PGW-C και SGW-U / PGW-U αναφέρεται ως Sx. Ένας από τους σχεδιαστικούς στόχους αυτού του έργου ήταν να ορίσει ένα πρωτόκολλο που θα ήταν ανθεκτικό στο μέλλον και θα μπορούσε να επαναχρησιμοποιηθεί και έτσι όταν ανατέθηκε η εργασία του 5G στο 3GPP, αποφασίστηκε να επαναχρησιμοποιηθεί το ίδιο πρωτόκολλο και για τη N4. Ωστόσο, το PFCP έχει εξελιχθεί για να πληροί τις απαιτήσεις 5GS, π.χ. για να υποστηρίξει Ethernet PDU Session type που δεν ήταν διαθέσιμος εκείνη τη στιγμή στο EPS.[14][29]

Το PFCP καθορίζεται στο 3GPP TS 29.244. Τρέχει πάνω από το UDP και ο αριθμός θύρας προορισμού UDP για ένα μήνυμα PFCP Request είναι ο 8805. Η στοίβα πρωτοκόλλου Control Plane απεικονίζεται στο σχήμα παρακάτω. Επίσης, είναι δυνατή η μεταφορά πακέτων επιπέδου χρήστη μεταξύ SMF και UPF μέσω του σημείου αναφοράς N4.[29]



Εικόνα 4.5: Στοίβα πρωτοκόλλου PFCP επιπέδου ελέγχου [29]

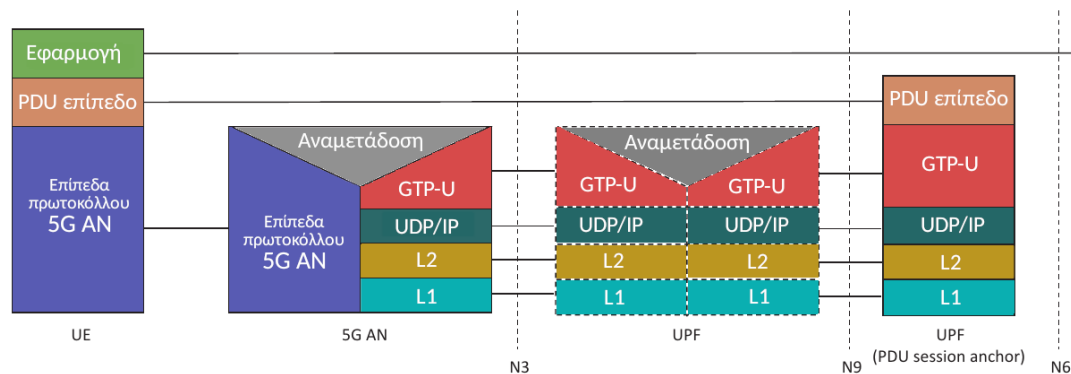
Υπάρχουν δύο τύποι διαδικασιών PFCP (και σχετικά μηνύματα). **Διαδικασίες που σχετίζονται με κόμβο** και **διαδικασίες που σχετίζονται με την περίοδο σύνδεσης**. Οι διαδικασίες που σχετίζονται με τον κόμβο χρησιμοποιούνται για τη δημιουργία συσχέτισης σε επίπεδο κόμβου μεταξύ της λειτουργίας CP (SMF) και της λειτουργίας UP (UPF) και για την επικοινωνία πληροφοριών επιπέδου κόμβου μεταξύ των λειτουργιών CP και UP. Οι διαδικασίες που σχετίζονται με την περίοδο σύνδεσης χρησιμοποιούνται για τη διαχείριση των συνεδριών PFCP που αντιστοιχούν σε μεμονωμένες συνεδρίες PDU.[29]

#### 4.1.5 GPRS Tunneling Protocol για User Plane (GTP-U)

Στην παράγραφο αυτή θα αναφερθούμε σε ένα πρωτόκολλο που χρησιμοποιήθηκε και σε τηλεπικοινωνιακά συστήματα προηγούμενης γενιάς, το GPRS πρωτόκολλο σήραγγας (GPRS Tunneling Protocol, GTP). Το GTP γενικότερα είναι μία ομάδα πρωτοκόλλων επικοινωνίας που βασίζονται σε IP και χρησιμοποιούνται για τη μεταφορά γενικών πακέτων ραδιοπηρεσιών (General Packet Radio Service, GPRS) σε δίκτυα GSM, UMTS και LTE. Μεγαλύτερο ενδιαφέρον στο 5G αποκτά το GTP-U μέρος αυτού του πρωτοκόλλου καθώς αξιοποιείται στη μετάδοση πακέτων που διακινούνται με τη βοήθεια του επιπέδου χρήστη.

Τα δύο κύρια συστατικά, λοιπόν, του GTP είναι το τμήμα Control Plane του GTP (GTP-C) και το τμήμα User Plane του GTP (GTP-U). Το GTP-C είναι το πρωτόκολλο ελέγχου που χρησιμοποιείται στα 3G / GPRS και 4G / EPS για τον έλεγχο και τη διαχείριση των συνδέσεων PDN και των σηράγγων User

Plane που δημιουργούν τη διαδρομή User Plane. Το GTP-U χρησιμοποιεί έναν μηχανισμό σήραγγας για τη μεταφορά της κίνησης δεδομένων των χρηστών και διασχίζει τη μεταφορά UDP.



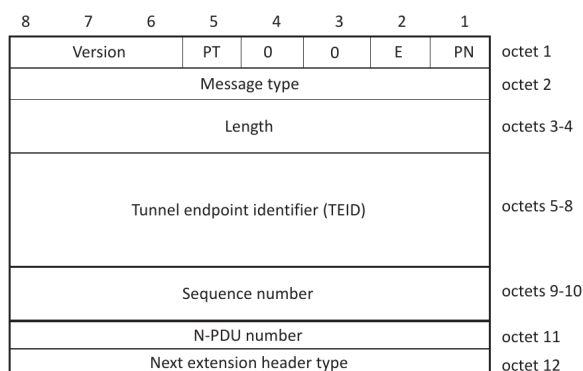
Εικόνα 4.6: Στοιβία πρωτοκόλλου επιπέδου χρήστη για PDU συνεδρία [27]

Στο 5GS, το GTP-U έχει επαναχρησιμοποιηθεί για να μεταφέρει δεδομένα User Plane μέσω των διεπαφών N3 και N9 (και N4), αλλά το πρωτόκολλο ελέγχου για τη διαχείριση των ταυτοτήτων της σήραγγας κ.λπ. χρησιμοποιεί αντ' αυτού HTTP / 2 και NGAP, τα οποία περιγράφηκαν παραπάνω. Το GTP-C χρησιμοποιείται μόνο όταν το 5GC συνεργάζεται με το EPC. Εδώ θα περιγράψουμε λοιπόν μόνο το GTP-U.[27][31]

Οι σήραγγες GTP-U χρησιμοποιούνται μεταξύ δύο αντίστοιχων κόμβων GTP-U για το διαχωρισμό της κίνησης σε διαφορετικές ροές επικοινωνίας. Ένα τοπικό Tunnel Endpoint Identifier (TEID), η διεύθυνση IP και η θύρα UDP προσδιορίζουν μοναδικά ένα τελικό σημείο σήραγγας σε κάθε κόμβο, όπου το TEID που έχει εκχωρηθεί από την οντότητα λήψης πρέπει να χρησιμοποιηθεί για την επικοινωνία.[31]

Στο 5GC, οι σήραγγες GTP-U δημιουργούνται παρέχοντας GTP-U TEIDs και διευθύνσεις IP μεταξύ (R) AN και SMF. Αυτή η σηματοδότηση μεταφέρεται με HTTP / 2 μεταξύ SMF και AMF και με NGAP μεταξύ AMF και (R) AN. Επομένως, δεν υπάρχει χρήση του GTP-C στο 5GC για τη διαχείριση των σηράγγων GTP-U. Η στοιβία πρωτοκόλλου επιπέδου χρήστη για μια συνεδρία PDU φαίνεται στο σχήμα 4.6.[27][31]

Μια διαδρομή GTP αναγνωρίζεται σε κάθε κόμβο με διεύθυνση IP και αριθμό θύρας UDP. Μια διαδρομή μπορεί να χρησιμοποιηθεί για πολλαπλές σήραγγες GTP και μπορεί να υπάρχουν πολλαπλές διαδρομές μεταξύ δύο οντοτήτων που υποστηρίζουν GTP. Το TEID που υπάρχει στην κεφαλίδα GTP-U υποδεικνύει σε ποια σήραγγα ανήκει ένα συγκεκριμένο ωφέλιμο φορτίο(payload). Έτσι, τα πακέτα πολυπλέκονται και αποπλέκονται από το GTP-U μεταξύ ενός δεδομένου ζεύγους Tunnel Endpoints. Η κεφαλίδα GTP-



Εικόνα 4.7: Κεφαλίδα GTP-U[27]

Η κεφαλίδα GTP-U αποτελείται από 12 οκτάδες. Οι οκτάδες 1-2 περιέχουν πληροφορίες σχετικά με την έκδοση, τον τύπο μηνύματος, το μήκος και τον προορισμό. Οι οκτάδες 3-4 περιέχουν το μήκος της σήραγγας. Οι οκτάδες 5-8 περιέχουν τον Tunnel Endpoint Identifier (TEID). Οι οκτάδες 9-10 περιέχουν τον αριθμό της ακολουθίας. Η οκτάδα 11 περιέχουν τον αριθμό της PDU και η οκτάδα 12 περιέχουν τον τύπο της επόμενης κεφαλίδας επέκτασης.



U φαίνεται στο σχήμα 4.7. Το πρωτόκολλο GTP-U ορίζεται στο 3GPP TS 29.281.[27][31]

#### 4.1.6 Επεκτάσιμο πρωτόκολλο ελέγχου ταυτότητας (Extensible Authentication Protocol, EAP)

Το Extensible Authentication Protocol (EAP) είναι ένα πλαίσιο πρωτοκόλλου για την εκτέλεση ελέγχου ταυτότητας, συνήθως μεταξύ ενός UE και ενός δικτύου. Εισήχθη για πρώτη φορά στο IETF για το πρωτόκολλο Point-to-Point (PPP) προκειμένου να επιτρέψει τη χρήση πρόσθετων μεθόδων ελέγχου ταυτότητας μέσω του PPP. Από τότε έχει εισαχθεί και σε πολλά άλλα σενάρια, όπως για παράδειγμα ως πρωτόκολλο ελέγχου ταυτότητας για το Internet key exchange (IKEv2), καθώς και για έλεγχο ταυτότητας σε ασύρματα LAN χρησιμοποιώντας τις επεκτάσεις IEEE 802.11i και 802.1x.[31]

Το EAP είναι επεκτάσιμο υπό την έννοια ότι υποστηρίζει πολλαπλά πρωτόκολλα ελέγχου ταυτότητας και επιτρέπει τον καθορισμό νέων πρωτοκόλλων ελέγχου ταυτότητας εντός του πλαισίου EAP. Το EAP δεν είναι από μόνο του μια μέθοδο ελέγχου ταυτότητας, αλλά ένα κοινό πλαίσιο ελέγχου ταυτότητας που μπορεί να χρησιμοποιηθεί για την εφαρμογή συγκεκριμένων μεθόδων ελέγχου ταυτότητας. Αυτές οι μέθοδοι ελέγχου ταυτότητας αναφέρονται συνήθως ως μέθοδοι EAP.[31]

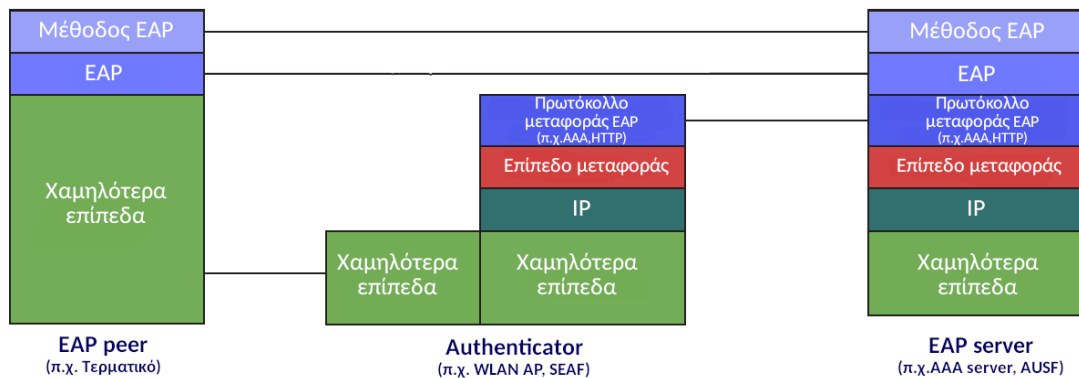
Το βασικό πρωτόκολλο EAP καθορίζεται στο IETF RFC 3748. Περιγράφει τη μορφή πακέτου EAP καθώς και βασικές λειτουργίες όπως η διαπραγμάτευση του επιθυμητού μηχανισμού ελέγχου ταυτότητας. Προσδιορίζει επίσης μερικές απλές μεθόδους ελέγχου ταυτότητας, για παράδειγμα με βάση κωδικούς μίας χρήσης καθώς και έλεγχο ταυτότητας πρόκλησης. Είναι δυνατό να οριστούν πρόσθετες μέθοδοι EAP εκτός από αυτές που ορίζονται στο IETF RFC 3748. Τέτοιες μέθοδοι EAP μπορεί να εφαρμόσουν άλλους μηχανισμούς ελέγχου ταυτότητας ή / και να χρησιμοποιήσουν άλλα διαπιστευτήρια όπως πιστοποιητικά δημόσιου κλειδιού ή κάρτες (U)SIM.[31]

Μερικές από τις μεθόδους EAP που τυποποιούνται από το IETF περιγράφονται εν συντομία παρακάτω:

- ▷ Το EAP-TLS βασίζεται στο TLS και ορίζει μια μέθοδο EAP για τον έλεγχο ταυτότητας και την παραγωγή κλειδιών βάσει πιστοποιητικών δημόσιου κλειδιού. Το EAP-TLS καθορίζεται στο IETF RFC 5216.
- ▷ Το EAP-AKA έχει οριστεί για έλεγχο ταυτότητας και δημιουργία κλειδιού χρησιμοποιώντας την κάρτα SIM UMTS και βασίζεται στη διαδικασία UMTS AKA. Το EAP-AKA καθορίζεται στο IETF RFC 4187.
- ▷ Το EAP-AKA0 είναι μια μικρή αναθεώρηση του EAP-AKA που παρέχει βελτιωμένο διαχωρισμό κλειδιών μεταξύ των κλειδιών που δημιουργούνται για διαφορετικά δίκτυα πρόσβασης. Το EAP-AKA0 ορίζεται στο IETF RFC 5448.

Εκτός από τις τυποποιημένες μεθόδους, υπάρχουν επίσης ιδιόκτητες μέθοδοι EAP που έχουν αναπτυχθεί, π.χ. σε εταιρικά δίκτυα WLAN. Το 5GS κάνει

εκτεταμένη χρήση του EAP-AKA0 για έλεγχο ταυτότητας τόσο σε προσβάσεις 3GPP όσο και σε πρόσβαση εκτός 3GPP.[2][31]



Εικόνα 4.8: Στοιβία πρωτοκόλλου EAP [2]

Η αρχιτεκτονική για το πρωτόκολλο EAP διακρίνει τρεις διαφορετικές οντότητες:

- I. **Η ζεύξη (peer) του EAP.** Αυτή είναι η οντότητα που ζητά πρόσβαση στο δίκτυο, συνήθως UE. Για χρήση EAP σε WLAN, και είναι επίσης γνωστή ως “supplicant”.
- II. **Ο επικυρωτής(authenticator).** Αυτός είναι ο φορέας που εκτελεί έλεγχο πρόσβασης, όπως το σημείο πρόσβασης SEAF ή WLAN ή ένα ePDG.
- III. **Ο διακομιστής(server) EAP.** Αυτός είναι ο διακομιστής ελέγχου ταυτότητας back-end που παρέχει υπηρεσία ελέγχου ταυτότητας στον έλεγχο ταυτότητας. Σε 5GS είναι το AUSF. Η αρχιτεκτονική πρωτοκόλλου EAP απεικονίζεται στο σχήμα 4.8.[2][31]

Η επικοινωνία EAP μεταξύ του peer και του server είναι κατα βάση διαφανής στον έλεγχο ταυτότητας (SEAF in 5GS). Επομένως, ο έλεγχος ταυτότητας δεν χρειάζεται να υποστηρίζει τη συγκεκριμένη μέθοδο EAP που χρησιμοποιείται, αλλά χρειάζεται μόνο για την προώθηση των μηνυμάτων EAP μεταξύ του peer και του διακομιστή EAP (AUSF σε 5GS).[2]

#### 4.1.7 IP security (IPSec)

Το IPsec είναι ένα πολύ ευρύ θέμα και έχουν γραφτεί πολλά βιβλία για αυτό. Για το λόγο αυτό, θα δώσουμε μια εισαγωγή υψηλού επιπέδου στις βασικές έννοιες του IPsec που εστιάζουν στα μέρη του IPsec που χρησιμοποιούνται στο 5GS.

Το IPsec παρέχει υπηρεσίες ασφαλείας τόσο για IPv4 όσο και για IPv6. Λειτουργεί στο επίπεδο IP, προσφέρει προστασία της κυκλοφορίας που τρέχει πάνω από το επίπεδο IP και μπορεί επίσης να χρησιμοποιηθεί για την προστασία των πληροφοριών κεφαλίδας IP στο επίπεδο IP. Το 5GS χρησιμοποιεί IPsec για την ασφαλή επικοινωνία σε διάφορες διεπαφές, σε ορισμένες περιπτώσεις μεταξύ κόμβων στο κεντρικό δίκτυο και σε άλλες περιπτώσεις μεταξύ του UE και του κεντρικού δικτύου. Για παράδειγμα, το

IPsec χρησιμοποιείται για την προστασία της κυκλοφορίας στο κεντρικό δίκτυο ως μέρος του πλαισίου NDS / IP. Το IPsec χρησιμοποιείται επίσης μεταξύ του UE και του N3IWF για την προστασία της σηματοδότησης NAS και της κυκλοφορίας επιπέδου χρήστη.[14][30]

Η αρχιτεκτονική ασφαλείας IPsec ορίζεται στο IETF RFC 4301. Το σύνολο των υπηρεσιών ασφαλείας που παρέχονται από το IPsec περιλαμβάνουν:

- Έλεγχο πρόσβασης
- Έλεγχο ταυτότητας προέλευσης δεδομένων
- Ακεραιότητα χωρίς σύνδεση
- Ανίχνευση και απόρριψη των επαναλήψεων
- Εμπιστευτικότητα
- Εμπιστευτικότητα περιορισμένης κυκλοφορίας.

Με τον έλεγχο πρόσβασης εννοούμε την υπηρεσία για την αποτροπή μη εξουσιοδοτημένης χρήσης ενός πόρου, όπως ένας συγκεκριμένος διακομιστής ή ένα συγκεκριμένο δίκτυο. Η υπηρεσία ελέγχου ταυτότητας προέλευσης δεδομένων επιτρέπει στον παραλήπτη των δεδομένων να επαληθεύσει την ταυτότητα του διεκδικούμενου αποστολέα των δεδομένων. Η ακεραιότητα χωρίς σύνδεση είναι η υπηρεσία που διασφαλίζει ότι ένας δέκτης μπορεί να ανιχνεύσει εάν τα ληφθέντα δεδομένα έχουν τροποποιηθεί στη διαδρομή από τον αποστολέα. Ωστόσο, δεν ανιχνεύει εάν τα πακέτα έχουν αναπαραχθεί (επαναληφθεί) ή αναδιαταχτεί. Ο έλεγχος ταυτότητας προέλευσης δεδομένων και η ακεραιότητα χωρίς σύνδεση χρησιμοποιούνται συνήθως μαζί. Η ανίχνευση και η απόρριψη των επαναλήψεων είναι μια μορφή μερικής ακεραιότητας ακολουθίας, όπου ο δέκτης μπορεί να ανιχνεύσει εάν ένα πακέτο έχει αναπαραχθεί. Η εμπιστευτικότητα είναι η υπηρεσία που προστατεύει την κυκλοφορία από την ανάγνωση μη εξουσιοδοτημένων μερών. Ο μηχανισμός για την επίτευξη της εμπιστευτικότητας με το IPsec είναι η κρυπτογράφηση, όπου το περιεχόμενο των πακέτων IP μεταμορφώνεται χρησιμοποιώντας έναν αλγόριθμο κρυπτογράφησης έτσι ώστε να γίνεται ακατανόητο. Η εμπιστευτικότητα περιορισμένης ροής κυκλοφορίας είναι μια υπηρεσία σύμφωνα με την οποία το IPsec μπορεί να χρησιμοποιηθεί για την προστασία ορισμένων πληροφοριών σχετικά με τα χαρακτηριστικά της ροής της κυκλοφορίας, π.χ., διευθύνσεις πηγής και προορισμού, μήκος μηνύματος ή συχνότητα μήκους πακέτων.[14]

Το IPsec ορίζει δύο πρωτόκολλα για την προστασία δεδομένων, το Encapsulated Security Payload (ESP) και το Authentication Header (AH). Το πρωτόκολλο ESP ορίζεται στο IETF RFC 4303 και το AH στο IETF RFC 4302, και τα δύο από το 2005.

Το ESP παρέχει ακεραιότητα και εμπιστευτικότητα, ενώ το AH παρέχει ακεραιότητα μόνο. Μια άλλη διαφορά είναι ότι το ESP προστατεύει μόνο το περιεχόμενο του πακέτου IP (συμπεριλαμβανομένης της κεφαλίδας ESP και μέρους του τρέιλερ ESP), ενώ το AH προστατεύει το πλήρες πακέτο IP, συμπεριλαμβανομένης της κεφαλίδας IP και της κεφαλίδας AH.

Τα ESP και AH χρησιμοποιούνται συνήθως ξεχωριστά, αλλά είναι δυνατόν, αν και δεν είναι συνηθισμένο, να χρησιμοποιούνται μαζί και τότε το ESP χρησιμοποιείται συνήθως για εμπιστευτικότητα και το AH για προστασία ακεραιότητας.[14][30]

### 4.1.8 Πρωτόκολλο ελέγχου ροής μετάδοσης (Stream Control Transmission Protocol, SCTP)

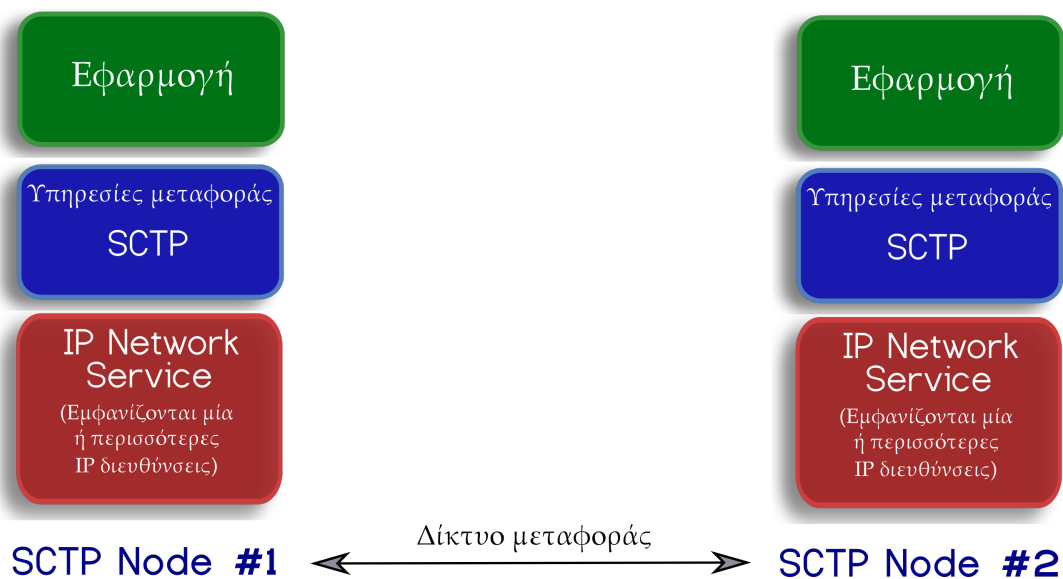
Το Πρωτόκολλο ελέγχου ροής μετάδοσης (Stream Control Transmission Protocol, SCTP) είναι ένα πρωτόκολλο μεταφοράς, που λειτουργεί σε ισοδύναμο επίπεδο στη στοίβα ως UDP (User Datagram Protocol) και TCP. Σε σύγκριση με το TCP και το UDP, το SCTP είναι πιο πλούσιο σε λειτουργικότητα και επίσης πιο ανεκτικό απέναντι σε αστοχίες δικτύου. Παρόλο που τόσο το TCP όσο και το UDP χρησιμοποιούνται ως πρωτόκολλα μεταφοράς στο 5GS, δεν θα τα περιγράψουμε στα πλαίσια αυτής της εργασίας υποθέτοντας ότι οι περισσότεροι αναγνώστες έχουν μια βασική κατανόηση αυτών των πρωτοκόλλων. Το SCTP, από την άλλη πλευρά, χρησιμοποιείται ως πρωτόκολλο μεταφοράς μέσω της διεπαφής N2, είναι ένα λιγότερο γνωστό πρωτόκολλο μεταφοράς και επομένως παρουσιάζεται εν συντομία σε αυτήν την ενότητα.[2]

Σε σύγκριση με το UDP από το 1980 και το TCP από το 1981, το SCTP είναι ένα μάλλον νέο πρωτόκολλο. Η αρχική έκδοση καθορίστηκε στο IETF RFC 2960 το 2000, αλλά έκτοτε έχει ξεπεραστεί από μια νέα έκδοση στο IETF RFC 4960 από το 2007. Το κίνητρο για το σχεδιασμό του SCTP ήταν να ξεπεραστούν ορισμένοι περιορισμοί και ζητήματα του TCP που είναι ιδιαίτερα γνωστά στα τηλεπικοινωνιακά περιβάλλοντα. Αυτοί οι περιορισμοί καθώς και ομοιότητες και διαφορές μεταξύ UDP / TCP και SCTP, παρουσιάζονται και στον πίνακα παρακάτω.[13]

Το SCTP μοιράζεται πολλές βασικές δυνατότητες με UDP ή TCP. Το SCTP παρέχει (παρόμοια με το TCP και σε αντίθεση με το UDP) αξιόπιστη μεταφορά διασφαλίζοντας ότι τα δεδομένα φτάνουν στον προορισμό χωρίς σφάλμα. Επίσης, όμοια με το TCP και σε αντίθεση με το UDP, το SCTP είναι ένα πρωτόκολλο προσανατολισμένο στη σύνδεση, που σημαίνει ότι όλα τα δεδομένα μεταξύ δύο τελικών σημείων SCTP μεταφέρονται ως μέρος μιας περιόδου σύνδεσης (ή συσχέτισης(association), όπως καλείται από το SCTP).[2]

Η συσχέτιση SCTP πρέπει να εγκαθιδρυθεί μεταξύ των τελικών σημείων προτού πραγματοποιηθεί οποιαδήποτε μεταφορά δεδομένων. Με το TCP, η περίοδος λειτουργίας ρυθμίζεται χρησιμοποιώντας μια ανταλλαγή μηνυμάτων τριών κατευθύνσεων μεταξύ των δύο τελικών σημείων. Ένα ζήτημα με τη ρύθμιση περιόδου λειτουργίας TCP είναι ότι είναι ευάλωτο σε λεγόμενες επιθέσεις πλημμύρας SYN που μπορεί να προκαλέσουν υπερφόρτωση του διακομιστή TCP. Το SCTP έχει λύσει αυτό το πρόβλημα χρησιμοποιώντας μια ανταλλαγή μηνυμάτων τεσσάρων κατευθύνσεων για τη ρύθμιση συσχέτισης, συμπεριλαμβανομένης της χρήσης ενός ειδικού «cookie» που προσδιορίζει τον συσχετισμό. Αυτό καθιστά τη ρύθμιση συσχέτισης SCTP κάπως πιο περίπλοκη, αλλά φέρνει επιπλέον αντοχή σε αυτούς τους τύπους επιθέσεων. Μια συσχέτιση SCTP, καθώς και η θέση του SCTP στη στοίβα πρωτοκόλλου, απεικονίζεται στο σχήμα 4.9. Όπως μπορούμε να διακρίνουμε, ένας συσχετισμός SCTP μπορεί να χρησιμοποιεί πολλαπλές διευθύνσεις IP σε κάθε τελικό σημείο.[13]

Όπως και το TCP, το SCTP είναι προσαρμοσμένο στα ποσοστά. Αυτό σημαίνει ότι θα μειώσει ή θα αυξήσει δυναμικά το ρυθμό μεταφοράς δεδομένων, ανάλογα με τις συνθήκες συμφόρησης στο δίκτυο. Οι μηχανισμοί



Εικόνα 4.9: Συσχέτιση SCTP [2]

προσαρμογής ρυθμού μιας περιόδου σύνδεσης SCTP έχουν σχεδιαστεί για να συμπεριφέρονται συνεργατικά με συνεδρίες TCP που προσπαθούν να χρησιμοποιήσουν το ίδιο εύρος ζώνης.[2]

Όμοια με το UDP, το SCTP είναι προσανατολισμένο στα μηνύματα, πράγμα που σημαίνει ότι το SCTP διατηρεί τα όρια των μηνυμάτων και παραδίδει πλήρη μηνύματα (που ονομάζονται “chunks” από το SCTP). Το TCP, από την άλλη πλευρά, είναι προσανατολισμένο σε byte με την έννοια ότι παρέχει τη μεταφορά μιας ροής byte χωρίς οποιαδήποτε έννοια των ξεχωριστών μηνυμάτων εντός αυτής της ροής byte. Αυτό είναι επιθυμητό για παράδοση, για παράδειγμα, ενός αρχείου δεδομένων ή μιας ιστοσελίδας, αλλά μπορεί να μην είναι βέλτιστο για τη μεταφορά ξεχωριστών μηνυμάτων. Έτσι, εάν μια εφαρμογή στέλνει ένα μήνυμα X bytes και άλλο μήνυμα Y bytes μέσω TCP συνεδρίας, τα μηνύματα θα λαμβάνονται ως μία ροή bytes X + Y στο τέλος λήψης. Οι εφαρμογές που χρησιμοποιούν TCP πρέπει συνεπώς να προσθέσουν τη δική τους σήμανση εγγραφής για να διαχωρίσουν τα μηνύματά τους. Απαιτείται επίσης ειδικός χειρισμός για να διασφαλιστεί ότι τα μηνύματα γίνονται “flushed out” από το buffer αποστολής έτσι ώστε να διασφαλιστεί ότι ένα πλήρες μήνυμα μεταφέρεται σε εύλογο χρόνο. Αυτό συμβαίνει διότι το TCP περιμένει κανονικά το buffer αποστολής να υπερβεί ένα συγκεκριμένο μέγεθος πριν από την αποστολή δεδομένων και κατά συνέπεια μπορεί να δημιουργήσει σημαντικές καθυστερήσεις εάν οι δύο πλευρές ανταλλάσσουν σύντομα μηνύματα και πρέπει να περιμένουν την απάντηση πριν συνεχίσουν.[2][13]

Μια σύγκριση μεταξύ SCTP, TCP και UDP παρέχεται στον Πίνακα 4.1. Περισσότερες λεπτομέρειες σχετικά με το multi-streaming και το multi-homing παρέχονται παρακάτω.[2]

	SCTP	TCP	UDP
Προσανατολισμός στη σύνδεση	NAI	NAI	OXI
Αξιόπιστη Μετάδοση	NAI	NAI	OXI
Διατήρηση ορίων μηνύματος	NAI	OXI	NAI
Παράδοση με παραγγελία	NAI	NAI	OXI
Παράδοση χωρίς παραγγελία	NAI	OXI	NAI
Checksum δεδομένων	NAI(32-bit)	NAI(16-bit)	NAI(16-bit)
Έλεγχος ροής και συμφόρησης	NAI	NAI	OXI
Πολλές ροές εντός μιας περιόδου σύνδεσης	NAI	OXI	OXI
Υποστήριξη multi-homing	NAI	OXI	OXI
Προστασία απο επιθέσεις SYN flooding	NAI	OXI	OXI

Πίνακας 4.1: Σύγκριση πρωτοκόλλων μετάδοσης [2]

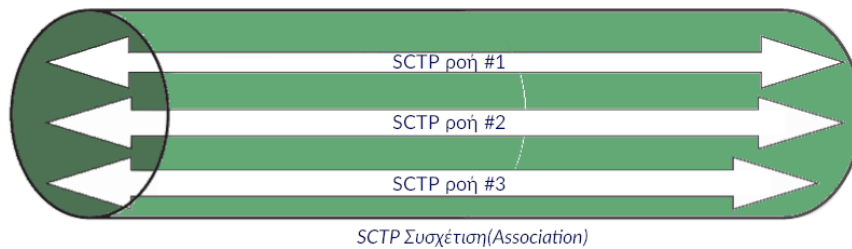
### Πολλαπλές Ροές (Multi-streaming)

Το TCP παρέχει αξιόπιστη μεταφορά και αυστηρή παράδοση δεδομένων κατά την μετάδοση δεδομένων, ενώ το UDP δεν παρέχει αξιόπιστη μεταφορά ή αυστηρή παράδοση της μετάδοσης. Ορισμένες εφαρμογές χρειάζονται αξιόπιστη μεταφορά, αλλά είναι ικανοποιημένοι με μόνο μερική παραγγελία των δεδομένων και άλλες εφαρμογές θα ήθελαν αξιόπιστη μεταφορά αλλά δεν χρειάζονται συντήρηση ακολουθίας. Για παράδειγμα, στην τηλεφωνία, είναι απαραίτητο μόνο να διατηρηθεί η σειρά των μηνυμάτων που επηρεάζουν τον ίδιο πόρο (π.χ. την ίδια κλήση). Άλλα μηνύματα συσχετίζονται ήπια και μπορούν να παραδοθούν χωρίς να χρειάζεται να διατηρηθεί μια πλήρη σειρά ακολουθίας για ολόκληρη τη συνεδρία. Σε αυτές τις περιπτώσεις, το λεγόμενο μπλοκάρισμα head-of-line που προκαλείται από το TCP μπορεί να οδηγήσει σε περιττή καθυστέρηση. Το μπλοκάρισμα head-of-line συμβαίνει, για παράδειγμα, όταν το πρώτο μήνυμα ή τμήμα χάθηκε για κάποιο λόγο. Σε αυτήν την περίπτωση τα επόμενα πακέτα ενδέχεται να έχουν παραδοθεί με επιτυχία στον προορισμό, αλλά το επίπεδο TCP στην πλευρά λήψης δεν θα παραδώσει τα πακέτα στα ανώτερα στρώματα έως ότου αποκατασταθεί η σειρά ακολουθίας.[2][13]

Το SCTP επιλύει αυτό το πρόβλημα εφαρμόζοντας μια λειτουργία πολλαπλών ροών (το όνομα Πρωτόκολλο μετάδοσης ελέγχου ροής προέρχεται από αυτήν τη δυνατότητα). Αυτή η δυνατότητα επιτρέπει στα δεδομένα να διαιρευθούν σε πολλές ροές που μπορούν να παραδοθούν με ανεξάρτητο έλεγχο ακολουθίας μηνυμάτων. Η απώλεια μηνύματος σε μία ροή θα επηρεάσει τότε μόνο τη ροή όπου συνέβη η απώλεια μηνύματος (τουλάχιστον αρχικά), ενώ όλες οι άλλες ροές μπορούν να συνεχίσουν να ρέουν. Οι ροές παραδίδονται εντός του ίδιου συσχετισμού SCTP και επομένως υπόκεινται στον ίδιο ρυθμό και έλεγχο συμφόρησης. Έτσι, η επιβάρυνση που προκαλείται από το σήμα SCTP ελέγχου μειώνεται σημαντικά.[2][13]

Η πολλαπλή ροή εφαρμόζεται στο SCTP αποσυνδέοντας την αξιόπιστη μεταφορά δεδομένων από την αυστηρή σειρά μετάδοσης των δεδομένων. Αυτό διαφέρει από το TCP, όπου οι δύο έννοιες είναι συνδεδεμένες. Στο SCTP, χρησιμοποιούνται δύο τύποι αριθμών ακολουθίας.

Ο αριθμός ακολουθίας μεταφοράς χρησιμοποιείται για τον εντοπισμό απώλειας πακέτων και τον έλεγχο των αναμεταδόσεων. Σε κάθε ροή, το SCTP εκχωρεί έπειτα έναν επιπλέον αριθμό ακολουθίας, τον αριθμό ακολουθίας



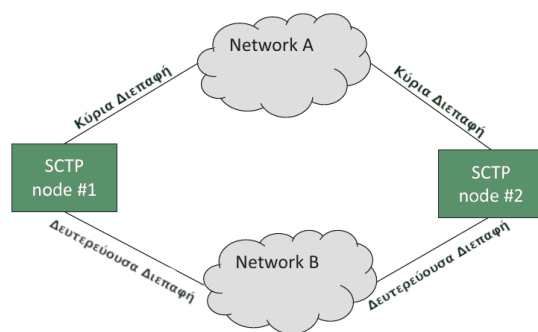
Εικόνα 4.10: Multistreaming με SCTP [2]

ροής. Οι αριθμοί ακολουθίας ροής καθορίζουν την ακολουθία παράδοσης δεδομένων σε κάθε ανεξάρτητη ροή και χρησιμοποιούνται από τον παραλήπτη για την παράδοση των πακέτων σε σειρά ακολουθίας για κάθε ροή.[2][13]

Το SCTP καθιστά επίσης δυνατή την πλήρη παράκαμψη της αλληλουχίας της υπηρεσίας παράδοσης, έτσι ώστε τα μηνύματα να παραδίδονται στον χρήστη του SCTP με την ίδια σειρά που φτάνουν επιτυχώς. Αυτό είναι χρήσιμο για εφαρμογές που απαιτούν αξιόπιστη μεταφορά, αλλά δεν χρειάζονται διαδοχική παράδοση ή έχουν τα δικά τους μέσα για τη διαχείριση της αλληλουχίας των ληφθέντων πακέτων.[2]

### Multi-homing

Μια άλλη βασική πτυχή του SCTP που είναι μια βελτίωση σε σύγκριση με το TCP είναι τα χαρακτηριστικά multihoming. Σε ένα δίκτυο τηλεπικοινωνιών, είναι πολύ σημαντικό να διατηρούνται αξιόπιστα μονοπάτια επικοινωνίας για να αποφεύγεται η διακοπή της υπηρεσίας και άλλα προβλήματα λόγω των βασικών προβλημάτων μετάδοσης δικτύου.



Εικόνα 4.11: Multi-homing με SCTP [2]

τον κόμβο απρόσιτο. Οι περιττές διαδρομές δικτύου και οι συνδέσεις δικτύου είναι συνεπώς δύο συστατικά σε ευρέως διαθέσιμα συστήματα τηλεπικοινωνιών.[2]

Μια περίοδος σύνδεσης TCP περιλαμβάνει μία μόνο διεύθυνση IP σε κάθε τελικό σημείο και εάν σε μία από αυτές τις διευθύνσεις IP δεν είναι δυνατή η πρόσβαση, η περίοδος λειτουργίας αποτυγχάνει. Είναι επομένως περίπλοκο να χρησιμοποιείται το TCP για να παρέχουμε ευρέως διαθέσιμη

Παρόλο που τα πρωτόκολλα δρομολόγησης IP θα μπορούσαν να βρουν εναλλακτικές διαδρομές σε περίπτωση αποτυχίας δικτύου, οι χρονικές καθυστερήσεις έως τη σύγκλιση του πρωτοκόλλου δρομολόγησης και η ανάγκη της συνδεσιμότητας είναι συνήθως μη αποδεκτές σε ένα δίκτυο τηλεπικοινωνιών. Επίσης, εάν ένας κόμβος δικτύου είναι μονής κατοικίας, δηλαδή έχει μόνο μία σύνδεση δικτύου, η αποτυχία αυτής της συγκεκριμένης σύνδεσης θα έκανε

δυνατότητα μεταφοράς δεδομένων χρησιμοποιώντας κεντρικούς υπολογιστές πολλαπλών οικιακών, δηλαδή, όπου τα τελικά σημεία είναι προσβάσιμα μέσω πολλαπλών διευθύνσεων IP. Το SCTP, από την άλλη πλευρά, έχει σχεδιαστεί για να χειρίζεται πολλούς κεντρικούς υπολογιστές και κάθε τελικό σημείο μιας συσχέτισης SCTP μπορεί να αναπαρασταθεί από πολλές διευθύνσεις IP. Αυτές οι διευθύνσεις IP μπορεί επίσης να οδηγήσουν σε διαφορετικές διαδρομές επικοινωνίας μεταξύ των τελικών σημείων SCTP. Για παράδειγμα, οι διευθύνσεις IP ενδέχεται να ανήκουν σε διαφορετικά τοπικά δίκτυα ή σε διαφορετικά backbone δίκτυα. (Σημειώνεται ότι τα τελευταία χρόνια έχουν αναπτυχθεί επεκτάσεις TCP για να επιτρέψουν τη λειτουργία πολλαπλών διαδρομών και για το TCP).[2]

Κατά τη δημιουργία μιας ένωσης SCTP, τα τελικά σημεία ανταλλάσσουν λίστες διευθύνσεων IP. Κάθε τελικό σημείο μπορεί να επιτευχθεί σε οποιαδήποτε από τις ανακοινωθέν διευθύνσεις IP. Μία από τις διευθύνσεις IP σε κάθε τελικό σημείο ορίζεται ως η κύρια και οι υπόλοιπες γίνονται δευτερεύουσες. Εάν η πρωτεύουσα διεύθυνση αποτύχει για οποιονδήποτε λόγο, τα πακέτα SCTP μπορούν να σταλούν στη δευτερεύουσα διεύθυνση IP χωρίς να το γνωρίζει η εφαρμογή. Όταν η κύρια διεύθυνση IP γίνει ξανά διαθέσιμη, οι επικοινωνίες μπορούν να μεταφερθούν ξανά. Οι πρωτογενείς και δευτερεύουσες διεπαφές ελέγχονται και παρακολουθούνται χρησιμοποιώντας μια διαδικασία “καρδιακού παλμού (heartbeat)” που ελέγχει τη συνδεσιμότητα των διαδρομών (εικόνα 4.11).[2]

#### 4.1.9 Γενική ενθυλάκωση δρομολόγησης (Generic Routing Encapsulation, GRE)

Το GRE είναι ένα πρωτόκολλο που έχει σχεδιαστεί για την εκτέλεση μιας σήραγγας(tunneling) ενός πρωτοκόλλου επιπέδου δικτύου έναντι ενός άλλου πρωτοκόλλου επιπέδου δικτύου. Είναι γενικό, με την έννοια ότι παρέχει ενθυλάκωση ενός αυθαίρετου πρωτοκόλλου επιπέδου δικτύου (π.χ. IP ή MPLS) σε σχέση με ένα άλλο αυθαίρετο πρωτόκολλο επιπέδου δικτύου.

Αυτό διαφέρει από πολλούς άλλους μηχανισμούς σήραγγας, όπου ένα ή και τα δύο πρωτόκολλα είναι συγκεκριμένα, όπως IPv4-in-IPv4 (IETF RFC 2003) ή Generic Packet Tunneling over IPv6 (IETF RFC 2473).

Το GRE χρησιμοποιείται επίσης για πολλές διαφορετικές εφαρμογές και σε πολλές διαφορετικές αναπτύξεις δικτύου εκτός της περιοχής τηλεπικοινωνιών. Δεν είναι πρόθεση αυτής της εργασίας να συζητήσουμε πτυχές για όλα αυτά τα σενάρια, αντ' αυτού, εστιάζουμε στις ιδιότητες του GRE που σχετίζονται περισσότερο με το 5G.[33]

Η βασική λειτουργία ενός πρωτοκόλλου σήραγγας είναι ότι ένα πρωτόκολλο

Application layer
Transport layer (e.g., UDP)
Network layer (e.g., IP)
Tunneling layer (e.g., GRE)
Network layer (e.g., IP)
Layers 1 and 2 (e.g., Ethernet)

Εικόνα 4.12: Παράδειγμα στοίβας πρωτοκόλλου κατά τη χρήση GRE tunneling [2]

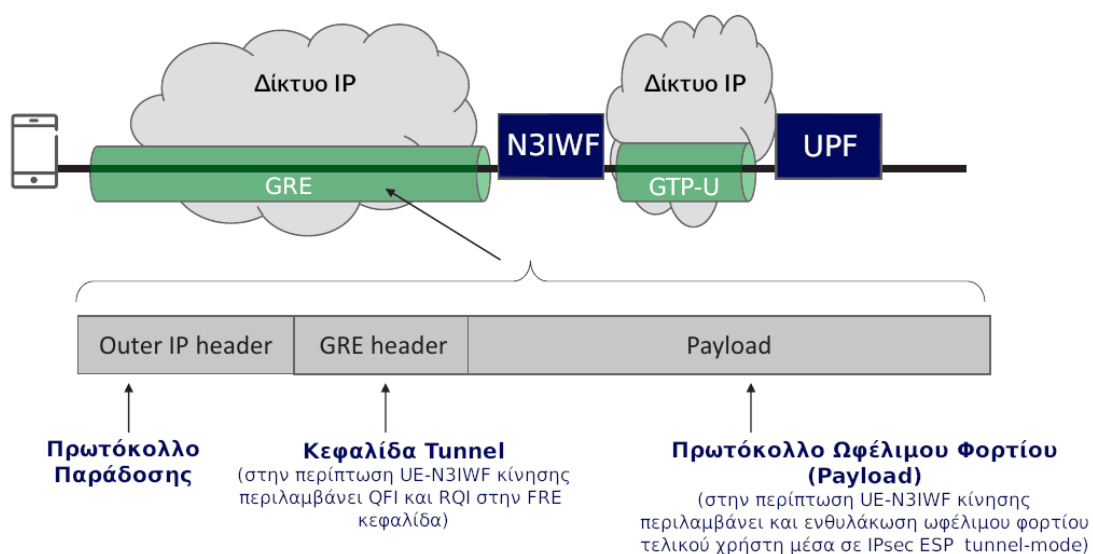


δικτύου, το οποίο ονομάζουμε πρωτόκολλο ωφέλιμου φορτίου(payload), ενθυλακώνεται σε άλλο πρωτόκολλο παράδοσης. Θα πρέπει να σημειωθεί ότι η ενθυλάκωση είναι ένα βασικό συστατικό οποιασδήποτε στοίβας πρωτοκόλλου όπου ένα πρωτόκολλο ανώτερου στρώματος είναι ενθυλακωμένο σε ένα πρωτόκολλο χαμηλότερης στρώσης. Αυτή η πτυχή της ενθυλάκωσης, ωστόσο, δεν πρέπει να θεωρείται ως σήραγγα. Όταν χρησιμοποιείται σήραγγα, αυτό που συχνά συμβαίνει είναι ότι ένα πρωτόκολλο layer-3 όπως το IP είναι ενθυλακωμένο σε διαφορετικό πρωτόκολλο layer-3 ή σε άλλο στιγμιότυπο του ίδιου πρωτοκόλλου. Η προκύπτουσα στοίβα πρωτοκόλλου μπορεί να μοιάζει με αυτήν που φαίνεται στην εικόνα 4.12.[33]

Ακολουθούν ορισμένες χρήσιμες ορολογίες:

- **Πρωτόκολλο πακέτου και ωφέλιμου φορτίου:** Το πακέτο και το πρωτόκολλο που πρέπει να ενθυλακωθεί (τα τρία κορυφαία κουτιά στη στοίβα πρωτοκόλλου στην εικόνα 4.12).[2]
- **Πρωτόκολλο ενθυλάκωσης (ή σήραγγας):** Το πρωτόκολλο που χρησιμοποιείται για την ενθυλάκωση του πακέτου ωφέλιμου φορτίου, δηλαδή, GRE (το τρίτο κουτί από κάτω στην εικόνα 4.12).[2]
- **Πρωτόκολλο παράδοσης:** Το πρωτόκολλο που χρησιμοποιείται για την παράδοση του ενθυλακωμένου πακέτου στο τελικό σημείο της σήραγγας (το δεύτερο κουτί από κάτω στην εικόνα 4.12).[2]

Η βασική λειτουργία του GRE είναι ότι ένα πακέτο του πρωτοκόλλου A (το πρωτόκολλο ωφέλιμου φορτίου) που πρόκειται να διοχετευτεί σε έναν προορισμό ενθυλακώνεται πρώτα σε ένα πακέτο GRE (το πρωτόκολλο σήραγγας). Το πακέτο GRE στη συνέχεια ενσωματώνεται σε ένα άλλο πρωτόκολλο B (το πρωτόκολλο παράδοσης) και αποστέλλεται στον προορισμό μέσω ενός δικτύου μεταφοράς του πρωτοκόλλου παράδοσης. Έπειτα, ο δέκτης αποσυμπιέζει το πακέτο και επαναφέρει το αρχικό πακέτο ωφέλιμου φορτίου του τύπου πρωτοκόλλου.[33]



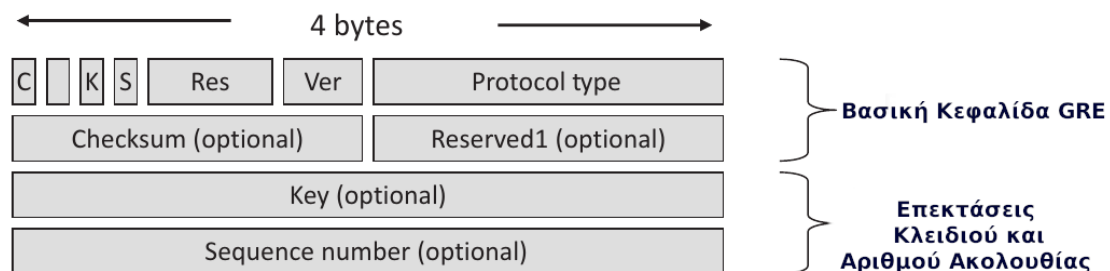
Εικόνα 4.13: Παράδειγμα GRE tunnel μεταξύ δύο κόμβων δικτύου με IPv4 πρωτόκολλο παράδοσης [2]

Στο 5GS, το GRE χρησιμοποιείται κυρίως για τη μεταφορά των πακέτων (PDU) μεταξύ UE και N3IWF. Το GRE εδώ επιτρέπει την τιμή QFI και την ένδειξη RQI ανταποκρινόμενα στο QoS ώστε να μεταφέρονται στην κεφαλίδα GRE μαζί με την ενθυλακωμένη PDU. Τα QFI και RQI περιλαμβάνονται στο πεδίο κλειδιού GRE. Η εικόνα 4.13 δείχνει ένα παράδειγμα PDU που μεταφέρεται σε σήραγγα GRE μεταξύ UE και N3IWF μέσω πρωτοκόλλου παράδοσης IP.[33]

Το GRE καθορίζεται στο IETF RFC 2784. Υπάρχουν επίσης πρόσθετα RFC που περιγράφουν τον τρόπο χρήσης του GRE σε συγκεκριμένα περιβάλλοντα ή με συγκεκριμένα πρωτόκολλα ωφέλιμου φορτίου ή / και παράδοσης. Μία επέκταση στη βασική προδιαγραφή GRE που έχει ιδιαίτερη σημασία για το EPS είναι η επέκταση πεδίου GRE Key που καθορίζεται από το IETF RFC 2890. Η επέκταση πεδίου Key περιγράφεται περαιτέρω ως μέρος της μορφής πακέτου παρακάτω.[2]

### Μορφή πακέτου GRE

Η μορφή κεφαλίδας GRE απεικονίζεται στην εικόνα 4.14. Η σημαία C υποδεικνύει εάν υπάρχουν τα πεδία Checksum και Reserved1 δηλαδή εάν έχει οριστεί η σημαία C, υπάρχουν τα πεδία Checksum και Reserved1. Σε αυτήν την περίπτωση, το Checksum περιέχει ένα άθροισμα ελέγχου της κεφαλίδας GRE καθώς και το πακέτο ωφέλιμου φορτίου. Το πεδίο Reserved1, εάν υπάρχει, έχει οριστεί σε όλα μηδέν. Εάν δεν έχει οριστεί η σημαία C, τα πεδία Checksum και Reserved1 δεν υπάρχουν στην κεφαλίδα. Οι σημαίες K και S υποδεικνύουν αν υπάρχει ο αριθμός κλειδιού και / ή ακολουθίας αντίστοιχα.[2]



Εικόνα 4.14: Κεφαλίδα GRE και η επέκταση κλειδιού και αριθμού ακολουθίας [2]

Το πεδίο Type Protocol περιέχει τον τύπο πρωτοκόλλου του πακέτου ωφέλιμου φορτίου. Αυτό επιτρέπει στο τελικό σημείο λήψης να αναγνωρίζει τον τύπο πρωτοκόλλου του πακέτου που έχει “απο-ενθυλακωθεί”. [2][33] Ο σκοπός του πεδίου Key είναι να προσδιορίσει μια μεμονωμένη ροή κυκλοφορίας μέσα σε μια σήραγγα GRE. Το GRE από μόνο του δεν καθορίζει τον τρόπο με τον οποίο τα δύο τελικά σημεία καθορίζουν ποια πεδία κλειδιού θα χρησιμοποιήσουν. Αυτό αφήνεται σε εφαρμογές ή καθορίζεται από άλλα πρότυπα που χρησιμοποιούν GRE. Το πεδίο Key θα μπορούσε, για παράδειγμα, να διαμορφωθεί στατικά στα δύο τελικά σημεία ή να δημιουργηθεί δυναμικά χρησιμοποιώντας κάποιο πρωτόκολλο σηματοδότησης μεταξύ των τελικών σημείων. Στο 5GS το πεδίο κλειδιού χρησιμοποιείται

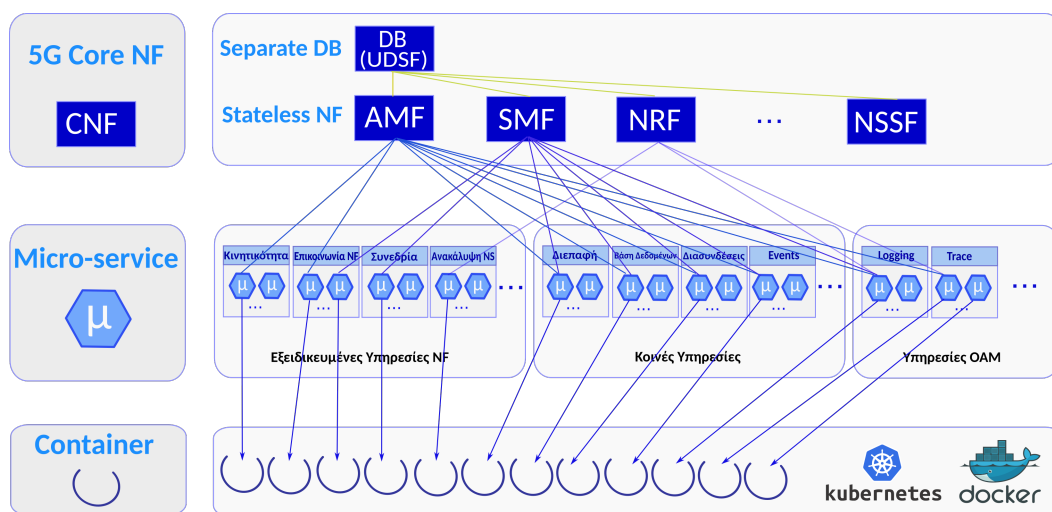
μεταξύ UE και N3IWF για τη μεταφορά της τιμής QFI και του RQI. Το QFI παίρνει 6 bit και το RQI ένα bit από τα διαθέσιμα 32 bit στο βασικό πεδίο. Αυτό περιγράφεται λεπτομερέστερα στο 3GPP TS 24.502.[2][33]

Το πεδίο Αριθμός ακολουθίας χρησιμοποιείται για τη διατήρηση της ακολουθίας των πακέτων μέσα στη σήραγγα GRE. Ο κόμβος που εκτελεί την ενθυλάκωση εισάγει τον αριθμό ακολουθίας και ο δέκτης τον χρησιμοποιεί για να προσδιορίσει τη σειρά με την οποία στάλθηκαν τα πακέτα.[2][33]

## 4.2 Νέες Εφαρμοζόμενες τεχνολογίες

Ένα από τα μεγαλύτερα πλεονεκτήματα που ωφελεί η τεχνολογίες 5G και Beyond είναι ότι μπορούν να προσαρμοστούν και να εφαρμοστούν ήδη γνωστές τεχνικές των υπολογιστικών συστημάτων και δικτύων και υποστηρίζουν τις σύγχρονες τεχνολογίες. Μερικές που έχουν ορισθεί, ως προς χρήση, στο χρονοδιάγραμμα του Beyond και για τις οποίες δημοσιεύονται συνεχώς έρευνες στα επιστημονικά περιοδικά περιγράφονται παρακάτω.

### 4.2.1 Μικροϋπηρεσίες (Microservices)



Εικόνα 4.15: Παράδειγμα δομής 5G με microservices [43]

Οι μικροϋπηρεσίες είναι μια αρχιτεκτονική και οργανωτική προσέγγιση στην ανάπτυξη λογισμικού όπου αντί να αναπτυχθεί το λογισμικό με μονολιθικό τρόπο, αποτελείται από μικρές ανεξάρτητες υπηρεσίες που επικοινωνούν μέσω καλά καθορισμένων API. Συχνά θεωρείται μια παραλλαγή της προσέγγισης αρχιτεκτονικής προσανατολισμένη στις υπηρεσίες. Ο γενικός στόχος της αρχιτεκτονικής μικροϋπηρεσιών είναι να κάνει τις εφαρμογές ευκολότερες στην κλιμάκωση καθώς και την ταχύτερη ανάπτυξη τους, επιτρέποντας την καινοτομία και την επιτάχυνση του χρόνου προς την αγορά για νέες δυνατότητες. Ωστόσο, έρχονται επίσης με αυξημένη πολυπλοκότητα, συμπεριλαμβανομένης της διαχείρισης, ενορχήστρωσης και δημιουργούν νέες μεθόδους διαχείρισης δεδομένων.[43]

Ο διαχωρισμός μικροϋπηρεσιών έχει πολλά οφέλη καθώς τα στιγμιότυπα των μικροϋπηρεσιών έχουν πολύ μικρότερο εύρος λειτουργικότητας και επομένως οι αλλαγές μπορούν να αναπτυχθούν πιο γρήγορα. Επίσης, ένα μεμονωμένο χαρακτηριστικό μπορεί να εφαρμοστεί σε ένα μικρό σύνολο μικροϋπηρεσιών και όχι σε ολόκληρο το πακέτο και τη λειτουργία 5GC. Επιπλέον, τα στιγμιότυπα των μικροϋπηρεσιών μπορούν να προστεθούν / αφαιρεθούν κατόπιν αιτήματος για να αυξηθεί / μειωθεί η επεκτασιμότητα των λειτουργιών τους. Τέλος, οι μικροϋπηρεσίες μπορούν να έχουν ανεξάρτητους κύκλους αναβάθμισης λογισμικού.[43]

Επομένως, αντί να αναπτυχθούν επαναλαμβανόμενα στιγμιότυπα μικροϋπηρεσιών, ο χειριστής μπορεί να αναπτύξει λειτουργίες κατά παραγγελία στην απαιτούμενη κλίμακα. Αυτή η προσέγγιση ενισχύει περαιτέρω την αποτελεσματικότητα της χρήσης πόρων και απλοποιεί σημαντικά την ανάπτυξη νέων λειτουργιών, επειδή ο χειριστής μπορεί να προσθέσει λειτουργίες και να κάνει αναβαθμίσεις σε ένα σύνολο μικροϋπηρεσιών χωρίς να επηρεάσει τις γειτονικές υπηρεσίες.[43]

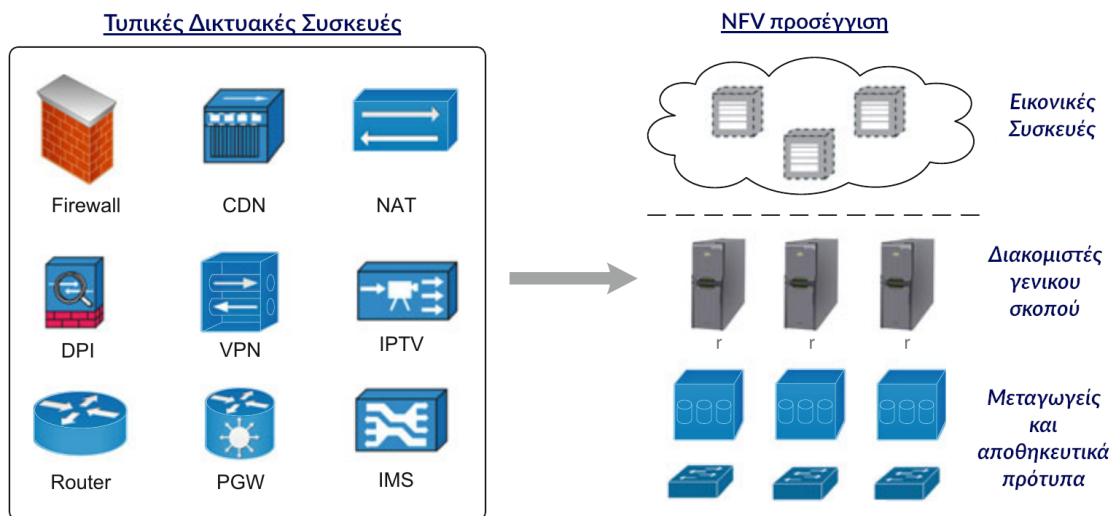
#### 4.2.2 Τεχνικές Εικονικοποίησης (Virtualization και Containerization)

##### Λειτουργία εικονικοποίησης δικτύου (Network Function Virtualization, NFV)

Η λειτουργία εικονικοποίησης λειτουργίας δικτύου (NFV) είναι μια έννοια που αξιοποιεί την εικονικοποίηση δηλαδή τη δυνατότητα μετατροπής των λειτουργιών των κόμβων δικτύου σε εικονικές συναρτήσεις που μπορούν να συνδεθούν περαιτέρω για να επιτρέψουν διαφορετικές υπηρεσίες επικοινωνίας. Μια ή περισσότερες εικονικές μηχανές που λειτουργούν σε διαφορετικούς κόμβους δικτύου, όπως οι μεταγωγείς πακέτων και οι διακομιστές(servers) μπορούν να χρησιμοποιηθούν για την εκτέλεση μιας λειτουργίας εικονικού δικτύου.

Το NFV χρησιμοποιεί το ήδη υπάρχον εμπορικό υλικό για την εκτέλεση τεχνικών εικονικοποίησης λογισμικού για εφαρμογή λειτουργιών δικτύου. Δηλαδή αντί να έχουμε διαφορετικό hardware για κάθε μία λειτουργία, για παράδειγμα ξεχωριστή συσκευή firewall ή vpn ή cdn όπως φαίνεται και στην εικόνα, έχουμε εικονικοποιημένες αυτές τις λειτουργίες στον υπάρχον εξοπλισμό, δημιουργώντας ακόμη και πολλαπλές περιπτώσεις αυτών χωρίς να χρειάζεται να προσθέσουμε υλική υποδομή.[13][32]

Το πλαίσιο λειτουργίας του NFV επιτρέπει την διαχείριση λειτουργιών εικονικού δικτύου προσανατολισμένη στην καθυστέρηση και η σημασία του είναι καταλυτική ιδιαίτερα σε τεχνικές τεμαχισμού δικτύου(network slicing), όπως θα δούμε στην επόμενη παράγραφο.[32]



Εικόνα 4.16: Προσέγγιση βασισμένη σε NFV για τις λειτουργίες δικτύου [32]

Η αρχιτεκτονική του NFV αποτελείται από τρία βασικά στοιχεία:

1. Τον ενορχηστρωτή εικονικοποίησης λειτουργίας δικτύου, που εκτελεί την οργάνωση και λειτουργία των πόρων, όπως πιστοποίηση και εξουσιοδότηση του διαχειριστή λειτουργίας εικονικού δικτύου.[32]
2. Ο διαχειριστής λειτουργιών του εικονικού δικτύου που χειρίζεται αιτήματα για πόρους NFV υποδομής καθώς και διαχειρίζεται τον κύκλο ζωής της υπηρεσίας δικτύου.[32]
3. Ο διαχειριστής εικονικής υποδομής είναι υπεύθυνος για τον έλεγχο και τη διαχείριση των NFV πόρων του δικτύου του operator.[32]

Τα πλεονεκτήματα από τη χρήση της τεχνικής εικονικοποίησης είναι:[13][32]

- ▷ Μείωση των κεφαλαιουχικών δαπανών επιτρέποντας στους φορείς εκμετάλλευσης τη λειτουργία δικτύου χωρίς αγορά υλικού καθώς και πληρωμή σύμφωνα με τη χρήση.
- ▷ Επιτρέπει επίσης στους φορείς εκμετάλλευσης να μειώσουν τις λειτουργικές δαπάνες που απαιτούνται για χώρο, ψύξη, ισχύ και συντήρηση εξοπλισμού.
- ▷ Προσθέτει περισσότερη ευελιξία στο σύστημα επιτρέποντας ευκολότερη και γρήγορη κλιμάκωση των Υπηρεσιών καθώς και ευκολότερη προσαρμογή σε cloud συστήματα.
- ▷ Ευκολότερη Διαχείριση από ένα ή περισσότερα κεντρικά πεδία ελέγχου

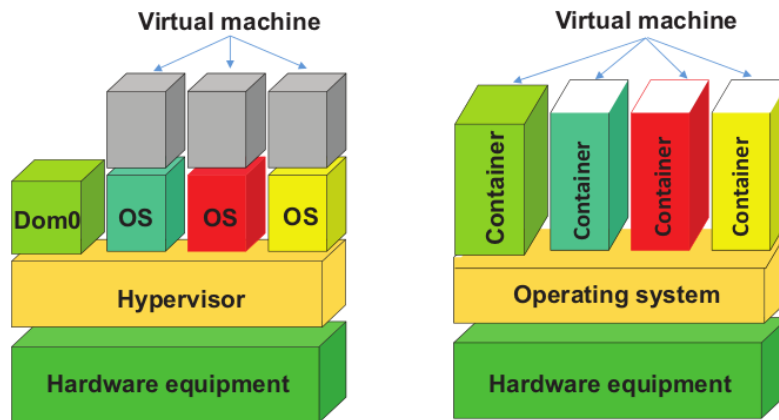
### Χρήση Containers(Containerization)

Λόγο του ότι υπάρχει αστοχία στην Ελληνική μετάφραση αυτού του όρου ως προς την τεχνολογική περιγραφή του, θα χρησιμοποιήσουμε τον Αγγλικό όρο και θα κάνουμε μία αναφορά σε αυτή την τεχνολογία, την οποία όμως και θα χρησιμοποιήσουμε κατά την υλοποίηση του 5G NSA που περιγράφεται στο επόμενο κεφάλαιο. Τα container είναι απομονωμένα το ένα από το άλλο και μοιράζονται πυρήνες λειτουργικού συστήματος μεταξύ όλων των κοντέινερ. Χρησιμοποιούνται ευρέως σε τομείς όπου υπάρχει ανάγκη βελτιστοποίησης πόρων υλικού για την εκτέλεση πολλαπλών εφαρμογών και για τη βελτίωση της ευελιξίας και της παραγωγικότητας. Επιπλέον, τα οικολογικά συστήματα και εργαλεία για περιβάλλον βασιζόμενο σε containers π.χ., το Kubernetes, επεκτείνεται γρήγορα.[34]

Τα containers είναι ιδιαίτερα χρήσιμα για εφαρμογές τηλεπικοινωνιών

- Όπου η χαμηλή καθυστέρηση, η ανθεκτικότητα και η φορητότητα είναι βασικές απαιτήσεις - π.χ. σε περιβάλλοντα Edge Computing.
- Για την υλοποίηση βραχυχρόνιων υπηρεσιών, δηλαδή για εξαιρετικά ευέλικτες εφαρμογές.

Σε μηχανική μάθηση ή τεχνητή νοημοσύνη όταν είναι χρήσιμο να χωριστεί ένα πρόβλημα σε ένα μικρό σύνολο εργασιών αναμένεται ότι τα κοντέινερ θα βοηθήσουν σε κάποιο βαθμό την αυτοματοποίηση.[34]



Εικόνα 4.17: Τεχνικές εικονικοποίησης [13]

### 4.2.3 Τεχνολογίες νέφους (Cloud computing)

Το cloud computing επιτρέπει στους χρήστες να χρησιμοποιούν κατά ζήτηση διαμοιραζόμενους πόρους που περιλαμβάνουν τόσο υλικούς πόρους υποδομής όσο και λογισμικό. Το cloud στη γενική περίπτωση ακολουθεί τρεις τύπους μοντέλων δανομής όπως δείχνει η εικόνα, δηλαδή infrastructure as a service (IAAS), platform as service (PAAS), and software as service (SAAS) ανάλογα με τις απαιτήσεις του χρήστη. Το Software as a Service αναφέρεται στην on demand ζήτηση λογισμικού χωρίς να χρειάζεται εγκατάσταση σε τοπικό προσωπικό υπολογιστή, καθώς το λογισμικό που διατίθεται στους χρήστες

εκτελείται στο cloud( τέτοια παραδείγματα είναι το Gmail, το Dropbox κλπ). [34]

Το platform as a Service επιτρέπει στους χρήστες να χρησιμοποιούν πλατφόρμες ανάπτυξης εφαρμογών διαθέτοντας βάση δεδομένων, περιηγητές, λειτουργικά συστήματα και περιβάλλοντα εκτέλεσης γλωσσών προγραμματισμού με την πιο διαδεδομένη υπηρεσία να είναι η Amazon web Service. [34]

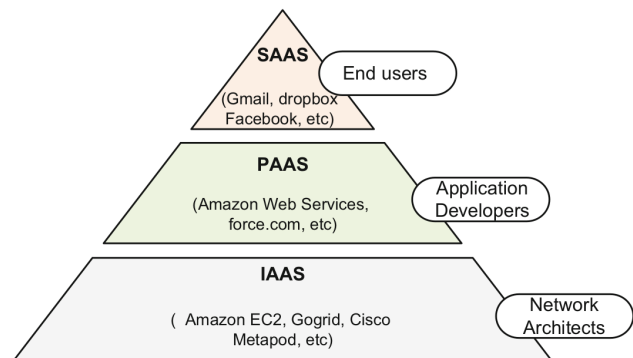
Στο Infrastructure as a Service (IAAS), ολόκληροι εικονικοποιημένοι υπολογιστικοί πόροι προσφέρονται σαν υπηρεσία μέσω του ίντερνετ. Τέτοιες υπηρεσίες παρέχουν μεγάλες εταιρείες όπως για παράδειγμα η Amazon, η Cisco και η Google.[34]

Οι παραπάνω υπηρεσίες μπορεί να υλοποιούνται σε διαφορετικά επίπεδα όπως δημόσια cloud,ιδιωτικά, υβριδικά. Σε κάθε περίπτωση όμως κατά την εφαρμογή τους σε 5G δίκτυα θα πρέπει να ικανοποιούν τις απαιτήσεις των παρόχων, των χρηστών και των επιχειρήσεων και να παρέχουν αξιοπιστία, βιωσιμότητα, ασφάλεια και ιδιωτικότητα, κλιμάκωση και ανοχή στα σφάλματα. [34]

Επομένως, μια στρατηγική που βασίζεται στο cloud επιτρέπει στους παρόχους υπηρεσιών να επιταχύνουν την ανάπτυξη νέων υπηρεσιών, επιτρέποντας πρακτικές όπως το DevOps, ενώ η δυνατότητα γρήγορης αναβάθμισης ή μείωσης των υπηρεσιών επιτρέπει τη βελτιστοποίηση της χρήσης πόρων σε πραγματικό χρόνο, σε ανταπόκριση με την αυξημένη κίνηση δεδομένων. [34]

Υπάρχουν αρκετές αρχές σχεδιασμού εγγενούς νέφους που ισχύουν για όλες τις εγκαταστάσεις, όπως:

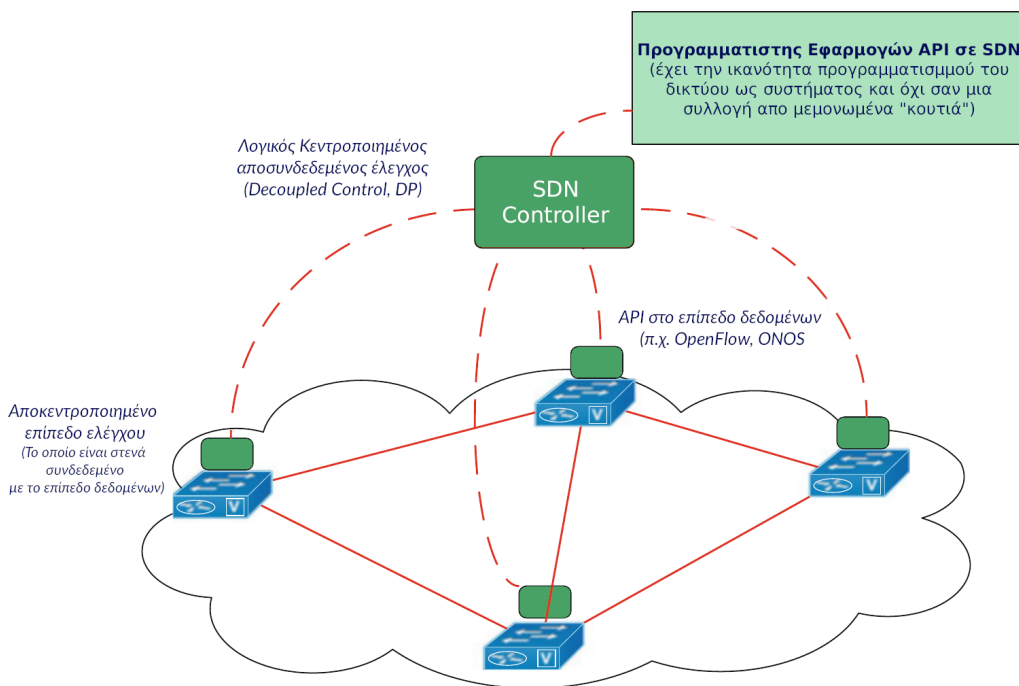
- **Ανεξαρτησία υπερδομής:** Οι εφαρμογές που βασίζονται στο Cloud είναι ανεξάρτητες από οποιαδήποτε υποκείμενη υποδομή και πόρους.
- **Αποσύνθεση λογισμικού και διαχείριση κύκλου ζωής:** Το λογισμικό αποσυντίθεται σε μικρότερα, πιο εύχρηστα κομμάτια, χρησιμοποιώντας αρχιτεκτονικές μικροπηρεσιών. Κάθε κομμάτι μπορεί να αναπτυχθεί, να κλιμακωθεί και να αναβαθμιστεί μεμονωμένα χρησιμοποιώντας ένα περιβάλλον CaaS (Container as a Service).
- **Ευελιξία:** Σε εφαρμογές παλαιού τύπου, το MTBF (μέσος χρόνος μεταξύ αστοχιών) υλικού ήταν η βασική μέτρηση για την ανθεκτικότητα. Το cloud, αντ' αυτού βασίζεται στη διανομή και την ανεξαρτησία των στοιχείων λογισμικού που χρησιμοποιούν αυτόματη κλιμάκωση και ανάκαμψη. Αυτό σημαίνει ότι οι αστοχίες σε μια εφαρμογή θα πρέπει να προκαλούν μόνο προσωρινή απώλεια χωρητικότητας και να μην κλιμακώνονται ποτέ σε πλήρη επανεκκίνηση και απώλεια υπηρεσίας.



Εικόνα 4.18: Μοντέλα Cloud Υπηρεσιών [32]

- **Βελτιστοποιημένη κατάσταση κατάστασης:** Ο τρόπος διαχείρισης της κατάστασης εξαρτάται από τον τύπο της κατάστασης / δεδομένων και το πλαίσιο της κατάστασης. Επομένως, δεν υπάρχει τρόπος χειρισμού «ενός μεγέθους για όλους» όσον αφορά την κατάσταση και τα δεδομένα, αλλά πρέπει να υπάρχει ισορροπία μεταξύ απόδοσης, ανθεκτικότητας και ευελξία.
- **Ενορχήστρωση και αυτοματοποίηση:** Αυξάνεται ένα τεράστιο όφελος των εγγενών εφαρμογών cloud αυτοματοποίηση μέσω, για παράδειγμα, ενός επιπέδου CaaS που βασίζεται σε Kubernetes. Ένα CaaS επιτρέπει αυτόματη κλιμάκωση μικροσυσκευών, αυτόματη επούλωση αποτυχημένων κοντέινερ και λογισμικό αναβαθμίσεις, συμπεριλαμβανομένων δοκιμών καναρινιών (δοκιμές μικρής κλίμακας) πριν από μεγαλύτερες αναπτύξεις.

#### 4.2.4 Δικτύωση βασισμένη στο λογισμικό (Software Defined Network, SDN)



Εικόνα 4.19: Δικτύωση Βασισμένη στο λογισμικό [32]

Η δικτύωση βασισμένη στο λογισμικό είναι μία τεχνολογία δικτύου που επιτρέπει στους χρήστες να έχουν πρόσβαση στο δίκτυο, με διαχωρισμό του επιπέδου ελέγχου από τις υποκείμενες συσκευές δικτύου, πιο αναβαθμισμένη ασφάλεια, χαμηλότερο λειτουργικό κόστος και μειωμένες κεφαλαιουχικές δαπάνες. Στο δίκτυο που καθορίζεται από λογισμικό, η εργασία προώθησης πακέτων εκτελείται από τον κεντρικό ελεγκτή δικτύου μέσω προγραμματιζόμενων διεπαφών.[13]

Η κεντροποιημένη αρχιτεκτονική του SDN προσδίδει μια πιο εύκολη διαχείριση των δικτύων μεγάλης κλίμακας διαχωρίζοντας τις λειτουργίες του



επιπέδου ελέγχου και του επιπέδου δεδομένων όπως φαίνεται και στην εικόνα 4.19.

Το λογικό επίπεδο ελέγχου έχει τη δυνατότητα ευκολότερης διαμόρφωσης μαζί με αποτελεσματικές λειτουργίες διαχείρισης. Μερικοί συνήθεις SDN controllers είναι οι Floodlight, Onix, and NOX ενώ το OpenFlow είναι το πιο διαδεδομένο πρωτόκολλο διεπαφών για το έλεγχο της ροής πακέτων.[13]

Οι controllers διαιρούνται σε δύο κατηγορίες ως τοπικοί ελεγκτές που συνδέονται σε έναν ή περισσότερους μεταγωγείς που με τη σειρά τους συνδέονται με τον root, το δεύτερο τύπο ελεγκτών, που εκτός από αυτή τη διαχείριση εκτελεί και κάποιες λειτουργίες χρήσιμες για μια πιο διευρυμένη οπτική του δικτύου από μεριά του ελεγκτή. Τέτοια παραδείγματα είναι το Hyperflow και το Onix που επίσης βοηθούν στη μείωση του φόρτου στον controller.[13]

Άρα γίνεται κατανοητό ότι η κεντροποιημένη διαχείριση που προσφέρει το SDN, και επ' ακολούθως τα κατανεμημένα συστήματα, είναι το κλειδί για τον τεμαχισμό του δικτύου και τον έλεγχο των slices από ένα κέντρο διαχείρισης των operators αλλά και από τους πελάτες που διαχειρίζονται τους αναγκαίους πόρους μέσω διεπαφής προγραμματισμού εφαρμογών(API). [13]

#### 4.2.5 Αυτοματοποίηση

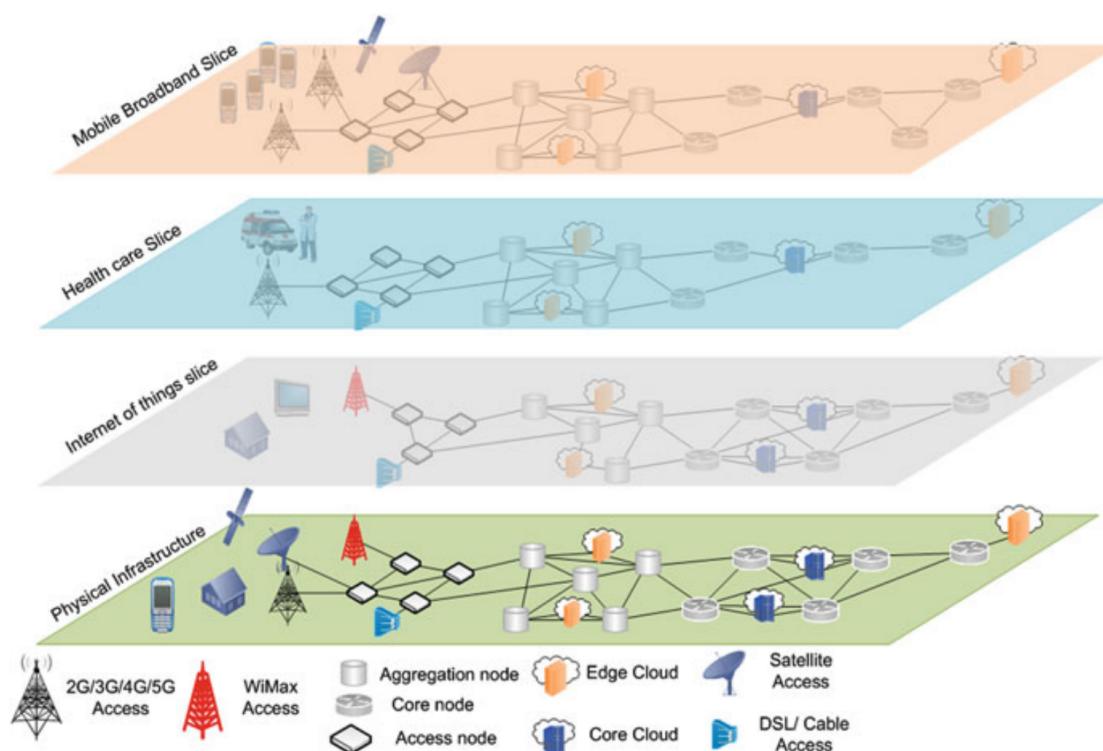
Ένας από τους κύριους μοχλούς για την εξέλιξη του κεντρικού δικτύου είναι το όραμα για την παροχή δικτύων που εκμεταλλεύονται τις τεχνολογίες αυτοματισμού. Σε όλο τον ευρύτερο τομέα του ICT, η Μηχανική Μάθηση, η Τεχνητή Νοημοσύνη και ο Αυτοματισμός οδηγούν σε μεγαλύτερη αποτελεσματικότητα στον τρόπο κατασκευής και λειτουργίας των συστημάτων. Εντός των τομέων 3GPP, ο αυτοματισμός εντός της Έκδοσης 15 και της Έκδοσης 16 αναφέρεται κυρίως σε Δίκτυα Αυτο-Οργάνωσης (SON), τα οποία παρέχουν *Αυτοδιαμόρφωση*, *Αυτο-Βελτιστοποίηση* και *Αυτοθεραπεία*. Αυτές οι τρεις έννοιες υπόσχονται μεγαλύτερη αξιοπιστία για τους τελικούς χρήστες και μικρότερο χρόνο διακοπής λειτουργίας για τους παρόχους υπηρεσιών.[13]

Αυτές οι τεχνολογίες ελαχιστοποιούν το κόστος κύκλου ζωής των δικτύων κινητής τηλεφωνίας μέσω της εξάλειψης της μη αυτόματης διαμόρφωσης των στοιχείων δικτύου καθώς και της δυναμικής βελτιστοποίησης και αντιμετώπισης προβλημάτων.[13]

## 4.3 Τεμαχισμός Δικτύου (Network Slicing)

### 4.3.1 Η ανάγκη του τεμαχισμού του δικτύου

Όπως αναφέραμε και στο πρώτο κεφάλαιο κατά την πραγματοποίηση του 5G δικτύου αντιμετωπίζουμε και κάποιες προκλήσεις με σκοπό την επιτυχημένη υλοποίηση του ώστε να ενεργοποιηθούν χρήστες με eMBB, mMTC, και URLLC. Για το λόγο αυτό έπρεπε να επανασχεδιαστούν τα δίκτυα αλλά και όπως αναφέραμε να δημιουργηθούν λογικά δίκτυα για τους διαφορετικούς τύπους υπηρεσιών. Το network slicing είναι υποψήφια μέθοδος ώστε να επιτρέψει ένα μεγάλο εύρος υπηρεσιών και εφαρμογών όπως e-health, επαυξημένη πραγματικότητα, έξυπνα συστήματα μεταφοράς, τραπέζης, αγροτικά συστήματα κλπ..[32]



Εικόνα 4.20: Τεμαχισμός Δικτύου 5G [32]

Όπως απεικονίζεται και στην παραπάνω εικόνα που αποτελεί ένα παράδειγμα τεμαχισμού δικτύου, κάθε λογικό δίκτυο να μπορεί να έχει ανεξάρτητο έλεγχο με δυνατότητα on demand δημιουργίας δικτύου. Συγκεκριμένα, “τεμαχίζεται” μια φυσική υποδομή δικτύου σε εικονικά δίκτυα, ώστε να εξυπηρετεί IoT υπηρεσίες, ένα άλλο τμήμα να υποστηρίζει υπηρεσίες υγείας αλλά και κατανομή πόρων που είναι κατάλληλη για ευρυζωνικά δίκτυα. Καταχρηστικά έγινε χρήση του όρου “τεμαχισμός” καθώς οι πόροι στην ουσία μοιράζονται στα virtual machines των slices.[32]

Τέτοιοι πόροι παρουσιάζονται στο κάτω μέρος της ανωτέρω εικόνας μπορεί για παράδειγμα να είναι τα σημεία ασύρματης πρόσβασης, οι κεραίες για παράδειγμα που συνδέεται ένας τελικός χρήστης μέσω της

συσκευής του, σημεία πρόσβασης δικτύων WiMax, δορυφόρους αλλά και backhaul διατάξεις όπως πολυπλέκτες(εικονικούς ή μη), μεταγωγείς με υποστήριξη openflow πρωτοκόλλου, δρομολογητές ή ακόμα και ολοκληρωμένες λύσεις cloud τεχνολογιών. Άρα όλοι οι προαναφερόμενοι πόροι μπορούν μέσω τεχνικών εικονικοποίησης και λογισμικών να κατανεμηθούν και να επαναχρησιμοποιηθούν.[32]

”  
 Συνεπώς, μπορούμε να ορίσουμε ως Network Slicing μια υπηρεσία λογικού δικτύου, που διαμορφώνει και κατανέμει ένα σύνολο καθορισμένων πόρων που απαιτούνται για επιχειρηματικό σκοπό ή απο τους πελάτες. Επιτρέπει δηλαδή την ισχυρή και ευέλικτη ικανότητα δημιουργίας πολλαπλών λογικών δικτύων πάνω απο μία κοινή φυσική υποδομή. Ο τεμαχισμός του δικτύου(network slicing) διακρίνεται σε οριζόντιο και κάθετο.”

Η πρόκληση αυτή προήλθε απο την ανάγκη των τελικών χρηστών για αυξημένη ζήτηση πόρων λόγω μεγάλης αύξησης του αριθμού των end-devices καθώς και των διαφορετικών απαιτήσεων και χρήσεων του δικτύου αλλά και τελικά απο την ανταπόκριση των παρόχων έχοντας ως πρώτο μέλημα τους την εξοικονόμηση χρημάτων και ενέργειας κάνοντας χρήση νέων τεχνολογιών.[32]

Τα παραδοσιακά δίκτυα είναι one-size και έτσι, αντί να χρησιμοποιούμε ένα μονολιθικό δίκτυο που εξυπηρετεί πολλαπλές περιπτώσεις, οι τεχνολογικές εξελίξεις όπως η εικονικοποίηση, το SDN αλλά και άλλες τεχνικές που είδαμε στην προηγούμενη ενότητα, μας επιτρέπουν να δημιουργήσουμε λογικά δίκτυα πάνω από ένα κοινό επίπεδο υποδομής.[32]

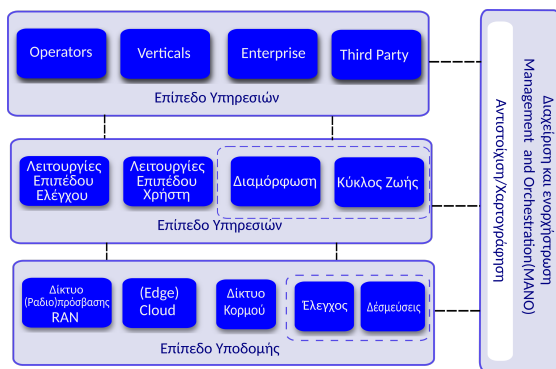
Συνεπώς μια κατάτμηση του δικτύου υλοποιεί ένα πλήρες δίκτυο για κάθε είδους πρόσβαση και ενεργοποίηση της παροχής υπηρεσιών. Άρα οι χρησιμοποιούμενοι πόροι φυσικής ή εικονικής υποδομής μπορεί να αξιοποιηθούν στο Network Slice ή να διαμοιραστούν σε άλλα Network Slice.[32]

Το αρχιτεκτονικό όραμα της υποδομής 5G από το πρόγραμμα συνεργασίας δημόσιου και ιδιωτικού τομέα (5G-PPP) πρότεινε τον διαχωρισμό της αρχιτεκτονικής slicing network σε πέντε επίπεδα. Το επίπεδο υπηρεσίας, το επίπεδο υποδομής, το επίπεδο ενορχήστρωσης, το επίπεδο επιχειρησιακής λειτουργίας και το επίπεδο λειτουργίας δικτύου.[32]

Από την άλλη πλευρά η κοινοπραξία των operators Next Generation Mobile Network(NGMN) πρότεινε τη διαίρεση της αρχιτεκτονικής του δικτύου που αφορά κυρίως τις ευρυζωνικές επικοινωνίες ώστε να διακρίνεται σε τρία επίπεδα: επιχειρηματική εφαρμογή, επιχειρηματική ενεργοποίηση και πόρος υποδομής.[32]

### 4.3.2 Λειτουργία του Slicing

Για καλύτερη κατανόηση θα αναφέρουμε ένα παράδειγμα γενικού πλαισίου(ενός framework) για τον τεμαχισμό δικτύου 5G με τρία επίπεδα. Εκτός από αυτά τα τρία επίπεδα, υπάρχει και η οντότητα διαχείρισης και ενορχήστρωσης (Management and Orchestration, MANO), όπου εκτελεί τη μετάφραση των μοντέλων υπηρεσιών και των περιπτώσεων χρήσης, σε slices. [32]



Εικόνα 4.21: Επίπεδα Framework για τον τεμαχισμό δικτύου 5G [32]

Το πρώτο επίπεδο, το επίπεδο υποδομής, ασχολείται με τη φυσική υποδομή δικτύου που καλύπτει και το δίκτυο κορμού και το δίκτυο πρόσβασης. Επίσης εκτελεί έλεγχο υποδομής και κατανομή πόρων στα slices. [32]

Το επίπεδο λειτουργίας δικτύου εκτελεί την ενθυλάκωση των λειτουργιών που απαιτούνται στη διαμόρφωση λειτουργιών δικτύου και στη διαχείριση κύκλου ζωής. Αυτές οι λειτουργίες δικτύου συνδέονται στη συνέχεια μαζί για να παρέχουν

μια υπηρεσία από άκρο σε άκρο τελικά, σε operators, για εφαρμογή vertical slicing σε διάφορους τομείς, ακόμα και σε third party applications. [32]

Έτσι, όλα αυτά συμβάλλουν ώστε να προσδίδουν end-to-end υπηρεσίες στους ενοικιαστές (ως ενοικιαστές εννοούμε φυσικά τους χρήστες που μπορούν να έχουν πρόσβαση στους κοινόχρηστους πόρους με συγκεκριμένα προνόμια και δικαιώματα πρόσβασης). [32]

Οι βασικές αρχές τώρα που θα πρέπει να διέπουν ένα σύστημα slicing εφαρμοζόμενο με σύγχρονες τεχνικές είναι κυρίως:

- Η Απομόνωση των slices αρχικά που αποτελεί και την πιο βασική ιδιότητα που θα πρέπει να διασφαλιστεί καθώς εγγυάται στους διαφορετικούς ενοικιαστές των slices ότι το μισθωμένο κομμάτι δικτύου τους είναι ανεξάρτητο από τα άλλα και δεν μπορεί να παραβιαστεί/τροποποιηθεί από εξωτερικούς παράγοντες. Ακόμη, διαμοιράζει δίκαια τους πόρους με πρόσθετη δυνατότητα επιβολής ορίων στη χρήση πόρων δικτύου. [33]
- Η ελαστικότητα που επιτρέπει τη δυναμική αλλαγή πόρων που διατίθενται σε διαφορετικούς ενοικιαστές των slices για την αποτελεσματική χρήση των πόρων. Η ελαστικότητα μπορεί να πραγματοποιηθεί από μετεγκατάσταση των λειτουργιών εικονικού δικτύου, κλιμάκωση προς τα πάνω / κάτω των εκχωρημένων πόρων, και επαναπρογραμματισμός των λειτουργιών ελέγχου και δεδομένων. [33]
- Η προσαρμογή που διασφαλίζει ότι έχουν διατεθεί κοινόχρηστοι πόροι σε διαφορετικούς ενοικιαστές χρησιμοποιείται αποτελεσματικά. Αναμένεται ότι η προσαρμογή θα προσφερθεί στο μέλλον από πολλές κάθετες βιομηχανίες (το vertical slicing όπως το ονομάζουμε). [33]

Για να ενεργοποιήσουμε την προσαρμογή και να κατοχυρώσουμε τόσο την ελαστικότητα και το isolation μπορούν να αξιοποιηθούν τεχνικές όπως η εικονικοποίηση των λειτουργιών του δικτύου, η δικτύωση βασισμένη στο λογισμικό, η χρήση containers και η ενορχήστρωση δικτύου, παρέχοντας κατανομή πόρων με ευέλικτο τρόπο χρησιμοποιώντας την ίδια φυσική υποδομή σε περισσότερα slices όπως αναφέραμε και προηγουμένως. [32]

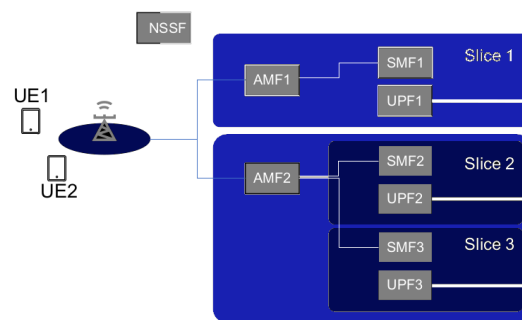
Όλες αυτές οι τεχνικές που αναφέραμε αν και μπορούν να υλοποιηθούν και να αξιοποιηθούν στο χώρο του ενοικιαστή-πελάτη, η χρήση του 5G και Beyond,

ενδείκνυται να χρησιμοποιούνται αυτές οι τεχνικές σε τεχνολογίες cloud με τη φυσική υποδομή να βρίσκεται στην κατοχή του operator. [32]

### Παράδειγμα Εφαρμογής Network Slicing στο 5G

Κάνοντας χρήση όλων των προηγούμενων τεχνικών που αναλύσαμε μπορούμε να τεμαχίσουμε, ή πιο σωστά να δημιουργήσουμε instances των λειτουργιών τόσο του RAN δικτύου πρόσβασης περιλαμβάνοντας προαιρετική κατανομή πόρων, όσο και του core δικτύου του 5G που επιτρέπει σε μία μόνο συσκευή να συνδεθεί σε περισσότερα απο ένα slices ταυτόχρονα, ένα χαρακτηριστικό που δεν υποστηρίχθηκε στην αρχιτεκτονική EPC του 4G.[32]

Συγκεκριμένα,όπως φαίνεται και στο απλοποιημένο παράδειγμα στην εικόνα. δημιουργήσαμε διαφορετικά instances για τις βασικές λειτουργίες του 5G core όπως αυτές που παρέχουν λειτουργίες πιστοποίησης, σηματοδότησης και διευθυνσιοδότησης αλλά και της ροής δεδομένων δηλαδή τις AMF, SMF και UPF.[32]



Στην εικόνα για παράδειγμα, η συσκευή User Equipment 1 συνδέεται στο slice 1 όπου αποτελείται απο τα AMF, SMF και UPF. Η συσκευή User Equipment 2 συνδέεται ταυτόχρονα και στο slice 1 και στο slice 2 καθένα απο αυτά περιλαμβάνουν τα SMF και UPF αλλά χρησιμοποιούν το ίδιο AMF 2.[32]

Εικόνα 4.22: Παράδειγμα Network Slicing στο 5G [32]

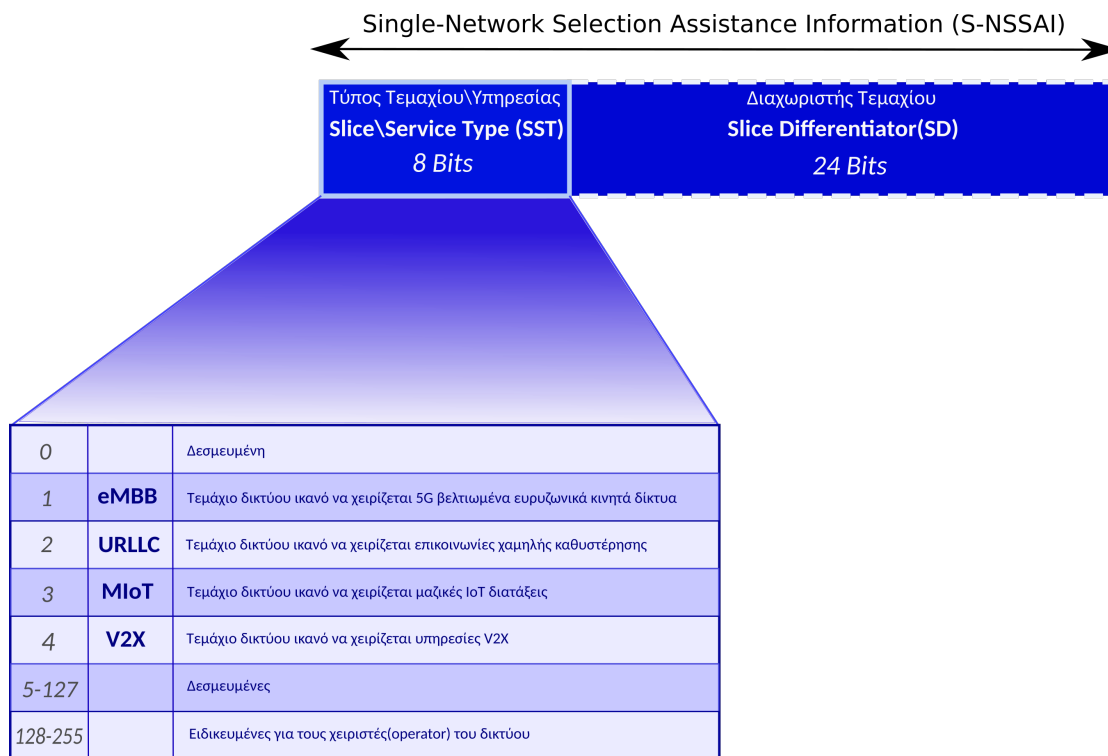
#### 4.3.3 Single Network Slice Selection Assistance Information (S-NSSAI)

Ένα συγκεκριμένο network slice του 5G αναγνωρίζεται απο μία παράμετρο που ονομάζεται Απλές Βοηθητικές Πληροφορίες για επιλογή Slice δικτύου(S-NSSAI)“Single Network Slice Selection Assistance Information” και αποτελείται απο δύο υποπαραμέτρους, τον τύπο Slice/service(SST) και τον προαιρετικό διαχωριστή slices(SD). Το SD χρησιμοποιείται για τη διάκριση μεταξύ πολλαπλών slices του ίδιου τύπου και ως εκ τούτου έχουν το ίδιο SST. Μία ανάλυση ενός πακέτου S-NSSAI αναπαριστάται στην εικόνα 4.23. [44]

Το ραδιοδίκτυο που εξυπηρετεί τη συσκευή θα χρησιμοποιεί μία ή περισσότερες ζητούμενες τιμές S-NSSAI από τη συσκευή για να κάνει την αρχική επιλογή του AMF.[44]

Το NSSF έχει ως μοναδικό ρόλο να υποστηρίξει την επιλογή των slice δικτύων βάσει ενός συνδυασμού S-NSSAI τιμών που ορίζονται για το δίκτυο, ζητούνται από τη συσκευή και επιτρέπονται εντός της συνδρομής.

Για να μπορέσει ένα UE να αποκτήσει πρόσβαση σε ένα Network Slice, το UE πρέπει να το καταχωρίσει στο δίκτυο και αυτό γίνεται με τη διαδικασία Εγγραφής. Προκειμένου να ενεργοποιηθεί η υποστήριξη για πολλαπλά τμήματα δικτύου για το ίδιο UE, υπάρχει η ανάγκη αποστολής ενός ή



Εικόνα 4.23: Κάτοψη του S-NSSAI [2]

περισσότερων S-NSSAI ταυτόχρονα από το UE στο δίκτυο και από το δίκτυο στο UE. Επομένως, ένα ή περισσότερα S-NSSAI μπορούν να παρέχονται σε ένα NSSAI. Ενώ μερικές φορές.[44]

#### 4.3.4 Πλεονεκτήματα χρήσης

Τέλος, εκτός από τα πλεονεκτήματα που αναφέρθηκαν κατά τη διάρκεια της παρουσίας σε κάθε ενότητα, συνοπτικά μπορούμε να αναφέρουμε ότι η αναφερόμενη τεχνολογία του Network Slicing στο 5G είναι μια τεχνολογία που ήδη θα πρωτοστατήσει, εφόσον βασίζεται σε τεχνικές που κυριαρχούν στον κόσμο των δικτύων και όχι μόνο και όταν υπάρχει συνδυασμός αυτών (όπως αναμένεται και στο 5g), έχουμε αρκετά οφέλη όπως:[32]

- Καλύτερη “customer experience” ανα προσαρμογή πελάτη και βελτιστοποίηση
- Αξιόπιστη υλοποίηση για τις λειτουργίες eMBB, mMTC και URLLC που αναφερθήκαμε στην εισαγωγή
- Συντομεύει ο χρόνος αγοράς και έναρξης του πελάτη λόγω της ταχύτερης υλοποίησης μιας υποδομής
- Απλούστερη και οικονομικότερη διαχείριση πόρων
- Αυξάνονται οι αυτοματισμοί
- Ελαστικότητα και ευελιξία των παρεχόμενων υπηρεσιών
- Μειωμένοι κίνδυνοι λόγω της απομόνωσης των υπηρεσιών

## 4.4 Διαχωρισμός Λειτουργιών (Function Split)

### 4.4.1 Κίνητρα για διαχωρισμό λειτουργιών του 5G

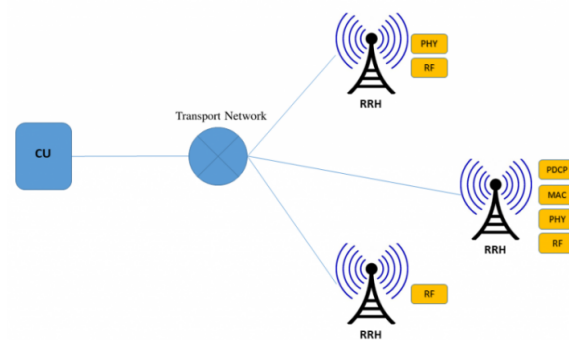
Στο μέλλον, οι μελλοντικές φορητές λύσεις πρέπει να αντιμετωπίζουν διαφορετικές απαιτήσεις με βάση τις περιοχές ανάπτυξης και το κοινωνικοοικονομικό περιβάλλον τους. Ενώ στη Δυτική Ευρώπη και τη Βόρεια Αμερική απαιτούνται συγκεκριμένες επιδόσεις δικτύων κινητών δικτύων, όπως υψηλότερη απόδοση και χαμηλότερη καθυστέρηση, στην Αφρική και στις αγροτικές περιοχές του κόσμου είναι ένα εντελώς διαφορετικό σύνολο δεικτών απόδοσης, συμπεριλαμβανομένων των εφαρμογών με λιγότερες απαιτήσεις backhaul και χαμηλό κόστος ανάπτυξη, πλην όμως σημαντικές για αγροτικές εφαρμογές ή απομακρυσμένο έλεγχο γεωργικών μηχανημάτων. Λαμβάνοντας υπόψη αυτά τα διαφορετικά σύνολα απαιτήσεων, τα μελλοντικά δίκτυα κινητής τηλεφωνίας πρέπει να είναι αρκετά δυναμικά για να αντιμετωπίσουν αυτά τα ζητήματα αναλόγως.[34]

Οι πάροχοι κινητής τηλεφωνίας στις ανεπτυγμένες χώρες εξακολουθούν να αντιμετωπίζουν υψηλότερα ποσοστά χρήσης δεδομένων από τους συνδρομητές. Για να αντιμετωπιστεί αυτό, οι πάροχοι κινητής τηλεφωνίας πρέπει να ξοδέψουν πολλά για νέο εξοπλισμό και υπηρεσίες που αυξάνει τις κεφαλαιουχικές δαπάνες (capital expenditures, CAPEX) και τα λειτουργικά έξοδα (operating expenses, OPEX). Αυτό μειώνει σημαντικά την κερδοφορία και ανάγκασε τους παρόχους κινητής

τηλεφωνίας να βρουν νέους τρόπους επέκτασης της χωρητικότητας των δικτύων τους, ενώ παραμένουν κερδοφόροι. Στο άλλο άκρο, στις αναπτυσσόμενες χώρες και στις αγροτικές περιοχές των ανεπτυγμένων χωρών, οι πάροχοι κινητής τηλεφωνίας αντιμετωπίζουν την πρόκληση της παροχής αποδεκτών υπηρεσιών, ενώ επιτυγχάνουν τους οικονομικούς τους στόχους λαμβάνοντας υπόψη το χαμηλό μέσο όρο εσόδων ανά χρήστη (Average revenue per user, ARPU). Αυτό το παράδειγμα απαιτεί μια εντελώς νέα και δυναμική αρχιτεκτονική για μελλοντικά δίκτυα κινητής τηλεφωνίας και ιδιαίτερα 5G.[34]

Η νέα αρχιτεκτονική του RAN, το κεντρικό RAN (C-RAN) που έχει αποκτήσει πρόσφατα δυναμική, αποσυνδέει τις περισσότερες λειτουργίες Base Station (BS) από Remote Radio Heads (RRHs) που θα συγκεντρωθούν στις Κεντρικές Μονάδες (CUs). Όλα τα RRH συνδέονται με CU μέσω του δικτύου μεταφοράς.

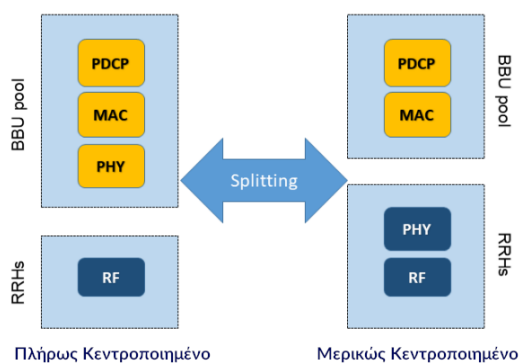
Το Σχήμα ??, δείχνει τη δομή του C-RAN με τρία RRHs που συνδέεται μέσω δικτύου μεταφοράς σε ένα CU. Οι λειτουργίες που μπορούν να αποσυνδεθούν περιλαμβάνουν κωδικοποίηση καναλιού και αποκωδικοποίηση



Εικόνα 4.24: Δομή C-RAN με τρία RRHs συνδεδεμένα με το δίκτυο μεταφοράς [38]

διόρθωσης σφαλμάτων, διαμόρφωση / αποδιαμόρφωση, χαρτογράφηση πόρων / αποσυμπίεση, εκτίμηση και εξίσωση καναλιών, γρήγορος μετασχηματισμός Fourier (FFT) και την αντίστροφη, αναλογική-σε-ψηφιακή και ψηφιακή-σε-αναλογική μετατροπή, και μετάδοση και λήψη ραδιοφώνου κεραίας. [36][38]

Η μελλοντική εξέλιξη του RAN τείνει προς δυναμικές λειτουργικές διασπάσεις. Ενώ το gateway (αθροιστής) λειτουργεί ως μεσολαβητής μεταξύ του RAN και του κεντρικού δικτύου, η λειτουργικότητα του RAN θα κατανέμεται μεταξύ DUs και CUs όπως ορίζεται στο 5G. Σε ορισμένα σενάρια, αυτά τα στοιχεία μπορούν να συγκρουστούν μαζί και να δημιουργήσουν μια φυσική οντότητα με διαφορετικές εικονικές λειτουργίες. Η κεντρική ανάπτυξη βασικής ζώνης προτείνεται αρχικά να επιτρέψει την εξισορρόπηση φορτίου μεταξύ διαφορετικών σταθμών βάσης. Επομένως, στις περισσότερες περιπτώσεις, η κατανεμημένη πλέον μονάδα (Distributed Unit, DU) θα συνεγκατασταθεί με το Remote Radio Head (RRH) για να εκτελέσει όλες τις υπολογιστικές απαιτητικές εργασίες επεξεργασίας, όπως γρήγορος μετασχηματισμός Fourier / αντίστροφος γρήγορος μετασχηματισμός Fourier (FFT / IFFT) που δεν εξαρτώνται από το φορτίο και δεν παρουσιάζουν κέρδη από κοινού. Το CU μπορεί να διαχωριστεί ή να συνεγκατασταθεί με τον αθροιστή ανάλογα με τη διαθεσιμότητα των FrontHauls (FH). [34][35]



Εικόνα 4.25: Ευέλικτος διαχωρισμός λειτουργιών Cloud-RAN [38]

Η λογική τοπολογία του FH θα διαφοροποιηθεί στα μελλοντικά δίκτυα 5G. Όπως αναφέρθηκε προηγουμένως, η κεντρική συνεργατική επεξεργασία απαιτεί ένα δίκτυο FH να συγκεντρώνει (να διανέμει) πληροφορίες από (σε) πολλαπλά RRHs σε BBU ή να μεταφέρει πληροφορίες μεταξύ BBUs. Κάτι τέτοιο όμως δεν αποτελεί τη βέλτιστη λύση που μπορεί να εφαρμοστεί για διαφορετικά σενάρια ανάπτυξης με βάση διαφορετικές μορφολογίες. Ως εκ τούτου, ως μέρος του πλαισίου

3GPP, έχει προταθεί πολλαπλός διαχωρισμός λειτουργιών για την κάλυψη αυτών των διαφορετικών απαιτήσεων. Η υπάρχουσα ιδέα C-RAN (split 8) είναι η βέλτιστη λύση για δίκτυα με τέλεια FH. Αναμένεται η δυναμική διάσπαση λειτουργιών μεταξύ CU και DUs να είναι η προσέγγιση για συστήματα 5G και μετά. Ενώ οι CU θα διατηρήσουν λειτουργίες που μοιάζουν με BBU, οι DU θα μοιάζουν περισσότερο με το RRH όσον αφορά τις δυνατότητες επεξεργασίας. Σε περίπτωση απαιτήσεων για πιο ευαίσθητη καθυστέρηση υπηρεσιών σε 5G, με βάση την κατάλληλη διαθεσιμότητα FH, το MAC-PHY split θα είναι η προτιμώμενη λύση. [34][35][39]

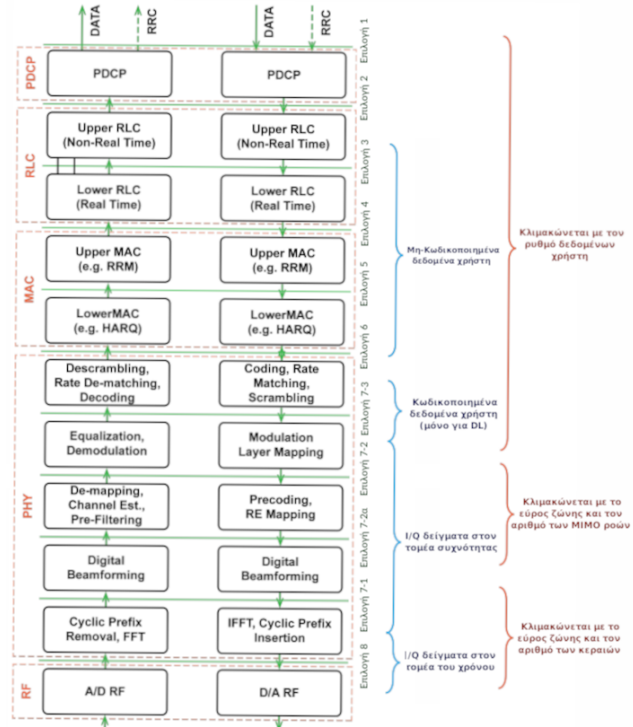


### 4.4.2 Επιλογές Λογικού διαχωρισμού 5G λειτουργιών

Οι επιλογές για το διαχωρισμό έχουν ήδη προταθεί από τους φορείς ανάπτυξης και διαχείρισης του 5G, οι οποίοι και θα καταλήξουν στην πιο αποδοτική επιλογή από αυτές ανάλογα με την εφαρμογή. Η νέα αρχιτεκτονική του RAN, το κεντρικό RAN (C-RAN) που έχει αποκτήσει πρόσφατα δυναμική, αποσυνδέει τις περισσότερες λειτουργίες Base Station (BS) από Remote Radio Heads (RRHs) που θα συγκεντρωθούν στις Κεντρικές Μονάδες (CUs). Όλα τα RRH συνδέονται με την κεντρική μονάδα (CU) μέσω του δικτύου μεταφοράς.

Όπως εξηγήθηκε, το C-RAN είναι η υψηλότερη συγκεντρωτική αρχιτεκτονική: οι περισσότερες λειτουργίες επεξεργασίας, ελέγχου και διαχείρισης μεταφέρονται στο BBU pool και η βασική λειτουργικότητα RF παραμένει σε RRHs. Ωστόσο, λόγω διαφόρων απαιτήσεων εφαρμογών, ένα πλήρως συγκεντρωτικό σύστημα δεν είναι βέλτιστο σε όλα τα σενάρια. Για παράδειγμα, οι χρήστες uRLLC χρειάζονται πιο αποκεντρωμένες λειτουργικές διασπάσεις για τη μείωση της καθυστέρησης HARQ. Με το διαχωρισμό και την παράλληλη χρήση νέων, ήδη γνωστών τεχνολογιών, που καθορίζουν το περιβάλλον με λογισμικό (π.χ. SDN / NFV), ο χειριστής C-RAN εφαρμόζει έναν ευέλικτο διαχωρισμό λειτουργικότητας αντί ενός πλήρως συγκεντρωτικού συστήματος που σχετίζεται άμεσα με τις απαιτήσεις εφαρμογής.

Τα κύρια πλεονεκτήματα της C-RAN αρχιτεκτονικής είναι ότι απλοποιεί τη δομή των Remote Radio Heads (RRHs) και ενεργοποιεί τεχνολογίες εικονικοποίησης και τεμαχισμού δικτύου μεταβαίνοντας από υποδομές που καθορίζονται από υλικό, σε υποδομές που καθορίζονται από περιβάλλον λογισμικού. Επίσης, απαιτεί μικρότερο λειτουργικό κόστος καθώς και κόστος ανάπτυξης και λιγότερη κατανάλωση ενέργειας. Επιπρόσθετα, επιτρέπει την ευέλικτη κατανομή μιας ομάδας (pool) από υπολογιστικούς πόρους και ραδιο-πόρους και ελέγχει τις μεταβάσεις από κατανεμημένα BS σε ένα κεντρικό RAN. Τέλος, μεγιστοποιεί την αποδοτικότητα του φάσματος και τη χρήση υλικού.



Εικόνα 4.26: Επιλογές διαχωρισμού λειτουργιών [38]

Ακολουθεί μία καταγραφή των επιλογών όπως έχουν δοθεί απ την 3GPP.

- **Επιλογή 1 (Διαχωρισμός RRC/PDCP)**  
Όμοιος όπως στο LTE Rel. 12 DC επιλογή 1A [35]
- **Επιλογή 2 (Διαχωρισμός PDCP/RLC)**  
Όμοιος όπως στο LTE Rel. 12 DC επιλογή 3C για UP (σημειώνεται ως F1 διεπαφή στην έκδοση 15 και αναφέρθηκε στο προηγούμενο κεφάλαιο)  
  
Αυτή η επιλογή εκτελεί τις λειτουργίες PDCP στο BBU και μπορεί να χρησιμοποιεί οποιονδήποτε τύπο δικτύου fronthaul. Το κύριο πλεονέκτημα αυτής της επιλογής είναι η δυνατότητα συγκέντρωσης διαφορετικών τεχνολογιών RRH (π.χ. 5G, LTE και WiFi).[35][36]
- **Επιλογή 3 (intra-RLC διαχωρισμός)**  
Το μεγαλύτερο μέρος του RLC βρίσκεται στην CU. Όλες οι λειτουργίες που σχετίζονται με το ARQ και οι λειτουργίες σε πραγματικό χρόνο (όπως η συνάθροιση) βρίσκονται στην Remote Unit(RU).  
  
Το επίπεδο RLC και άλλα επίπεδα πάνω από αυτό εικονοποιούνται στο BBU (ή CU). Η αστοχία μέσω δικτύου μεταφοράς μπορεί επίσης να ανακτηθεί χρησιμοποιώντας τον μηχανισμό ARQ από άκρο σε άκρο στο CU. Αυτό μπορεί να παρέχει προστασία για κρίσιμα δεδομένα. Η επιλογή αυτή μειώνει επίσης τους περιορισμούς καθυστέρησης fronthaul καθώς ο προγραμματισμός σε πραγματικό χρόνο εκτελείται τοπικά στο RRH(όπως το aggregation).[36][38][39]
- **Επιλογή 4(Διαχωρισμός MAC/RLC)**  
Το στρώμα MAC και τα επίπεδα πάνω από αυτό συγκεντρώνονται σε CU με κεντρικό προγραμματισμό (όπως το MAC είναι σε CU) για πολλά RRH. Αυτό το διαχωρισμό επιτρέπει συγχρονισμένο συντονισμό πολλαπλών κυττάρων για CoMP και eICIC, αλλά απαιτεί fronthaul χαμηλής καθυστέρησης και έχει σημαντικά έξοδα ανάπτυξης.[35][36]
- **Επιλογή 5 (Διαχωρισμός intra-MAC)**  
Στην επιλογή αυτή, αποφάσεις προγραμματισμού υψηλού επιπέδου,( π.χ. τεχνικές ICIC, CoMP), θα εκτελεστούν στην Centralized Unit(CU), ενώ διεργασίες κρίσιμης σημασίας(π.χ. HARQ) θα εκτελεστούν στο DU.[36][38]
- **Επιλογή 6 (Διαχωρισμός MAC/PHY)**  
Το πλήρες επίπεδο MAC βρίσκεται στο επίπεδο CU PHY που εφαρμόζεται στο CU. Αυτή η διάσπαση απαιτεί αλληλεπιδράσεις χρονισμού επιπέδου-πλαίσιου μεταξύ CU και DU, καθώς οι καθυστερήσεις FH θα επηρεάσουν το χρονοδιάγραμμα και τον προγραμματισμό HARQ.[36][39]
- **Επιλογή 7 (Διαχωρισμός intra- PHY)**  
Στην επιλογή αυτή υπάρχουν επι μέρους επιλογές οι οποίες διαχωρίζουν τις εσωτερικές λειτουργίες στο PHY. Ειδικότερα, διακρίνονται οι παρακάτω επιλογές.[36]

- **Επιλογή 7.1**

Η εισαγωγή / αφαίρεση των I / FFT και CP πραγματοποιείται σε DU και το υπόλοιπο PHY βρίσκεται στη CU. Τα δείγματα I / Q στον τομέα συχνότητας ανταλλάσσονται μέσω της διεπαφής. Σε σύγκριση με την επιλογή 8 μόνο τα δείγματα που σχετίζονται με κατελιημένους δευτερεύοντες φορείς πρέπει να ανταλλάσσονται αντί για δείγματα τομέα χρόνου που αντικατοπτρίζουν ολόκληρο το εύρος ζώνης του συστήματος.[36][39]

- **Επιλογή 7.2 και 7.2α**

Η Προ-κωδικοποίηση και η ψηφιακή διαμόρφωση δέσμης τμήματα αυτού, εκτελούνται στο DU. Σε αυτήν την περίπτωση, οι απαιτήσεις FH κλιμακώνονται με τον αριθμό των επιπέδων MIMO και όχι τον αριθμό των θυρών κεραίας, όπως συμβαίνει στην επιλογή 7.1. [35][36]

- **Επιλογή 8 (Βασικό C-RAN)**

Αυτός ο διαχωρισμός γνωστός ως C-RAN, αποτελεί τον υψηλότερο συγκεντρωτισμός και συντονισμός λειτουργιών που επιτρέπει μια πιο αποτελεσματική διαχείριση πόρων και μπορεί να πραγματοποιηθεί μόνο με ένα ιδανικό fronthaul που καταναλώνει πολύ υψηλό εύρος ζώνης και έχει πολύ χαμηλά όρια καθυστέρησης.[35][36][39]

Τέλος, αξίζει να σημειώσουμε ότι ο διαχωρισμός στο RAN δεν χρειάζεται να είναι ο ίδιος για το UL και DL, για παράδειγμα μπορεί να χρησιμοποιηθεί η επιλογή 7.2 ή 7.2 για το UL και η επιλογή 7.3 για το DL. Επιπλέον, σημειώνουμε ότι εκτός από τις δραστηριότητες της 3GPP, μία ομάδα εμπόρων δικτύου έχει ήδη επικεντρωθεί σε ένα βελτιωμένο Common Public Radio Interface (CPRI)<sup>1</sup> πρότυπο(eCPRI)που αποτελείται από όλες τις επολογές 7.x που περιγράφηκαν παραπάνω.[34]

---

<sup>1</sup>Πρότυπο που ορίζει τη διεπαφή μεταξύ του ραδιοεξοπλισμού(Radio Equipment,(RE) και του ελέγχου του ραδιοεξοπλισμού (Radio Equipment Control, REC)[34]

## ΜΕΡΟΣ ΙΙ

### Πειραματική Διαδικασία



## Κεφάλαιο 5

# Υλοποίηση αυτόνομου και μη αυτόνομου συστήματος 5G

**Γ**ια την υλοποίηση τόσο του αυτόνομου όσο και του μη αυτόνομου συστήματος 5G έχουν αναπτυχθεί λύσεις έτοιμες προς λειτουργία σε ήδη υπάρχοντα τηλεπικοινωνιακά συστήματα, υποστηριζόμενα από το ήδη υπάρχον 4g(μη αυτόνομο σύστημα), καθώς και αυτόνομες λύσεις κυρίως για ερευνητικούς σκοπούς. Και στις δύο περιπτώσεις η ανάπτυξη στηρίζεται είτε σε ανοιχτά πρότυπα και ανοιχτό κώδικα, είτε σε κλειστού κώδικα συστήματα που επιδέχονται απλά την εγκατάσταση και όχι την περαιτέρω ανάπτυξη από τους χειριστές.

Αν και μεγάλες εμπορικές εταιρείες(Ericsson, Nokia κλπ) παρέχουν κλειστού κώδικα συστήματα, υπάρχουν και μη κερδοσκοπικοί φορείς που διανέμουν δωρεάν τον κώδικα και βασίζονται στη συλλογική ανάπτυξη αυτού παρέχοντας και το δίκτυο κορμού και το δίκτυο πρόσβασης σε ορισμένες περιπτώσεις, ενώ σε κάποιες χρησιμοποιείται προσομοιωτής(emulator) του δικτύου πρόσβασης. Μερικές από αυτές τις εργασίες είναι:

- **5GCore**  
Σύστημα 5G που έχει αναπτυχθεί με γλώσσα προγραμματισμού python
- **free5GC**  
Ανοιχτού κώδικα δίκτυο κορμού 5G βασισμένο στην έκδοση 15 της 3GPP
- **Internship-5GCN**  
Εφαρμογή RESTful υπηρεσιών δικτύου μεταξύ κόμβων του επιπέδου ελέγχου(AMF,NRF,SMF,UDM).
- **OAI-CN**  
Αυτή η εργασία εφαρμόζει την αυτόνομη ανάπτυξη του 5G με τη χρήση προσομοιωτή για το RAN αλλά και την μη αυτόνομη λειτουργία με τον συνδυασμό του μη αυτόνομου 5G με τη χρήση συσκευών USRP από τη μεριά του RAN.
- **Open5GS**  
Είναι μια εργασία ανοιχτού κώδικα αναπτυγμένη σε γλώσσα προγραμματισμού C που εφαρμόζει το 5GC και το EPC, όπως ορίζει για παράδειγμα η έκδοση 16 της 3GPP για το δίκτυο κορμού NR/LTE.

Στην εργασία αυτή και ειδικότερα στο κεφάλαιο αυτό θα ασχοληθούμε με την ανοιχτού κώδικα ανάπτυξη κάνοντας χρήση αυτόνομων και μη αυτόνομων συστημάτων όπως αυτά αναπτύχθηκαν από τον μη κερδοσκοπικό οργανισμό “OpenAirInterface Software Alliance(OSA)” και θα αναφέρεται ως OpenAirInterface(OAI).

## 5.1 Προετοιμασία υλικού και λογισμικού εξοπλισμού

Στην παράγραφο συνοψίζεται ο βασικός εξοπλισμός και η παραμετροποίηση που υφίσταται προκειμένου να εγκατασταθεί και να λειτουργήσει το σύστημα 5G σε κάθε περίπτωση, όπως ορίζεται από τους υπεύθυνους ανάπτυξης. Η όλη ανάπτυξη γίνεται υπό την άδεια OAI Public License V1.1

Η όλη ανάπτυξη έγινε πάνω σε ένα σύστημα cloud με τις δυνατότητες να εγκαθίστανται τόσο σε φυσικά μηχανήματα (bare metal) όσο και σε εικονικές μηχανές (Virtual Machines) με εικονικοποιημένο το ανώτερο λειτουργικό σύστημα. Επίσης, πριν από κάθε εγκατάσταση θα πρέπει να ενημερώνονται τα αποθετήρια του λειτουργικού συστήματος ώστε να εγκαθιστούν τις πιο πρόσφατες εκδόσεις των προς εγκατάσταση λογισμικών.

Στη συνέχεια, σε περιβάλλον γραμμής εντολών(CLI) όπου αναφέρεται το σύμβολο “\$” σημαίνει ότι κατά την εκτέλεση εντολών από τερματικό ο χρήστης έχει περιορισμένα δικαιώματα και προσβάσεις στο σύστημα αρχείων, όπως ένας κανονικός χρήστης δηλαδή, ενώ όπου αναδεικνύεται το σύμβολο της δίσωσης “#” ο χρήστης μπορεί να εκτελεί εντολές ως διαχειριστής συστήματος(root). Για να εκτελέσει ένας κανονικός χρήστης εντολή ως διαχειριστής αρκεί πριν την εντολή να προσθέσει την λέξη “sudo”<sup>1</sup> και να εισάγει τον κωδικό διαχειριστή όταν του ζητηθεί.



Εικόνα 5.1: Υλική υποδομή εφαρμογής της πειραματικής διαδικασίας

<sup>1</sup>Προέρχεται από τη έκφραση Super User DO και δίνει δικαιώματα διαχειριστή στον χρήστη

### 5.1.1 Δίκτυο Κορμού

Όπως αναφέραμε και στο θεωρητικό μέρος της εργασίας, απο την έναρξη της μετάβασης των δικτύων κορμού απο κυκλωματικά δίκτυα σε δίκτυα βασισμένα σε IP, άνοιξε ο δρόμος για την χρήση νέων τεχνολογιών όπως αυτές που περιγράφηκαν στο κεφάλαιο 4 (SDN, εικονικοποίηση, containers, κλπ). Συνεπώς, στο δίκτυο κορμού τα προαπαιτούμενα σχετίζονται κυρίως με το λογισμικό.

#### Λειτουργικό σύστημα

Κατά την εγκατάσταση τόσο του δικτύου κορμό όσο και του δικτύου πρόσβασης χρησιμοποιήθηκε λειτουργικό σύστημα Ubuntu 18.04 με προεγκατεστημένο πυρήνα Linux όπως διανέμεται απο την εταιρεία Canonical Ltd., ώστε να φιλοξενήσει την ανάπτυξη του δικτύου 5G σε φυσικό και εικονικό επίπεδο.

#### Εγκατάσταση Βοηθητικού Λογισμικού

Για την εγκατάσταση των διαφόρων οντοτήτων του πυρήνα χρησιμοποιήθηκε η τεχνολογία containerization. Αν και υπάρχουν αρκετά λογισμικά για ανάπτυξη και διαχείριση containers, στη συγκεκριμένη υλοποίηση έγινε χρήση του λογισμικού Docker που διατίθεται με τη μορφή CLI (Command Line Interpreter) δηλαδή δια μέσου γραμμής εντολών απο το τερματικό του Ubuntu.

Ένα άλλο λογισμικό που βοήθησε στην διαχείριση και εγκατάσταση των πηγαίων αρχείων είναι το λογισμικό Git που διαχειρίζεται αποθετήρια και αποτελεί το "διαδικτυακό εργαστήριο" των προγραμματιστών για την ανάπτυξη, εξέλιξη, διόρθωση και συντήρηση του κώδικα των οντοτήτων.

Θα κάνουμε χρήση ορισμένων μόνο εντολών αυτών των προγραμμάτων που είναι χρήσιμα για την υλοποίηση σε κάθε περίπτωση, εξηγώντας παράλληλα, ως σχόλια, και την λειτουργία τους.

Τέλος, για την ανάγνωση και τον έλεγχο των πακέτων δεδομένων που διακινούνται χρησιμοποιούμε το κατάλληλο λογισμικό wireshark με υποστήριξη γραφικού περιβάλλοντος(GUI) αλλά και με τη χρήση γραμμής εντολών(CLI)

#### Παραμετροποίηση Δικτύου

Σύμφωνα με την επίσημη σελίδα του Docker, πριν δημιουργηθεί ένα εσωτερικό δίκτυο αποτελούμενο απο διευθύνσεις που αντιστοιχούν στα containers, πρέπει να ενεργοποιηθεί η προώθηση της κίνησης των πακέτων απο τα containers προς εξωτερικά δίκτυα. Για να επιτευχθεί αυτό πρέπει να γίνουν δύο ρυθμίσεις στον πυρήνα Linux.

1. Διαμόρφωση πυρήνα Linux ώστε να επιτρέπει IP προώθηση

```
$ sysctl net.ipv4.conf.all.forwarding=1
```

2.Αλλαγή πολιτικών στον πίνακα καταχώρησης των IPs(iptables) ώστε να δέχεται διευθύνσεις απο εξωτερικά δίκτυα χαρακτηρίζοντας τις IPv4 απο DROP σε ACCEPT



```
1 $ sudo iptables -P FORWARD ACCEPT
```

3.Απενεργοποίηση της έκδοσης 6 των IPs(IPv6) και έλεγχος απενεργοποίησης

```
1 $ sudo sysctl -w net.ipv6.conf.all.disable_ipv6=1
2 $ sudo sysctl -w net.ipv6.conf.default.disable_ipv6=1
3 $ sudo sysctl -w net.ipv6.conf.lo.disable_ipv6=1
```

Με κάθε επανεκκίνηση του υπολογιστή οι παραπάνω εντολές θα πρέπει να εκτελούνται εξ αρχής.

## 5.1.2 Δίκτυο Πρόσβασης

Το δίκτυο πρόσβασης απαιτεί και τη μεγαλύτερη παραμετροποίηση του λειτουργικού συστήματος αλλά και των υλικών πόρων. Και αυτό γιατί η διαχείριση του μεταδιδόμενου σήματος απαιτεί σταθερότητα και στη συχνότητα και στην ισχύ. Οι εξαρτήσεις επίσης του δικτύου πρόσβασης από λειτουργίες της επεξεργαστικής μονάδας αλλά και του πυρήνα του λειτουργικού καθιστούν ευάλωτη την εγκατάσταση του δικτύου πρόσβασης.

Όσον αφορά το λειτουργικό σύστημα εφαρμόζεται, την εγκατάσταση βοηθητικού λογισμικού και την παραμετροποίηση δικτύου ισχύουν ότι και στην περίπτωση του δικτύου κορμού.

### Έλεγχος βασικών λειτουργιών πυρήνα

Το τρέχον λογισμικό OpenAirInterface.org απαιτεί υπολογιστές βασισμένους στην αρχιτεκτονική Intel για τους στόχους eNB ή UE. Αυτή η απαίτηση οφείλεται σε βελτιστοποιημένες λειτουργίες επεξεργασίας σήματος(DSP) που κάνουν βαριά χρήση ακέραιων διεργασιών SIMD<sup>2</sup> (SSE, SSE2, SSS3, SSE4 και AVX2).Οι λειτουργίες αυτές,ή flags όπως εμφανίζονται στα χαρακτηριστικά του πυρήνα, θα πρέπει να αναζητούνται ξεχωριστά πριν την εγκατάσταση εκτελώντας την εντολή

```
1 $ grep sse /proc/cpuinfo
```

όπου αντικαθιστούμε τη λειτουργία sse με την κάθε διαφορετική λειτουργία που θέλουμε να εξετάσουμε.

Αν δεν υπάρχει μία από αυτές τις λειτουργίες δεν καθίσταται δυνατή η ορθή λειτουργία του δικτύου πρόσβασης, κάτι που μπορεί να συμβαίνει κατά την χρήση εικονικών μηχανών έναντι VMs απ' ότι διαπιστώθηκε κατά την πειραματική διαδικασία.

### Παραμετροποίηση λειτουργικού συστήματος και διαχείριση ενέργειας

Ένα από τα οφέλη που παρέχει το 5G είναι η χαμηλή καθυστέρηση. Έτσι, απαιτείται το λειτουργικό σύστημα να διαθέτει πυρήνα χαμηλής

<sup>2</sup>Single instruction, multiple data (SIMD) είναι μια κατηγορία παράλληλων υπολογιστών σε ταξινόμηση Flynn. Περιγράφει υπολογιστές με πολλαπλά στοιχεία επεξεργασίας που εκτελούν την ίδια λειτουργία σε πολλά σημεία δεδομένων ταυτόχρονα. Τέτοιες μηχανές εκμεταλλεύονται τον παραλληλισμό σε επίπεδο δεδομένων, αλλά όχι ταυτόχρονα: υπάρχουν ταυτόχρονοι (παράλληλοι) υπολογισμοί, αλλά μόνο μία διαδικασία σε μια δεδομένη στιγμή

καθυστερήσης, δηλαδή πυρήνα που να δίνει προτεραιότητα στην χαμηλή καθυστέρηση των δεδομένων απο ότι στη ρυθμαπόδοση. Για το λόγο αυτό εγκαταστήσαμε τον πυρήνα χαμηλής καθυστέρησης και συγκεκριμένα το πακέτο linux-image-5.4.0-37-lowlatency. Η επιλογή χαμηλής καθυστέρησης πυρήνα αν γίνεται και στο δίκτυο κορμού και στο δίκτυο πρόσβασης, θα πρέπει να είναι της ίδιας έκδοσης. Επίσης, απαιτείται απενεργοποίηση των καταστάσεων που ρυθμίζουν την ενεργειακή απόδοση του επεξεργαστή καθόσον αυτό το επιτυγχάνουν μεταβάλλοντας τη συχνότητα λειτουργίας. Έτσι, απο το BIOS του εκάστοτε υπολογιστή απενεργοποιούμε οποιαδήποτε χαρακτηριστικά επενεργούν στη διαχειριστή ενέργειας (sleep καταστάσεις, και συγκεκριμένα C-states).

Οι τεχνολογίες διαχείρισης της ισχύς του επεξεργαστή καθορίζονται απο τις προδιαγραφές ACPI και διακρίνονται σε δύο κατηγορίες ή καταστάσεις.

#### 1. Καταστάσεις απόδοσης ισχύος (καταστάσεις ACPI P-states)

Οι καταστάσεις P παρέχουν έναν τρόπο κλιμάκωσης της συχνότητας και της τάσης στην οποία λειτουργεί ο επεξεργαστής έτσι ώστε να μειωθεί η κατανάλωση ισχύος της CPU. Ο αριθμός των διαθέσιμων καταστάσεων P μπορεί να είναι διαφορετικός για κάθε μοντέλο CPU, ακόμη και εκείνων από την ίδια οικογένεια.

Η κατάσταση P ουσιαστικά του επεξεργαστή είναι η δυνατότητα λειτουργίας του επεξεργαστή σε διαφορετικά επίπεδα τάσης και/ή συχνότητας(δηλαδή τα σημεία λειτουργίας). Γενικά, το P0 είναι η υψηλότερη κατάσταση με αποτέλεσμα τη μέγιστη απόδοση, ενώ τα P1, P2 και ούτω καθεξής, θα εξοικονομήσουν ενέργεια, αλλά με κάποιες επιπτώσεις στην απόδοση της CPU.

#### 2. Καταστάσεις αδράνειας επεξεργαστή (καταστάσεις ACPI C-states)

Οι καταστάσεις C είναι καταστάσεις όταν η CPU έχει μειώσει ή απενεργοποιήσει τις επιλεγμένες λειτουργίες. Διαφορετικοί επεξεργαστές υποστηρίζουν διαφορετικούς αριθμούς C-καταστάσεων στις οποίες είναι απενεργοποιημένα διάφορα μέρη της CPU. Γενικά, οι υψηλότερες καταστάσεις C απενεργοποιούν περισσότερα μέρη της CPU, γεγονός που μειώνει σημαντικά την κατανάλωση ενέργειας. Οι επεξεργαστές μπορεί να έχουν βαθύτερες καταστάσεις C που δεν εκτίθενται στο λειτουργικό σύστημα.

Οι αρχικές καταστάσεις είναι:

Το C0 είναι η κατάσταση λειτουργίας, που σημαίνει ότι η CPU κάνει χρήσιμη δουλειά Το C1 είναι η πρώτη κατάσταση αδράνειας Το C2 είναι η δεύτερη κατάσταση αδράνειας: Το εξωτερικό μπλοκ ελεγκτή εισόδου / εξόδου διακόπτει τον επεξεργαστή. Για παράδειγμα όταν ένας λογικός επεξεργαστής είναι αδρανής (κατάσταση C εκτός του C0), η συχνότητα του είναι συνήθως 0 (HALT).

Συνεπώς, οι καταστάσεις C είναι καταστάσεις αδρανούς εξοικονόμησης ενέργειας, σε αντίθεση με τις καταστάσεις P, οι οποίες είναι καταστάσεις εξοικονόμησης ενέργειας εκτέλεσης. Η κατάσταση P σημαίνει ότι ο πυρήνας της CPU είναι επίσης σε κατάσταση C0 επειδή πρέπει να τροφοδοτείται για την

εκτέλεση ενός κώδικα. Κατά τη διάρκεια μιας κατάστασης P, ο επεξεργαστής εξακολουθεί να εκτελεί οδηγίες, ενώ κατά τη διάρκεια μιας κατάστασης C (εκτός από C0), ο επεξεργαστής είναι αδρανής, πράγμα που σημαίνει ότι τίποτα δεν εκτελείται.

Απο την έκδοση 3.9 του πυρήνα Linux έχει προστεθεί ένας νεος οδηγός(driver) intel\_pstate της CPU για τη διαχείριση p-καταστάσεων για intel επεξεργαστές όπως αυτοί που περιέχονται στο hardware που χρησιμοποιήσαμε. Αυτό το πρόγραμμα οδήγησης υποστηρίζει πρόσφατα χαρακτηριστικά και θερμικό έλεγχο των σύγχρονων επεξεργαστών Intel. Το όνομά του προέρχεται από τα P-States.

Το πρόγραμμα οδήγησης CPU (acpi\_cpufreq) μέσω της γραμμής εντολών μπορεί να απενεργοποιήσει τις p-καταστάσεις χρησιμοποιώντας την επιλογή intel\_pstate = disable.

Άρα για να επιτύχουμε μία σταθερή συχνότητα του επεξεργαστή που θα μεταδίδει αυτή τη σταθερότητα και στη μετάδοση τους σήματος θα πρέπει:

- Να απενεργοποιηθούν όλα τα χαρακτηριστικά διαχείρισης ενέργειας(C-states) απο το BIOS καθώς και οποιαδήποτε λειτουργία κλιμακώνει τη συχνότητα(Intel SpeedStep). Σε μερικές περιπτώσεις αυτό μπορεί να γίνει και απο το λογισμικό cpufreqtool.
- Απενεργοποίηση των παράλληλων νημάτων(hyperhtreating) τόσο στο BIOS όσο και στον πυρήνα Linux. Αυτό μπορούμε να το ελέγξουμε με την εντολή

```
$ grep cpu MHz /proc/cpuinfo
```

- Απενεργοποίηση p-state και c-state απο το BIOS και απο τον πυρήνα Linux προσθέτοντας όπως αναφέραμε το intel\_pstate = disable στις επιλογές του Linux boot(συνήθως ο GRUB<sup>3</sup> είναι ο προεπιλεγμένος boot loader του Linux)

Στη περίπτωση μας προσθέσαμε την εντολή GRUB\_CMDLINE\_LINUX\_DEFAULT="quiet intel\_pstate=disable και processor.max\_cstate=1 intel\_idle.max\_cstate=0 idle=poll στο αρχείο /etc/default/grub και επανεκκινήσαμε το GRUB

- Προσθήκη "blacklist intel\_powerclamp" στο τέλος του αρχείου /etc/modprobe.d/blacklist.conf για να θέσει σε μαύρη λίστα το intel\_powerclamp" module<sup>4</sup>. Εάν δεν υπάρχει το αρχείο αυτό το δημιουργούμε καθώς το αρχείο /etc/modprobe.d λαμβάνει υπόψιν τις εξαρτήσεις και τις παραμέτρους των modules που προστίθενται ή αφαιρούνται.

Για ευκολία στην επιτήρηση της cpu μπορεί να εγκατασταθεί και το λογισμικό i7z utility.

Για να απενεργοποιηθεί η κλιμάκωση της συχνότητας της CPU εγκαθιστούμε

<sup>3</sup>GRand Unified Bootloader, GRUB είναι λειτουργία που αναλαμβάνει το BIOS κατά την εκκίνηση, να φορτώσει τον εαυτό του, να φορτώσει τον πυρήνα Linux στη μνήμη και, στη συνέχεια, να μετατρέψει την εκτέλεση στον πυρήνα. Μόλις ο πυρήνας αναλάβει, το GRUB έχει κάνει τη δουλειά του και δεν χρειάζεται πλέον.

<sup>4</sup>Ένα module είναι μία διαφορετική ενότητα ενός προγράμματος ή υλικού

το λογισμικό cpufrequtils. Η διαδικασία εγκατάστασης και ρύθμισης είναι η εξής:

```
1 $ sudo apt-get update
2 $ sudo apt-get install cpufrequtils
3 $ sudo vi /etc/default/cpufrequtils
```

Στην πρώτη γραμμή κάνουμε αναβάθμιση αποθετηρίων που όπως αναφέραμε γίνεται πριν από κάθε εγκατάσταση λογισμικού και έπειτα στη δεύτερη γραμμή εγκαθιστούμε το cpufrequtils. Στην τρίτη εντολή ανοίγουμε με τον κειμενογράφο vi το αρχείο /etc/default/cpufrequtils και προσθέτουμε στο τέλος την εξίσωση GOVERNOR="performance". Αποθηκεύουμε το αρχείο και έξοδος(στο vi αυτό γίνεται πατώντας το esc και εισάγοντας :wq). Στη συνέχεια απενεργοποιούμε και τις ondemand ρυθμίσεις στο παρασκήνιο, έτσι ώστε μετά την επανεκκίνηση να μην χρειαστεί η ίδια διαδικασία(επιστρέφει στις αρχικές ρυθμίσεις). Αυτό γίνεται με τις παρακάτω εντολές.

```
1 $ sudo update-rc.d ondemand disable
2 $ sudo /etc/init.d/cpufrequtils restart
```

Ελέγχουμε τελικά τις ρυθμίσεις της cpu με την εντολή cpu-info που μας εμφανίζει κάθε μπλοκ πληροφοριών για κάθε επεξεργαστή οι οποίες θα πρέπει να λειτουργούν στην μέγιστη ταχύτητα του επεξεργαστή.

### 5.1.3 Διεπαφές

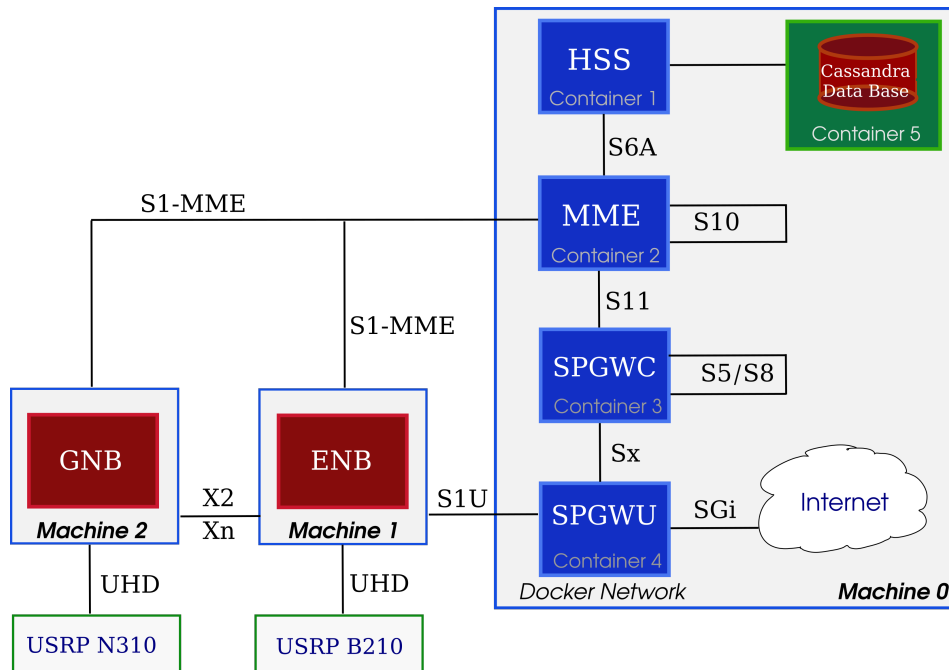
Η συνδεσμολογία μεταξύ των δικτύων πυρήνα και πρόσβασης απαιτεί μεγάλο ρυθμό μετάδοσης δεδομένων και για το λόγο αυτό το κανάλι μετάδοσης έχει ελάχιστες απαιτήσεις, δηλαδή θα πρέπει να αποτελείται τουλάχιστον από σειριακό καλώδιο usb 3.0, από καλώδιο UTP CAT.6 και από οπτική ίνα με υποδοχέα SFP+ που υποστηρίζει 10G ρυθμό μετάδοσης, όπου απαιτείται σε κάθε περίπτωση. Το καλώδιο Cat 6 αποτελεί μία μεγάλη αναβάθμιση από το Cat 5e. Μπορεί να διαχειριστεί ταχύτητα μέχρι 10 Gigabit στα 250 MHz. Για να αντιμετωπίσει επίσης το θέμα του crosstalking (παρεμβολές) έχει εσωτερική θωράκιση που διαχωρίζει το ένα καλώδιο από το άλλο. Οι θύρες που συνδέονται τα καλώδια UTP θα πρέπει να υποστηρίζουν το πρότυπο fast ethernet.

## 5.2 Υλοποίηση μη αυτόνομης λειτουργίας 5G

Η πρώτη εφαρμογή που θα υλοποιήσουμε είναι ένα μη αυτόνομο σύστημα 5G το οποίο αποτελείται από ένα Virtual Machine που φιλοξενεί το δίκτυο κορμού, ένα Virtual Machine που φιλοξενεί το δίκτυο πρόσβασης το οποίο με τη σειρά του συνδέεται με δύο συσκευές που αποτελούν την κεφαλή του ραδιοσυστήματος και ονομάζονται Universal Software Radio Peripheral (USRP). Με τη σειρά τους είναι αυτά που θα εκπέμπουν και θα λάβουν το σήμα από τη συσκευή χρήστη.

Το σχέδιο που υλοποιήσαμε κατά την διαδικασία παρουσιάζεται στην παρακάτω εικόνα 5.2.

Στη συνέχεια αναλύουμε τα στάδια υλοποίησης σε κάθε μέρος του δικτύου.



Εικόνα 5.2: Σχέδιο υλοποίησης μη αυτόνομου 5G συστήματος

### 5.2.1 Δίκτυο κορμού

Στο πρώτο VM, εγκαθιστούμε σε docker containers τις οντότητες που αποτελούν το δίκτυο κορμού όπως αυτό περιγράφηκε στο θεωρητικό μέρος για τη μη αυτόνομη λειτουργία.

Αρχικά θα πρέπει να κατεβάσουμε εντός του VM τα απαραίτητα αρχεία από το αποθετήριο του github της OAI, δηλαδή από την ιστοσελίδα <https://github.com/OPENAIRINTERFACE>. Η πιο πρόσφατη έκδοση είναι η ανάπτυξη 2021.w06 δηλαδή αυτή που δημοσιεύθηκε την 6η εβδομάδα του 2021. Εφόσον ολοκληρωθεί η ανάπτυξη, από develop έκδοση μετατρέπεται σε master. Ακολουθεί η διαδικασία αποθήκευσης των αρχείων αυτών στον τοπικό υπολογιστή.

#### Αποθήκευση αποθετηρίων στο τοπικό VM

```

1 $ git clone https://github.com/OPENAIRINTERFACE/openair-epc-fed.git
2 $ cd openair-epc-fed
3 $ git checkout 2021.w06
4 $ ./scripts/syncComponents.sh --hss-branch v1.1.1 --mme-branch 2020.w47
5 \
6 \
7 \
8 \
9 \
10 \
11 \
12 \
13 \
14 \
15 \
16 \
17 \
18 \
19 \
20 \
21 \
22 \
23 \
24 \
25 \
26 \
27 \
28 \
29 \
30 \
31 \
32 \
33 \
34 \
35 \
36 \
37 \
38 \
39 \
40 \
41 \
42 \
43 \
44 \
45 \
46 \
47 \
48 \
49 \
50 \
51 \
52 \
53 \
54 \
55 \
56 \
57 \
58 \
59 \
60 \
61 \
62 \
63 \
64 \
65 \
66 \
67 \
68 \
69 \
70 \
71 \
72 \
73 \
74 \
75 \
76 \
77 \
78 \
79 \
80 \
81 \
82 \
83 \
84 \
85 \
86 \
87 \
88 \
89 \
90 \
91 \
92 \
93 \
94 \
95 \
96 \
97 \
98 \
99 \
100 \
101 \
102 \
103 \
104 \
105 \
106 \
107 \
108 \
109 \
110 \
111 \
112 \
113 \
114 \
115 \
116 \
117 \
118 \
119 \
120 \
121 \
122 \
123 \
124 \
125 \
126 \
127 \
128 \
129 \
130 \
131 \
132 \
133 \
134 \
135 \
136 \
137 \
138 \
139 \
140 \
141 \
142 \
143 \
144 \
145 \
146 \
147 \
148 \
149 \
150 \
151 \
152 \
153 \
154 \
155 \
156 \
157 \
158 \
159 \
160 \
161 \
162 \
163 \
164 \
165 \
166 \
167 \
168 \
169 \
170 \
171 \
172 \
173 \
174 \
175 \
176 \
177 \
178 \
179 \
180 \
181 \
182 \
183 \
184 \
185 \
186 \
187 \
188 \
189 \
190 \
191 \
192 \
193 \
194 \
195 \
196 \
197 \
198 \
199 \
200 \
201 \
202 \
203 \
204 \
205 \
206 \
207 \
208 \
209 \
210 \
211 \
212 \
213 \
214 \
215 \
216 \
217 \
218 \
219 \
220 \
221 \
222 \
223 \
224 \
225 \
226 \
227 \
228 \
229 \
230 \
231 \
232 \
233 \
234 \
235 \
236 \
237 \
238 \
239 \
240 \
241 \
242 \
243 \
244 \
245 \
246 \
247 \
248 \
249 \
250 \
251 \
252 \
253 \
254 \
255 \
256 \
257 \
258 \
259 \
260 \
261 \
262 \
263 \
264 \
265 \
266 \
267 \
268 \
269 \
270 \
271 \
272 \
273 \
274 \
275 \
276 \
277 \
278 \
279 \
280 \
281 \
282 \
283 \
284 \
285 \
286 \
287 \
288 \
289 \
290 \
291 \
292 \
293 \
294 \
295 \
296 \
297 \
298 \
299 \
300 \
301 \
302 \
303 \
304 \
305 \
306 \
307 \
308 \
309 \
310 \
311 \
312 \
313 \
314 \
315 \
316 \
317 \
318 \
319 \
320 \
321 \
322 \
323 \
324 \
325 \
326 \
327 \
328 \
329 \
330 \
331 \
332 \
333 \
334 \
335 \
336 \
337 \
338 \
339 \
340 \
341 \
342 \
343 \
344 \
345 \
346 \
347 \
348 \
349 \
350 \
351 \
352 \
353 \
354 \
355 \
356 \
357 \
358 \
359 \
360 \
361 \
362 \
363 \
364 \
365 \
366 \
367 \
368 \
369 \
370 \
371 \
372 \
373 \
374 \
375 \
376 \
377 \
378 \
379 \
380 \
381 \
382 \
383 \
384 \
385 \
386 \
387 \
388 \
389 \
390 \
391 \
392 \
393 \
394 \
395 \
396 \
397 \
398 \
399 \
400 \
401 \
402 \
403 \
404 \
405 \
406 \
407 \
408 \
409 \
410 \
411 \
412 \
413 \
414 \
415 \
416 \
417 \
418 \
419 \
420 \
421 \
422 \
423 \
424 \
425 \
426 \
427 \
428 \
429 \
430 \
431 \
432 \
433 \
434 \
435 \
436 \
437 \
438 \
439 \
440 \
441 \
442 \
443 \
444 \
445 \
446 \
447 \
448 \
449 \
450 \
451 \
452 \
453 \
454 \
455 \
456 \
457 \
458 \
459 \
460 \
461 \
462 \
463 \
464 \
465 \
466 \
467 \
468 \
469 \
470 \
471 \
472 \
473 \
474 \
475 \
476 \
477 \
478 \
479 \
480 \
481 \
482 \
483 \
484 \
485 \
486 \
487 \
488 \
489 \
490 \
491 \
492 \
493 \
494 \
495 \
496 \
497 \
498 \
499 \
500 \
501 \
502 \
503 \
504 \
505 \
506 \
507 \
508 \
509 \
510 \
511 \
512 \
513 \
514 \
515 \
516 \
517 \
518 \
519 \
520 \
521 \
522 \
523 \
524 \
525 \
526 \
527 \
528 \
529 \
530 \
531 \
532 \
533 \
534 \
535 \
536 \
537 \
538 \
539 \
540 \
541 \
542 \
543 \
544 \
545 \
546 \
547 \
548 \
549 \
550 \
551 \
552 \
553 \
554 \
555 \
556 \
557 \
558 \
559 \
560 \
561 \
562 \
563 \
564 \
565 \
566 \
567 \
568 \
569 \
570 \
571 \
572 \
573 \
574 \
575 \
576 \
577 \
578 \
579 \
580 \
581 \
582 \
583 \
584 \
585 \
586 \
587 \
588 \
589 \
590 \
591 \
592 \
593 \
594 \
595 \
596 \
597 \
598 \
599 \
600 \
601 \
602 \
603 \
604 \
605 \
606 \
607 \
608 \
609 \
610 \
611 \
612 \
613 \
614 \
615 \
616 \
617 \
618 \
619 \
620 \
621 \
622 \
623 \
624 \
625 \
626 \
627 \
628 \
629 \
630 \
631 \
632 \
633 \
634 \
635 \
636 \
637 \
638 \
639 \
640 \
641 \
642 \
643 \
644 \
645 \
646 \
647 \
648 \
649 \
650 \
651 \
652 \
653 \
654 \
655 \
656 \
657 \
658 \
659 \
660 \
661 \
662 \
663 \
664 \
665 \
666 \
667 \
668 \
669 \
670 \
671 \
672 \
673 \
674 \
675 \
676 \
677 \
678 \
679 \
680 \
681 \
682 \
683 \
684 \
685 \
686 \
687 \
688 \
689 \
690 \
691 \
692 \
693 \
694 \
695 \
696 \
697 \
698 \
699 \
700 \
701 \
702 \
703 \
704 \
705 \
706 \
707 \
708 \
709 \
710 \
711 \
712 \
713 \
714 \
715 \
716 \
717 \
718 \
719 \
720 \
721 \
722 \
723 \
724 \
725 \
726 \
727 \
728 \
729 \
730 \
731 \
732 \
733 \
734 \
735 \
736 \
737 \
738 \
739 \
740 \
741 \
742 \
743 \
744 \
745 \
746 \
747 \
748 \
749 \
750 \
751 \
752 \
753 \
754 \
755 \
756 \
757 \
758 \
759 \
760 \
761 \
762 \
763 \
764 \
765 \
766 \
767 \
768 \
769 \
770 \
771 \
772 \
773 \
774 \
775 \
776 \
777 \
778 \
779 \
780 \
781 \
782 \
783 \
784 \
785 \
786 \
787 \
788 \
789 \
790 \
791 \
792 \
793 \
794 \
795 \
796 \
797 \
798 \
799 \
800 \
801 \
802 \
803 \
804 \
805 \
806 \
807 \
808 \
809 \
810 \
811 \
812 \
813 \
814 \
815 \
816 \
817 \
818 \
819 \
820 \
821 \
822 \
823 \
824 \
825 \
826 \
827 \
828 \
829 \
830 \
831 \
832 \
833 \
834 \
835 \
836 \
837 \
838 \
839 \
840 \
841 \
842 \
843 \
844 \
845 \
846 \
847 \
848 \
849 \
850 \
851 \
852 \
853 \
854 \
855 \
856 \
857 \
858 \
859 \
860 \
861 \
862 \
863 \
864 \
865 \
866 \
867 \
868 \
869 \
870 \
871 \
872 \
873 \
874 \
875 \
876 \
877 \
878 \
879 \
880 \
881 \
882 \
883 \
884 \
885 \
886 \
887 \
888 \
889 \
890 \
891 \
892 \
893 \
894 \
895 \
896 \
897 \
898 \
899 \
900 \
901 \
902 \
903 \
904 \
905 \
906 \
907 \
908 \
909 \
910 \
911 \
912 \
913 \
914 \
915 \
916 \
917 \
918 \
919 \
920 \
921 \
922 \
923 \
924 \
925 \
926 \
927 \
928 \
929 \
930 \
931 \
932 \
933 \
934 \
935 \
936 \
937 \
938 \
939 \
940 \
941 \
942 \
943 \
944 \
945 \
946 \
947 \
948 \
949 \
950 \
951 \
952 \
953 \
954 \
955 \
956 \
957 \
958 \
959 \
960 \
961 \
962 \
963 \
964 \
965 \
966 \
967 \
968 \
969 \
970 \
971 \
972 \
973 \
974 \
975 \
976 \
977 \
978 \
979 \
980 \
981 \
982 \
983 \
984 \
985 \
986 \
987 \
988 \
989 \
990 \
991 \
992 \
993 \
994 \
995 \
996 \
997 \
998 \
999 \
1000 \

```

Στην πρώτη εντολή δημιουργούμε ένα αντίγραφο αρχείων του αποθετηρίου στον τοπικό υπολογιστή και συγκεκριμένα μέσα στο VM του δικτύου κορμού. Στη δεύτερη εντολή (Change Directory, cd) γίνεται είσοδος στο φάκελο που έχει κατέβει στο VM και περιέχει τα αρχεία και στην τρίτη εντολή (git checkout) μπορούμε να περιηγηθούμε στην έκδοση που επιθυμούμε εντός του αποθετηρίου και οποιαδήποτε εγκατάσταση γίνει λαμβάνει τα αρχεία της έκδοσης που ακολουθεί την εντολή. Η τέταρτη εντολή είναι ένα μικρό πρόγραμμα γραμμένο σε Bash που συγχρονίζει την κάθε οντότητα με μία συγκεκριμένη και ελεγμένη έκδοση, υποψήφια προς εγκατάσταση.

### **Δημιουργία εικόνων containers**

Στη συνέχεια δημιουργούμε με τη βοήθεια του docker εικόνες με τα υποψήφια containers που το κάθε ένα αντιπροσωπεύει και μία οντότητα του 5G non stand alone. Οι εικόνες αυτές θα πρέπει να εκτελεστούν αργότερα σε ένα περιβάλλον docker για να αρχίσει να εκτελείται και το container με τη σειρά του.

#### **Home Subscriber Server**

```
1 $ docker build --target oai-hss --tag oai-hss:production \
2     --file component/oai-hss/docker/Dockerfile.ubuntu18.04 \
3     component/oai-hss
4 $ docker image prune --force
5 $ docker image ls
```

Η πρώτη εντολή δημιουργεί ένα αρχείο εικόνας με τη βοήθεια του αρχείου Dockerfile που δέχεται τον πηγαίο κώδικα του προγράμματος που θέλουμε να αναπτύξουμε σε container και τις απαραίτητες εντολές για την υλοποίηση της εικόνας. Επιπλέον, περιέχει το όνομα και μια ετικέτα για περαιτέρω συσχέτισμό με άλλα containers καθώς και τη διαδρομή αποθήκευσης της τελικής εικόνας και του αρχείου Dockerfile.

Η δεύτερη εντολή διαγράφει τυχόν αχρησιμοποίητα docker images και αντικείμενα που μπορεί να υπάρχουν και η τρίτη εντολή κάνει εμφανίζει πληροφορίες των εικόνων που έχουν δημιουργηθεί.

Όμοια δημιουργούμε και εικόνες για τις άλλες λειτουργίες.

#### **Mobility Management Entity**

```
1 $ docker build --target oai-mme --tag oai-mme:production \
2     --file component/oai-mme/docker/Dockerfile.ubuntu18.04 \
3     component/oai-mme
4 $ docker image prune --force
5 $ docker image ls
```

#### **Service Packet Gateway Control plane**

```
1 $ docker build --target oai-spgwc --tag oai-spgwc:production \
2     --file component/oai-spgwc/docker/Dockerfile.ubuntu18.04 \
3     component/oai-spgwc
4 $ docker image prune --force
5 $ docker image ls
```

#### **Service Packet Gateway User plane**

```

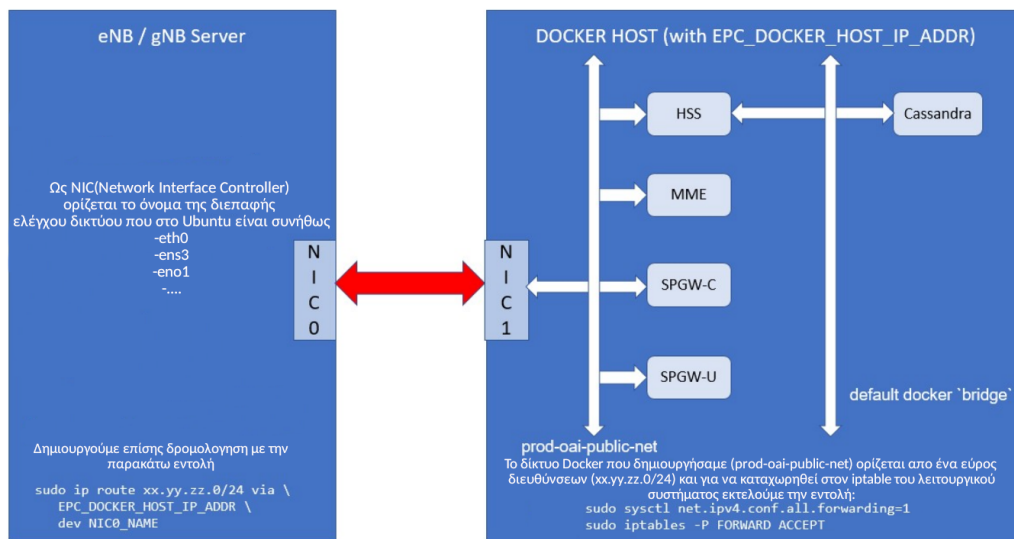
1 $ docker build --target oai-spgwu-tiny --tag oai-spgwu-tiny:production
  \
2         --file component/oai-spgwu-tiny/docker/Dockerfile.
  ubuntu18.04 \
3         component/oai-spgwu-tiny
4 $ docker image prune --force
5 $ docker image ls

```

Εφόσον δημιουργήσαμε εικόνες containers για κάθε οντότητα, θα πρέπει τώρα να εκτελέσουμε σε περιβάλλον docker αυτές τις εικόνες για να λειτουργήσουν τα containers ως στοιχεία του EPC δικτύου πυρήνα του μη αυτόνομου 5G δικτύου.

### Εκτέλεση και Διαμόρφωση των Containers

Η βασική λογική σχεδίασης του δικτύου φαίνεται στο παρακάτω σχήμα.



Εικόνα 5.3: Συνδεσιμότητα eNB/gNB server με το Docker δίκτυο κορμού [45]

Η πρόσβαση σε ένα container από τον ίδιο server όπου έχουν αναπτυχθεί είναι εύκολη διαδικασία. Όταν όμως πρόσβαση σε αυτό το δίκτυο docker γίνεται από άλλο μηχάνημα server τότε θα πρέπει να ακολουθηθεί η ροή που περιγράφει η εικόνα 5.3. Αυτή η διαδικασία περιγράφεται στα παρακάτω βήματα.

Αρχικά, δημιουργούμε ένα δίκτυο διευθύνσεων που θα ονομάζεται prod-oai-public-net από το οποίο θα διευθυνσιοδοτούνται τα containers.

```

1 $ docker network create --attachable --subnet 192.168.61.0/26 --ip-
  range 192.168.61.0/26 prod-oai-public-net

```

Έπειτα εισάγουμε το δίκτυο αυτό στο routing table των server του eNB και gNB ώστε να δρομολογείται η κίνηση από το δίκτυο πρόσβασης στο δίκτυο κορμού και ειδικότερα στο δίκτυο των containers. Αυτό γίνεται εκτελώντας στους servers του RAN την εντολή

```

1 $ sudo ip route add 192.168.61.0/24 via xx.yy.zz.kk dev NIC_0

```

όπου στα xx.yy.zz.kk εισάγουμε τη διεύθυνση ip που φιλοξενεί το EPC\_DOCKER και NIC\_0 το όνομα της διεπαφής του server του RAN σε

κάθε περίπτωση(εκτελούμε την παραπάνω εντολή σε όσους server είναι εγκατεστημένοι οι κόμβοι B).

Στη συνέχεια αναπτύσσουμε τα container εκτελώντας run στις εικόνες όπως παρακάτω

```

1 $ docker run --name prod-cassandra -d -e CASSANDRA_CLUSTER_NAME="OAI
   HSS Cluster" \
2     -e CASSANDRA_ENDPOINT_SNITCH=GossipingPropertyFileSnitch
   cassandra:2.1
3 $ docker run --privileged --name prod-oai-hss -d --entrypoint /bin/bash
   oai-hss:production -c "sleep infinity"
4 $ docker network connect prod-oai-public-net prod-oai-hss
5 $ docker run --privileged --name prod-oai-mme --network prod-oai-public
   -net \
6     -d --entrypoint /bin/bash oai-mme:production -c "sleep
   infinity"
7 $ docker run --privileged --name prod-oai-spgwc --network prod-oai-
   public-net \
8     -d --entrypoint /bin/bash oai-spgwc:production -c "sleep
   infinity"
9 $ docker run --privileged --name prod-oai-spgwu-tiny --network prod-oai-
   -public-net \
10    -d --entrypoint /bin/bash oai-spgwu-tiny:production -c "
   sleep infinity"

```

Η διαμόρφωση των containers με τις παραμέτρους που αρμόζουν στο δίκτυο που έχουμε φτιάξει ξεκινά με τη βάση δεδομένων που αποτελεί και το μέσο αποθήκευσης δεδομένων που αφορούν κυρίως τους συνδρομητές, που θα πρέπει να πιστοποιηθούν και να εγκριθούν για να τους επιτραπεί η χρήση του δικτύου 5G.

```

1 $ docker cp component/oai-hss/src/hss_rel14/db/oai_db.cql prod-
   cassandra:/home
2 $ docker exec -it prod-cassandra /bin/bash -c "nodetool status"
3 $ Cassandra_IP=`docker inspect --format="{{range .NetworkSettings.
   Networks}}{{.IPAddress}}{{end}}" prod-cassandra `
4 $ docker exec -it prod-cassandra /bin/bash -c "cqlsh --file /home/
   oai_db.cql ${Cassandra_IP}"

```

Έτσι, στην πρώτη γραμμή αντιγράφουμε το αρχείο cql που αποτελεί αρχείο της βάσεις δεδομένων Cassandra της εταιρείας Apache. Το αρχείο αυτό περιέχει τις διαθέσιμες παραμέτρους τις οποίες χρειάζεται το δίκτυο και αφορούν τους συνδρομητές. Αυτές οι παράμετροι περιγράφονται στον εξοπλισμό χρήστη και δτη δοαμόρφωση της κάρτας SIM.

Η εισαγωγή των παραμέτρων αυτών στη βάση δεδομένων γίνεται με τη βοήθεια της οντότητας HSS καθώς και ο εμπλουτισμός αυτών κατα την εγγραφή για παράδειγμα ενός νέου συνδρομητή. Αφού καταχωρήσουμε μία IP για την οντότητα HSS στη συνέχεια με τη βοήθεια python<sup>5</sup> script εισάγονται παράμετροι προς αποθήκευση. Παρακάτω, εισάγονται οι παράμετροι για την περίπτωση μας.

```

1 $ HSS_IP=`docker exec -it prod-oai-hss /bin/bash -c "ifconfig eth1 |
   grep inet" | sed -f ./ci-scripts/convertIpAddrFromIfconfig.sed `
2 $ python3 component/oai-hss/ci-scripts/generateConfigFiles.py --kind=
   HSS --cassandra=${Cassandra_IP} \

```

<sup>5</sup>Το σκριπτ είναι γραμμένο στην έκδοση 3 της python



```

3     --hss_s6a=${HSS_IP} --apn1=apn1.carrier.com --apn2=apn2.
      carrier.com \
4     --users=200 --imsi=320230100000001 \
5     --ltek=0c0a34601d4f07677303652c0462535b --op=63
      bfa50ee6523365ff14c1f45f88737d \
6     --nb_mmes=1 --from_docker_file
7 $ docker cp ./hss-cfg.sh prod-oai-hss:/openair-hss/scripts
8 $ docker exec -it prod-oai-hss /bin/bash -c "cd /openair-hss/scripts &&
      chmod 777 hss-cfg.sh && ./hss-cfg.sh"

```

Το python script αποθηκεύει στον τοπικό server, εκτός των container, τα δεδομένα. Συνεπώς θα πρέπει να τα αντιγράψουμε εντός του δικτύου των containers και συγκεκριμένα στο container HSS. Έπειτα, δίνουμε δικαιώματα διαχειριστή ανάγνωσης και εγγραφής των δεδομένων αυτών από το HSS container. Αυτά γίνονται με τις εντολές 3 και 4 αντίστοιχα.

Η ίδια διαδικασία ακολουθείται και για την οντότητα MME χωρίς να χρειάζεται κάποια παραμετροποίηση καθώς είναι ήδη προσαρμοσμένη στις ανάγκες υλοποίησης των containers.

```

1 $ MME_IP=`docker inspect --format="{{range .NetworkSettings.Networks
      }}"{{.IPAddress}}{{end}}" prod-oai-mme`
2 $ SPGW0_IP=`docker inspect --format="{{range .NetworkSettings.Networks
      }}"{{.IPAddress}}{{end}}" prod-oai-spgwc`
3 $ python3 component/oai-mme/ci-scripts/generateConfigFiles.py --kind=
      MME \
4     --hss_s6a=${HSS_IP} --mme_s6a=${MME_IP} \
5     --mme_s1c_IP=${MME_IP} --mme_s1c_name=eth0 \
6     --mme_s10_IP=${MME_IP} --mme_s10_name=eth0 \
7     --mme_s11_IP=${MME_IP} --mme_s11_name=eth0 --spgwc0_s11_IP=${
      SPGW0_IP} \
8     --mcc=320 --mnc=230 --tac_list="5 6 7" --from_docker_file
9 $ docker cp ./mme-cfg.sh prod-oai-mme:/openair-mme/scripts
10 $ docker exec -it prod-oai-mme /bin/bash -c "cd /openair-mme/scripts &&
      chmod 777 mme-cfg.sh && ./mme-cfg.sh"

```

Για την οντότητα SPGW-C θα πρέπει να εισάγουμε τις διευθύνσεις των DNS server, καθώς το SPGW-C είναι η οντότητα που θα συνδέσει την ολική δικτύωση με ένα άλλο δίκτυο. Στην περίπτωση μας για τη μετάφραση των Domain names σε διευθύνσεις χρησιμοποιήσαμε τους DNS της Google (8.8.8.8 και 8.8.4.4)

```

1 $ python3 component/oai-spgwc/ci-scripts/generateConfigFiles.py --kind=
      SPGW-C \
2     --s11c=eth0 --sxc=eth0 --apn=apn1.carrier.com \
3     --dns1_ip=8.8.8.8 --dns2_ip=8.8.4.4 --from_docker_file
4 $ docker cp ./spgwc-cfg.sh prod-oai-spgwc:/openair-spgwc
5 $ docker exec -it prod-oai-spgwc /bin/bash -c "cd /openair-spgwc &&
      chmod 777 spgwc-cfg.sh && ./spgwc-cfg.sh"

```

Τέλος, η τελευταία διαμόρφωση είναι αυτή του container που περιέχει την οντότητα SPGWU

```

1 $ python3 component/oai-spgwu-tiny/ci-scripts/generateConfigFiles.py --
      kind=SPGW-U \
2     --sxc_ip_addr=${SPGW0_IP} --sxu=eth0 --slu=eth0 --
      from_docker_file
3 $ docker cp ./spgwu-cfg.sh prod-oai-spgwu-tiny:/openair-spgwu-tiny
4 $ docker exec -it prod-oai-spgwu-tiny /bin/bash -c "cd /openair-spgwu-
      tiny && chmod 777 spgwu-cfg.sh && ./spgwu-cfg.sh"

```

Κατα την ολοκλήρωση εκτέλεσης των παραπάνω εντολών, η έξοδος του τερματικού διαφέρει ανα περίπτωση επιβεβαιώνοντας την ορθή εκτέλεση αυτών.

Σε περίπτωση αποτυχίας μιας ανάπτυξης θα πρέπει να γίνει εξ αρχής ανάπτυξη όλων των containers.

## 5.2.2 Δίκτυο πρόσβασης

Το δίκτυο πρόσβασης το οποίο στοχεύει να ακολουθήσει τις προτάσεις της 3GPP αποτελείται από δύο servers, με τις προδιαγραφές που περιγράψαμε στα προαπαιτούμενα, καθώς και από δύο USRP που αποτελούν το άκρο του δικτύου πρόσβασης, αποτελούν τους κόμβους eNB και gNB και αλληλεπιδρούν με τη συσκευή του χρήστη. Ο κώδικας που διατίθεται προς εγκατάσταση από την OpenAirInterface βρίσκεται στα αποθετήρια του gitlab της Eurecom. Ο πηγαίος κώδικας βρίσκεται σε ένα build script με την ονομασία `build_oai` εντός της διαδρομής του αποθετηρίου `openairinterface5g/cmake_targets` και περιέχει δυαδικά αρχεία-binaries<sup>6</sup> για διάφορες πλατφόρμες υλικού και περιπτώσεις χρήσεις.

Θεωρούμε επίσης δεδομένο ότι έχουμε εγκαταστήσει σε όλες τις περιπτώσεις του RAN τον πυρήνα χαμηλής καθυστέρησης Linux. Για να δούμε ποιον πυρήνα χρησιμοποιεί το λειτουργικό σύστημα κατά τη διάρκεια λειτουργίας εκτελούμε `uname -r`

Τα κύρια oai binaries αρχεία που έχουν δοκιμαστεί από την CI/CD διαδικασία είναι:

- To LTE UE: *lte-uesoftmodem*
- To 5G UE: *nr-uesoftmodem*
- To LTE eNodeB: *lte-softmodem*
- To 5G gNodeB: *nr-softmodem*
- To LTE PHY simulators: *dlsim και ulsim*
- To 5G PHY simulators: *nr\_dlschsim nr\_dlsim nr\_pbchsim nr\_pucchsim nr\_ulschsim nr\_ulsim polartest smallblocktest ulsim ldpctest*

Επίσης, δημιουργεί και κάποια άλλα scripts τα οποία χρησιμοποιούνται περισσότερο σε προσομοιώσεις του μη αυτόνομου δικτύου. Τέτοιες περιπτώσεις μπορεί να είναι σενάρια προσομοίωσης χωρίς χρήση δικτύου κορμού(noS1), προσομοίωση εξοπλισμού χρήστη, κεραιών κλπ.

Το σύστημα build για το OAI χρησιμοποιεί το εργαλείο `cmake` το οποίο δημιουργεί `makefiles`, απαραίτητα αρχεία για την υλοποίηση και ολοκλήρωση της εγκατάστασης. Το `build_oai` script είναι ένα σκριπτ που περιλαμβάνει `cmake`, `make` και εντολές κελύφους(shell) του linux προκειμένου να γίνει ευκολότερο το build και η χρήση του OAI λογισμικού.

<sup>6</sup>Εκτελέσιμα αρχεία συνδεδεμένα με μερισμένες βιβλιοθήκες

### Δημιουργία εκτελέσιμων eNodeB και gNodeB

Μετά το κατέβασμα στους τοπικούς server (όπου έχουμε εγκαταστήσει το RAN σε κάθε περίπτωση) των πηγαίων αρχείων, μία απλή build εντολή μπορεί να χρησιμοποιηθεί για να λάβουν υποστήριξη όλα τα binaries αρχεία όλων των περιπτώσεων softmodem που αναφέραμε παραπάνω. Έτσι εκτελούμε στον φάκελο όπου κατεβάσαμε από το git τα αρχεία τα κάτωθι:

```

1 $ cd <your oai installation directory>/openairinterface5g/
2 $ source oaienv
3 $ cd cmake_targets/
4 $ ./build_oai -I -w USRP --eNB --UE --nrUE --gNB

```

Παρακάτω εξηγούμε τα ορίσματα της εντολής build\_oai:

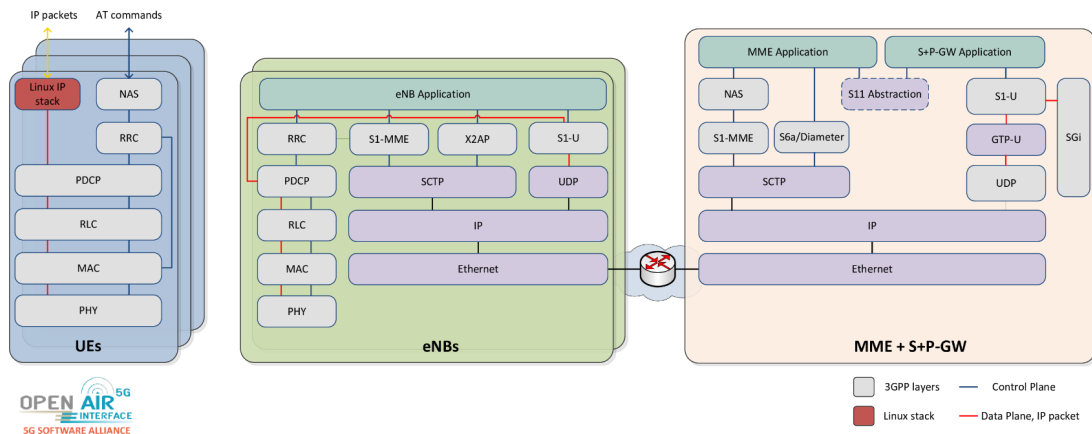
- Το -I όρισμα εγκαθιστά προαπαιτούμενα πακέτα για να γίνει το build των softmodems και χρειάζεται μόνο την πρώτη φορά
- Το -w όρισμα χρησιμοποιείται για να υποστηρίξει ραδιοκεφαλές που πρέπει πρόκειται να χρησιμοποιηθούν (στην συγκεκριμένη περίπτωση τα usrps).
- Το όρισμα -eNB είναι για τη δημιουργία του εκτελέσιμου lte-softmodem και όλων των απαραίτητων κοινόχρηστων βιβλιοθηκών
- Το όρισμα -gNB είναι για τη δημιουργία του εκτελέσιμου nr-softmodem και όλων των απαραίτητων κοινόχρηστων βιβλιοθηκών
- Το όρισμα -UE είναι για τη δημιουργία του εκτελέσιμου lte-uesoftmodem και όλων των απαραίτητων κοινόχρηστων βιβλιοθηκών (για προσομοίωση εξοπλισμού χρήστη)
- Το όρισμα -nrUE είναι για τη δημιουργία του εκτελέσιμου nr-uesoftmodem και όλων των απαραίτητων κοινόχρηστων βιβλιοθηκών (για προσομοίωση εξοπλισμού χρήστη)

Είναι δυνατόν να επιλέγεται και μεμονωμένα η κάθε περίπτωση από τις παραπάνω. Μετά την ολοκλήρωση του build, τα binaries αρχεία είναι διαθέσιμα στον φάκελο cmake\_targets/ran\_build/build. Αντίγραφα των αρχείων αυτών υπάρχουν και στον φάκελο /target/bin με όλα τα επιθέματα της έκδοσης 15 της 3GPP.

Ένα απλό διάγραμμα block με το UE να συνδέεται στο eNB φαίνεται παρακάτω.

Επιπλέον, στον φάκελο αρχείων targets/PROJECTS/GENERIC-LTE-EPC/CONF υπάρχει ένα σύνολο αρχείων διαμόρφωσης στα οποία πρέπει να εισάγουμε την διεύθυνση ip του MME και τη διεύθυνση eNB/gNB αντίστοιχα, ανάλογα με την περίπτωση καθώς επίσης και το όνομα της διεπαφής. Επίσης, θα πρέπει να εισάγουμε και τη διεύθυνση του gNB στο αρχείο διαμόρφωσης του eNB στη γραμμή επιλογής διεύθυνσης, δηλαδή τη διεπαφή X2.

Τα αρχεία αυτά φέρουν ονομασία που χαρακτηρίζει τη λειτουργικότητα τους, δηλαδή για ποιον κόμβο αναφέρονται (eNB/gNB), την ζώνη



Εικόνα 5.4: Διάγραμμα Block του OpenAirInterface[45]

συχνοτήτων, τον αριθμό των Physical Resource Block (PRB)<sup>7</sup> και για που προορίζονται (για παράδειγμα για το `usrp-b210`), όπως για παράδειγμα `enb.band7.tm1.50PRB.usrpb210.conf`.

Όσον αφορά τη διαμόρφωση του αρχείου για το eNB και την αλλαγή του IPv4 πεδίου με την ip του EPC server όπως φαίνεται στο παρακάτω πλαίσιο

```

////////// MME parameters:
mme_ip_address = ( ipv4 = "***YOUR_EPC_IP_ADDR**";
ipn6 = "192:168:30::17";
active = "yes";
preference = "ipv4";
    
```

Εισάγουμε επίσης και την ip του eNB server καθώς και το όνομα της διεπαφής NIC που αντιστοιχεί στην S1 διεπαφή

```

NETWORK_INTERFACES :
ENB_INTERFACE_NAME_FOR_S1_MME = "eth0";
ENB_IPV4_ADDRESS_FOR_S1_MME = "***YOUR_ENB_IP_ADDR**";
ENB_INTERFACE_NAME_FOR_S1U = "eth0";
ENB_IPV4_ADDRESS_FOR_S1U = "***YOUR_ENB_IP_ADDR**";
ENB_PORT_FOR_S1U = 2152; # Spec 2152
ENB_IPV4_ADDRESS_FOR_X2C = "***YOUR_ENB_IP_ADDR**";
ENB_PORT_FOR_X2C = 36422; # Spec 36422
    
```

Όμοια εισάγουμε και τις αντίστοιχες ip στο αρχείο διαμόρφωσης του gNB όπως και πριν στα αντίστοιχα πεδία καθώς και τη διεύθυνση για τη διεπαφή X2 ώστε να επικοινωνεί το eNB με το gNB.

<sup>7</sup>Ένα PRB είναι το μικρότερο στοιχείο κατανομής πόρων που έχει εκχωρηθεί από τον scheduler του eNB/gNB

```

///X2
enable_x2 = "yes";
t_reloc_prep = 1000; /* unit: millisecond */
tx2_reloc_overall = 2000; /* unit: millisecond */
target_enb_x2_ip_address = (
ipv4 = "***YOUR_ENB_IP_ADDR***";
ipv6 = "192:168:30::17";
preference = "ipv4";

);

NETWORK_INTERFACES :

GNB_INTERFACE_NAME_FOR_S1_MME = "eth0";
GNB_IPV4_ADDRESS_FOR_S1_MME = "***YOUR_GNB_IP_ADDR***";
GNB_INTERFACE_NAME_FOR_S1U = "eth0";
GNB_IPV4_ADDRESS_FOR_S1U = "***YOUR_GNB_IP_ADDR***";
GNB_PORT_FOR_S1U = 2152; # Spec 2152
GNB_IPV4_ADDRESS_FOR_X2C = "***YOUR_GNB_IP_ADDR***";
GNB_PORT_FOR_X2C = 36422; # Spec 36422
;

```

### Universal Software Radio Peripheral (USRP)

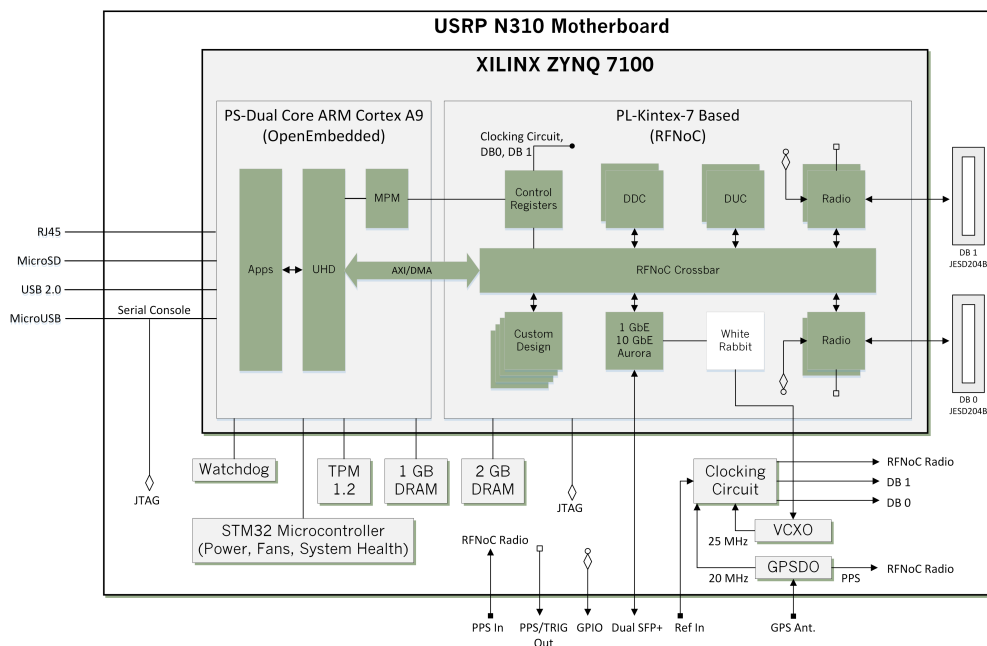
Όπως αρκετές φορές αναφέραμε κατά τη διάρκεια της εργασίας, ως ραδιο κεφαλή (radio head) χρησιμοποιήσαμε συσκευές USRP. Το Universal Software Radio Peripheral (USRP), ραδιοσύστημα βασισμένο στο λογισμικό, είναι ένας συντονιζόμενος πομποδέκτης για το σχεδιασμό, την παραγωγή πρωτοτύπων και την ανάπτυξη συστημάτων ραδιοεπικοινωνίας. Για την εγκατάσταση τους απαιτείται η εγκατάσταση οδηγών (drivers) και συγκεκριμένα οι οδηγοί UHD όπου εικόνες αυτών υπάρχουν προεγκατεστημένοι στα λογισμικά των USRP. Το UHD επίσης διαθέτει API όπου μέσω γλώσσας προγραμματισμού Python μπορεί ο χρήστης να επικοινωνήσει, να διαχειριστεί, να αναβαθμίσει και γενικότερα να ελέγξει τη λειτουργία του USRP. Παρακάτω περιγράφουμε τα δύο μοντέλα που χρησιμοποιήσαμε.

#### USRP N310

Το N310 μοντέλο είναι από τις τελευταίες εκδόσεις USRP της εταιρείας Ettus σχεδιασμένο ειδικά για το 5G-NR. Υποστηρίζει μέχρι και 100MHz εύρος ζώνης και διαθέτει θύρες SFP+ 1G και 10G για σύνδεση με οπτική ίνα, καθώς και θύρα ethernet για διαχείριση μέσου του δικτύου. Σε αντίθεση με άλλα USRP προηγούμενης γενιάς, διαθέτει λογισμικό Linux με εύκολη αναβάθμιση μέσω αποθετηρίων mender καθώς έχει προεγκατεστημένη την έκδοση ανοικτού κώδικα λογισμικού API UHD 3.11.0 με αναβάθμιση σε επόμενες εκδόσεις (με

την βοήθεια mender). Επίσης, δέχεται και προγραμματισμό του επεξεργαστή FPGA που διαθέτει για RFNoC(RF Network on Chip) framework. Επιπλέον, περιλαμβάνει πλατφόρμα TPM( Trusted Platform Module) που ενεργοποιεί χαρακτηριστικά ασφαλείας όπως κρυπτογράφηση αρχείων.[46]

Η συσκευή USRP N310 απλοποιεί τον έλεγχο και τη διαχείριση ενός δικτύου ραδιοφώνων, εισάγοντας τη μοναδική δυνατότητα εκτέλεσης απομακρυσμένων εργασιών, όπως ενημέρωση λογισμικού, επανεκκίνηση, επαναφορά εργοστασιακών ρυθμίσεων, αυτοέλεγχος, εντοπισμός σφαλμάτων κεντρικού υπολογιστή / ARM και παρακολούθηση της υγείας του συστήματος.[46]



Εικόνα 5.5: Διάγραμμα Block μητρικής κάρτας Ettus Usrc N310[46]

Το USRP N310 είναι μία από τις υψηλότερες συσκευές πυκνότητας καναλιών στην αγορά SDR, προσφέροντας τέσσερα κανάλια RX και τέσσερα TX σε συντελεστή μορφής RU μισού πλάτους. Το RF front end χρησιμοποιεί δύο πομποδέκτες AD9371, την τελευταία τεχνολογία RFIC από Analog Devices. Κάθε κανάλι παρέχει έως 100 MHz στιγμιαίου εύρους ζώνης και καλύπτει ένα εκτεταμένο εύρος συχνοτήτων από 10 MHz έως 6 GHz.[46]

Οι χρήστες μπορούν να δημιουργήσουν πρωτότυπα και να αναπτύξουν αξιόπιστα σχέδια για μια ποικιλία εφαρμογών SDR, όπως ασύρματα testbeds, απομακρυσμένες κεφαλές ραδιοφώνου, παρακολούθηση φάσματος και πολλά άλλα.[46]

**Η συσκευή αυτή χρησιμοποιήθηκε ως Radio Head για το gNB.**

### **USRP B210**

Το USRP B210 παρέχει μια πλήρως ενσωματωμένη πλατφόρμα Universal Software Radio Peripheral (USRP™) με συνεχή κάλυψη συχνοτήτων από 70 MHz - 6 GHz. Σχεδιασμένο για πειραματισμό χαμηλού κόστους, συνδυάζει τον πομποδέκτη άμεσης μετατροπής AD9361 RFIC που παρέχει έως και 56MHz

εύρους ζώνης σε πραγματικό χρόνο, ένα ανοιχτό και επαναπρογραμματιζόμενο Spartan6 FPGA και γρήγορη συνδεσιμότητα SuperSpeed USB 3.0. Η πλήρης υποστήριξη του λογισμικού USRP Hardware Driver™ (UHD) επιτρέπει την εύκολη και άμεση έναρξη της ανάπτυξης με το λογισμικό GNU Radio, ώστε ο χρήστης να δημιουργεί πρωτότυπους σταθμούς βάσης GSM με OpenBTS. [46]

Υπάρχει πλήθος εφαρμογών χρήσης όπως FM και τηλεοπτική μετάδοση, κινητό, GPS, WiFi, ISM και άλλα. Το ενσωματωμένο RF frontend στο USRP B210 έχει σχεδιαστεί με τις νέες αναλογικές συσκευές AD9361, έναν πομποδέκτη άμεσης μετατροπής ενός τσιπ, ικανός να μεταδίδει έως και 56 MHz εύρους ζώνης σε πραγματικό χρόνο. Το B210 χρησιμοποιεί και τις δύο αλυσίδες σήματος του AD9361, παρέχοντας συνεκτική δυνατότητα MIMO. Η ενσωματωμένη επεξεργασία σήματος και ο έλεγχος του AD9361 πραγματοποιείται από ένα Spartan6 XC6SLX150 FPGA συνδεδεμένο σε έναν κεντρικό υπολογιστή χρησιμοποιώντας το SuperSpeed USB 3.0. Η απόδοση σε πραγματικό χρόνο USRP B210 συγκρίνεται με τετραγωνικό ρυθμό 61,44MS / s, παρέχοντας τα πλήρη 56 MHz στιγμιαίου εύρους ζώνης RF στον κεντρικό υπολογιστή για επιπλέον επεξεργασία χρησιμοποιώντας το GNU Radio ή εφαρμογές που χρησιμοποιούν το UHD API. [46]

**Η συσκευή αυτή χρησιμοποιήθηκε ως Radio Head για το eNB.**

### 5.2.3 Εξοπλισμός χρήστη

Ένα τηλεπικοινωνιακό σύστημα ή ένα σύστημα επικοινωνίας γενικότερα αποσκοπεί στην end-to-end ολοκληρωμένη συνδεσιμότητα ώστε να απολαμβάνουν την ποιότητα υπηρεσιών οι χρήστες. Εκτός των προδιαγραφών της κινητής συσκευής θα πρέπει να αναφερθούμε και στην κάρτα SIM, που αποτελεί ένα module των παρόχων ώστε να ταυτοποιούν και να εξουσιοδοτούν συσκευές που επιθυμούν να κάνουν χρήση του δικτύου τους.

#### Κινητή συσκευή χρήστη

Για την πειραματική διαδικασία χρησιμοποιήσαμε κινητή "έξυπνη" συσκευή, από το σύνολο των δοκιμασμένων συσκευών που προτείνει η OAI. **Συγκεκριμένα, χρησιμοποιήσαμε το μοντέλο Pixel 5G της εταιρείας Google.** Ως προαπαιτούμενο, σύμφωνα με της οδηγίες της OAI, ήταν να αλλάξουμε το firmware της συσκευής στην έκδοση "11.0.0 (RD1A.201105.003.B1, Nov 2020, EU carriers)"

#### Subscriber Identity Module(SIM)

Για την αναγνώριση, όπως προαναφέραμε, της συσκευής του χρήστη θα πρέπει να ενσωματωθούν ορισμένα χαρακτηριστικά και παράμετροι του παρόχου, που πιστοποιούν τον χρήστη, συγκρίνοντας αυτές τις παραμέτρους. Ο πάροχος αποθηκεύει σε ένα προφίλ με τις απαραίτητες παραμέτρους για κάθε χρήστη, στη βάση δεδομένων και αντλούνται από εκεί μέσω της οντότητας HSS. Για τον χρήστη αυτές οι παράμετροι αποθηκεύονται σε μία κάρτα με μικρή χωρητικότητα που ονομάζεται Μονάδα Ταυτότητας Συνδρομητή (Subscriber Identity Module, SIM) ή δεσμεύοντας ένα μικρό μέρος της μονάδας

αποθήκευσης της συσκευής χρήστη που στην περίπτωση αυτή ονομάζεται Embedded SIM (e-SIM) καθώς οι παράμετροι και οι ρυθμίσεις λαμβάνονται από το διαδίκτυο και δεν υπάρχει φυσική SIM. Η φυσική κάρτα SIM κατασκευάζεται με επιταξιακές μεθόδους και η δομή της είναι αυτή που φαίνεται στο σχήμα 5.6.

Συνεπώς κάθε κινητή μονάδα για να συνδεθεί με ένα δίκτυο GSM θα πρέπει απαραίτητως να διαθέτει στο εσωτερικό της μία κάρτα SIM ή πληροφορίες e-SIM. Και στις δύο περιπτώσεις η διάθεση SIM/e-SIM γίνεται από τον πάροχο και αποτελεί την ταυτότητα για έναν συνδρομητή αφού περιλαμβάνει απαραίτητες πληροφορίες για αυτόν και για το δίκτυο του με το οποίο συνδέεται, καθώς και μια περιορισμένη ποσότητα μνήμης.[47]

Από τη στιγμή που θα αφαιρεθεί από τη κινητή μονάδα, η κινητή μονάδα δεν μπορεί να χρησιμοποιηθεί πέραν από κλήσεις εκτάκτου ανάγκης (112).

Μια κάρτα SIM διαθέτει έναν μικροεπεξεργαστή, μια μνήμη ROM που χρησιμοποιείται για τις λειτουργίες του δικτύου (αναγνωριστικά, πιστοποίηση κτλ.) και μια μνήμη EPROM που την χρησιμοποιεί ο χρήστης για τα δικά του προσωπικά του δεδομένα. Η εισαγωγή των απαραίτητων πληροφοριών στην κάρτα έγινε με κατάλληλη συσκευή και με το λογισμικό pySim που διατίθεται για εκδόσεις Linux.[47]

Οι παράμετροι αυτές που εισαγάγαμε στη SIM και αποτελούν τις πιο βασικές (για φωνητική κλήση χρειάζεται περαιτέρω εισαγωγή παραμέτρων όπως MSISDN, IMPI, IMPU, Domain, P-CSCF) είναι[47]:

- **Mobile Country Code (MCC)**

Ο κωδικός χώρας κινητής τηλεφωνίας αποτελείται από τρία δεκαδικά ψηφία. Το πρώτο ψηφίο του κωδικού χώρας για κινητά προσδιορίζει τη γεωγραφική περιοχή που εδρεύει ο πάροχος.

- **Mobile Network Code (MNC)**

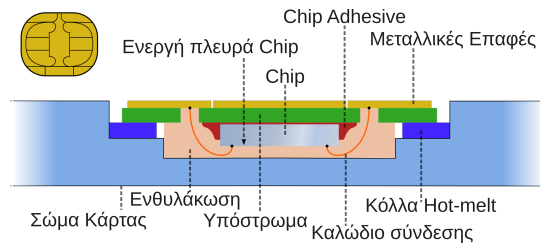
ο κωδικός δικτύου κινητής τηλεφωνίας αποτελείται από δύο ή τρία δεκαδικά ψηφία (για παράδειγμα: το MNC του 001 δεν είναι το ίδιο με το MNC του 01) και χαρακτηρίζει τον εκάστοτε πάροχο υπηρεσιών.

- **Public Land Mobile Network (PLMN)**

Ο αριθμός PLMN είναι μία ένωση των MCC και MNC

- **International mobile equipment identity (IMEI)**

Το IMEI είναι ένας μοναδικός αριθμός συσκευής για τον κινητό σταθμό. Περιέχει 15 ψηφία και έτσι καταλαμβάνει συνήθως οκτώ byte. Αποτελείται από τον εξαψήφιο κωδικό έγκρισης τύπου, δύο ψηφία κωδικού κατασκευαστή, έναν εξαψήφιο σειριακό αριθμό και ένα ψηφίο ελέγχου. Το IMEI αποθηκεύεται στο κινητό τηλέφωνο και στο μητρώο αναγνώρισης εξοπλισμού (EIR) σε κεντρική τοποθεσία.



Εικόνα 5.6: Δομή κάρτας SIM [48]



- **ICC Identification(ICCID)**

Το ICCID είναι ένας μοναδικός αριθμός αναγνώρισης για την SIM κάρτα. Έχει κωδικοποίηση BCD και μήκος 10 bytes.

- **International mobile subscriber identity (IMSI)**

Το IMSI είναι η μοναδική ταυτότητα συνδρομητή στο σύστημα GSM. Είναι κωδικοποιημένο με BCD και έχει μήκος εννέα bytes. Αποτελείται από τον κωδικό χώρας κινητής τηλεφωνίας (MCC), τον κωδικό δικτύου κινητής τηλεφωνίας (MNC) και έναν σειριακό αριθμό που έχει εκχωρηθεί από τον διαχειριστή δικτύου. Το IMSI συνήθως δεν μεταδίδεται ποτέ μέσω της εναέριας διεπαφής ως καθαρό κείμενο, προκειμένου να αποφευχθεί η παράνομη ανίχνευση της θέσης ενός κινητού σταθμού. Αντί για το IMSI, το TMSI χρησιμοποιείται συνήθως μαζί με το Location Area Information(LAI)<sup>8</sup> για σκοπούς αναγνώρισης.

- **Individual key (Ki) and cipher key (Kc)**

Τα Ki και Kc είναι μυστικά κλειδιά για συμμετρικούς κρυπτογραφικούς αλγόριθμους. Το Ki είναι το κλειδί ειδικά για την κάρτα και για τον κρυπτογραφικό υπολογισμό της αυθεντικότητας της SIM και το Kc χρησιμοποιείται για την κρυπτογράφηση δεδομένων που μεταδίδονται μεταξύ του κινητού σταθμού και του σταθμού βάσης μέσω της εναέριας διασύνδεσης.

- **Mobile station ISDN number (MSISDN)**

Το MSISDN είναι ο αριθμός κλήσης του κινητού σταθμού και είναι ανεξάρτητος από την ταυτότητα του συνδρομητή (IMSI).

- **Access Point Name (APN)**

Το όνομα σημείου πρόσβασης (APN) είναι το όνομα μιας πύλης(Gateway) μεταξύ ενός δικτύου κινητής τηλεφωνίας GSM, GPRS, 3G ή 4G και ενός άλλου δικτύου υπολογιστών, συχνά του δημόσιου Διαδικτύου(internet). Στη συγκεκριμένη περίπτωση ορίσαμε το oai.ipv4.

- **Service Provider Name (SPN)**

Είναι το όνομα του παρόχου όπου στην περίπτωση της πειραματικής διαδικασίας της εργασίας είναι το OpenAirInterface.

Εκτός των παραπάνω παραμέτρων κατά τον προγραμματισμό της κάρτας SIM εισήχθη και η επιλογή του αλγορίθμου Milenage. Οι λειτουργίες ελέγχου ταυτότητας 3GP και δημιουργίας κλειδιών (MILENAGE) έχουν αναπτυχθεί μέσω των συνεργατικών προσπαθειών των οργανωτικών συνεργατών 3GPP. Μπορούν να χρησιμοποιηθούν μόνο για την ανάπτυξη και λειτουργία 3G κινητών επικοινωνιών και υπηρεσιών. Δεν απαιτούνται πρόσθετες απαιτήσεις ή εξουσιοδοτήσεις για την εφαρμογή αυτών των αλγορίθμων.[47]

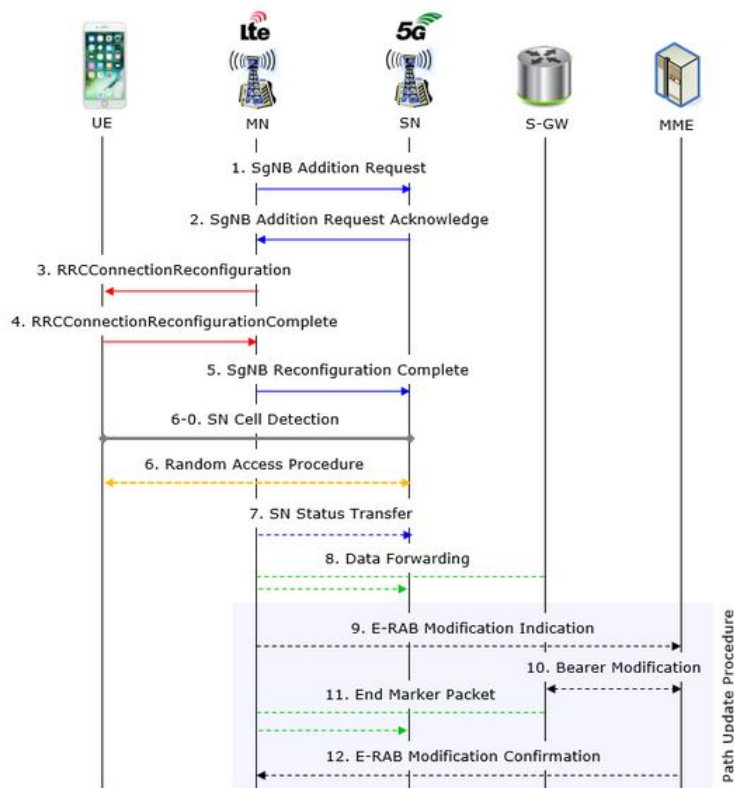
Κατα τη πειραματική διαδικασία χρησιμοποιήσαμε μία επαναπρογραμματιζόμενη κάρτα USIM<sup>9</sup> της εταιρείας OpenCell.

<sup>8</sup>Το LAI είναι η μοναδική πληροφορία θέσης του κινητού σταθμού. Χρησιμοποιείται σε συνδυασμό με το TMSI για τη δημιουργία μιας μοναδικής ταυτότητας συνδρομητή.

<sup>9</sup>Απο την είσοδο στην αγορά του UMTS ονομάστηκε USIM καθώς οι SIM βελτιώθηκαν περιλαμβάνοντας νέα στοιχεία

### 5.2.4 Λειτουργία

Η λειτουργία του μη αυτόνομου συστήματος αναπαρίσταται στο σχήμα 5.7. Η λειτουργία ξεκινά με την αρχική εγκαθίδρυση του επιπέδου ελέγχου (control plane) μεταξύ του UE και του RAN eNB και στη συνέχεια εγκαθιδρύεται το επίπεδο χρήστη (user plane) μεταξύ του UE και του gNB υπό την λειτουργία του εύρους συχνοτήτων που αντιστοιχούν στο 5G FR1 Band n78 (3.5 GHz). Το δίκτυο πρόσβασης είναι 4G-based υποστηρίζοντας την έκδοση 15 της 3GPP όπως περιγράψαμε και στο θεωρητικό μέρος. Επίσης, η λειτουργία βασίζεται στην επιλογή 5G TDD Duplexing και το μέγιστο εύρος ζώνης που επιτυγχάνεται είναι τα 40MHz και το σχήμα κεραιών ήταν μονής εισόδου μονής εξόδου (Simple Input Simple Output, SISO).



Εικόνα 5.7: Αναπαράσταση λειτουργίας μη αυτόνομου 5G[45]

Αφού έχουμε συνδέσει το gNB server με το USRP N310 και το eNB με το USRP B210 ενεργοποιούμε αρχικά τα containers στο δίκτυο κορμού και έπειτα στο δίκτυο πρόσβασης εκτελούμε τα παρακάτω scripts με τη σειρά που τα παρουσιάζουμε παρακάτω.

Αρχικά εκτελούμε το script που ενεργοποιεί το eNB και το αντίστοιχο usrp B210 και είναι υπεύθυνο να διατηρήσει την συνδεσιμότητα μέσω του πεδίου ελέγχου. Η σύνδεση του eNB με τον server που φιλοξενεί το eNB με το USRP πρέπει να γίνεται με usb 3.0.

```
$ sudo ./lte-softmodem -0 ../../../../targets/PROJECTS/GENERIC-LTE-EPC/CONF/enb.band7.tm1.50PRB.usrb210.conf
```

Απο την άλλη το gNB χρησιμοποιεί FR2 συχνότητες που έχουν μεγαλύτερο

εύρος ζώνης και αφιερώνεται εξ' ολοκλήρου για την διακίνηση δεδομένων. Η εντολή ενεργοποίησης του gNB και του αντίστοιχου usrp N310 είναι:

```
1 $ sudo ./nr-softmodem -0 ../../../../targets/PROJECTS/GENERIC-LTE-EPC/CONF
  /gnb.band78.tm1.106PRB.usrpn300.conf
```

Αξίζει να σημειώσουμε ότι για τη σύνδεση του server που φιλοξενεί το gNB με το USRP χρειάστηκε οπτική ίνα με ρυθμό δεδομένων 10G για την σωστή λειτουργία του, καθώς επίσης και ρύθμιση της διεπαφής απο 1500mtu που είναι ως προεπιλογή απο το λειτουργικό Ubuntu, σε 9000mtu.

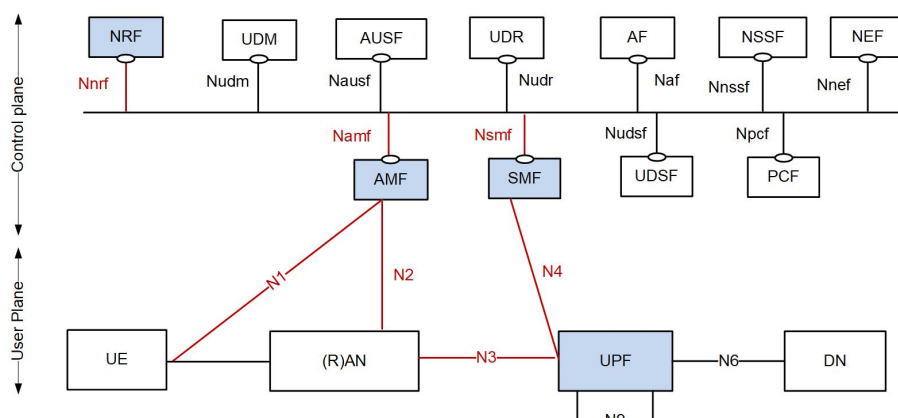
Τέλος, απενεργοποιούμε τη λειτουργία Airplane mode απο την κινητή συσκευή χρήστη και αναμένουμε τη σύνδεση. Μετά τη σύνδεση είναι δυνατή η επικοινωνία με το εξωτερικό δίκτυο internet αλλά και με μικρές παραμετροποιήσεις, επιτυγχάνεται και τηλεφωνική σύνδεση εντός του δικτύου που έχουμε φτιάξει, συνδέοντας δεύτερη τηλεφωνική συσκευή.

Για κάθε περίπτωση απο τα δύο παραπάνω scripts μπορούμε να εξάγουμε σε αρχεία τα logs τους, προσθέτοντας απλά στο τέλος της κάθε εντολής το `| tee **YOUR_LOG_FILE**`.

Όπως αναφέραμε και παραπάνω, η περίπτωση του μη αυτόνομου συστήματος 5G έχει υιοθετηθεί απο τους παρόχους των δικτύων για μια πρώιμη εμπορική κυκλοφορία που μπορεί να φέρει το όνομα "Δίκτυα 5G". Ο τρόπος λειτουργίας του όμως αν και αποτελεί βασική αρχή για τα δίκτυα πέμπτης γενιάς δεν αγγίζει αυτό που αναμένεται να προσδώσει το αυτόνομο 5G δίκτυο.

### 5.3 Υλοποίηση αυτόνομης λειτουργίας 5G

Η περίπτωση του αυτόνομου συστήματος 5G αποτελεί μία προσέγγιση του 5G όπου αναμένεται να διατεθεί τα επόμενα χρόνια, αποτελώντας μία επανάσταση των τηλεπικοινωνιακών δικτύων.



Εικόνα 5.8: Λειτουργίες αυτόνομου 5G που περιλαμβάνει η υλοποίηση[45]

Στο τμήμα αυτό της εργασίας θα περιγράψουμε τα στάδια εγκατάστασης ενός πειραματικού αυτόνομου συστήματος 5G που μπορεί να χρησιμοποιηθεί για εργαστηριακούς σκοπούς, όπως διανέμεται απο την OpenAirInterface. Απο εκεί θα εξάγουμε ένα αρχείο καταγραφής των οντοτήτων και πως

αλληλεπιδρούν μεταξύ τους αλλά και με προσομοιωτές κεραιών και συσκευών χρήστη( μιας και δεν έχει κυκλοφορήσει έκδοση 5G SA απο την OAI που να λειτουργεί με πραγματικά gNB και UE) απο το λογισμικό Wireshark.

Επίσης, ισχύουν και εδώ οι ρυθμίσεις και παραμετροποίηση που περιγράφηκε στην ενότητα 5.1, καθώς η υλοποίηση γίνεται απο το αποθετήριο της OAI με τη βοήθεια τεχνικών containers για τις λειτουργίες το δικτύου κορμού.

Οι οντότητες που περιέχει η έκδοση αυτόνομου 5G που υλοποιήσαμε περιλαμβάνει τις οντότητες που είναι χρωματισμένες στην εικόνα 5.9.

Παρακάτω περιγράφουμε την υλοποίηση με χρήση containers του δικτύου κορμού και την υλοποίηση του δικτύου πρόσβασης και του UE με τη χρήση προσομοιωτών. Στη συνέχεια περιγράφεται η λειτουργία για την εξαγωγή των αρχείων Wireshark.

### 5.3.1 Δίκτυο κορμού

Το δίκτυο κορμού περιέχει τις λειτουργίες που διακρίνονται με γαλάζιο χρώμα στην εικόνα 5.9 ενώ οι υπόλοιπες λειτουργίες πρόκειται να αναπτυχθούν και να διανεμηθούν μελλοντικά απο την OAI

#### Αποθήκευση αποθετηρίου στο τοπικό VM

Ακολουθώντας την παρακάτω διαδικασία αποθηκεύουμε στο τοπικό VM τα απαραίτητα αρχεία, απο το αποθετήριο της OAI, που χρειάζονται για την εγκατάσταση και λειτουργία του 5G SA.

```

1 $ git clone https://gitlab.eurecom.fr/oai/cn5g/oai-cn5g-fed.git
2 $ cd oai-cn5g-fed
3 $ git checkout master
4 $ git pull origin master
5 $ ./scripts/syncComponents.sh -h
6 $ ./scripts/syncComponents.sh --spgww-tiny-branch gtp_extension_header
7 -----
8 OAI-AMF      component branch : develop
9 OAI-SMF      component branch : develop
10 OAI-NRF      component branch : develop
11 OAI-SPGW-U   component branch : gtp_extension_header
12 -----
13 ....

```

Όμοια και εδώ δημιουργούμε ένα κλώνο του αποθετηρίου με τη βοήθεια του git προγράμματος και αποθηκεύουμε στο τοπικό VM την έκδοση master. Έπειτα το script στις δύο τελευταίες εντολές αποθηκεύει τις εκδόσεις που έχουν δοκιμαστεί ότι λειτουργούν και αποτελούν τις πιο πρόσφατες εκδόσεις.

#### Δημιουργία εικόνων containers

Στη συνέχεια με την γνωστή πλέον διαδικασία δημιουργίας εικόνων containers, δημιουργούμε εικόνες για κάθε μία οντότητα.

Για την εικόνα της οντότητας AMF

```

1 $ docker build --target oai-amf --tag oai-amf:develop \
2   --file component/oai-amf/docker/Dockerfile.ubuntu.18.04
3   \
4     component/oai-amf
5 $ docker image prune --force
6 $ docker image ls
7 oai-amf                develop                f478bafd7a06        1
   minute ago           258MB
8 ...

```

Για την εικόνα της οντότητας SMF

```

1 $ docker build --target oai-smf --tag oai-smf:develop \
2   --file component/oai-smf/docker/Dockerfile.ubuntu.18.04
3   \
4     component/oai-smf
5 $ docker image prune --force
6 $ docker image ls
7 oai-smf                develop                f478bafd7a06        1
   minute ago           274MB
8 ...

```

Για την εικόνα της οντότητας NRF

```

1 $ docker build --target oai-nrf --tag oai-nrf:develop \
2   --file component/oai-nrf/docker/Dockerfile.ubuntu.18.04
3   \
4     component/oai-nrf
5 $ docker image prune --force
6 $ docker image ls
7 oai-nrf                develop                04334b29e103        1
   minute ago           280MB
8 ...

```

Για την εικόνα της οντότητας SPGW-U

```

1 $ docker build --target oai-spgwu-tiny --tag oai-spgwu-tiny:gtp-ext-
2   header \
3   --file component/oai-upf-equivalent/docker/Dockerfile.
4   ubuntu18.04 \
5     component/oai-upf-equivalent
6 $ docker image prune --force
7 $ docker image ls
8 oai-spgwu-tiny        gtp-ext-header        dec6311cef3b
   1 minute ago         255MB
9 ...

```

## Διαμόρφωση containers

Το docker-compose αρχείο έχει παραμέτρους διαμόρφωσης για όλα τα στοιχεία του δικτύου κορμού. Το αρχείο αυτό είναι προ-διαμορφωμένο με παραμέτρους ώστε να προσδίδουν ένα σενάριο παραδείγματος λειτουργίας και όχι για χρήση με πραγματικό εξοπλισμού gNB και UE. Τα δεδομένα και οι παράμετροι της συσκευής χρήστη αποθηκεύονται σε μία MySQL βάση δεδομένων και η είσοδος νέων παραμέτρων ή συσκευών χρήστη γίνεται ως εξής:

```

1 #Login to mysql container once the container is running
2 (docker-compose-host)$ docker exec -it mysql /bin/bash
3 (mysql-container)$ mysql -uroot -plinux -D oai_db
4 mysql> INSERT INTO users VALUES
5 (imsi,msisdn,imei,NULL,'PURGED',50,40000000,100000000,47,0000000000,1,
   key,0,0,0x40,'ebd07771ace8677a',opc);

```

Η σειρά ανάπτυξης των containers είναι

$mysql \mapsto oai - nrf \mapsto oai - amf \mapsto oai - smf \mapsto oai - upf$

ή χωρίς την προσθήκη nrf

$mysql \mapsto oai - amf \mapsto oai - smf \mapsto oai - upf$

## Δημιουργία δικτύου

Το docker-compose.yaml αρχείο έχει την δυνατότητα δημιουργίας ενός δικτύου για τα containers αυτόματα, αν και αυτή η επιλογή είναι απενεργοποιημένη εκ των προτέρων και μπορεί να ενεργοποιηθεί αφαιρώντας τα σημεία που θέτουν ως σχόλια τις παρακάτω εντολές.

```

1 networks:
2   public_net:
3     driver: bridge
4     name: demo-oai-public-net
5     ipam:
6       config:
7         - subnet: 192.168.70.128/26
8     driver_opts:
9       com.docker.network.bridge.name: "demo-oai"

```

Στην περίπτωση που ο χρήστης επιθυμεί ο ίδιος να δημιουργήσει ένα δίκτυο για τα containers στον υπολογιστή που τα φιλοξενεί, τότε εκτελεί τις παρακάτω εντολές για να το δημιουργήσει και να ελέγξει την δημιουργία του. Επίσης, εκτελούμε και τις εντολές στο τέλος για να επιτρέψουμε την κίνηση ipv4 κατα προτεραιότητα καθώς και για καταχώρηση του δικτύου στον ip table του λειτουργικού.

```

1 $ docker network create \
2   --driver=bridge \
3   --subnet=192.168.70.128/26 \
4   -o "com.docker.network.bridge.name="demo-oai" \
5   demo-oai-public-net
6
7 $ ifconfig demo-oai
8 $ docker network ls
9 $ sudo sysctl net.ipv4.conf.all.forwarding=1
10 $ sudo iptables -P FORWARD ACCEPT

```

## 5.3.2 Δίκτυο πρόσβασης και UE

### Εγκατάσταση προσομοιωτών

Το UERANSIM είναι μια εφαρμογή ανοιχτού κώδικα state-of-the-art 5G UE και RAN (gNodeB). Μπορεί να θεωρηθεί ως κινητό τηλέφωνο 5G και σταθμός βάσης σε βασικούς όρους. Το έργο μπορεί να χρησιμοποιηθεί για τη δοκιμή 5G Core Network και τη μελέτη συστήματος 5G γενικότερα.

Τα βήματα εγκατάστασης με τη μορφή εντολών είναι τα παρακάτω

```

1 $ cd ~
2 $ git clone https://github.com/aligungr/UERANSIM
3 $ sudo apt update
4 $ sudo apt upgrade
5 $ sudo apt install make
6 $ sudo apt install g++
7 $ sudo apt install openjdk-11-jdk
8 $ sudo apt install maven
9 $ sudo apt install libsctp-dev lksctp-tools
10 $ sudo apt install iproute2
11 $ sudo snap install cmake --classic
12 $ cd ~/UERANSIM
13 $ make

```

Μετά την επιτυχή εγκατάσταση μπορούμε στο φάκελο /UERANSIM/build να βρούμε τις παρακάτω λειτουργίες

- nr-gnb | Βασικό εκτελέσιμο αρχείο για το 5G gNB (RAN)
- nr-ue | Βασικό εκτελέσιμο αρχείο για το 5G UE
- nr-cli | CLI εργαλείο για 5G gNB και UE
- nr-binder | Ένα εργαλείο για τη χρήση της σύνδεσης στο Διαδίκτυο του UE
- libdevbnd.so | Δυναμική βιβλιοθήκη για nr-binder

Η διαμόρφωση αποτελεί το σημαντικότερο μέρος των προσομοιωτών ώστε να επικοινωνεί και να λειτουργεί σωστά με το δίκτυο πρόσβασης. Άρα πρέπει να γίνει προσεκτική διαμόρφωση των αρχείων yaml για κάθε περίπτωση, που περιλαμβάνουν όσα περιγράψαμε και στην περίπτωση προγραμματισμού της πραγματικής SIM για το Non Stand Alone. Τα δύο αυτά αρχεία έχουν ονομαστούν oai-gnb και oai-ue για την καλύτερη διάκριση κατά την εκτέλεση. Αυτά αμφότερα αποθηκεύονται στη διαδρομή /UERANSIM/build.

Η παράμετροι που εισάγουμε στα αρχεία yaml είναι:

Για το oai-gnb.yaml που αφορά τον προσομοιωτή RH

```

1 TAC - 0xa000
2 MCC - 208
3 MNC - 95
4 NSSAI SST - 222
5 NSSAI SD - 123

```

Για το oai-ue.yaml που αφορά τον προσομοιωτή User Equipment

```

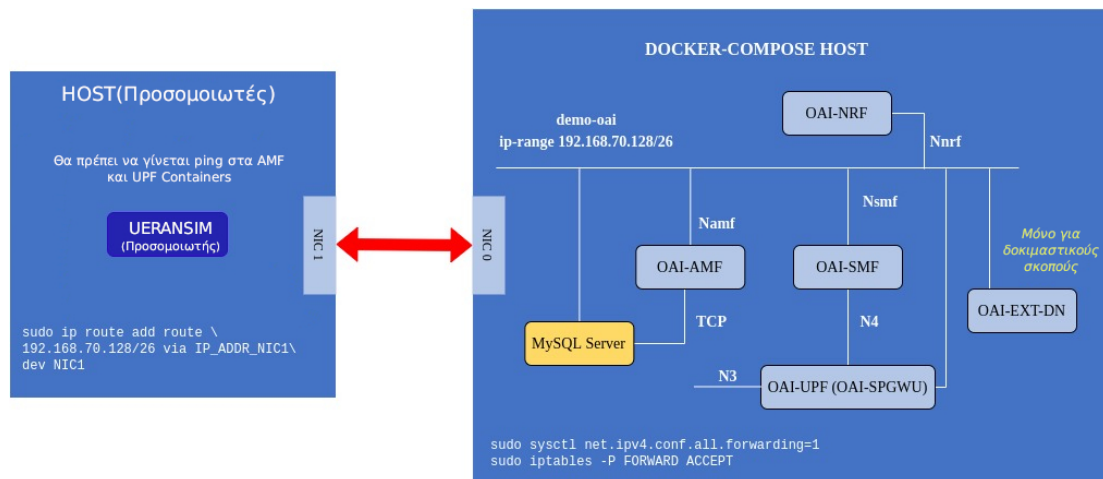
1 IMSI - 208950000000031
2 IMEI - 55000000000001
3 Secret Key (K) - 0x0C0A34601D4F07677303652C0462535B
4 OPc - 0x63bfa50ee6523365ff14c1f45f88737d
    
```

### Λειτουργία

Αφού δημιουργήσαμε ένα δίκτυο Docker όπως και στην ενότητα 5.2 για τη μη αυτόνομη περίπτωση, θα πρέπει να επιτρέψουμε τη δρομολόγηση μεταξύ του HOST και του DOCKER-COMPOSE HOST.

Το Dockerfile είναι ένα απλό αρχείο κειμένου που περιέχει τις εντολές που ένας χρήστης θα μπορούσε να καλέσει για να συγκεντρώσει ένα images, ενώ το Docker Compose είναι ένα εργαλείο για τον καθορισμό και την εκτέλεση εφαρμογών Docker πολλαπλών containers.

Απο την άλλη το Docker Compose καθορίζει τις υπηρεσίες που αποτελούν την εφαρμογή, που έχουμε αναπτύξει, στο docker-compose.yaml, ώστε να μπορούν να εκτελούνται μαζί σε ένα απομονωμένο περιβάλλον. Λαμβάνει δηλαδή μια εφαρμογή που εκτελείται σε μία εντολή εκτελώντας απλώς το docker-compose. Το Docker compose χρησιμοποιεί το Dockerfile εάν προστεθεί μια εντολή build στο docker-compose.yml του έργου. Η ροή εργασίας του Docker θα πρέπει να είναι η δημιουργία ένα κατάλληλου Dockerfile για κάθε εικόνα που θέλουμε να δημιουργήσουμε και, στη συνέχεια, χρησιμοποιώντας τη σύνθεση για να συγκεντρώσουμε τις εικόνες χρησιμοποιώντας την εντολή build.



Εικόνα 5.9: Συνδεσιμότητα προσομοιωτών gNB και UE με το Docker δίκτυο κορμού [45]

Συνεπώς θα πρέπει να επιτρέψουμε τη δρομολόγηση μεταξύ των δύο υπολογιστών και των δικτύων τους. Άρα στην πλευρά του host εκτελούμε

```

1 $sudo ip route add 192.168.70.128/26 via 192.168.7.176 dev enp5s0
    
```

όπως επιδεικνύει και η εικόνα 5.9 ενώ επιτρέπουμε και την καταχώρηση στο ip table όπως αναφέραμε νωρίτερα.

Στη συνέχεια εκτελούμε το script στο VM (όπου βρίσκεται το δίκτυο κορμού) που ενεργοποιεί τα containers των οντοτήτων. Ειδικότερα,



```
1 (docker-compose-host)$ ./core-network start
```

που βρίσκεται εντός της διαδρομής /oai/oai-cn-fed/docker-compose. Για να σταματήσουμε τη λειτουργία του δικτύου κορμού αντικαθιστούμε τη λέξη start με τη λέξη stop. Η εκτύπωση στην οθόνη του τερματικού μας δείχνει και πως εξελίσσεται η διαδικασία δημιουργίας των οντοτήτων, καθώς επίσης και αν το σύστημα είναι υγιές μετά την ολοκλήρωση της δημιουργίας των containers.

Μπορούμε να εξάγουμε και αρχεία log απο για να τυχόν αποσφαλμάτωση αλλά και να δούμε την πλήρη λειτουργία της κάθε οντότητας. Αυτό γίνεται ως εξής

```
1 (docker-compose-host)$ docker logs oai-amf > amf.log
2 (docker-compose-host)$ docker logs oai-smf > smf.log
3 (docker-compose-host)$ docker logs oai-nrf > nrf.log
4 (docker-compose-host)$ docker logs oai-spgwu > spgwu.log
```

Για την εκτέλεση και λειτουργία των gnb και UE εκτελούμε αντίστοιχα τις δύο συναρτήσεις με τα αρχεία διαμόρφωσης για κάθε περίπτωση.

```
1 cd ~/UERANSIM/build
2
3 ./nr-gnb -c ../config/oai-gnb.yaml
4 ./nr-ue -c ../config/oai-ue.yaml
```

Είναι σημαντικό να παρατηρούμε συνεχώς την έξοδο του τερματικού για τυχόν σφάλματα που μπορεί να προκύψουν καθ' όλη τη διαδικασία, τόσο της ανάπτυξης όσο και της λειτουργίας.

## Κεφάλαιο 6

# Σχολιασμός αποτελεσμάτων και μελλοντικές εξελίξεις

**Σ**ΤΟ ΤΕΛΕΥΤΑΙΟ ΚΕΦΑΛΑΙΟ ΤΗΣ ΕΡΓΑΣΙΑΣ ΕΞΆΓΟΥΜΕ ΤΑ ΣΥΜΠΕΡΆΣΜΑΤΑ ΠΟΥ ΠΡΟΈΚΥΨΑΝ ΑΠΟ ΤΗΝ ΠΕΙΡΑΜΑΤΙΚΉ ΔΙΑΔΙΚΑΣΊΑ ΚΑΙ ΤΑ ΣΧΟΛΙΑΖΟΥΜΕ ΒΑΣΙΖΌΜΕΝΟΙ ΣΤΗΝ ΘΕΩΡΗΤΙΚΉ ΠΡΟΣΈΓΓΙΣΗ ΤΟΥ ΠΡΏΤΟΥ ΜΈΡΟΥΣ ΤΗΣ ΕΡΓΑΣΙΑΣ.

Έπειτα, παραθέτουμε την μελλοντική πορεία που αναμένεται να έχει το σύστημα 5G, τόσο για το δίκτυο κορμού, όσο και του δικτύου πρόσβασης, και που σκοπεύει να χρησιμοποιηθεί. Κλείνοντας, έχουμε χρέος να συμπεριλάβουμε ορισμένες νέες τεχνολογίες που μελετούνται ερευνητικά και θα εκτοξευθεί η σημασία τους με τον συνδυασμό αυτών με τις επόμενες γενεές δικτύων που θα ακολουθήσουν, και αναφέρονται ως συστήματα Beyond, που η σημασία της λέξης σημαίνει τα επιτεύγματα που θα υπάρξουν πέρα από το 5G.

### 6.1 Σχολιασμός αποτελεσμάτων πειραματικής διαδικασίας

Τα συμπεράσματα της πειραματικής διαδικασίας περιλαμβάνουν παρατηρήσεις που εξήχθησαν από την διαδικασία αλλά και σχολιασμούς πάνω σε πακέτα δεδομένων που ελήφθησαν με το λογισμικό Tshark. Αρχικά, θα αναφερθούμε στα συμπεράσματα του μη αυτόνομου συστήματος 5G και έπειτα για το αυτόνομο σύστημα 5G.

#### 6.1.1 Μη αυτόνομο σύστημα 5G

##### Παρατηρήσεις ως προς τη διαδικασία

Η πειραματική διαδικασία αν και ολοκληρώθηκε κατά το μεγαλύτερο μέρος της με επιτυχία, δεν επετεύχθη ολοκληρωμένη σύνδεση καθώς υπήρχε πρόβλημα στην επικοινωνία του sctp πρωτοκόλλου που έχει επιπτώσεις στην διασύνδεση του δικτύου πρόσβασης με το δίκτυο κορμού. Παρόλα αυτά μπορούμε να εξάγουμε αποτελέσματα από τη συνολική διαδικασία και να χρησιμοποιήσουμε πακέτα της OpenAirInterface ώστε να μπορέσουμε να

εξηγήσουμε τη λειτουργία αλλά και να γίνει εμφανές η διαφορά ενός μη αυτόνομου συστήματος 5G με το αυτόνομο 5G.

Κατά την πειραματική διαδικασία δείξαμε πως έχει βελτιωθεί το 4G ώστε να διαχωρίζεται το control απο το user plane για την ταχύτερη μεταφορά δεδομένων χωρίς πρόσθετες εγκαθιδρύσεις των σημείων ελέγχου και πιστοποίησης του χρήστη. Άρα σε κάθε νέα σύνδεση γίνεται ο έλεγχος και η πιστοποίηση το χρήστη και έπειτα μπορούν τα πακέτα δεδομένων να διαχειρίζονται απο το επίπεδο χρήστη επιτυγχάνοντας έτσι μεγαλύτερη ευρωστία(robustness) αλλά και ταχύτητα μεταφοράς δεδομένων απο το 4G.

Ως προς τη διαδικασία, κάναμε χρήση του φάσματος συχνοτήτων 5G FR1 Band n78 (3.5 GHz) με το USRP N310 όπου αποτέλεσε το gNB και χρησιμοποιείται για τα δεδομένα του επιπέδου χρήστη και το enB για τη σηματοδότηση του επιπέδου ελέγχου σε ένα σχήμα που χαρακτηρίζεται μονής εισόδου-μονής εξόδου(Simple Input Simple Output,SISO). -Η διάρκεια της πειραματικής δοκιμής είναι 10- 15 δευτερόλεπτα. Μετά την παρέλευση αυτού του χρόνου η MME οντότητα μπλοκάρει τη λειτουργία της και το σύστημα σταματά να λειτουργεί.

Για την μελέτη του handover θα μπορούσαμε να εγκαταστήσουμε μεταξύ των usrps έναν εξασθενιτή που θα μείωνε το σήμα της μιας κεραίας δημιουργώντας έτσι συνθήκες κινούμενου χρήστη, καθώς η χαμηλή ισχύς των κεραίων του usrp δεν επιτρέπουν τον πειραματισμό σε πραγματικές συνθήκες.

### **Κατάσταση της διασυνδεσιμότητας**

Κατα την πειραματική διαδικασία με τη διασύνδεση του παρατηρήθηκε ότι το τηλέφωνο αρχικά δέχεται τη διαμόρφωση που παρέχεται από το OAI eNB που σημαίνει ότι επικυρώνεται το RRC και X2AP. Επίσης, υπάρχει επιτυχής διαδικασία τυχαίας πρόσβασης που ερμηνεύεται ότι το PRACH αποκωδικοποιείται σωστά στο gNB και το τηλέφωνο λαμβάνει και αποκωδικοποιεί σωστά msg2 (NR PDCCH Format 1\_0 και NR PDSCH). Το msg3 μεταδίδεται στο gNB σύμφωνα με τη διαμόρφωση που αποστέλλεται στο msg2 και λαμβάνεται σωστά στο gNB. Ακόμη, γίνεται επιτυχής εναλλαγή διαδρομής της κίνησης επιπέδου χρήστη από την κυψέλη 4G σε 5G (μήνυμα τροποποίησης E-RAB) όπου επιβεβαιώνεται με το S1AP.

Ως προς την κυκλοφορία κατερχόμενης ζεύξης το PDCCH DCI format 1\_1 και το αντίστοιχο PDSCH αποκωδικοποιούνται από το τηλέφωνο και λαμβάνονται σήματα ACK / NACK (μορφή PUCCH 0) στο gNB.

Τέλος, η κυκλοφορία UL / DL από άκρο σε άκρο γίνεται με επικυρωμένες διαδικασίες HARQ (ping, iperf).Αξίζει να σημειώσουμε ότι η μέγιστη κυκλοφορία δεδομένων που ισχύει για την κατερχόμενη ζεύξη είναι 3Mbps ενώ για την ανερχόμενη ζεύξη 1Mbps καθότι πρόκειται για δοκιμαστική πλατφόρμα μη αυτόνομου 5G αν και ορισμένες απώλειες πακέτων ενδέχεται να εξακολουθούν να συμβαίνουν ακόμη και σε ιδανικές συνθήκες καναλιού.

### **Ανάλυση Πακέτων δεδομένων**

Αν και δεν εξαγάγαμε πακέτα δεδομένων απο το wireshark, μπορούμε να χρησιμοποιήσουμε αυτά που εξήχθησαν απο την OpenAirInterface για να μπορούμε να συγκρίνουμε την αυτόνομη και μη αυτόνομη διαδικασία. Αρχικά,

παραθέτουμε το στιγμιότυπο ενός πακέτου όπως εξήχθη από το Wireshark, και αφορά το δίκτυο κορμού του μη αυτόνομου 5G συστήματος.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	127.0.0.1	127.0.0.10	TCP	76	39854 → 3868 [SYN] Seq=0 Win=65495 Len=0 MSS=65495 SACK_PERM=1 TSval=347038854 TSecr=0 WS=128
2	0.000026935	127.0.0.10	127.0.0.1	TCP	76	3868 → 39854 [SYN, ACK] Seq=0 Ack=1 Win=65483 Len=0 MSS=65495 SACK_PERM=1 TSval=985161814 TSecr=347038854 WS=128
3	0.000043250	127.0.0.1	127.0.0.10	TCP	68	39854 → 3868 [ACK] Seq=1 Ack=1 Win=65536 Len=0 TSval=347038854 TSecr=985161814
4	0.013506874	127.0.0.1	127.0.0.10	DIAMETER	392	cmd=Capabilities-Exchange Request(257) flags=R... appl=Diameter Common Messages(0) h2h=15423f6 e2e=5b32c109
5	0.013530964	127.0.0.10	127.0.0.1	TCP	68	3868 → 39854 [ACK] Seq=1 Ack=325 Win=65280 Len=0 TSval=985161828 TSecr=3470388567
6	0.016749687	127.0.0.10	127.0.0.1	DIAMETER	456	cmd=Capabilities-Exchange Answer(257) flags=... appl=Diameter Common Messages(0) h2h=15423f6 e2e=5b32c109
7	0.016769457	127.0.0.1	127.0.0.10	TCP	68	39854 → 3868 [ACK] Seq=325 Ack=389 Win=65152 Len=0 TSval=3470388571 TSecr=985161831
8	1.402875230	127.0.12.2	127.0.12.1	PFCP	75	Sx Association Setup Request
9	1.403938803	127.0.12.1	127.0.12.2	PFCP	79	Sx Association Setup Response
10	5.777340678	192.168.0.16	192.168.0.14	SCTP	84	INIT
11	5.777510631	192.168.0.14	192.168.0.16	SCTP	308	INIT_ACK
12	5.777862413	192.168.0.16	192.168.0.14	SCTP	280	COOKIE_ECHO
13	5.777941493	192.168.0.14	192.168.0.16	SCTP	52	COOKIE_ACK
14	5.778596565	192.168.0.16	192.168.0.14	SIAP	124	S1SetupRequest
15	5.778644124	192.168.0.14	192.168.0.16	SCTP	64	SACK
16	5.781067722	192.168.0.14	192.168.0.16	SIAP	92	S1SetupResponse
17	5.781656774	192.168.0.16	192.168.0.14	SCTP	64	SACK
18	6.404486740	127.0.12.2	127.0.12.1	PFCP	60	Sx Heartbeat Request
19	6.405140298	127.0.12.1	127.0.12.2	PFCP	60	Sx Heartbeat Response
20	11.404932933	127.0.12.1	127.0.12.2	PFCP	60	Sx Heartbeat Request
21	11.405140590	127.0.12.2	127.0.12.1	PFCP	60	Sx Heartbeat Response
22	11.405552741	127.0.12.2	127.0.12.1	PFCP	60	Sx Heartbeat Request
23	11.405928518	127.0.12.1	127.0.12.2	PFCP	60	Sx Heartbeat Response
24	16.406451627	127.0.12.2	127.0.12.1	PFCP	60	Sx Heartbeat Request
25	16.406971387	127.0.12.1	127.0.12.2	PFCP	60	Sx Heartbeat Response
26	19.417389703	192.168.0.16	192.168.0.14	SIAP/NAS-EPS	160	InitialUplinkMessage, Attach request, PDN connectivity request
27	19.421007662	127.0.0.1	127.0.0.10	DIAMETER	348	cmd=3GPP-Authentication-Information Request(318) flags=RP... appl=3GPP S6a/S6d(16777251) h2h=15423f7 e2e=0
28	19.421046309	127.0.0.10	127.0.0.1	TCP	68	3868 → 39854 [ACK] Seq=389 Ack=605 Win=65280 Len=0 TSval=985181235 TSecr=3470407975
29	19.424295492	127.0.0.10	127.0.0.1	DIAMETER	364	cmd=3GPP-Authentication-Information Answer(318) flags=P... appl=3GPP S6a/S6d(16777251) h2h=15423f7 e2e=0
30	19.424325789	127.0.0.1	127.0.0.10	TCP	68	39854 → 3868 [ACK] Seq=605 Ack=685 Win=65280 Len=0 TSval=3470407978 TSecr=985181238
31	19.426994654	192.168.0.14	192.168.0.16	SIAP/NAS-EPS	144	DownlinkNASTransport, Authentication request
32	19.444419115	192.168.0.16	192.168.0.14	SIAP/NAS-EPS	140	UplinkNASTransport, Authentication response
33	19.448165469	192.168.0.14	192.168.0.16	SIAP/NAS-EPS	120	DownlinkNASTransport, Security mode command
34	19.467433656	192.168.0.16	192.168.0.14	SIAP/NAS-EPS	148	UplinkNASTransport, Security mode complete

Εικόνα 6.1: Ανάλυση πακέτου δικτύου κορμού 5G NSA [45]

Αρχικά, η έναρξη της διαδικασίας γίνεται με την διασύνδεση των οντοτήτων MME και HSS με τη βοήθεια πρωτοκόλλου TCP και του Diameter. Το Diameter είναι ένα πρωτόκολλο ελέγχου ταυτότητας, εξουσιοδότησης και καταμέτρησης για δίκτυα υπολογιστών. Αφού επιτευχθεί το handshake, σειρά έχει η ενεργοποίηση της διεπαφής Sx όπου ενώνει το SPGWC και το SPGWU μέσω του πρωτοκόλλου Packet Forwarding Control Protocol (PFCP) που εισήχθη στο CUPS για τη διασύνδεση του επιπέδου ελέγχου με το επίπεδο χρήστη, όπως διακρίνεται στην αρίθμηση του πακέτου στο 8 και 9 νούμερο.

Στη συνέχεια (από το 10 έως το 17) μέσω του πρωτοκόλλου SCTP επικοινωνεί το δίκτυο κορμού με τα εξωτερικά δίκτυα, που στη συγκεκριμένη περίπτωση είναι το δίκτυο πρόσβασης. Χαρακτηριστικά μπορούμε να διακρίνουμε το handshake του SCTP πρωτοκόλλου και πως αυτό διαφέρει από το TCP handshake. Όσον αφορά τα πακέτα από 18 έως 25 στην ανάλυση του Wireshark παρατηρούμε ότι το πρωτόκολλο PFCP βρολίσκεται στη διαδικασία πρωτοκόλλου heartbeat. Ένα πρωτόκολλο heartbeat χρησιμοποιείται γενικά για τη διαπραγμάτευση και την παρακολούθηση της διαθεσιμότητας ενός πόρου, όπως μια κυμαινόμενη διεύθυνση IP. Συνήθως όταν ένας heartbeat ξεκινά σε ένα μηχανήμα, θα εκτελεί μια διαδικασία εκλογής με άλλα μηχανήματα στο δίκτυο heartbeat για να προσδιορίσει ποια μηχανή, εάν υπάρχει, κατέχει τον πόρο. Έτσι, θα υπάρχει η εναλλαγή ώστε το SPGWU να μπορεί να χρησιμοποιεί ελεύθερα τους πόρους του συστήματος για να διακινήσει το πακέτο, δίνοντας ουσία σε αυτό που αναφέραμε ως διαχωρισμός επιπέδων ελέγχου και δεδομένων.

Στο πακέτο 26 έχουμε το πρώτο σήμα NAS όπου μία συσκευή ζητά είσοδο στο δίκτυο κορμού και PDN συνδεσιμότητα. Η διαδικασία σύνδεσης PDN χρησιμοποιείται από το UE για να ζητήσει τη ρύθμιση ενός προεπιλεγμένου φορέα EPS σε ένα PDN. Το UE ζητά συνδεσιμότητα σε ένα PDN στέλνοντας ένα μήνυμα PDN CONNECTIVITY REQUEST στο δίκτυο.

35	19.476495781	127.0.0.1	127.0.0.10	DIAMETER	336 cmd=3GPP-Update-Location-Request(316) flags=RP-- appl=3GPP S6a/S6d(16777251) h2h=15423f8 e2e=0
36	19.478526862	127.0.0.10	127.0.0.1	TCP	68 3868 -- 39854 [ACK] Seq=685 Ack=873 Win=65288 Len=0 TSval=985181285 TSecr=3479408024
37	19.479709938	127.0.0.10	127.0.0.1	DIAMETER	1076 cmd=3GPP-Update-Location-Answer(316) flags=-P- appl=3GPP S6a/S6d(16777251) h2h=15423f8 e2e=0
38	19.479728498	127.0.0.1	127.0.0.10	TCP	68 39854 -- 3868 [ACK] Seq=873 Ack=1693 Win=64640 Len=0 TSval=3479408034 TSecr=985181294
39	19.482483482	127.0.11.1	127.0.11.2	GTPV2	245 Create Session Request
40	19.486374214	127.0.13.1	127.0.13.2	GTPV2	237 Create Session Request
41	19.490142688	127.0.12.1	127.0.12.2	PFPCP	166 Sx Session Establishment Request
42	19.490657618	127.0.12.2	127.0.12.1	PFPCP	114 Sx Session Establishment Response
43	19.492052861	127.0.13.2	127.0.13.1	GTPV2	160 Create Session Response
44	19.493657753	127.0.11.2	127.0.11.1	GTPV2	160 Create Session Response
45	19.497941977	192.168.0.14	192.168.0.16	SIAP/NAS-EPS	288 InitialContextSetupRequest, Attach accept, Activate default EPS bearer context request
46	19.537423662	192.168.0.16	192.168.0.14	SIAP	128 UECapabilityInfoIndication, UECapabilityInformation
47	19.738374541	192.168.0.14	192.168.0.16	SCTP	64 SACK
48	19.738763870	192.168.0.16	192.168.0.14	SIAP/NAS-EPS	184 InitialContextSetupResponse, UplinkNASTransport, Attach complete, Activate default EPS bearer context accept
49	19.740085064	127.0.11.1	127.0.11.2	GTPV2	91 Modify Bearer Request
50	19.741636429	127.0.13.1	127.0.13.2	GTPV2	78 Modify Bearer Request
51	19.745298974	127.0.12.1	127.0.12.2	PFPCP	144 Sx Session Modification Request
52	19.745734121	127.0.12.2	127.0.12.1	PFPCP	75 Sx Session Modification Response
53	19.747069389	127.0.13.2	127.0.13.1	GTPV2	90 Modify Bearer Response
54	19.748329033	127.0.11.2	127.0.11.1	GTPV2	90 Modify Bearer Response
55	19.946369385	192.168.0.14	192.168.0.16	SCTP	64 SACK
56	21.406335818	127.0.12.1	127.0.12.2	PFPCP	60 Sx Heartbeat Request
57	21.4063518603	127.0.12.2	127.0.12.1	PFPCP	60 Sx Heartbeat Response
58	21.407436804	127.0.12.2	127.0.12.1	PFPCP	60 Sx Heartbeat Request
59	21.407871964	127.0.12.1	127.0.12.2	PFPCP	60 Sx Heartbeat Response
60	26.408410246	127.0.12.2	127.0.12.1	PFPCP	60 Sx Heartbeat Request
61	26.409045821	127.0.12.1	127.0.12.2	PFPCP	60 Sx Heartbeat Response

Εικόνα 6.2: Ανάλυση πακέτου δικτύου κορμού 5G NSA-επισύναψη συσκευής χρήστη στο δίκτυο [45]

Το δίκτυο κορμού πιστοποιεί τη συσκευή του χρήστη με διασταυρώνοντας πληροφορίες της κάρτας SIM με πληροφορίες καταχωρημένες στη βάση δεδομένων του δικτύου κορμού με τη βοήθεια της οντότητας HSS όπως αυτή συνεργάζεται με την οντότητα MME, και αυτό φαίνεται και στην ανωτέρω ανάλυση του δικτύου κορμού. Η εναλλαγή μηνυμάτων πιστοποίησης και ασφάλειας μεταξύ των δύο δικτύων (κορμού και πρόσβασης) γίνεται αντιληπτή στα πακέτα 31 έως 38.

Στο LTE, οι σήραγγες GTP (GPRS Tunneling Protocol) χρησιμοποιούνται μεταξύ δύο κόμβων που επικοινωνούν μέσω διεπαφής που βασίζεται σε GTP, για να διαχωρίσουν την κίνηση σε διαφορετικές ροές επικοινωνίας. Μια σήραγγα GTP αναγνωρίζεται σε κάθε κόμβο με ένα TEID (Tunnel Endpoint Identifier), μια διεύθυνση IP και έναν αριθμό θύρας UDP. Η πλευρά λήψης μιας σήραγγας GTP εκχωρεί τοπικά την τιμή TEID που πρέπει να χρησιμοποιήσει η πλευρά μετάδοσης. Το GTPv2 περιλαμβάνει ένα ενημερωμένο επίπεδο ελέγχου που επιτρέπει τη μετάδοση μηνυμάτων ελέγχου μεταξύ των MME, S-GW, PDN GW κ.λ.π.. Έτσι, τα πακέτα 39 έως 44 ενεργοποιούν το πρωτόκολλο GTPv2 για τις διεπαφές S11, S5/S8 και SX όπως δείχνει και το σχήμα 5.2. Τελικά, η επισύναψη της συσκευής χρήστη (UE) ολοκληρώνεται με το πακέτο 49, ενεργοποιώντας την πρόσβαση στον EPS φορέα, όπου μέσα από τους φορείς (bearers) και μέσω του πρωτοκόλλου GTPv2 δημιουργούνται ροές που εξυπηρετούν τόσο τη σηματοδότηση όσο και τη διακίνηση πακέτων.

Όπως παρατηρούμε, η επιτυχημένη σύνδεση μιας συσκευής δημιουργείται μετά από 19,738 δευτερόλεπτα και με έναν συνολικό αριθμό 48 πακέτων.

### 6.1.2 Αυτόνομο σύστημα 5G

Η λογική υλοποίησης του αυτόνομου συστήματος στηρίζεται στην αρχιτεκτονική που παρουσιάζει η εικόνα 5.9 όπου οι λειτουργίες NRF, AMF και SMF χρησιμοποιούνται για το επίπεδο ελέγχου και η λειτουργία UPF για το επίπεδο χρήστη και μάλιστα υπάρχει μεγάλο ερευνητικό ενδιαφέρον πάνω στις διάφορες υλοποιήσεις που μπορεί να δεχθεί το UPF για την ευρωστία στην διακίνηση των δεδομένων.

Πριν ενεργοποιήσουμε τα containers εκτελούμε το λογισμικό tshark που αποτελεί CLI έκδοση του wireshark, έτσι ώστε να καταγράψουμε την κίνηση των πακέτων του δικτύου-bridge που ονομάσαμε demo-oai και περιλαμβάνει τις οντότητες και διαμορφώνεται απο το script docker-compose-host. Η διαδικασία αυτή μας βοηθά να έχουμε μία εικόνα της κίνησης εντός του δικτύου κορμού του αυτόνομου συστήματος 5G που υλοποιήσαμε. Αυτό γίνεται με την εντολή

```
1 (docker-compose-host)$ tshark -i demo-oai -w 5gcn-deployment.pcap
```

και απο τα αποτελέσματα που λαμβάνουμε γίνεται φανερό ότι πρόκειται για ένα αυτόνομο δίκτυο 5G το οποίο βασίζεται στις υπηρεσίες (Serviced-Based Architecture, SBA) και χρησιμοποιεί πρωτόκολλο HTTP/1.1 για την μεταξύ των οντοτήτων επικοινωνία.

Μία εικόνα του δικτύου και των διευθύνσεων που έχουν λάβει οι οντότητες, παρουσιάζεται στον παρακάτω πίνακα

Container	Ip-address	Περιγραφή
mysql	192.168.70.131	Βάση δεδομένων
oai-amf	192.168.70.132	Οντότητα AMF
oai-smf	192.168.70.133	Οντότητα SMF
oai-nrf	192.168.70.130	Οντότητα NRF
oai-spgwu	192.168.70.134	Οντότητα SPGWU
oai-ext-dn	192.168.70.135	Εξωτερικό δίκτυο για δοκιμή
Host Machine	192.168.70.129	Μηχάνημα φιλοξενίας containers

Πίνακας 6.1: Διευθυνσιοδότηση οντοτήτων

### Σενάριο ελέγχου με εκτέλεση του UERANSIM

Για να ελέγξουμε εάν μια περίοδο λειτουργίας PDN έχει εγκαθιδρυθεί σωστά, υπάρχει ένα επιπλέον εξωτερικό δίκτυο δεδομένων μόνο για αυτόν τον σκοπό επίδειξης, το οποίο έχει υλοποιηθεί και αυτό σε container. Μπορούμε να φτάσουμε στο UERANSIM UE χρησιμοποιώντας αυτό το container για να επικυρώσουμε την εγκατάσταση της περιόδου λειτουργίας PDN. Για να γίνει κατανοητή η διαδικασία, αναλύουμε παρακάτω τη ροή πακέτων.

Πριν εκτελέσουμε το σκριπτ ./core-network ώστε να θέσουμε σε λειτουργία την κίνηση, λαμβάνουμε ένα πακέτο απο το tshark στο δίκτυο demo-oai ώστε να δούμε την επικοινωνία μηνυμάτων μεταξύ smf ↔ nrf ↔ upf.

13	1.697982	192.168.70.133	192.168.70.130	HTTP/JSON	414	POST /nrf-nfm/v1/subscriptions HTTP/1.1 , JavaScript Object Notation (application/json)
15	1.697765	192.168.70.130	192.168.70.133	HTTP/JSON	456	HTTP/1.1 201 Created , JavaScript Object Notation (application/json)
23	1.707682	192.168.70.133	192.168.70.130	HTTP/JSON	980	PUT /nrf-nfm/v1/nf-instances/2e0a241f-132d-44c6-b63d-027cd15d59b20 HTTP/1.1 , JavaScript Object Notat
25	1.708090	192.168.70.130	192.168.70.133	HTTP/JSON	901	HTTP/1.1 201 Created , JavaScript Object Notation (application/json)
35	6.016914	192.168.70.134	192.168.70.130	HTTP/JSON	577	PUT /nrf-nfm/v1/nf-instances/1eb55e75-5f8d-4eac-a8d7-344436fbd923 HTTP/1.1 , JavaScript Object Notat
40	6.016784	192.168.70.130	192.168.70.133	HTTP/JSON	688	POST /nsm-nfstatus-notify/v1/subscriptions HTTP/1.1 , JavaScript Object Notation (application/json)
42	6.017693	192.168.70.133	192.168.70.134	PFPCP	72	PFPCP Association Setup Request
43	6.017662	192.168.70.133	192.168.70.130	HTTP	131	HTTP/1.1 204 No Content
48	6.017774	192.168.70.134	192.168.70.133	PFPCP	78	PFPCP Association Setup Response

Εικόνα 6.3: Ανταλλαγή μηνυμάτων μεταξύ SMF,NRF και UPF [45]

Παρατηρούμε ότι η οντότητα SMF ζητά απο το NRF να εγγραφεί γεγονόςτα καταχώρησης/διαγραφής όπως δείχνει το πακέτο 13 με το POST request που αιτείται. Στο πακέτο 23 γίνεται εγγραφή SMF με το NRF (PUT request). Στο

πακέτο 35 το UPF(SPGWU) γίνεται η εγγραφή με το NRF και στο πακέτο 40 όπου λαμβάνεται ένα POST request και το NRF ενημερώνει το SMF για την καταχώρηση του UPF. Το αίτημα και η απάντηση για τη συσχέτιση UPF PFCP φαίνεται στα πακέτα 42,46.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.70.134	192.168.70.130	TCP	74	55350 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1153268208 TSecr=0 WS=128
2	0.000037	192.168.70.130	192.168.70.134	TCP	74	80 → 55350 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=255781681 TSecr=1153268208 WS=128
3	0.000057	192.168.70.134	192.168.70.130	TCP	66	55350 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1153268208 TSecr=255781681
4	0.000119	192.168.70.134	192.168.70.130	HTTP	292	PATCH /nrf-nfm/v1/nf-instances/1eb55e75-5fed-4eac-a8d7-344436fbd523 HTTP/1.1 (application/json)
5	0.000129	192.168.70.130	192.168.70.134	TCP	66	80 → 55350 [ACK] Seq=1 Ack=227 Win=65024 Len=0 TSval=255781681 TSecr=1153268208
6	0.000489	192.168.70.130	192.168.70.134	HTTP	163	HTTP/1.1 204 No Content
7	0.000495	192.168.70.134	192.168.70.130	TCP	66	55350 → 80 [ACK] Seq=227 Ack=98 Win=64256 Len=0 TSval=1153268208 TSecr=255781681
8	0.000569	192.168.70.134	192.168.70.130	TCP	66	55350 → 80 [FIN, ACK] Seq=227 Ack=98 Win=64256 Len=0 TSval=1153268208 TSecr=255781681
9	0.000606	192.168.70.130	192.168.70.134	TCP	66	80 → 55350 [FIN, ACK] Seq=98 Ack=228 Win=65024 Len=0 TSval=255781681 TSecr=1153268208
10	0.000625	192.168.70.134	192.168.70.130	TCP	66	55350 → 80 [ACK] Seq=228 Ack=99 Win=64256 Len=0 TSval=1153268208 TSecr=255781681
11	0.682295	192.168.70.134	192.168.70.133	PFCP	58	Sx Heartbeat Request
12	0.682424	192.168.70.133	192.168.70.134	PFCP	58	Sx Heartbeat Response
13	2.349438	192.168.18.184	192.168.70.132	SCTP	82	INIT
14	2.349586	02:42:c0:a8:46:	Broadcast	ARP	42	Who has 192.168.70.129? Tell 192.168.70.132
15	2.349591	02:42:af:f9:2c:	02:42:c0:a8:46:	ARP	42	192.168.70.129 is at 02:42:af:f9:2c:90
16	2.349636	192.168.70.132	192.168.18.184	SCTP	306	INIT_ACK
17	2.349757	192.168.18.184	192.168.70.132	SCTP	278	COOKIE_ECHO
18	2.349802	192.168.70.132	192.168.18.184	SCTP	50	COOKIE_ACK
19	2.360253	192.168.18.184	192.168.70.132	SCTP	162	DATA
20	2.360303	192.168.70.132	192.168.18.184	SCTP	62	SACK
21	2.360914	192.168.70.132	192.168.18.184	SCTP	574	DATA
22	2.364138	192.168.18.184	192.168.70.132	SCTP	62	SACK
23	4.392052	192.168.18.184	192.168.70.132	SCTP	130	DATA
24	4.397147	02:42:c0:a8:46:	Broadcast	ARP	42	Who has 192.168.70.131? Tell 192.168.70.132
25	4.397194	02:42:c0:a8:46:	02:42:c0:a8:46:	ARP	42	192.168.70.131 is at 02:42:c0:a8:46:83

Εικόνα 6.4: Ανάλυση πακέτου δικτύου κορμού 5G SA-αρχική σύνδεση

Όπως παρατηρούμε απο την εικόνα 6.4 η έναρξη της διαδικασίας γίνεται με τη χρήση πρωτοκόλλου TCP και των διεργασιών του handshake για την μεταξύ τους επικοινωνία των οντοτήτων SPGWU και NRF. Έπειτα, με το heartbeat του SPGWU με το SMF, ελέγχεται η συνδεσιμότητα τους. Μπορούμε να παρατηρήσουμε και ένα πρωτόκολλο ARP που αντιστοιχίζει τις MAC διευθύνσεις των διεπαφών με τις IP διευθύνσεις (στη συγκεκριμένη περίπτωση κλάσης C) του δικτύου. Αυτό, βρίσκεται στο πακέτο 13, μετά την έναρξη του SCTP πρωτοκόλλου και στα πακέτα 16 έως 23 γίνεται η διαδικασία handshake του SCTP πρωτοκόλλου η οποία, όπως είναι εμφανές, διαφέρει αισθητά απο αυτή του TCP που όπως αναφέραμε είναι ευάλωτο σε λεγόμενες επιθέσεις flooding SYN που μπορεί να προκαλέσουν υπερφόρτωση του διακομιστή TCP. Το SCTP έχει λύσει αυτό το πρόβλημα χρησιμοποιώντας μια ανταλλαγή μηνυμάτων τεσσάρων κατευθύνσεων για τη ρύθμιση συσχέτισης, συμπεριλαμβανομένης της χρήσης ενός ειδικού «cookie» που προσδιορίζει τον συσχετισμό και προλαμβάνει των ανωτέρω επιθέσεων. Το SCTP είναι υπεύθυνο για τη σύνδεση το δικτύου πυρήνα και πιο συγκεκριμένα με τη λειτουργία AMF.

Αφού λάβει το δίκτυο κορμού τα δεδομένα χρήστη, θα πρέπει να επικοινωνήσει με τη βάση δεδομένων για να εξακριβώσει τη συνδρομή του. Επομένως, μέσω των πρωτοκόλλων TCP εγκαθιδρύεται η σύνδεση και με το πρωτόκολλο MySQL, για παράδειγμα το πακέτο 29, επικοινωνούν οι δύο πλευρές, δηλαδή ο server που είναι το container που υλοποιεί τη βάση δεδομένων και ο client που ζητά πρόσβαση στα δεδομένα και στην προκειμένη περίπτωση είναι η οντότητα AMF.

Καθώς η άντληση των δεδομένων απο τη βάση δεδομένων πρέπει να τηρεί όλες τις προϋποθέσεις ασφαλείας, διότι διαχειρίζεται ευαίσθητα δεδομένα χρήστη, η 3GPP στις προδιαγραφές του 5G εισήγαγε το πρωτόκολλο TLS.

Επομένως, οι λειτουργίες του πυρήνα δικτύου 5G υποστηρίζουν πρωτοποριακά πρωτόκολλα ασφαλείας όπως το TLS 1.2 και 1.3 για την

No.	Time	Source	Destination	Protocol	Length	Info
16	2.349636	192.168.70.132	192.168.18.184	SCTP	366	INIT_ACK
17	2.349757	192.168.18.184	192.168.70.132	SCTP	278	COOKIE_ECHO
18	2.349802	192.168.70.132	192.168.18.184	SCTP	50	COOKIE_ACK
19	2.360253	192.168.18.184	192.168.70.132	SCTP	162	DATA
20	2.360303	192.168.70.132	192.168.18.184	SCTP	62	SACK
21	2.363914	192.168.70.132	192.168.18.184	SCTP	574	DATA
22	2.364138	192.168.18.184	192.168.70.132	SCTP	62	SACK
23	4.392052	192.168.18.184	192.168.70.132	SCTP	130	DATA
24	4.397147	02:42:c0:a8:46...	Broadcast	ARP	42	Who has 192.168.70.131? Tell 192.168.70.132
25	4.397194	02:42:c0:a8:46...	02:42:c0:a8:4...	ARP	42	192.168.70.131 is at 02:42:c0:a8:46:83
26	4.397269	192.168.70.132	192.168.70.131	TCP	74	34608 -- 3306 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=3849507364 TSecr=0 WS=128
27	4.397301	192.168.70.131	192.168.70.132	TCP	74	3306 -- 34608 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=2629468657 TSecr=3849507364 WS=128
28	4.397324	192.168.70.132	192.168.70.131	TCP	66	34608 -- 3306 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3849507364 TSecr=2629468657
29	4.397664	192.168.70.131	192.168.70.132	MySQL	144	Server Greeting proto=10 version=5.7.33
30	4.397700	192.168.70.132	192.168.70.131	TCP	66	34608 -- 3306 [ACK] Seq=1 Ack=79 Win=64256 Len=0 TSval=3849507364 TSecr=2629468657
31	4.397900	192.168.70.132	192.168.70.131	MySQL	102	Login Request user=
32	4.397917	192.168.70.131	192.168.70.132	TCP	66	3306 -- 34608 [ACK] Seq=79 Ack=37 Win=65200 Len=0 TSval=2629468658 TSecr=3849507365
33	4.399170	192.168.70.132	192.168.70.131	TLSv1.2	264	Client Hello
34	4.399184	192.168.70.131	192.168.70.132	TCP	66	3306 -- 34608 [ACK] Seq=79 Ack=235 Win=65152 Len=0 TSval=2629468659 TSecr=3849507366
35	4.405605	192.168.70.131	192.168.70.132	TLSv1.2	2088	Server Hello, Certificate, Server Key Exchange, Certificate Request, Server Hello Done
36	4.405659	192.168.70.132	192.168.70.131	TCP	66	34608 -- 3306 [ACK] Seq=235 Ack=2101 Win=64128 Len=0 TSval=3849507372 TSecr=2629468665
37	4.406858	192.168.70.132	192.168.70.131	TLSv1.2	171	Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
38	4.407239	192.168.70.131	192.168.70.132	TLSv1.2	308	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
39	4.407423	192.168.70.132	192.168.70.131	TLSv1.2	266	Application Data
40	4.407544	192.168.70.131	192.168.70.132	TLSv1.2	117	Application Data
41	4.407595	192.168.70.132	192.168.70.131	TLSv1.2	102	Application Data
42	4.407649	192.168.70.131	192.168.70.132	TLSv1.2	106	Application Data
43	4.407704	192.168.70.132	192.168.70.131	TLSv1.2	184	Application Data
44	4.408151	192.168.70.131	192.168.70.132	TLSv1.2	381	Application Data
45	4.409282	192.168.70.132	192.168.70.131	TLSv1.2	215	Application Data
46	4.409584	192.168.70.131	192.168.70.132	TLSv1.2	147	Application Data
47	4.409675	192.168.70.132	192.168.70.131	TLSv1.2	176	Application Data
48	4.409848	192.168.70.131	192.168.70.132	TLSv1.2	147	Application Data

Εικόνα 6.5: Ανάλυση πακέτου δικτύου πρόσβασης 5G SA-Πιστοποίηση εξωτερικού δικτύου

προστασία της επικοινωνίας στο επίπεδο μεταφοράς και του πλαισίου OAuth 2.0 στο επίπεδο εφαρμογής για να διασφαλιστεί ότι έχουν πρόσβαση μόνο εξουσιοδοτημένες λειτουργίες δικτύου, μια υπηρεσία που προσφέρεται από άλλη λειτουργία.

Η λειτουργία του πρωτοκόλλου TLSv1.2 φαίνεται στην επικοινωνία μεταξύ της βάσης δεδομένων και της AMF, από το πακέτο 33 και μετά όπου γίνεται η διασύνδεση και με την απαραίτητη κρυπτογράφηση, και πιστοποίηση δίνεται η πρόσβαση στα δεδομένα.

Από το πακέτο 49 ξεκινάει η εγκαθίδρυση σύνδεσης με το δίκτυο πρόσβασης και επομένως με τη συσκευή χρήστη, στέλνοντας πακέτα Selective Acknowledgment (SACK). Οι εφαρμογές SCTP υποβάλλουν δεδομένα για μετάδοση σε μηνύματα (ομάδες bytes) στο επίπεδο μεταφοράς SCTP. Το SCTP τοποθετεί τα μηνύματα και τις πληροφορίες ελέγχου σε ξεχωριστά κομμάτια-chunks- (κομμάτια δεδομένων και κομμάτια ελέγχου), όπου το καθένα αναγνωρίζεται από μια κεφαλίδα κομματιού. Το πρωτόκολλο μπορεί να κατακερματιστεί ένα μήνυμα σε πολλά κομμάτια δεδομένων, αλλά κάθε κομμάτι δεδομένων περιέχει δεδομένα από ένα μόνο μήνυμα χρήστη. Το SCTP ομαδοποιεί τα κομμάτια σε πακέτα SCTP.

### Δημιουργία περιβάλλοντος PDU συνεδρίας για το UPF

Εφόσον έχει επιτευχθεί σύνδεση μεταξύ AMF και βάσης δεδομένων, η συσκευή χρήστη επικοινωνεί με μηνύματα NAS με το δίκτυο κορμού όπως δείχνει η εικόνα 4.1. Έτσι, έχουμε ανταλλαγή μηνυμάτων AMF και UE για την άμεση πιστοποίηση μέσω του πρωτοκόλλου NAS και ειδικότερα με την περίπτωση πρωτοκόλλου 5GSM, για τη διαχείριση των συνεδριών PDU και του QoS για το επίπεδο χρήστη. Από το πακέτο 59 και έπειτα γίνεται η επικοινωνία του NRF με το SMF. Το SMF λαμβάνει τα στοιχεία συνδρομής UE (συνήθως από το UDM και το PCF) και διατυπώνει ένα αίτημα εγκατάστασης περιόδου



No.	Time	Source	Destination	Protocol	Length	Info
49	4.410596	192.168.70.132	192.168.18.184	SCTP	606	SACK DATA
50	4.411128	192.168.18.184	192.168.70.132	SCTP	142	SACK DATA
51	4.412630	192.168.70.132	192.168.18.184	SCTP	422	SACK DATA
52	4.413379	192.168.18.184	192.168.70.132	SCTP	190	SACK DATA
53	4.415858	192.168.70.132	192.168.18.184	SCTP	1198	SACK DATA
54	4.416253	192.168.18.184	192.168.70.132	SCTP	98	SACK DATA
55	4.426276	192.168.18.184	192.168.70.132	SCTP	118	DATA
56	4.426310	192.168.70.132	192.168.18.184	SCTP	62	SACK
57	4.450305	192.168.70.132	192.168.70.131	TCP	66	34608 → 3306 [ACK] Seq=953 Ack=2911 Win=64128 Len=0 TSval=3849567417 TSecr=2629468670
58	5.195109	192.168.70.135	12.1.1.2	ICMP	98	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no response found!)
59	5.682640	192.168.70.134	192.168.70.133	PFPCP	58	Sx Heartbeat Request
60	5.682802	192.168.70.133	192.168.70.134	PFPCP	58	Sx Heartbeat Response
61	5.691181	192.168.70.133	192.168.70.130	TCP	74	33494 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1185208059 TSecr=0 WS=128
62	5.691234	192.168.70.130	192.168.70.133	TCP	74	80 → 33494 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=2933092549 TSecr=1185208059 WS=128
63	5.691253	192.168.70.133	192.168.70.130	TCP	66	33494 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1185208059 TSecr=2933092549
64	5.691318	192.168.70.133	192.168.70.130	HTTP	292	PATCH /nnrf-nfm/v1/nf-instances/2e0a241f-132d-44c6-be3d-027cd15d5b20 HTTP/1.1 (application/json)
65	5.691330	192.168.70.130	192.168.70.133	TCP	66	80 → 33494 [ACK] Seq=1 Ack=227 Win=65024 Len=0 TSval=2933092549 TSecr=1185208059
66	5.691651	192.168.70.130	192.168.70.133	HTTP	163	HTTP/1.1 204 No Content
67	5.691672	192.168.70.133	192.168.70.130	TCP	66	33494 → 80 [ACK] Seq=227 Ack=98 Win=64256 Len=0 TSval=1185208059 TSecr=2933092549
68	5.691745	192.168.70.133	192.168.70.130	TCP	66	33494 → 80 [FIN, ACK] Seq=227 Ack=98 Win=64256 Len=0 TSval=1185208059 TSecr=2933092549
69	5.691788	192.168.70.130	192.168.70.133	TCP	66	80 → 33494 [FIN, ACK] Seq=98 Ack=228 Win=65024 Len=0 TSval=2933092550 TSecr=1185208059
70	5.691802	192.168.70.133	192.168.70.130	TCP	66	33494 → 80 [ACK] Seq=228 Ack=99 Win=64256 Len=0 TSval=1185208060 TSecr=2933092550
71	6.214273	192.168.70.135	12.1.1.2	ICMP	98	Echo (ping) request id=0x0013, seq=2/512, ttl=64 (no response found!)
72	6.417229	192.168.18.184	192.168.70.132	SCTP	146	DATA
73	6.419305	02:42:c0:a8:46	Broadcast	ARP	42	Who has 192.168.70.130? Tell 192.168.70.132
74	6.419363	02:42:c0:a8:46	02:42:c0:a8:46	ARP	42	192.168.70.130 is at 02:42:c0:a8:46:82
75	6.419377	192.168.70.132	192.168.70.130	TCP	74	40266 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1319218380 TSecr=0 WS=128
76	6.419421	192.168.70.130	192.168.70.132	TCP	74	80 → 40266 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM=1 TSval=519847797 TSecr=1319218380 WS=128
77	6.419446	192.168.70.132	192.168.70.130	TCP	66	40266 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1319218380 TSecr=519847797
78	6.419566	192.168.70.132	192.168.70.130	TCP	217	40266 → 80 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=151 TSval=1319218380 TSecr=519847797 [TCP segment of a reassembled PDU]
79	6.419584	192.168.70.130	192.168.70.132	TCP	66	80 → 40266 [ACK] Seq=1 Ack=152 Win=65024 Len=0 TSval=519847797 TSecr=1319218380
80	6.420017	192.168.70.130	192.168.70.132	HTTP	862	HTTP/1.1 200 OK (application/json)
81	6.420063	192.168.70.132	192.168.70.130	TCP	66	40266 → 80 [ACK] Seq=152 Ack=797 Win=64128 Len=0 TSval=1319218381 TSecr=519847798
82	6.420230	192.168.70.132	192.168.70.130	HTTP	66	GET /nnrf-disco/v1/nf-instances?target-nf-type=SMF&requester-nf-type=AMF HTTP/1.1
83	6.420276	192.168.70.130	192.168.70.132	TCP	66	80 → 40266 [FIN, ACK] Seq=797 Ack=153 Win=65024 Len=0 TSval=519847798 TSecr=1319218381
84	6.420291	192.168.70.132	192.168.70.130	TCP	66	40266 → 80 [ACK] Seq=153 Ack=798 Win=64128 Len=0 TSval=1319218381 TSecr=519847798
85	6.421519	02:42:c0:a8:46	Broadcast	ARP	42	Who has 192.168.70.133? Tell 192.168.70.132
86	6.421575	02:42:c0:a8:46	02:42:c0:a8:46	ARP	42	192.168.70.133 is at 02:42:c0:a8:46:85

Εικόνα 6.6: Ανάλυση πακέτου δικτύου πρόσβασης 5G SA-Επικοινωνία με εξωτερικό δίκτυο

σύνδεσης PFCP (Packet Forward Control Packet) για να προγραμματίσει το UPF να δημιουργήσει ένα περιβάλλον διαχείρισης συνεδρίας (δηλαδή, PDU Session) για το UE.

Η εικόνα 6.8 δείχνει πως το SMF χρησιμοποιεί το PFCP μέσω της διεπαφής N4 για να δημιουργήσει στοιχεία διαχείρισης συνεδρίας πάνω απο το UPF για το PDU Session του UE.

Στο πακέτο μηνύματος PFCP Session Establishment request περιλαμβάνονται τα ακόλουθα στοιχεία πληροφοριών (Information Elements, Ies) για ταξινόμηση UE, ουρά, προγραμματισμό και σήμανση / παρατήρηση.

#### -PDR (Packet Detection Rule)

- Περιλαμβάνει πληροφορίες ανίχνευσης πακέτου (Packet Detection Information, PDI) για την ταξινόμηση της κυκλοφορίας DL χρησιμοποιώντας 5-tuple για την χαρτογράφηση της κυκλοφορίας DL (για παράδειγμα SDF) σε μια ροή QoS (δηλαδή, SDF Binding) εντός της περιόδου σύνδεσης PDU. Το UL PDI χρησιμοποιείται για την επαλήθευση του UL στην ροή QoS πριν το UPF προωθήσει την κίνηση του UE στο DN
- Χαρτογράφηση ροής QoS δεδομένων πριν το UPF προωθήσει την κυκλοφορία του UE στο δίκτυο δεδομένων (Data Network, DN)
- Pointers για FARs, QERs, URRs και BARs
- Προτεραιότητα για τον προσδιορισμό του πότε θα χρησιμοποιηθούν το PDR και τα αντίστοιχα FAR, QER, URR και BAR

No.	Time	Source	Destination	Protocol	Length	Info
49	4.410506	192.168.70.132	192.168.18.184	NGAP/NAS-5GS	606	DownlinkNASTransport, Authentication request
50	4.411128	192.168.18.184	192.168.70.132	NGAP/NAS-5GS	142	UplinkNASTransport, Authentication response
51	4.412630	192.168.70.132	192.168.18.184	NGAP/NAS-5GS	422	DownlinkNASTransport
52	4.413379	192.168.18.184	192.168.70.132	NGAP/NAS-5GS	190	UplinkNASTransport
53	4.415858	192.168.70.132	192.168.18.184	NGAP/NAS-5GS	1198	InitialContextSetupRequest
54	4.416253	192.168.18.184	192.168.70.132	NGAP	98	InitialContextSetupResponse
55	4.426276	192.168.18.184	192.168.70.132	NGAP/NAS-5GS	118	UplinkNASTransport
56	4.426310	192.168.70.132	192.168.18.184	SCTP	62	SACK
57	4.450305	192.168.70.132	192.168.70.131	TCP	66	34608 - 3306 [ACK] Seq=953 Ack=2911 Win=64128 Len=0 TSval=384...
58	5.195109	192.168.70.135	12.1.1.2	ICMP	98	Echo (ping) request id=0x0013, seq=1/256, ttl=64 (no respons...
59	5.682640	192.168.70.134	192.168.70.133	PFCP	58	PFCP Heartbeat Request
60	5.682802	192.168.70.133	192.168.70.134	PFCP	58	PFCP Heartbeat Response
61	5.691181	192.168.70.133	192.168.70.130	TCP	74	33494 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
62	5.691234	192.168.70.130	192.168.70.133	TCP	74	80 - 33494 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SA...
63	5.691253	192.168.70.133	192.168.70.130	TCP	66	33494 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1185208059...
64	5.691318	192.168.70.133	192.168.70.130	HTTP	292	PATCH /nnrf-nfm/v1/nf-instances/2e0a241f-132d-44c6-be3d-027cd...
65	5.691330	192.168.70.130	192.168.70.133	TCP	66	80 - 33494 [ACK] Seq=1 Ack=227 Win=65024 Len=0 TSval=29330925...
66	5.691651	192.168.70.130	192.168.70.133	HTTP	163	HTTP/1.1 204 No Content
67	5.691672	192.168.70.133	192.168.70.130	TCP	66	33494 - 80 [ACK] Seq=227 Ack=98 Win=64256 Len=0 TSval=1185208...
68	5.691745	192.168.70.133	192.168.70.130	TCP	66	33494 - 80 [FIN, ACK] Seq=227 Ack=98 Win=64256 Len=0 TSval=11...
69	5.691788	192.168.70.130	192.168.70.133	TCP	66	80 - 33494 [FIN, ACK] Seq=98 Ack=228 Win=65024 Len=0 TSval=29...
70	5.691802	192.168.70.133	192.168.70.130	TCP	66	33494 - 80 [ACK] Seq=228 Ack=99 Win=64256 Len=0 TSval=1185208...
71	6.214273	192.168.70.135	12.1.1.2	ICMP	98	Echo (ping) request id=0x0013, seq=2/512, ttl=64 (no respons...
72	6.417229	192.168.18.184	192.168.70.132	NGAP/NAS-5GS	146	UplinkNASTransport
73	6.419305	02:42:c0:a8:46:84	Broadcast	ARP	42	Who has 192.168.70.130? Tell 192.168.70.132
74	6.419363	02:42:c0:a8:46:82	02:42:c0:a8:46:84	ARP	42	192.168.70.130 is at 02:42:c0:a8:46:82
75	6.419377	192.168.70.132	192.168.70.130	TCP	74	40266 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...
76	6.419421	192.168.70.130	192.168.70.132	TCP	74	80 - 40266 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SA...
77	6.419446	192.168.70.132	192.168.70.130	TCP	66	40266 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1319218380...
78	6.419566	192.168.70.132	192.168.70.130	HTTP	217	GET /nnrf-disc/v1/nf-instances?target-nf-type=SMF&requester-n...
79	6.419584	192.168.70.130	192.168.70.132	TCP	66	80 - 40266 [ACK] Seq=1 Ack=152 Win=65024 Len=0 TSval=51984779...
80	6.420017	192.168.70.130	192.168.70.132	HTTP	862	HTTP/1.1 200 OK (application/json)
81	6.420063	192.168.70.132	192.168.70.130	TCP	66	40266 - 80 [ACK] Seq=152 Ack=797 Win=64128 Len=0 TSval=131921...
82	6.420230	192.168.70.132	192.168.70.130	TCP	66	40266 - 80 [FIN, ACK] Seq=152 Ack=797 Win=64128 Len=0 TSval=1...
83	6.420276	192.168.70.130	192.168.70.132	TCP	66	80 - 40266 [FIN, ACK] Seq=797 Ack=153 Win=65024 Len=0 TSval=5...
84	6.420291	192.168.70.132	192.168.70.130	TCP	66	40266 - 80 [ACK] Seq=153 Ack=798 Win=64128 Len=0 TSval=131921...
85	6.421519	02:42:c0:a8:46:84	Broadcast	ARP	42	Who has 192.168.70.133? Tell 192.168.70.132
86	6.421575	02:42:c0:a8:46:85	02:42:c0:a8:46:84	ARP	42	192.168.70.133 is at 02:42:c0:a8:46:85
87	6.421593	192.168.70.132	192.168.70.133	TCP	74	47636 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 T...

Εικόνα 6.7: Επικοινωνία μέσω μηνυμάτων NAS

### -FAR (Packet Forwarding Rule)

- Λειτουργίες επεξεργασίας πακέτων της αλυσίδας υπηρεσιών, όπως προώθηση, αντίγραφα, αποστολή στο Control Plane κλπ...
- Σήμανση QoS (π.χ. DSCP) στο DN

Αξίζει να σημειώσουμε ότι η τιμή QFI που δημιουργείται από το SMF, αποστέλλεται στα UPF, gNB και UE για μια δεδομένη ροή QoS, έτσι ώστε όταν όλες οι οντότητες αποδέχονται τη ρύθμιση περιόδου λειτουργίας PDU, το QFI 9 αντιπροσωπεύει τη συμπεριφορά QoS της προεπιλεγμένης ρύθμισης QoS Flow για τη συνεδρία PDU. Σε άλλες υλοποιήσεις μπορεί να δημιουργείται επιπλέον και QER (QoS Enforcement Rule), BAR (Buffer Action Rule) και QoS Flow Identifier.

### Δημιουργία περιβάλλοντος PDU για το gNB και UE

Μετά τη δημιουργία του περιβάλλοντος συνεδρίας (SM Context) στο UPF, ένα παρόμοιο περιβάλλον συνεδρίας πρέπει επίσης να δημιουργηθεί στο gNB και το UE αντίστοιχα για τη ρύθμιση της UE PDU Session και την προεπιλεγμένη QoS Flow (δηλαδή, μια από άκρο σε άκρο PDU Session, από UE, gNB σε UPF). Άρα πρέπει να περιέχει και τα μηνύματα N1 και N2 για τη ρύθμιση των frames SM για το UE και το gNB αντίστοιχα.

Το ακόλουθο στιγμιότυπο του wireshark δείχνει το μήνυμα N2 από το SMF προς το AMF με το AMF να διατυπώνει το προφίλ QoS στο gNB.

Απο την ανάλυση του πακέτου γίνεται κατανοητό ότι το SMF συμβουλεύει το gNB μέσω της διεπαφής N2 HTTP1.1 με όλα τα απαραίτητα QoS IE για την εγκατάσταση συνεδρίας PDU της UE. Αυτό έχει σχεδιαστεί για να λάβει το

```

pcfap
No.    Time           Source           Destination      Protocol    Length  Info
--    -
60 5.682802      192.168.70.133  192.168.70.134  PCFAP      58      PCFAP Heartbeat Response
93 6.422580      192.168.70.133  192.168.70.134  PCFAP      169     PCFAP Session Establishment Request
98 6.422880      192.168.70.134  192.168.70.133  PCFAP      112     PCFAP Session Establishment Response
116 6.427566      192.168.70.133  192.168.70.134  PCFAP      142     PCFAP Session Modification Request

▶ Frame 93: 169 bytes on wire (1352 bits), 169 bytes captured (1352 bits)
▶ Ethernet II, Src: 02:42:c0:a8:46:85 (02:42:c0:a8:46:85), Dst: 02:42:c0:a8:46:86 (02:42:c0:a8:46:86)
▶ Internet Protocol Version 4, Src: 192.168.70.133, Dst: 192.168.70.134
▶ User Datagram Protocol, Src Port: 8805, Dst Port: 8805
▼ Packet Forwarding Control Protocol
  ▶ Flags: 0x21, SEID (S)
  ▶ Message Type: PCFAP Session Establishment Request (50)
  ▶ Length: 123
  ▶ SEID: 0x0000000000000000
  ▶ Sequence Number: 3
  ▶ Spare: 0
  ▶ Node ID : IPv4 address: 192.168.70.133
  ▶ F-SEID : SEID: 0x0000000000000001, IPv4 192.168.70.133
  ▼ Create PDR : [Grouped IE]
    ▶ IE Type: Create PDR (1)
    ▶ IE Length: 55
    ▶ PDR ID : 1
    ▶ Precedence : 0
    ▶ PDI : [Grouped IE]
    ▶ Outer Header Removal : GTP-U/UDP/IPv4
    ▶ FAR ID : Dynamic by CP 1
  ▼ Create FAR : [Grouped IE]
    ▶ IE Type: Create FAR (3)
    ▶ IE Length: 22
    ▶ FAR ID : Dynamic by CP 1
  ▼ Apply Action :
    ▶ IE Type: Apply Action (44)
    ▶ IE Length: 1
    ▶ Flags: 0x02, FORW (Forward)
  ▼ Forwarding Parameters : [Grouped IE]
    ▶ IE Type: Forwarding Parameters (4)
    ▶ IE Length: 5
    ▼ Destination Interface : Core
      ▶ IE Type: Destination Interface (42)
      ▶ IE Length: 1
      0000 .... = Spare: 0
      ... 0001 = Interface: Core (1)
  
```

Εικόνα 6.8: Εγκαθίδρυση συνεδρίας SMF προς UPF — PCFAP

gNB μια ανεξάρτητη απόφαση QoS για τη δημιουργία ασύρματης μεταφοράς για την επέκταση της σήραγγας N3 GTP-U του UE στο gNB. Αυτός ο διαχωρισμός του ελέγχου QoS μεταξύ της πρόσβασης και των βασικών δικτύων επιτρέπει στο 5GC να υποστηρίζει διαφορετικά ασύρματα και ασύρματα δίκτυα πρόσβασης με πολύ διαφορετικές δυνατότητες και χαρακτηριστικά QoS.

Απο παραπάνω εικόνα παρατηρούμε ότι τα UL και DL UE-AMBR (Συγκεντρωτικός μέγιστος ρυθμός μετάδοσης bit) είναι 20Mbps και 22 Mbps αντίστοιχα. Με άλλα λόγια, το gNB θα μειώσει οποιαδήποτε κίνηση AMBR εκτός GBR για το UE που υπερβαίνει τα 20Mbps για UL και 22Mbps για DL. Σε μια πιο σχολαστική ανάλυση του πακέτου εντοπίζουμε περαιτέρω στοιχεία όπως σε ποια IP βρίσκεται το gTPTunnel στο UPF, καθώς και το gTP-TEID για το UE. Αυτές οι πληροφορίες είναι σημαντικές για να προωθήσει το gNB την UL κυκλοφορία UE στο UPF για το DN.

Επίσης, υπάρχουν πληροφορίες QFI που αναγνωρίζουν την default QoS Flow απο το UE στο DN. Επιπρόσθετα περιγράφει το χαρακτηριστικό QoS (π.χ. βέλτιστη προσπάθεια χωρίς GBR) της προεπιλεγμένης ροής QoS στη συνεδρία PDU του UE.

Πρόσθετες πληροφορίες υπάρχουν και για την επιλογή του Network Slicing, βάσει αυτών που αναφέραμε στο θεωρητικό μέρος, ακολουθούμενα απο έναν ακέραιο αριθμό που αριθμούν το πακέτο.

Εικόνα 6.9: Αποστολή N2 μηνύματος του SMF προς το AMF για το gNB

Μετά απο τα παραπάνω το UE μπορεί τώρα να στείλει το πρώτο του πακέτο UL στο DN επειδή:

- ▷ Το UE έχει μια προεπιλεγμένη ροή QoS για να ταιριάζει με την κυκλοφορία UL στο DRB (Data Radio Bearer) που προσδιορίζεται από το QFI στο gNB
- ▷ Το gNB γνωρίζει τη διεύθυνση IP του UPF και το TEID του UE από το μήνυμα SST για προώθηση της κίνησης UL στο UPF και στο DN

Κατα τη σύνδεση, δοκιμαστικά χρησιμοποιήσαμε το εργαλείο τερματικό ring που στέλνει μηνύματα ICMP<sup>1</sup> Echo Request σε ένα άλλο τερματικό ή υπολογιστή γενικότερα, για να επιβεβαιώσει την ύπαρξη, τη σύνδεση και το χρόνο που χρειάζεται το μήνυμα να φτάσει σε αυτόν τον υπολογιστή.

Εικόνα 6.10: Αποστολή σημάτων ring για επιβεβαίωση σύνδεσης

Απο το πακέτο 124 και μετά αναλαμβάνει τη διακίνηση των δεδομένων

<sup>1</sup>Το πρωτόκολλο ICMP διαφέρει από τα πρωτόκολλα TCP και UDP διότι συνήθως δεν χρησιμοποιείται από τις εφαρμογές που εκτελούνται σε κάποιον υπολογιστή, αλλά από το λειτουργικό του συστήμα

το πρωτόκολλο GTP. Το GTP-U χρησιμοποιεί έναν μηχανισμό σήραγγας για τη μεταφορά της κίνησης δεδομένων των χρηστών και διασχίζει τη μεταφορά UDP ή ICMP ανάλογα με την περίπτωση και αναγνωρίζεται και αναγνωρίζεται σε κάθε κόμβο με μια διεύθυνση IP και την αντίστοιχη πόρτα. Στο 5GS, το GTP-U έχει επαναχρησιμοποιηθεί για να μεταφέρει δεδομένα User Plane μέσω των διεπαφών N3 και N9 (και N4), εφόσον όπως αναφέραμε και πριν η διαχείριση των ταυτοτήτων της σήραγγας και άλλα στοιχεία ελέγχου, χρησιμοποιήθηκε το πρωτόκολλο HTTP1.1 και το NGAP.

Οι σήραγγες GTP-U δημιουργούνται παρέχοντας GTP-U TEIDs και διευθύνσεις IP μεταξύ (R)AN και SMF. Αυτή η σηματοδότηση μεταφέρεται με HTTP1.1 μεταξύ SMF και AMF και με NGAP μεταξύ AMF και (R) AN. Επομένως, δεν υπάρχει χρήση του GTP-C στο 5GC για τη διαχείριση των σηράγγων GTP-U. Τέλος, παρατηρούμε ότι μια διαδρομή χρησιμοποιείται για τη σήραγγα GTP<ICMP> και GTP<UDP> με το TEID που υπάρχει στην κεφαλίδα GTP-U να υποδεικνύει σε ποια σήραγγα ανήκει κάθε φορά ένα συγκεκριμένο ωφέλιμο φορτίο(payload).

Η μη αυτόνομη λειτουργία που αναλύσαμε στην αρχή του κεφαλαίου στηρίζεται στη διασύνδεση με σημείο αναφοράς τις διεπαφές και χρησιμοποιεί για την επικοινωνία το πρωτόκολλο scrp για τη διασύνδεση.

Απο την άλλη η αυτόνομη λειτουργία όπως φαίνεται είναι βασισμένη στα πρωτόκολλα(SBA) καθώς για την περιγραφή και για την διακίνηση των δεδομένων έγινε χρήση ενός πλήθους πρωτοκόλλων αλλά και η διατήρηση της συνδεσιμότητας γίνεται μέσω αυτών όπως για παράδειγμα η επικοινωνία των οντοτήτων στο δίκτυο κορμού, που γίνεται με το πρωτόκολλο HTTP και τη διαδικασία handshake που αυτό απαιτεί, αλλά και αυξημένα επίπεδα ασφαλείας με χρήση νεότερων εκδόσεων των πρωτοκόλλων ασφαλείας (όπως SEPP και TLSv1.3)

Αυτό πλεονεκτεί καθώς τα πρωτόκολλα αυτά βασίζονται στο λογισμικό και συνεπώς είναι εφικτή η υλοποίηση σε εικονικές μηχανές και containers όπου αποδεδειγμένα καταναλώνει λιγότερους πόρους απο ότι ένα φυσικό μηχάνημα και είναι ενεργειακά πιο αποδοτικό.

Η ταχύτητα που ο πυρήνας του αυτόνομου δικτύου δημιουργεί τις εσωτερικές διασυνδέσεις και διατηρεί τη συνδεσιμότητα αλλά και η επικοινωνία με εξωτερικά δίκτυα, και συγκεκριμένα με το δίκτυο πρόσβασης, είναι αρκετά ταχύτερη απο το μη αυτόνομο δίκτυο, που μπορούμε να το θεωρήσουμε ως την τελευταία βελτίωση των προηγούμενων γενεών(διότι ακολουθεί την αρχιτεκτονική και τη φιλοσοφία τους). Συγκεκριμένα, η ταχύτητα μιας πλήρους σύνδεσης στο αυτόνομο 5G σύστημα, έτοιμης προς μεταφορά δεδομένων ανέρχεται στα 6 δευτερόλεπτα περίπου, που είναι σχεδόν 3 φορές μικρότερος χρόνος απο το μη αυτόνομο σύστημα.

## 6.2 Μελλοντικές εξελίξεις

Το αυτόνομο σύστημα δεν έχει λάβει την τελική του υλοποίηση, συνεπώς η ανάλυση του αυτόνομου συστήματος αποτελεί από μόνο του μία μελλοντική πρόβλεψη που πρόκειται να υλοποιηθεί. Αν και μία σύντομη αναφορά για την συμβολή του 5G SA στην εξέλιξη της τεχνολογίας, έχει δοθεί κατά τη διάρκεια της εργασίας, στην παράγραφο αυτή συνεπώς θα αναφερθούμε στο πως τα δίκτυα κορμού και πρόσβασης θα συνεισφέρουν στην τεχνολογική αυτή πρόοδο.

Στην επόμενη ενότητα, έχουμε συμπυκνώσει κάποιες μελέτες ερευνητών που θεωρήθηκαν σημαντικές καθώς συμβαδίζουν με την μετέπειτα εξέλιξη και άλλων καινοτόμων τεχνολογιών που το 5G πρόκειται να εφαρμοστεί.

### 6.2.1 Βελτιώσεις του αυτόνομου 5G συστήματος

Όπως αναφέραμε στην εισαγωγή της εργασίας, οι προδιαγραφές 3GPP Release-15 καθορίζουν την πρώτη γενιά αρχιτεκτονικής και λειτουργικότητας δικτύου 5G. Είναι το αποτέλεσμα μιας μεγάλης δέσμευσης του κλάδου των τηλεπικοινωνιών. Το Release-15 ορίζει επίσης την Αρχιτεκτονική βάσει Υπηρεσιών για το 5G Core Network και την υποστήριξη για μη αξιόπιστη συνδεσιμότητα πρόσβασης σε non 3GPP. [2]

Το 3GPP Release-16 επεκτείνει τις προδιαγραφές 5G σε δύο κύριους τομείς - βελτιώνοντας την αρχιτεκτονική 5G και παρέχοντας υποστήριξη για ορισμένες επιλεγμένες νέες δυνατότητες υπηρεσίας, στοχεύοντας συγκεκριμένα περιπτώσεις χρήσης που θεωρείται ότι είναι σημαντικές για επιχειρήσεις και βιομηχανίες. Σε αυτήν την παράγραφο περιγράφουμε μερικές από τις βασικές βελτιώσεις που η έκδοση-16 έχει προμηγύσει.[2]

#### **Βελτίωση της αρχιτεκτονικής που βασίζεται στις υπηρεσίες**

Υπάρχουν τρεις κύριες πτυχές της αρχιτεκτονικής που εξετάστηκαν με βάση το Enhanced Serviced Based Architecture(eSBA) κατά τη μελέτη στο 3GPP:

- Προσθήκη έμμεσης επικοινωνίας και κατ'έξουσιοδότηση ανακάλυψη όπου η επικοινωνία μεταξύ των οντοτήτων μπορεί να γίνεται και με 'Service Communication Proxy' (SCP)
- Εισαγωγή συνόλων NF και συνόλων υπηρεσιών NF, ομαδοποιώντας λειτουργίες δικτύου
- Υποστήριξη για μεταφορά περιβάλλοντος μεταξύ Nfs ώστε να υπάρχει εύκολη εναλλαγή συστημάτων μεταξύ των πωλητών των δικτύων.[2]

#### **Αυτοματισμός δικτύου**

Η λειτουργικότητα του NWDAF έχει επεκταθεί σημαντικά στο 3GPP Release-16. Νέα συλλογή δεδομένων και νέα συμβάντα αναλυτικών στοιχείων έχουν καθοριστεί για την υποστήριξη μιας σειράς επιπλέον περιπτώσεων χρήσης, με το NWDAF να παρέχει στατιστικές πληροφορίες για το παρελθόν, είτε προγνωστικές πληροφορίες για το μέλλον σε 5GC, NF και AF. Διαφορετικές παρουσίες NWDAF ενδέχεται να ειδικεύονται σε διαφορετικές κατηγορίες αναλυτικών στοιχείων όπως περιγράφεται στο 3GPP TS 23.288.[2]

### Βελτίωση Network Slicing

Στο 3GPP Release-16, η επιλογή Network Slice βελτιώθηκε κατά τη συνεργασία με το EPS και υποστηρίζει επιπλέον την επιλογή χρήσης δευτερεύοντος ελέγχου ταυτότητας μεταξύ του UE και ενός εξωτερικού AAA στο Δίκτυο δεδομένων.[2]

### Βελτιωμένη ευελιξία ανάπτυξης SMF / UPF

Μία από τις κύριες παραδοχές στο Release-15 5GC είναι ότι μια συνεδρία PDU εξυπηρετείται από ένα μόνο SMF σε περιπτώσεις μη περιαγωγής. Ωστόσο, μια περίοδος σύνδεσης PDU μπορεί να εξυπηρετηθεί από ένα ή περισσότερα UPF. Απαιτείται τουλάχιστον ένα UPF (δηλαδή ένα PDU Session Anchor UPF – PSA), αλλά μπορεί να εισαχθούν επιπλέον UPFs όταν χρειάζεται. Ένας λόγος για την εισαγωγή ενός ενδιάμεσου UPF (I-UPF) μεταξύ του RAN και του PDU Session Anchor είναι εάν το UE έχει μετακινηθεί σε μια τοποθεσία όπου δεν υπάρχει σύνδεση N3 μεταξύ του κόμβου RAN που εξυπηρετεί και του PSA. Στη συνέχεια εισάγεται ένα I-UPF και αυτό το I-UPF θα έχει τη διασύνδεση N3 προς το RAN και μια διεπαφή N9 προς το PSA UPF. Επίσης, η λύση που ορίζεται στο Release-16 είναι ότι ένα ενδιάμεσο SMF (I-SMF) προστίθεται, όταν χρειάζεται, στην αρχιτεκτονική χωρίς περιαγωγή μεταξύ του AMF και του SMF.[2]

## 6.2.2 Προσθήκη νέων δυνατοτήτων στο δίκτυο κορμού

### Υποστήριξη βιομηχανικών IoT εφαρμογών

Νέες κατακόρυφες βιομηχανικές ομάδες παρουσιάζουν αναδυόμενες και προσοδοφόρες επιχειρηματικές ευκαιρίες για το 5G. Το 3GPP αναπτύσσει διάφορα εργαλεία για τη διευκόλυνση της χρήσης του συστήματος 5G για αυτές τις περιπτώσεις χρήσης, π.χ. Σιδηροδρομική μεταφορά μαζικής διαμετακόμισης, αυτοματοποίηση κτιρίων, εργοστάσιο του μέλλοντος, ηλεκτρονική υγεία, την έξυπνη πόλη, τη διανομή ηλεκτρικής ενέργειας, την κεντρική παραγωγή ενέργειας, την έξυπνη γεωργία καθώς και τις κρίσιμες αιτήσεις αποστολής. Ορισμένες από αυτές τις περιοχές έχουν διερευνηθεί από τη 3GPP και έχουν τεκμηριωθεί στο 3GPP TR 22.804.[2]

Στα ακόλουθα τέσσερα τμήματα περιγράφουμε τέσσερα θέματα που σχετίζονται με τη στήριξη των βιομηχανικών εφαρμογών IoT που αναφέρονται στην έκδοση 3GPP-16:

#### ▷ Υπηρεσίες τύπου 5G LAN

Υπάρχουν πολλά τμήματα της αγοράς στον τομέα των κατοικιών, γραφείων, επιχειρήσεων και εργοστασίων, όπου σήμερα αναπτύσσονται τεχνολογίες τοπικού δικτύου (LAN) και εικονικού ιδιωτικού δικτύου (VPN). Αυτός είναι ένας σημαντικός τομέας όπου το σύστημα 5G θα πρέπει να παρέχει υπηρεσίες με παρόμοιες λειτουργίες όπως LAN και VPN διατηρώντας τις βελτιωμένες δυνατότητες του (π.χ. υψηλή απόδοση, πρόσβαση σε μεγάλες αποστάσεις, κινητικότητα και ασφάλεια).[2]

#### ▷ Υποστήριξη μη δημόσιων δικτύων

Ένα μη δημόσιο δίκτυο (NPN) προορίζεται για την αποκλειστική χρήση

μιας ιδιωτικής οντότητας όπως μια επιχείρηση. Τα NPNs μπορούν να αναπτυχθούν ως εντελώς αυτόνομα δίκτυα ή μπορεί να ενσωματωθούν από ένα PLMN (δηλ. Δημόσιο δίκτυο), π.χ. μπορούν να προσφερθούν ως τμήμα(slice) δικτύου ενός PLMN.[2]

- ▷ **Εξαιρετικά αξιόπιστη επικοινωνία χαμηλής καθυστέρησης**  
Εφαρμογές όπως η ρομποτική χειρουργική επέμβαση σε απόσταση από ένα δίκτυο θα έχουν απαιτήσεις εξαιρετικά αξιόπιστης, πολύ διαθέσιμης και χαμηλής έως πολύ χαμηλής απόδοσης απο άκρο σε άκρο (όπως εύρος μικρότερη από 10 ms έως 1 ms και ενδέχεται να είναι σε θέση να επιτύχουν ακόμη καλύτερη απόδοση με βελτιώσεις στις τεχνολογίες NR) και ντετερμινιστικά και περιοδικά πρότυπα επικοινωνίας.[2]
- ▷ **5G δίκτυα με χρονική ευαισθησία**  
Η 3GPP αναπτύσσει υποστήριξη Time Sensitive Networking για εφαρμογές όπως βιομηχανικές υπηρεσίες IIoT και εφαρμογές εργοστασιακού αυτοματισμού, με βάση τις απαιτήσεις υπηρεσίας και απόδοσης που ορίζονται στο 3GPP TS 22.104. Οι απαιτήσεις για συγχρονισμό ρολογιού περιλαμβάνουν: μηχανισμό υποστήριξης για συγχρονισμό του συγκεκριμένου χρήστη ρολογιού ώρας των UE με ένα παγκόσμιο ρολόι και μηχανισμό συγχρονισμού του συγκεκριμένου χρήστη για το ρολόι ώρας των UE με ένα ρολόι εργασίας. Το σύστημα 5G πρέπει επίσης να υποστηρίζει δύο τύπους ρολογιών συγχρονισμού, τον τομέα παγκόσμιου χρόνου και τους τομείς ρολογιού εργασίας (έως 32). Αυτές οι απαιτήσεις θα ακολουθήσουν το πρότυπο IEEE 802.1AS-Rev / D7.3 που αφορά τομείς συγχρονισμού.[2]

### Χρήση σε περιπτώσεις αυτοκινούμενων οχημάτων

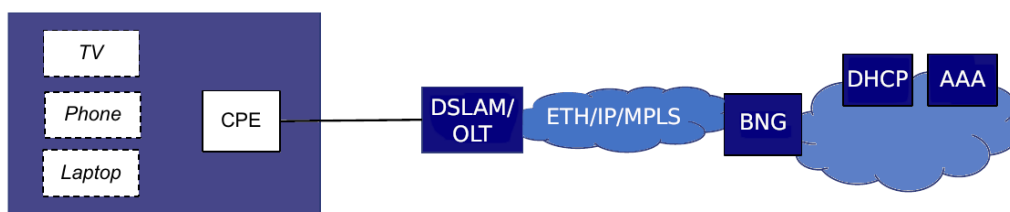
- ▷ **V2X σε EPS**  
Το 3GPP άρχισε να επιτρέπει τη χρήση LTE και EPS για την υποστήριξη απαιτήσεων της αυτοκινητοβιομηχανίας για την υποστήριξη περιπτώσεων χρήσης για επικοινωνίες με οχήματα που χρησιμοποιούν συνδεσιμότητα 3GPP, γνωστή και ως Vehicle-to-Everything (V2X) Η επικοινωνία με οχήματα απαιτεί τη δυνατότητα των οχημάτων να επικοινωνούν μεταξύ τους άμεσα, γνωστή ως επικοινωνία συσκευής σε συσκευή(D2D), καθώς και επικοινωνία μέσω της υποδομής(για παράδειγμα ενός cloud).[2][51]
- ▷ **V2X στο 5GS για NR**  
Στη Release-16, η 3GPP ξεκίνησε εργασίες για την υποστήριξη V2X έναντι NR χρησιμοποιώντας 5GC καθώς και NR ως δευτερεύον RAT χρησιμοποιώντας EPC (δηλ. EN-DC ή 5G σε EPC όπως περιγράφεται στο Κεφάλαιο 2). Η αρχιτεκτονική 5G V2X ακολουθεί τις βασικές αρχές υλοποίησης 5G, με πρόσθετες βελτιώσεις στην επικοινωνία NR-PC5 και τους μηχανισμούς διαμόρφωσης UE. Μέχρι σήμερα, για 5GS η υποστήριξη για MBMS δεν έχει ακόμη αναπτυχθεί και ως εκ τούτου οι υπηρεσίες μετάδοσης με βάση το Uu δεν είναι διαθέσιμες.[2][51]

### Ενσωμάτωση σταθερής πρόσβασης

Το 2016–2017 το Φόρουμ Ευρυζωνικότητας(Broadband Forum) και η 3GPP



άρχισαν να συζητούν τη δυνατότητα σύγκλισης δικτύου 5G, σύμφωνα με την οποία ένας ραδιοδηγός (Radio Guide, RG) θα λάβει υπηρεσία συνδεσιμότητας από τον πυρήνα 5G, αντικαθιστώντας βασικά το παλαιό κεντρικό δίκτυο ασύρματων γραμμών (BNG, AAA, DHCP κ.λπ.) με 5G Core (SMF, UPF, UDM κ.λπ.). Αυτό οφείλεται σε πολλούς φορείς που παρέχουν τόσο ενσύρματες όσο και ασύρματες υπηρεσίες, αναπτύσσοντας επί του παρόντος ξεχωριστή υποδομή δικτύου για κάθε πρόσβαση. Επίσης, προτάθηκαν ευκαιρίες ώστε να έχουν ένα κοινό πυρήνα 5G για πρόσβαση σε ενσύρματη γραμμή και ασύρματη πρόσβαση, επιτρέποντας, π.χ. σύγκλιση υπηρεσιών και εξοικονόμηση CAPEX / OPEX.[2][51]



Εικόνα 6.11: Τυπική πρόσβαση σε ασύρματη γραμμή [2]

### Πολλαπλή πρόσβαση PDU συνεδριών

Το 5GS υποστηρίζει την κινητικότητα μεταξύ 3GPP και αξιόπιστης πρόσβασης εκτός 3GPP στο Rel-15. Αυτό γίνεται μετακινώντας τις συνεδρίες PDU μεταξύ πρόσβασης 3GPP και πρόσβασης εκτός 3GPP. Κάθε συνεδρία PDU είναι επομένως σε δεδομένη στιγμή ενεργή μόνο σε μία πρόσβαση (είτε πρόσβαση 3GPP είτε μη 3GPP πρόσβαση). Αυτό σημαίνει ότι όλη η κίνηση αυτής της περιόδου σύνδεσης PDU μεταφέρεται σε έναν κοινό τύπο πρόσβασης και όλη η κίνηση μετακινείται μεταξύ των προσπελάσεων ταυτόχρονα.[2][51]

Ωστόσο, μπορεί να είναι ωφέλιμο να υπάρχει μια πιο γενική λύση όπου θα περιέχει Σύστημα διεύθυνσης: Ο τύπος πρόσβασης (3GPP και non-3GPP) μπορεί να επιλεγεί για κάθε ροή πακέτων (π.χ. IP 5-tuple ή εφαρμογή) ξεχωριστά, π.χ. όταν μια νέα εφαρμογή ή πακέτο ξεκινά η ροή.[2][51]

**Εναλλαγή:** Μια ροή πακέτου μπορεί να μετακινηθεί μεταξύ των τύπων πρόσβασης ανεξάρτητα από άλλες ροές πακέτων.

**Διαχωρισμός:** Μια ροή πακέτων (π.χ. IP 5-tuple) μπορεί ακόμη και να χωριστεί σε πρόσβαση 3GPP και πρόσβαση εκτός 3GPP ταυτόχρονα, ανά πακέτο.

Το σύστημα διεύθυνσης, εναλλαγής και διαχωρισμού επιτρέπει σε μία συνεδρία PDU να χρησιμοποιεί πόρους από πρόσβαση 3GPP και πρόσβαση εκτός 3GPP ταυτόχρονα για τη βελτίωση της συνολικής απόδοσης για μια συνεδρία PDU. Μια βασική ιδέα που εισήχθη για την υποστήριξη αυτή είναι η συνεδρία PDU πολλαπλής πρόσβασης (MA PDU Session) Πρόκειται για μια γενίκευση της τακτικής συνεδρίας PDU «μίας πρόσβασης», όπου η συνεδρία MA PDU μπορεί να έχει ταυτόχρονα πόρους User Plane σε 3GPP και πρόσβαση εκτός 3GPP. Από άποψη UPF, αυτό σημαίνει ότι υπάρχουν δύο σήραγγες N3 διαθέσιμες για τη συνεδρία PDU (και δύο σήραγγες N9 σε περίπτωση που τα ενδιάμεσα UPF βρίσκονται στη διαδρομή).

### 6.2.3 Προσθήκη νέων δυνατοτήτων στο δίκτυο πρόσβασης

#### Πολλαπλή πρόσβαση PDU συνεδριών

Η χρήση ασύρματης τεχνολογίας για backhaul έχει χρησιμοποιηθεί εκτενώς για πολλά χρόνια. Σε ορισμένες περιοχές του κόσμου, το ασύρματο backhaul αποτελεί περισσότερο από το 50% των συνδέσεων που χρησιμοποιούν ειδικές ζώνες συχνοτήτων άνω των 10 GHz. Το ασύρματο backhaul χρησιμοποιεί έτσι διαφορετική τεχνολογία και λειτουργεί σε διαφορετικά φάσματα, σε σύγκριση με τους συνδέσμους πρόσβασης (σταθμός βάσης / συσκευή). Το Relaying, που κυκλοφόρησε στην έκδοση 10 του LTE, είναι βασικά ένας ασύρματος σύνδεσμος backhaul, αν και με κάποιους περιορισμούς. Ωστόσο, μέχρι στιγμής δεν έχει χρησιμοποιηθεί στην πράξη σε σημαντικό βαθμό. Ένας λόγος είναι ότι οι ασύρματα συνδεδεμένες εφαρμογές μικρών κυψελών, για τις οποίες σχεδιάστηκε η αναμετάδοση, δεν έχουν ακόμη χρησιμοποιηθεί εκτενώς στην πράξη. Ένας άλλος λόγος είναι ότι οι χειριστές προτιμούν να χρησιμοποιούν τα πολύτιμα φάσματα χαμηλής συχνότητας για τη σύνδεση πρόσβασης. Όπως έχει ήδη αναφερθεί, η τρέχουσα ασύρματη βασίζεται βασίζεται σε τεχνολογίες που δεν είναι συμβατές με LTE. Η πρόσβαση στο ραδιόφωνο NR είναι καλά προετοιμασμένη για να υποστηρίξει τη σύνδεση backhaul και το μεγαλύτερο μέρος της απαραίτητης εργασίας είναι σε πρωτόκολλα υψηλότερου επιπέδου.[10]

#### Λειτουργία σε μη αδειοδοτούμενα φάσματα

Το φάσμα (spectrum) είναι θεμελιώδες για την ασύρματη επικοινωνία και υπάρχει μια ατελείωτη αναζήτηση για περισσότερα φάσματα για την κάλυψη των συνεχώς αυξανόμενων απαιτήσεων αυξημένης χωρητικότητας και υψηλότερων ποσοστών δεδομένων. Αυτός είναι ένας από τους λόγους για την υποστήριξη υψηλότερων συχνοτήτων των φορέων στο NR. Η πρώτη έκδοση του NR σχεδιάστηκε κυρίως για φάσματα με άδεια χρήσης. Τέτοια φάσματα προσφέρουν πολλά οφέλη αφού ο χειριστής μπορεί να σχεδιάσει το δίκτυο και να ελέγξει τις παρεμβολές. Το αδειοδοτημένο φάσμα είναι επομένως καθοριστικό για την παροχή εγγυήσεων ποιότητας υπηρεσίας και κάλυψης ευρείας περιοχής. Ωστόσο, το ποσό των αδειοδοτημένων φασμάτων στα οποία έχει πρόσβαση ένας χειριστής ενδέχεται να μην είναι επαρκές και υπάρχει συνήθως ένα κόστος που σχετίζεται με τη λήψη άδειας φάσματος.[10]

Τα φάσματα χωρίς άδεια, από την άλλη πλευρά, είναι ανοιχτά για οποιονδήποτε θέλει να τα χρησιμοποιήσει χωρίς κόστος, με την επιφύλαξη ενός συνόλου κανόνων, για παράδειγμα σχετικά με τη μέγιστη ισχύ μετάδοσης. Δεδομένου ότι οποιοσδήποτε μπορεί να χρησιμοποιήσει τα φάσματα, η κατάσταση παρεμβολών είναι συνήθως πολύ πιο απρόβλεπτη από ό, τι για τα φάσματα με άδεια. Κατά συνέπεια, η ποιότητα της υπηρεσίας και η διαθεσιμότητα δεν είναι εγγυημένα. Επιπλέον, η μέγιστη ισχύς μετάδοσης είναι μέτρια, καθιστώντας την ακατάλληλη για κάλυψη ευρείας περιοχής. Το Wi-Fi και το Bluetooth είναι δύο παραδείγματα συστημάτων επικοινωνίας που εκμεταλλεύονται φάσματα χωρίς άδεια στο εύρος χαμηλότερης συχνότητας: 2,4 GHz ή 5 GHz. Επιπλέον, ορισμένες από τις ζώνες υψηλότερης συχνότητας τις οποίες πιθανότατα θα αντιμετωπίσει το NR είναι χωρίς άδεια.[10]

Η χρήση φάσματος συχνοτήτων που ανήκουν στα mm-Wave και ανήκουν

στα μη αδειοδοτούμενα φάσματα προβλέπεται να χρησιμοποιηθεί στο μέλλον με τη χρήση πολλών μικρο κυψελών με χαμηλή ισχύ. [10]

### Μη ορθογώνια πολλαπλή πρόσβαση(NOMA)

Ένα μεγάλο τμήμα της ερευνητικής κοινότητας έχει στραφεί στην αναζήτηση νέων τρόπων διαμόρφωσης και πολυπλεξίας. Το NR χρησιμοποιεί κυρίως ορθογώνια πολλαπλή πρόσβαση, όπου διαφορετικές συσκευές χωρίζονται σε χρόνο και / ή συχνότητα. Ωστόσο, η μη ορθογώνια πρόσβαση έχει τη δυνατότητα αύξησης της χωρητικότητας σε ορισμένα σενάρια. Κατά τη διάρκεια των πρώτων σταδίων ανάπτυξης NR, η μη ορθογώνια πολλαπλή πρόσβαση (NOMA) μελετήθηκε εν συντομία αλλά είχε προτεραιότητα προς τα κάτω. Ωστόσο, οι μελέτες σχετικά με το NOMA βρίσκονται σε εξέλιξη στην έκδοση 15 και ενδέχεται να καταστούν σχετικές για το NR σε μεταγενέστερες εκδόσεις.[10]

### Machine-type επικοινωνία(MTC)

Η επικοινωνία τύπου μηχανήματος είναι ένας πολύ ευρύς όρος, που καλύπτει πολλές διαφορετικές περιπτώσεις και σενάρια χρήσης. Είναι σύνηθες να διαιρείται η επικοινωνία τύπου μηχανήματος σε μαζική επικοινωνία τύπου μηχανήματος και εξαιρετικά αξιόπιστη επικοινωνία χαμηλής καθυστέρησης (URLLC), όπως ήδη συζητήθηκε στην αρχή αυτής της εργασίας. Η μαζική επικοινωνία τύπου μηχανήματος αναφέρεται σε σενάρια όπου μια συσκευή στέλνει συνήθως πολύ μικρό αριθμό δεδομένων, έχει χαλαρές απαιτήσεις καθυστέρησης, αλλά και εξαιρετικά χαμηλή κατανάλωση ενέργειας και χαμηλό κόστος. Ο αριθμός των συσκευών αυτών είναι συχνά πολύ μεγάλος (όπως μικροί αισθητήρες). Τέτοια σενάρια θα αντιμετωπιστούν από το LTE και το NB-IoT για την εγγύς έως μεσοπρόθεσμη προοπτική, ιδίως για το μαζικό καθεστώς MTC χαμηλού επιπέδου.[10]

Ειδικοί μηχανισμοί, όπως οι δεσμευμένοι πόροι, έχουν εισαχθεί για να απλοποιήσουν τη συνύπαρξη μεταξύ NR και αυτών των τεχνολογιών πρόσβασης. Σε μακροπρόθεσμη προοπτική, το NR αναμένεται να εξελιχθεί με βελτιωμένη εγγενή υποστήριξη μαζικής επικοινωνίας τύπου μηχανήματος, εστιάζοντας κυρίως στο μαζικό MTC. Μειωμένη υποστήριξη εύρους ζώνης, λύσεις εκτεταμένης λειτουργίας ύπνου, σηματοδότηση αφύπνισης και μη ορθογώνιες κυματομορφές είναι παραδείγματα για το τι θα μπορούσε να είναι σημαντικό να μελετηθεί ως μέρος μιας τέτοιας εξέλιξης.[10]

### Device-to-device επικοινωνία (D2D)

Υποστήριξη για άμεση συνδεσιμότητα συσκευής σε συσκευή (D2D) , που αναφέρεται επίσης ως συνδεσιμότητα πλευρικού συνδέσμου, χρησιμοποιώντας το LTE που παρουσιάστηκε στην έκδοση 3GPP 12 με γνώμονα δύο κύριες περιπτώσεις χρήσης[10]:

- Επικοινωνία από συσκευή σε συσκευή, με έμφαση στην υπόθεση δημόσιας ασφάλειας
- Ανακάλυψη συσκευής σε συσκευή, που στοχεύει τη δημόσια ασφάλεια αλλά και τις περιπτώσεις εμπορικής χρήσης

Η έκδοση NR 15 δεν υποστηρίζει άμεση επικοινωνία μεταξύ συσκευών, αλλά είναι πιθανό υποψήφιο για μελλοντική κυκλοφορία. Αντί να εστιάζεται σε μια συγκεκριμένη περίπτωση χρήσης, η συνδεσιμότητα μεταξύ συσκευών πρέπει να θεωρείται ως ένα γενικό εργαλείο για την ενίσχυση της συνδεσιμότητας εντός του δικτύου 5G. Στην ουσία, η άμεση μεταφορά δεδομένων μεταξύ συσκευών θα πρέπει να ρυθμιστεί εάν το δίκτυο καταλήξει στο συμπέρασμα ότι αυτό είναι πιο αποτελεσματικό (απαιτεί λιγότερους πόρους) ή παρέχει καλύτερη ποιότητα (υψηλότεροι ρυθμοί δεδομένων ή / και χαμηλότερος λανθάνων χρόνος) σε σύγκριση με την έμμεση συνδεσιμότητα μέσω της υποδομής. Το δίκτυο θα πρέπει επίσης να μπορεί να διαμορφώνει συνδέσμους ρελέ βάσει συσκευών για να βελτιώνει την ποιότητα συνδεσιμότητας, για παράδειγμα για μαζικές συσκευές τύπου μηχανήματος με κακή ή καθόλου κάλυψη.[10]

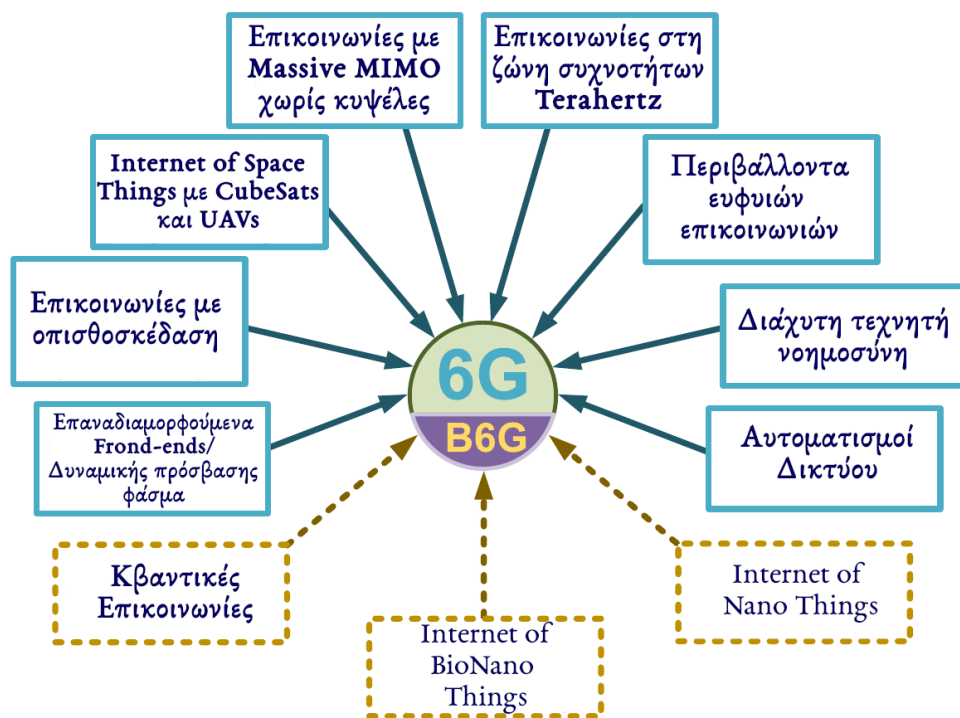
### Ευελιξία φάσματος και Duplex

Η ευελιξία Duplex είναι μια ευρεία περιοχή, με στόχο τη βελτίωση της χρήσης του διαθέσιμου φάσματος. Τα εργαλεία του NR από την αρχή - για παράδειγμα, τμήματα εύρους ζώνης, μια ευέλικτη δομή υποδοχής και συνάθροιση φορέα επίσης σε σχήματα διπλής όψης - παρέχουν μεγάλη ευελιξία και εξασφαλίζουν ότι το NR μπορεί να αναπτυχθεί σε ένα ευρύ φάσμα σεναρίων. Ωστόσο, μπορούν να εξεταστούν περαιτέρω βελτιώσεις σε αυτόν τον τομέα. Επί του παρόντος, το φάσμα FDD χωρίζεται σε ένα τμήμα κατερχόμενης ζεύξης και ένα τμήμα ανερχόμενης ζεύξης. Ωστόσο, αυτό που έχει σημασία από τεχνική άποψη δεν είναι κατά κύριο λόγο το "downlink vs uplink", αλλά η χαμηλή ισχύς έναντι υψηλής ισχύος. Η κάτω ζεύξη χρησιμοποιεί συνήθως υψηλή ισχύ και σχετικά υψηλές κεραιές πάνω από μία ταράτσα για παράδειγμα, ενώ ο ανερχόμενος σύνδεσμος χρησιμοποιεί σημαντικά χαμηλότερη ισχύ μετάδοσης και εγκαταστάσεις κεραιάς. Ως εκ τούτου, από τη σκοπιά παρεμβολών, μια μετάδοση χαμηλής ισχύος κατερχόμενης ζεύξης στο φάσμα ανερχόμενης ζεύξης δεν διαφέρει από μια μετάδοση ανερχόμενης ζεύξης χαμηλής ισχύος στο ίδιο φάσμα. Κατά συνέπεια, υπάρχουν ιδέες σχετικά με το να επιτρέπεται η μετάδοση κατερχόμενης ζεύξης και στις ζώνες ανερχόμενης ζεύξης. Σε κάποιο βαθμό, αυτό είναι το αντίστοιχο FDD στο δυναμικό TDD καθώς επιτρέπει μια δυναμική αλλαγή στην «κατεύθυνση μετάδοσης». Από τεχνική άποψη, το NR είναι καλά προετοιμασμένο για τέτοιες βελτιώσεις λόγω της ευέλικτης δομής υποδοχής.[10]

Τα πιθανά ζητήματα είναι κυρίως ρυθμιστικά. Ένας άλλος τομέας που σχετίζεται με τα φάσματα και τις πιθανές μελλοντικές βελτιώσεις είναι οι μετρήσεις παρεμβολών και το δυναμικό TDD. Το σχήμα TDD στο NR βασίζεται σε ένα δυναμικό πλαίσιο και το δυναμικό TDD είναι επομένως μέρος της έκδοσης 15. Ωστόσο, στην πράξη, τέτοιες αναπτύξεις περιορίζονται κυρίως σε μικρά κελιά. Σε μεγαλύτερα κελιά, με αντίστοιχα υψηλότερη ισχύ μετάδοσης κάτω ζεύξης, η παρεμβολή μεταξύ των κυττάρων απαιτεί συνήθως μια πιο στατική λειτουργία διπλής όψης. Μία δυνατότητα βελτίωσης του αριθμού των σεναρίων όπου είναι εφικτό το δυναμικό TDD θα μπορούσε να είναι να συμπεριληφθούν διάφοροι μηχανισμοί μέτρησης

παρεμβολών. Για παράδειγμα, εάν ο προγραμματιστής γνωρίζει την κατάσταση παρεμβολών για τις διάφορες συσκευές, μπορεί να προγραμματίσει δυναμικά για ορισμένες συσκευές, ενώ ακολουθεί μια πιο στατική προσέγγιση για άλλες συσκευές. Μπορούν επίσης να μελετηθούν διαφορετικοί μηχανισμοί συντονισμού παρεμβολών μεταξύ των κυττάρων.[10]

#### 6.2.4 6G και Beyond: Το μέλλον των ασύρματων συστημάτων επικοινωνίας



Εικόνα 6.12: Το οραμα που επιτρέπει τεχνολογίες συστημάτων ασύρματης επικοινωνίας 6G και πέραν αυτών [50]

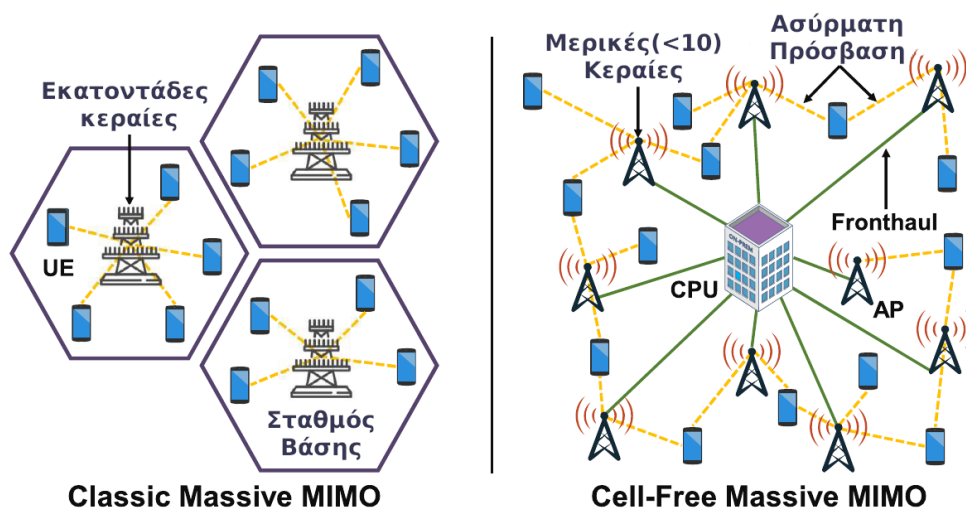
Το 6G και Beyond θα πληροί τις απαιτήσεις ενός πλήρως συνδεδεμένου κόσμου και θα παρέχει παντού και πανταχού ασύρματη συνδεσιμότητα. Οι μετασχηματιστικές λύσεις αναμένεται να δώσουν ώθηση στην εξυπηρέτηση ενός ταχέως αυξανόμενου αριθμού έξυπνων συσκευών και υπηρεσιών. Η εικόνα 6.12 προαναφέρει τις τεχνολογίες στις οποίες θα δώσει ώθηση το 6G(στα μπλε πλαίσια) καθώς και αυτές(στα διακεκομμένα πλαίσια) που μελετώνται για εφαρμογή στις τεχνολογίες πέραν του 6G(Beyond 6G, B6G)[50]

Σημαντικές τεχνολογικές ανακαλύψεις για την επίτευξη στόχων συνδεσιμότητας εντός 6G περιλαμβάνουν[50]:

- i ένα δίκτυο που λειτουργεί στη ζώνη THz με πολύ ευρύτερους πόρους φάσματος
- ii ευφυή περιβάλλοντα επικοινωνίας που επιτρέπουν ένα ασύρματο περιβάλλον διάδοσης με ενεργή μετάδοση και λήψη σήματος
- iii διάχυτη τεχνητή νοημοσύνη

- iv αυτοματισμοί δικτύων μεγάλης κλίμακας
- v μια αναδιαμορφώσιμη διεπαφή *frond-end* όλων των φασμάτων για δυναμική πρόσβαση φάσματος
- vi οπισθοδρομικές επικοινωνίες για εξοικονόμηση ενέργειας
- vii ενεργοποίηση *Internet of Space Things* από *CubeSats* και μη επανδρωμένων αεροσκαφών (*UAVs*)
- viii δίκτυα επικοινωνία με μαζικές *MIMO* χωρίς κυψέλες (*cell-free massive MIMO*)

Πηγαίνοντας πέρα από το 6G, σε αυτό που αποκαλούμε *Beyond*, πολλά υποσχόμενες τεχνολογίες πρώιμου σταδίου όπως το Διαδίκτυο των *NanoThings*, το Διαδίκτυο των *BioNanoThings* και οι κβαντικές επικοινωνίες, οι οποίες αναμένεται να έχουν εκτεταμένο αντίκτυπο στις ασύρματες επικοινωνίες, φαίνεται ότι θα ξεπροβάλλουν.[50]



Εικόνα 6.13: (Σύγκριση Cell-free MIMO και classic massive MIMO [50])

### Βασικά χαρακτηριστικά 6G και Beyond

Η βασική αρχή για την επίτευξη αυτών είναι αρχικά να υλοποιηθούν και να παραμετροποιηθούν δίκτυα που θα έχουν βασικά χαρακτηριστικά όπως τα παρακάτω

▷ **Χωρητικότητα συστήματος:** Αυτή η κατηγορία ασχολείται κυρίως με μετρήσεις που σχετίζονται με την απόδοση του συστήματος. Σε αυτά περιλαμβάνονται ο μέγιστος ρυθμός δεδομένων, ο ρυθμός δεδομένων εμπειρίας χρήστη, η μέγιστη φασματική απόδοση, η εμπειρική φασματική απόδοση, το μέγιστο εύρος ζώνης καναλιού, η χωρητικότητα κυκλοφορίας περιοχής και η πυκνότητα σύνδεσης. Σε αυτό το πλαίσιο, οι τιμές αυτές θα πρέπει να είναι εγγυημένες στο 95

▷ **Καθυστέρηση συστήματος:** Αυτή η κατηγορία περιλαμβάνει τη μέτρηση καθυστέρησης από άκρο σε άκρο, μαζί με το jitter καθυστέρησης. Σημειώνουμε ότι το jitter είναι νέα για το 6G που ποσοτικοποιεί τις διακυμάνσεις καθυστέρησης στο σύστημα, κάτι που απουσιάζει από το 5G.[50][51]

▷ **Διαχείριση συστήματος:** Αυτή η κατηγορία ασχολείται κυρίως με μετρήσεις που σχετίζονται με τη διαχείριση και ενορχήστρωση δικτύων όπως η ενεργειακή απόδοση, η αξιοπιστία και η κινητικότητα. Εδώ επίσης σημειώνουμε ότι ενώ το 5G δεν καθορίζει στόχους για τη μέτρηση ενεργειακής απόδοσης, το 6G εισάγει έναν στόχο ενεργειακής απόδοσης 1 Tb / J.[50][51]

▷ **Νέα παραδείγματα χρήσης φάσματος και σχεδίασης ραδιοσυστήματος:** Ενώ το 5G εξασφάλισε την υιοθέτηση του φάσματος mmWave, η ανάγκη για υψηλότερους ρυθμούς δεδομένων και συνεπώς μεγαλύτερα εύρη ζώνης καναλιού θα απαιτήσει την ενσωμάτωση του φάσματος terahertz (THz) και sub-THz εντός του 6G. Ταυτόχρονα, το άνοιγμα νέων ζωνών φάσματος θα απαιτήσει επίσης νέα ραδιοφωνικά σχέδια που μπορούν ταυτόχρονα να αισθανθούν και να επικοινωνήσουν σε όλο το φάσμα EM. Σε αυτή την κατεύθυνση μπορεί να χρησιμοποιηθούν τεχνολογίες ασύρματης οπτικής μετάδοσης ορατού φάσματος(Li-Fi) για την υλοποίηση ασφαλών ασύρματων συστημάτων σε συχνότητες τάξης Thz. [50][51]

▷ **Νέες Αρχιτεκτονικές Δικτύου:** Η κλασική αρχιτεκτονική ασύρματων δικτύων που βασίζεται σε κυψέλες δεν μπορεί να κλιμακωθεί για να ικανοποιήσει τις απαιτήσεις χωρητικότητας κυκλοφορίας περιοχής και πυκνότητας σύνδεσης που προτείνει το 6G. Αντ 'αυτού, το 6G θα πρέπει να ενσωματώσει υποδομή επικοινωνιών στον ίδιο τον ιστό του περιβάλλοντος.[50][51]

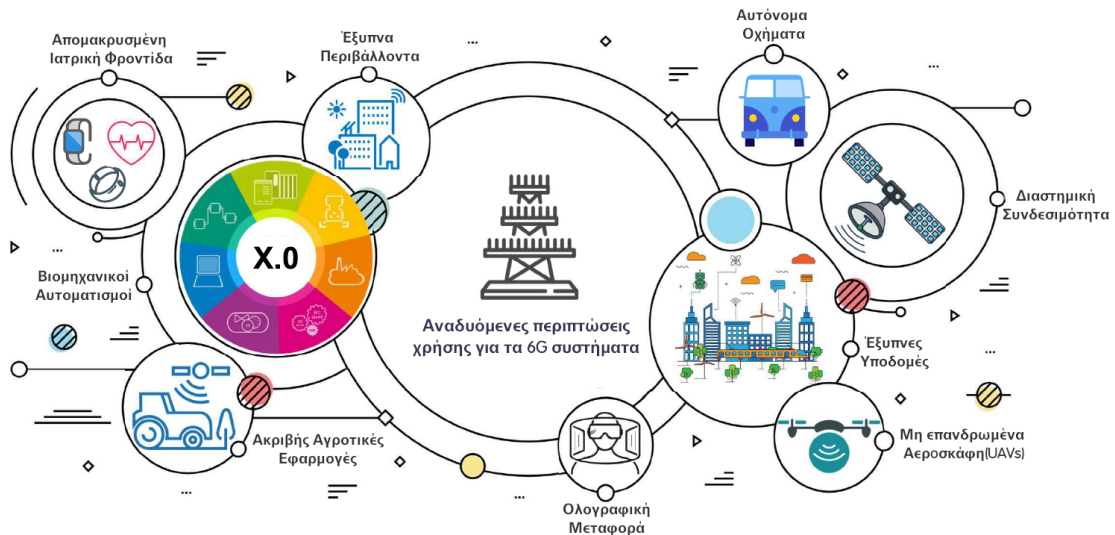
▷ **Αύξηση της νοημοσύνης και του αυτοματισμού:** Οι αυστηρές απαιτήσεις φασματικής απόδοσης, αξιοπιστίας και καθυστέρησης που σχετίζονται με το 6G υποδηλώνουν ότι η χειροκίνητη διαμόρφωση του δικτύου δεν θα είναι πλέον δυνατή. Αντίθετα, η νοημοσύνη και η αυτοματοποίηση του δικτύου θα καταλάβουν το επίκεντρο, βοηθώντας στη δημιουργία ενός ολοένα και πιο αυτόνομου δικτύου.[50][51]

▷ **Ενίσχυση της κάλυψης δικτύου πέρα από τον επίγειο τομέα:** Προκειμένου να επιτευχθεί πραγματική ασύρματη παρουσία, το 6G θα πρέπει να επεκταθεί πέρα από τα επίγεια δίκτυα, ενσωματώνοντας τόσο τη γειτονική όσο και τη deep-space συνδεσιμότητα.[50][51]

### Περιπτώσεις χρήσης

Τα διδάγματα που αντλήθηκαν από τη συνεχιζόμενη εξέλιξη των συστημάτων 5G θα χρησιμεύσουν ως το φόντο για περιπτώσεις χρήσης που θα εξυπηρετούνται καλύτερα από το 6G. Το 5G παρουσίασε για πρώτη φορά τις στοχευμένες περιπτώσεις χρήσης της ευρυζωνικής κινητής τηλεφωνίας (eMBB), της εξαιρετικά αξιόπιστης επικοινωνίας χαμηλής καθυστέρησης (URLLC) και των μαζικών επικοινωνιών τύπου μηχανής (mMTC), με σκοπό την εξυπηρέτηση μιας μεγάλης ποικιλίας εφαρμογών. Ωστόσο, υπάρχει πληθώρα εφαρμογών για τις οποίες το 5G δεν είναι αρκετά αυστηρό. Εφόσον η επιστήμη των υπολογιστών και τα τεχνολογικά επιτεύγματα είναι άμεσα συνδεδεμένα με την επιστήμη των δικτύων, το 6G τείνει να γίνει ένα δίκτυο

που θα αντικαταστήσει τα δίκτυα γενικότερα. Συνεπώς, οι χρήσεις του είναι αναρίθμητες. Ενδεικτικά αναφέρουμε ορισμένες χρήσεις παρακάτω που θα ενεργοποιηθούν από το 6G.[50]



Εικόνα 6.14: Περιπτώσεις χρήσης της 6G και Beyond τεχνολογίας [50]

*Τηλεπικοινωνίες με ολογραφήματα πολλαπλών αισθητήρων*  
Ενώ η εικονική πραγματικότητα (Virtual Reality, VR) και η επαυξημένη πραγματικότητα (Augmented Reality, AR) επωφελήθηκαν πάρα πολύ από το eMBB και το URLLC που εισήχθησαν ως μέρος του 5G, υπάρχουν πολλές εφαρμογές όπως η προηγμένη υγειονομική περίθαλψη, συμπεριλαμβανομένης της απομακρυσμένης διάγνωσης και της χειρουργικής επέμβασης, της υψηλής ανάλυσης ανίχνευσης για απομακρυσμένη εξερεύνηση και σχεδόν πραγματικές συναντήσεις βίντεο ατόμων που δεν μπορούν να εξυπηρετηθούν επαρκώς από ένα συνδυασμό AR και VR. Για το σκοπό αυτό, η ολογραφική τηλεμεταφορά έχει αναγνωριστεί ως ο φυσικός διάδοχος των λύσεων που βασίζονται σε AR και VR.[50]

*Απομακρυσμένη υγειονομική περίθαλψη σε πραγματικό χρόνο*  
Η επιτυχία των λύσεων απομακρυσμένης υγειονομικής περίθαλψης εξαρτάται κυρίως τόσο από την ποιότητα όσο και από τη διαθεσιμότητα της συνδεσιμότητας[50]

*Αυτόνομα κυβερνο-φυσικά(cyber-physical) συστήματα*  
Τα αυτόνομα οχήματα και τα μη επανδρωμένα αεροσκάφη(UAV) είναι μερικά από τα πολλά υποσχόμενα κυβερνο-φυσικά συστήματα που υπάρχουν σήμερα[50]

*Έξυπνοι Βιομηχανικοί Αυτοματισμοί*  
Τα τελευταία χρόνια, το Industry 4.0 υπήρξε η κινητήρια δύναμη πίσω από τη βιομηχανική αυτοματοποίηση με βάση τις έννοιες της βελτιστοποίησης της εφοδιαστικής αλυσίδας, του αυτόνομου εξοπλισμού, της κατασκευής



πρόσθετων, της ανάλυσης δεδομένων και του Διαδικτύου των πραγμάτων (IoT).[50]

#### *Διαστημική συνδεσιμότητα*

Ενώ η συνδεσιμότητα κοντά στη Γη και η συνδεσιμότητα στο “βαθύ σύμπαν” (deep-space) εξακολουθούν να εμφανίζονται στο 5G, υπάρχει μια μεγάλη ποικιλία περιπτώσεων χρήσης, από τη ραδιοαστρονομία και την τηλεπισκόπηση έως την πλοήγηση και την απομακρυσμένη διαχείριση που θα επωφεληθούν από τη διεισδυτική συνδεσιμότητα που προσφέρει το 6G.[50]

#### *Έξυπνα περιβάλλοντα και υποδομές*

Οι περιπτώσεις χρήσης που συζητήθηκαν μέχρι στιγμής αφορούν κυρίως τη χρήση συστημάτων τρίτων που επιδιώκουν τη μόχλευση προηγμένων τηλεπικοινωνιακών υποδομών. Ταυτόχρονα, η εξέλιξη αυτής της ίδιας της υποδομής είναι μια σημαντική περίπτωση χρήσης.[50]

#### *Διαδίκτυο των νανοπραγμάτων(Internet of NanoThings, IoNT)*

Εκτός από την ανάγκη για περισσότερους πόρους ραδιοφάσματος για να φιλοξενήσει μια πληθώρα ασύρματων συσκευών και υπηρεσιών, μια ποικιλία μετασχηματιστικών σεναρίων ασύρματων επικοινωνιών προβλέπεται επίσης να γίνει πραγματικότητα στο εγγύς μέλλον.[50]

#### *Διαδίκτυο των Βιονανοπραγμάτων για εφαρμογές υγείας*

Ιδιαίτερα σχετικό με το IoNT, με τα μοναδικά χαρακτηριστικά και τις εφαρμογές του, είναι η ιδέα του Internet of BioNanoThings (IoBNT). Για πρώτη φορά το 2015, το IoBNT έχει συγκεντρώσει σημαντική έλξη στις προσπάθειές του να συνδυάσει συνεργατικά τις τηλεπικοινωνίες με λύσεις υγειονομικής περίθαλψης[50]

#### *Κβαντικές Επικοινωνίες*

Καθώς τα δίκτυα συνεχίζουν να εξελίσσονται πέρα από το 6G, αναμένεται να ενσωματώσουν περισσότερο φάσμα, μεγαλύτερη ποικιλία διεπαφών πομποδέκτη, υψηλότερη πολυπλοκότητα στα επεξεργασμένα σήματα και αυστηρότερη απαίτηση αξιοπιστίας και, ως εκ τούτου, αναμένεται ότι οι υπολογιστικές απαιτήσεις των ασύρματων συστημάτων θα αυξηθεί επίσης με λύσεις πλέον να αναζητούνται στην επιστήμη της κβαντικής τεχνολογίας.[50]

Ακολουθεί ένας πίνακας που συγκεντρώνει τις περιπτώσεις χρήσεις και τα ανοικτά προς έρευνα θέματα που αφορούν το Beyond 6G.

Τεχνολογία που ενεργοποιείται	Βασικοί Δείκτες Απόδοσης	Ανοικτά προβλήματα
Ζώνες επικοινωνίας σε THz	Χωρητικότητα Συστήματος	-Κατασκευή και έλεγχος συστοιχιών -Έλεγχος αλγορίθμων σε πραγματικό στους πομποδέκτες -Πρωτόκολλα επικοινωνίας για συντονισμό πομπών, δεκτών και ανακλαστήρων -Σχεδιασμός πρωτοκόλλων δρομολόγησης
Περιβάλλοντα ευφυών επικοινωνιών	-Χωρητικότητα Συστήματος -Καθυστέρηση Συστήματος	-Ανταλλαγή μεταξύ διαστάσεων και κατανάλωσης ενέργειας -Συμβατότητα με υπάρχουσες τεχνολογίες -Δημιουργία προτύπων -Συμπερίληψη προηγμένων σεναρίων εφαρμογών -Λύσεις έξυπνης δέδμευσης πόρων -Βελτιστοποίηση και σχεδιασμός με γνώμονα το AI
Διάχυτη τεχνητή νοημοσύνη	-Χωρητικότητα Συστήματος -Καθυστέρηση Συστήματος -Διαχείριση συστήματος	-Γενικευμένοι αλγόριθμοι για ευρείες περιπτώσεις χρήσης -Αποτελεσματικές μετρήσεις σύγκρισης -Απουσία συνόλων δεδομένων υψηλής ποιότητας
Αυτοματισμοί δικτύου	-Καθυστέρηση Συστήματος -Διαχείριση συστήματος	-Ακριβείς ορισμοί προθέσεων -Αυτοματοποιημένα συμπεράσματα πραγματικού χρόνου -Τηλεμετρία εντός ζώνης
Επαναδιαμορφώσιμος front-end πομποδέκτης	Χωρητικότητα Συστήματος	-Νέος σχεδιασμός συσκευιών για όλα τα φάσματα επικοινωνιών -Επαναπρογραμματιζόμενα κυκλώματα, διασυνδέσεις και κεραίες -Νέες τεχνικές ενσωμάτωσης και πακεταρίσματος
Επικοινωνίες οπισθοσχεδάζομενου περιβάλλοντος	Χωρητικότητα Συστήματος	-Ενεργειακή και φασματική απόδοση -Σχεδιασμός πρωτοκόλλου
Internet of Space Things	-Χωρητικότητα Συστήματος -Διαχείριση συστήματος	-Σχεδιασμός πομποδεκτων πολλών ζωνών -Τεχνικές δρομολόγησης χαμηλής καθυστέρησης και χαμηλού overhead -Τεχνικές βελτίωσης handover με έξυπνη ποικιλομορφία gateway
Cell-Free massive MIMO	Χωρητικότητα Συστήματος	-Προγραμματισμός(scheduling) χρήστη -Βελτίωση τοποθεσίας των APs
Internet of Nano Things	-Χωρητικότητα Συστήματος -Διαχείριση συστήματος	-Βελτίωση αποδοτικότητας ισχύος -Έλεγχος παρεμβολών -Σχεδιασμός δικτυακών πρωτοκόλλων
Internet of BioNano Things	Χωρητικότητα Συστήματος	-Πειραματική επικύρωση -Αποθήκευση δεδομένων και επικύρωση
Κβαντικές επικοινωνίες	-Χωρητικότητα Συστήματος -Καθυστέρηση Συστήματος -Διαχείριση συστήματος	-Διόρθωση κβαντικών σφαλμάτων -Περίπλοκες κατανομές -Κλιμακούμενη ανάπτυξη

Πίνακας 6.2: Συγκεντρωτικός πίνακας νέων τεχνολογιών και ανοικτών θεμάτων

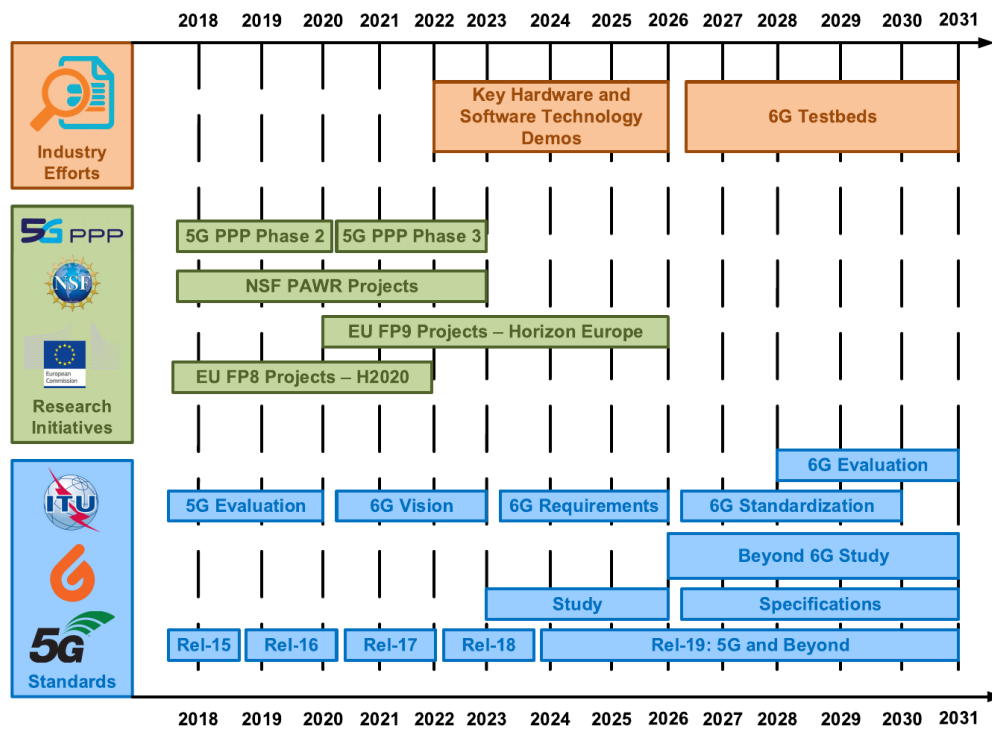
### 6.3 Επίλογος

Οι εργασίες για τις προδιαγραφές 3GPP μετά την Έκδοση-15 εστιάζονται στην προσθήκη δυνατοτήτων για πιο προηγμένες περιπτώσεις χρήσης και στην περαιτέρω βελτίωση της νέας αρχιτεκτονικής που βασίζεται στις υπηρεσίες. Η τεχνολογία 5G γενικά είναι σε καλή θέση για να διαδραματίσουν σημαντικό ρόλο για ένα ευρύ φάσμα εφαρμογών σε όλα τα μέρη μιας σύγχρονης κοινωνίας.

Νέες υπηρεσίες μπορεί να βασίζονται σε ένα σύνολο διαφορετικών τεχνολογιών πρόσβασης, όχι μόνο 5G / NR, και σε αποτελεσματική υποστήριξη στο 5G Core Network για ταυτόχρονη εξυπηρέτηση συσκευών που και οι δύο χρησιμοποιούν δίκτυα πρόσβασης με πολύ διαφορετικές δυνατότητες και ποικίλλουν σε αριθμό αρκετά δραματικά.

Οι απαιτήσεις για ένα δίκτυο που συλλέγει δεδομένα από εκατομμύρια μικρές φτηνές συσκευές αισθητήρων θα είναι φυσικά διαφορετικές από ένα δίκτυο που εξυπηρετεί μερικές συσκευές ενσωματωμένες ρομπότ που αποτελούν ένα μέρος μιας επιχειρηματικής διαδικασίας κατασκευής.

Οι δυνατότητες του θα είναι το κλειδί για την προσαρμογή των διαμορφώσεων δικτύου σε διαφορετικές υπηρεσίες και οι δυνατότητες μηχανικής εκμάθησης που αναμένεται να διαδραματίσουν σημαντικό ρόλο τόσο για την παρακολούθηση της απόδοσης όσο και για τον αυτόματο συντονισμό των διαμορφώσεων δικτύου για τη βελτιστοποίηση της χωρητικότητας, των εμπειριών των τελικών χρηστών και της συνολικής απόδοσης του δικτύου.



Εικόνα 6.15: Χρονοδιάγραμμα έργων για το 6G και Beyond συστήματα [50]

Παράλληλα με την ίδια την εξέλιξη της τεχνολογίας, θα αναπτυχθούν επίσης επιχειρηματικά μοντέλα για το συνολικό οικονομικό τοπίο. Καθώς το εύρος των αγορών-στόχων και των πελατών διευρύνεται σημαντικά, ο ρόλος του παρόχου υπηρεσιών μπορεί να αλλάξει με την πάροδο του χρόνου, προσθέτοντας νέες προσφορές από επιχείρηση σε επιχείρηση στο χαρτοφυλάκιο. Οι χειριστές θα επωφεληθούν από την παροχή υπηρεσιών πέρα από την καθαρή συνδεσιμότητα μέσω της δημιουργίας υπηρεσιών και λύσεων υψηλότερης αξίας και της στενής ολοκλήρωσης με τα δίκτυα πελατών τους.

Απο τις εφαρμογές και τις περιπτώσεις χρήσεις γίνεται κατανοητό ότι οι έρευνες για τις επόμενες γενιές μετά το 5G θα συνεχίσουν να συμβαδίζουν με τα σύγχρονα τεχνολογικά επιτεύγματα, παρέχοντας αξιόπιστες υπηρεσίες για την αδιάλειπτη επικοινωνία.

Συνοψίζοντας, με τη δημιουργία των προδιαγραφών 5G, η βιομηχανία έχει κάνει ένα σημαντικό βήμα προς τη δημιουργία μιας τεχνολογίας που μπορεί πραγματικά να πραγματοποιήσει το όραμα μιας κοινωνίας όπου απολαμβάνει όλα τα οφέλη από τη σύνδεση. Για να συμβεί αυτό, οι επιχειρηματικές αξίες και οι οδηγοί της αγοράς πρέπει να κατανοηθούν και να εφαρμοστούν με σαφήνεια για να κατευθύνουν τη μελλοντική εξέλιξη της τεχνολογίας 5G.

Ανυπομονούμε για τις συναρπαστικές στιγμές που βρίσκονται μπροστά μας.

# Βιβλιογραφία

- [1] Haesik Kim, *Design and Optimization for 5G Wireless Communications*, John Wiley & Sons Ltd (2020)
- [2] Stefan Rommer, Peter Hedman, Magnus Olsson, Lars Frid, Shabnam Sultana, Catherine Mulligan, *5G Core Networks Powering Digitalization*, Academic Press (2019)
- [3] 3GPP TS 23.501 V15.0.0 (2017-12) "System Architecture for the 5G System"(Stage 2)
- [4] 3GPP TS 23.501, V16.6.0 (2020-10) 3GPP Technical Specification 23.501, "System architecture for the 5G System (5GS)"
- [5] Θεολόγου Μ.Ε., *Δίκτυα Κινητών και Προσωπικών Επικοινωνιών (2η έκδοση)*, Εκδόσεις ΤΖΙΟΛΑ
- [6] 3GPP TS 23.502, V16.7.1 Release16 (2021-01) "Procedure for the 5G System (5GS)"
- [7] 3GPP TS 23.501, V16.6.0 Release16 (2020-10) "Procedure for the 5G System (5GS)"
- [8] 3GPP TS 23.503, 3GPP Technical Specification 23.503, "Policy and charging control framework for the 5G System (5GS)".
- [9] 3GPP TS 33.501, 3GPP Technical Specification 33.501, "Security architecture and procedures for 5G System".
- [10] Dahlman Erik, Parkvall Stefan, Sköld Johan, *5G NR-The next generation wireless access technology*, Academic Press (2018)
- [11] Sassan Ahmadi , *5G NR Architecture, Technology, Implementation, and Operation of 3gpp New Radio Standards*, Academic Press (2019)
- [12] Sasha Sirotkin, *5G Radio Access Network Architecture-The Dark Side of 5G Book*, John Wiley & Sons, 2021
- [13] Guy Pujolle, *Software Networks-Virtualization, SDN, 5G and Security*, John Wiley & Sons, 2015
- [14] Κωνσταντίνου Φ., Κανάτας Α., Πάντος Γ., *Συστήματα Κινητών Επικοινωνιών(2η Έκδοση)*, Εκδόσεις Παπασωτηρίου, 2013

- [15] 3GPP TS 38.321 version 15.6.0 Release 15, “5G-NR; Medium Access Control (MAC) protocol specification”
- [16] 3GPP TS 38.211 version 15.3.0 Release 15, “5G-NR; Physical channels and modulation”
- [17] 3GPP TS 38.300 version 15.11.0 Release 15, “NR and NG-RAN Overall description-Stage 2”
- [18] 3GPP TS 38.401 version 15.2.0 Release 15, “NG-RAN Architecture description”
- [19] Hao Jiang, Guan Gui, *Channel Modeling in 5G Wireless Communication Systems*, Springer, 2020
- [20] 3GPP TS 38.425 version 15.2.0 Release 15, “5G-NG-RAN; NR user plane protocol”
- [21] 3GPP TS 38.410 version 15.0.0 Release 15, “5G-NG-RAN; NG general aspects and principles”
- [22] 3GPP TS 38.470 version 16.2.0 Release 16, “5G-NG-RAN; F1 general aspects and principles”
- [23] 3GPP TS 38.460 version 15.0.0 Release 15, “5G-NG-RAN; E1 general aspects and principles”
- [24] <https://www.rfwireless-world.com/Tutorials/5G-NR-network-interfaces.html> [Προσπελάστηκε 25 Μαρτίου 2021]
- [25] 3GPP TS 24.501 version 15.3.0 Release 15, “5G Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3”
- [26] Kurose James, Ross Keith, *Δικτύωση Υπολογιστών*, Εκδόσεις Γκιούρδας(7η Έκδοση),2017
- [27] 3GPP TS 29.281 version 9.3.0 Release 9, “GPRS Tunnelling Protocol User Plane (GTPver.1-U)”
- [28] 3GPP TS 29.891 version 16.4.0 Release 16 “5G System; Access and Mobility Management Services(Stage 3)”
- [29] 3GPP TS 29.244 version 15.5.0 Release 15 “LTE; Interface between the Control Plane and the User Plane nodes ”
- [30] 3GPP TS 33.210 version 12.2.0 Release 12 “LTE; 3G security; Network Domain Security (NDS); IP network layer security ”
- [31] Magnus Olsson, Catherine Mulligan, “EPC and 4G Packet Networks. Driving the Mobile Broadband Revolution”, Academic Press, 2013
- [32] S. M. Ahsan Kazmi, Latif U. Khan, Nguyen H. Tran, Choong Seon Hong, “Network Slicing for 5G and Beyond Networks”, Springer International Publishing (2019)

- [33] 3GPP TS 24.502 version 15.4.0 Release 15 “5G; Access to the 3GPP 5G Core Network (5GCN) via non-3GPP access networks ”
- [34] P. Marsch, O. Bulakci, O. Questh, M. Boldi, *5G System Design Architectural and Functional Considerations and Long Term Research*, Wiley, 2018
- [35] Parallel Wireless, Inc., *5G NR Logical Architecture and its Functional Splits*
- [36] 3GPP, “TR 38.801. Technical Specification Group Radio Access Network; Study on new radio access technology: Radio access architecture and interfaces (Release 14)”, 2017
- [37] NGMN Alliance, “NGMN 5G White Paper”, Tech. Rep., 2015.
- [38] A. Garcia-Saavedra, J. X. Salvat, X. Li, and X. Costa-Perez, “WizHaul: On the Centralization Degree of Cloud RAN Next Generation Fronthaul”, IEEE Transactions on Mobile Computing, 2018.
- [39] J. Tang, R. Wen, T. Q. S. Quek and M. Peng, “Fully Exploiting Cloud Computing to Achieve a Green and Flexible C-RAN”, IEEE Communications Magazine, 2017.
- [40] Wan Lei, Anthony Soong, Liu Jianghua, Wu Yong, Brian Classon, Weimin Xiao David Mazzaresse, Zhao Yang, Tony Saboorian, *5G System Design: An End to End Perspective*, Springer, 2020
- [41] SAMSUNG Brochure, *Who & How: Making 5G NR Standards*
- [42] <https://www.3gpp.org/specifications/67-releases> [Προσπελάστηκε 03 Απριλίου 2021]
- [43] <https://5g.security/> [Προσπελάστηκε 09 Απριλίου 2021]
- [44] 3GPP, “TS 29.531 version 15.0.0 Release 15, 5G System; Network Slice Selection Services, Stage 3
- [45] [www.openairinterface.org](http://www.openairinterface.org), Gitlab [Προσπελάστηκε 13 Απριλίου 2021]
- [46] <https://www.ettus.com/all-products/USRP-N310/> [Προσπελάστηκε 25 Απριλίου 2021]
- [47] Wolfgang Rankl, Wolfgang Effing, *Smart Card Handbook*, J. Wiley (2003)
- [48] By Justin Ormont - Own work, CC BY-SA 3.0
- [49] <https://github.com/tim-ywliu/ue-ran-sim> [Προσπελάστηκε 25 Απριλίου 2021]
- [50] Ian F. Akyildiz, Ahan Kak, Shuai Nie, *6G and Beyond: The Future of Wireless Communications Systems*, IEEE 2020
- [51] Mojtaba Vaezi, Zhiguo Ding, H. Vincent Poor, *Multiple Access Techniques for 5G Wireless Networks and Beyond*, Springer, (2019)