



ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ
ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ
ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Τεχνολογίες Τεμαχισμού σε Δίκτυα Νέας Γενιάς

Γιώργος Γιάνναρος
A.M 711151063

Εισηγητής: Γιώργος Γιάνναρος, Φοιτητής

Επιβλέπων Καθηγητής: Αντώνης Μπόγγρης, Καθηγητής

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Τεχνολογίες Τεμαχισμού σε Δίκτυα Νέας Γενιάς

**Γιώργος Γιάνναρος
Α.Μ 711151063**

Εισηγητής:

Γιώργος Γιάνναρος, Φοιτητής

Εξεταστική Επιτροπή:

**Αντώνης Μπόγρης, Καθηγητής
Παναγιώτης Καρκαζής, Επ. Καθηγητής
Δημήτρης Καλλέργης, Λέκτορας Εφαρμογών**

Ημερομηνία εξέτασης 14/7/2021

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Γιώργος Γιάνναρος του Ιωάννη, με αριθμό μητρώου 711151063 φοιτητής του Πανεπιστημίου Δυτικής Αττικής της Σχολής Μηχανικών του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών, δηλώνω υπεύθυνα ότι:

«Είμαι συγγραφέας αυτής της πτυχιακής/διπλωματικής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.

Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Ο Δηλών

Γιώργος Γιάνναρος

Περίληψη

Στην παρούσα πτυχιακή εργασία μελετώνται οι τεχνολογίες τεμαχισμού εικονικοποίησης flowvisor, δικτύωση που καθορίζεται από λογισμικό (SDN)(Software-defined networking), NFV(network function virtualization), MEC(Multi-Access Edge Computing), Τεμαχισμός δικτύου ραδιοπρόσβασης (RAN slicing), OpenFlow και θα εξεταστούν σε 2 παραδείγματα, στα Data Centers και στα 5G δίκτυα. Πιο συγκεκριμένα, η διπλωματική θα χωριστεί σε 7 κεφάλαια, από τα οποία τα 1-4 θα αποτελούν το θεωρητικό μέρος και το 5 θα είναι το πρακτικό - πειραματικό μέρος. Τα κεφάλαια 6 και 7 θα περιέχουν τα συμπεράσματα, μελλοντικές εξελίξεις και βιβλιογραφία αντίστοιχα. Στο κεφάλαιο 1 θα γίνει λόγος για την κοπή δικτύου στα κέντρα δεδομένων και στο 5G. Στα κεφάλαια 2 και 3 θα μιλήσουμε γενικά με λίγα λόγια για τα κέντρα δεδομένων και το 5G αντίστοιχα. Στο κεφάλαιο 4 που είναι το μεγαλύτερο θα μιλήσουμε για την κοπή δικτύου στα κέντρα δεδομένων και στα 5G και RAN. Θα μιλήσουμε για τα πρότυπα ONF NGMN, τα πρωτόκολλα με βάση τα οποία γίνεται η κοπή δικτύων όπως τα SDN FlowVisor NFV, OpenFlow και Orion και θέματα – έννοιες που προκύπτουν όπως ασφάλεια QoS, QoE ή ο κύκλος ζωής του slice. Στο τέλος του κεφαλαίου 4 παρουσιάζονται 4 παραδείγματα κοπής δικτύου θεωρητικά με το πρωτόκολλο FlowVisor. Στο κεφάλαιο 5 εξετάζεται το πρακτικό κομμάτι όπου γίνεται η εκτέλεση του παραδείγματος 1 και η παρουσίαση του configuration, των αποτελεσμάτων του και των εργαλείων- προγραμμάτων του όπως είναι το ubuntu, το Mininet ή το javajdk.. Στο κεφάλαιο 6 αναφέρονται οι προκλήσεις και οι εξελίξεις, όπως το 6G. Στο κεφάλαιο 7 είναι ο επίλογος και στο τέλος περιλαμβάνονται ακρωνύμια και η βιβλιογραφία.

Λέξεις κλειδιά: Τεμαχισμός Δικτύου Data Centers, 5G, flowvisor, SDN, NFV, MEC, ONF, NGMN Orion, Mininet, QoS, QoE, Mininet

Περιεχόμενα

1. Εισαγωγή	9
2. Περί Data Center	10
2.1 Είδη κέντρων δεδομένων.....	10
2.2 Ασφάλεια κέντρων δεδομένων.....	11
2.3 Μορφές υπολογιστικού νέφους.....	12
2.4 Τα κέντρα δεδομένων του τώρα.....	12
3. Περί Δίκτυα 5G	13
3.1 Εφαρμογές.....	13
3.2 Επικοινωνίες Device to Device (D2D)	14
3.3 Επικοινωνίες Machine to Machine (M2M)	15
3.4 Θετικά 5G.....	16
3.5 Περί συχνοτήτων 5G	17
3.6 QoS και QoE στο 5G.....	17
3.7 Δίκτυο Ραδιοπρόσβασης (RAN)	18
3.8 Δίκτυο Ραδιοπρόσβασης υλοποιημένο στο νέφος (C-RAN).....	19
3.9 Αρχιτεκτονική 5G.....	19
4. Τεμαχισμός και εικονικοποίηση στα δίκτυα	21
4.1 Τεμαχισμός Data Center	22
4.1.1 Δικτύωση με Γνώμονα την Εφαρμογή	23
4.1.2 Ποιότητα Υπηρεσίας	23
4.1.3 Ποιότητα Εμπειρίας.....	23
4.1.4 Ασφάλεια.....	24
4.1.5 Δίκτυο που Καθορίζεται από το Λογισμικό (SDN)	24
4.1.5.1 OpenFlow	27
4.1.5.2 Flowvisor.....	28
4.2 Τεμαχισμός 5G	29
4.2.1 Λόγοι για τεμαχισμό 5G.....	29
4.2.2 Περί τεμαχισμού 5G.....	29
4.2.3 Αρχές 5G slicing.....	30

4.2.4 Εφαρμογές τεμαχισμού 5G.....	31
4.2.5 Εικονικοποίηση Λειτουργίας Δικτύου (NFV).....	32
4.2.6 Ericsson 5G Slicing	36
4.2.7 Nokia 5G Slicing	39
4.2.8 Huawei 5G Slicing	42
4.2.9 Λογισμηκοποίηση (Softwarization) 5G.....	44
4.2.10 Δίκτυο Κινητής Τηλεφωνίας Επομένης γενιάς (NGMN).....	46
4.2.11 Open Network Foundation (ONF).....	47
4.2.12 Κύκλος ζωής του Slice	48
4.2.13 Τεμαχισμός Δικτύου Ραδιοπρόσβασης (RAN Slicing)	48
4.3 Παραδείγματα τεμαχισμού δικτύου.....	51
4.3.1 Παράδειγμα 1	51
4.3.2 Παράδειγμα 2	52
4.3.3 Παράδειγμα 3	53
4.3.4 Παράδειγμα 4	58
4.3.5 Παράδειγμα 5 Αντιμετώπιση Ελαστικότητας	59
5. Πειραματική ενασχόληση	62
5.1 Παράδειγμα 1 SDN	62
5.2 Παράδειγμα 2 SDN	69
6. Προκλήσεις και μελλοντικές εξελίξεις.....	74
7. Επίλογος.....	76
Βιβλιογραφία	80

1. Εισαγωγή

Ο τεμαχισμός του φυσικού δικτύου σε εικονικά δίκτυα στις μέρες μας είναι το μέλλον της δικτύωσης. Οι πιο σημαντικές εφαρμογές που βρίσκει είναι στα κέντρα δεδομένων και στο νέο δίκτυο πέμπτης γενιάς 5G. Τα παραδοσιακά κέντρα δεδομένων εξελίχθηκαν σταδιακά σε εικονικά κέντρα δεδομένων (VDC). Αυτό σημαίνει ότι τα κτίρια δεν φιλοξενούν μόνο τον φυσικό εξοπλισμό, αλλά και πολλές εικονικές μηχανές. Η εικονικοποίηση φυσικών διακομιστών μπορεί να αποφέρει πολλά οφέλη στις εταιρείες, τους πελάτες τους και επιτρέπει στα εικονικά κέντρα δεδομένων να παρέχουν ευέλικτες και επεκτάσιμες λύσεις, με υψηλή διαθεσιμότητα και προσαρμογή, σύμφωνα με τις ανάγκες μιας επιχείρησης ή ενός πελάτη. Η εικονικοποίηση οδηγεί σε μείωση της δαπάνης κεφαλαίου capex και των δαπανών λειτουργίας opex, στην ευκολότερη διαχείριση της υποδομής, στη βελτιστοποίηση των πόρων, σε δυνατότητα για πληρωμή μόνο των πόρων που χρησιμοποιούνται, σε χαμηλότερη κατανάλωση, σε αυξημένη ασφάλεια, απόδοση, διαθεσιμότητα και επεκτασιμότητα. Ο τεμαχισμός των κέντρων δεδομένων γίνεται με την τεχνολογία SDN και το πρωτόκολλο Flowvisor.

Όσον αφορά το 5G, ο τεμαχισμός του δικτύου είναι απαραίτητη. Ο λόγος είναι γιατί πλέον με τα χαρακτηριστικά που έχει το 5G δηλαδή ταχύτητες μπορούν να φτάσουν και 20gbps, χαμηλή καθυστέρηση 1ms, χαμηλή κατανάλωση, υποστήριξη πολλών συσκευών και πολλών εφαρμογών όπως αισθητήρες IoT, έξυπνες πόλεις, σταθερό internet, αυτόματα αμάξια, που δεν μπορούσε το 4G. Αυτές οι εφαρμογές έχουν δικά τους χαρακτηριστικά και απαιτήσεις και δεν είναι δυνατόν να εφαρμοστούν όλες μαζί σε μια φυσική υποδομή 5G αποδοτικά: για παράδειγμα, μια εφαρμογή IoT με αισθητήρες που το πιο σημαντικό χαρακτηριστικό τους είναι η εξοικονόμηση ενέργειας γιατί λειτουργούν με μπαταρίες δεν μπορεί να έχει μετάδοση δεδομένων 1gbps γιατί δεν την χρειάζεται. Για αυτό τον λόγο πρέπει να φτιαχτούν εικονικά 5G δίκτυα όπου το καθένα θα έχει τα δικά του χαρακτηριστικά για να μπορούν οι εφαρμογές να εκτελεστούν αποδοτικά και να εκμεταλλευτούν τα θετικά της εικονικοποίησης που αναφέραμε παραπάνω στα κέντρα δεδομένων, καθώς η εικονικοποίηση στα κέντρα δεδομένων και στο 5G έχουν την ίδια λογική. Το network slicing στο 5G γίνεται με την τεχνολογία SDN και NFV.

2. Περί Data Center

Ένα Data Center είναι ένας χώρος π.χ. ένα κτίριο, μέσα στο οποίο βρίσκονται υπολογιστές, διακομιστές (servers) τείχη προστασίας, συστήματα αποθήκευσης, ελεγκτές παράδοσης εφαρμογών, καλώδια δικτύων που τα διασυνδέουν όπως switches, καλώδια ethernet και οπτικές ίνες. Επειδή αυτά τα στοιχεία αποθηκεύουν και διαχειρίζονται κρίσιμα δεδομένα και εφαρμογές η ασφάλεια κατά τον σχεδιασμό του κέντρου δεδομένων είναι πάρα πολύ σημαντική. Από όλα αυτά τα στοιχεία δημιουργούνται η υποδομή δικτύου, η υποδομή αποθήκευσης και οι υπολογιστικοί πόροι. Η υποδομή δικτύου συνδέει διακομιστές φυσικούς και εικονικοποιημένους υπηρεσίες κέντρου δεδομένων, αποθήκευση και εξωτερική συνδεσιμότητα με τοποθεσίες τελικού χρήστη. Στην υποδομή αποθήκευσης αποθηκεύονται τα αρχεία και όλα τα πράγματα που έχουν να κάνουν με το προϊόν που προσφέρεται στον χρήστη. Οι υπολογιστικοί πόροι είναι η επεξεργασία, η μνήμη, η τοπική αποθήκευση και η συνδεσιμότητα δικτύου των διακομιστών που χρησιμοποιούνται για τις εφαρμογές. Ένα data center συνήθως απασχολείται με το να αποθηκεύει, να επεξεργάζεται και να διαμοιράζει μεγάλες ποσότητες δεδομένων σε πελάτες (clients) με την λογική client-server. Για παράδειγμα ένας πελάτης μπορεί να αποθηκεύσει τη ιστοσελίδα του ώστε να είναι πρόσβαση από το διαδίκτυο ή να αποθηκεύσει κάποια αρχεία του.

Όσο περνάει ο καιρός, όλο και περισσότερες μεγάλες εταιρίες - επιχειρήσεις αναπτύσσουν το δικό τους data center για να εξυπηρετήσουν τις ανάγκες τους. Παρόλα αυτά δεν είναι απαραίτητο κάθε εταιρία να φτιάξει το δικό της data center καθώς πέρα ότι ένα data center είναι ακριβό για να φτιαχτεί υπάρχουν ήδη έτοιμα data centers από Cloud providers που μπορούν να ενοικιαστούν και να χρησιμοποιούν από τις επιχειρήσεις για να καλύψουν τις ανάγκες τους π.χ. για να αποθηκεύσουν το πληροφοριακό τους σύστημα ή να προσφέρουν υπηρεσίες σε πελάτες. Στο Cloud προκύπτουν κάποιοι ρολόι. Ο καταναλωτής που είναι άτομο ή οργανισμός που χρησιμοποιεί την υπηρεσία που προσφέρεται. Ο πάροχος που παρέχει την νεφοϋπολογιστική υπηρεσία. Ο ελεγκτής που αξιολογεί τις λειτουργίες του συστήματος πληροφοριών, την απόδοση και την ασφάλεια της νεφοϋπολογιστική υπηρεσίας. Ο μεσίτης που διαχειρίζεται τη χρήση, την απόδοση και την παροχή υπηρεσιών νέφους και διαπραγματεύεται σχέσεις μεταξύ παροχών και καταναλωτών. Ο φορέας που παρέχει συνδεσιμότητα και μεταφορά υπηρεσιών νέφους από τους παρόχους προς τους καταναλωτές. Οι Network Providers είναι αυτοί που δίνουν την δυνατότητα επικοινωνίας της επιχείρησης ή ενός ατόμου με το κέντρο δεδομένων. Τέτοιοι μπορεί να είναι οι προμηθευτές υπηρεσίας διαδικτύου.

2.1 Είδη κέντρων δεδομένων

Υπάρχουν διάφορα είδη κέντρων δεδομένων. Τα κέντρα δεδομένων επιχειρήσεων, κατασκευάζονται ανήκουν και λειτουργούν από εταιρίες και βελτιστοποιούνται για τους τελικούς χρήστες τους. Τα κέντρα δεδομένων επιχειρήσεων στεγάζονται στις εταιρίες.

Τα κέντρα δεδομένων συναθροίσεων. Το κέντρο δεδομένων συναθροίσεων είναι

ένας τύπος κέντρου δεδομένων όπου ο εξοπλισμός, ο χώρος και το εύρος ζώνης είναι διαθέσιμοι προς ενοικίαση σε πελάτες λιανικής. Οι εγκαταστάσεις παρέχουν χώρο, ρεύμα, ψύξη για τα συστήματα και φυσική ασφάλεια για τον διακομιστή, τον αποθηκευτικό εξοπλισμό και τον εξοπλισμό δικτύωσης άλλων εταιρειών. Οι πελάτες διατηρούν τον έλεγχο του σχεδιασμού και της χρήσης του εξοπλισμού τους, αλλά η καθημερινή διαχείριση του κέντρου δεδομένων και της εγκατάστασης εποπτεύεται από τον πάροχο συν εγκατάστασης πολλών ενοικιαστών

Ένα άλλο είδος είναι τα κέντρα δεδομένων cloud. Είναι μια οικονομικά αποδοτική εναλλακτική λύση για τη δημιουργία και την λειτουργία ενός κέντρου δεδομένων. Κάποιες εταιρίες που προσφέρουν υπηρεσίες cloud είναι η Amazon Web Services (AWS), Microsoft (Azure), και IBM Cloud. Ένα τεράστιο πλεονέκτημα του cloud είναι ότι οι πελάτες μπορούν να έχουν πρόσβαση στα δεδομένα τους από οποιοδήποτε σημείο και από οποιαδήποτε συσκευή laptop η κινητό τηλέφωνο αρκεί να έχουν πρόσβαση στο διαδίκτυο. Πράγμα το οποίο δεν είναι δύσκολο εφόσον υπάρχουν τα δίκτυα κινητής τηλεφωνίας 4G και 5G.

2.2 Ασφάλεια κέντρων δεδομένων

Ένα σημαντικό θέμα στα κέντρα δεδομένων cloud είναι η ασφάλεια. Διάφορα θέματα στην ασφάλεια μπορούν να συμβούν όπως παραβιάσεις δεδομένων, υπολογισμών, άρνηση υπηρεσίας, επιθέσεις πλημυρών κτλπ. Την ασφάλεια και τον έλεγχο τα αναλαμβάνουν οι πάροχοι του νέφους. Οι βασικές δομές ασφάλειας είναι οι πληροφορίες, η ταυτότητα των χρηστών και η υποδομή. Οι πληροφορίες ρέουν στη φυσική υποδομή από πολλούς χρήστες σε διαφορετικές συσκευές και γεωγραφικές περιοχές. Ο στόχος της ασφάλειας πληροφοριών είναι για την προστασία πληροφοριών και συστημάτων πληροφοριών από μη εξουσιοδοτημένη πρόσβαση, χρήση, αποκάλυψη, διακοπή, τροποποίηση ή καταστροφή. Με άλλα λόγια υπάρχει η απαίτηση προστασίας του απορρήτου, της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των δεδομένων.

Η εμπιστευτικότητα δεδομένων έχει να κάνει με την προστασία των δεδομένων και την μη αποκάλυψη αυτών σε άτομα μη εξουσιοδοτημένα. Αυτό μπορεί να γίνει από κάποιον κακόβουλο χρήστη που εκμεταλλεύεται κάποια χαρακτηριστικά και κενά ασφάλειας όπως είναι η πρόσβαση δεδομένων από πολλά σημεία από πολλές συσκευές και το ότι οι πόροι μοιράζονται σε επίπεδο δικτύου, κεντρικού υπολογιστή και εφαρμογής. Παρόλο που υπάρχει απομόνωση σε εικονικό επίπεδο το υλικό δεν διαχωρίζεται.

Η ακεραιότητα δεδομένων έχει να κάνει με το ότι τα δεδομένα δεν έχουν υποστεί για οποιοδήποτε λόγο διαγραφή, τροποποίηση, κλοπή η κατασκευή. Αυτά μπορεί να έχουν γίνει κατά λάθος ή σκόπιμα από ένα κακόβουλο άτομο όπως ένας υπάλληλος της εταιρίας που έχει πρόσβαση να τροποποιήσει ένα πρόγραμμα για να αποτύχει κάτω από κάποιες συνθήκες η έναν συγκεκριμένο χρόνο. Στο Cloud γίνονται έλεγχοι στους εργαζομένους δίνοντας τους δικαιώματα για να έχουν πρόσβαση σε συγκεκριμένους χώρους με την χρήση εταιρικών ηλεκτρονικών καρτών και κωδίκων πρόσβασης. Μια επίθεση που μπορεί να γίνει για να καθείς η ακμαιότητα δεδομένων είναι η επίθεση man in the middle. Ο κακόβουλος παίρνει πρόσβαση στην επικοινωνία μεταξύ 2 ατόμων που επικοινωνούν και μπορεί να κλέψει, να τροποποιήσει η και να δημιουργήσει τα δεδομένα αυτής της επικοινωνίας. Παρόλα αυτά ο πάροχος πρέπει να κρατάει αντίγραφα ασφαλείας των δεδομένων που φιλοξενεί και το θέμα της ακεραιότητας των δεδομένων είναι δικό του.

Η διαθεσιμότητα των δεδομένων έχει να κάνει με το πόσο διαθέσιμο είναι το cloud

που παρέχει την πληροφορία ή την υπηρεσία. Το Cloud θα πρέπει να είναι 24 ώρες την ημέρα διαθέσιμο και ένα έχει γρήγορη πρόσβαση στο διαδίκτυο. Παρόλα αυτά οι υπηρεσίες και οι πληροφορίες δεν είναι πάντα διαθέσιμες στους καταναλωτές για πολλούς λόγους. Ο πρώτος και σημαντικός είναι να τεθεί εκτός λειτουργίας ένας server λόγω επίθεσης όπως αυτή της άρνησης υπηρεσίας (DDOS) όπου στέλνονται πολλά πακέτα με την μορφή αίτησης στον server με αποτέλεσμα ο server να τα φτύσει και να μην μπορεί να εξυπηρετήσει τους κανονικούς πελάτες. Αυτό αντιμετωπίζεται συνήθως με ένα τείχος προστασίας. Παρόλα αυτά οι hackers μπορεί να εκμεταλλευτούν κάποιο κενό ασφαλείας και να ξεγελάσουν το τείχος προστασίας. Άλλος λόγος είναι να βγει εκτός λειτουργίας δηλαδή να καεί κάποιος server η οτιδήποτε εξάρτημα που δημιουργεί την φυσική υποδομή του cloud. Είναι λογικό αυτό αφού τίποτα δεν κρατάει για πάντα. Μπορεί το cloud να μην μπορεί να εξυπηρετήσει τους χρήστες επειδή μια συγκεκριμένη ώρα ζήτησαν πάρα πολλοί χρήστες μια υπηρεσία. Εκεί θα χρειαστούν περισσότεροι πόροι με την μορφή αναβάθμισης μνήμης, επεξεργαστικής ήσυχης και χώρου αποθήκευσης για να μπορούν να εξυπηρετηθούν οι χρήστες σε μια παρόμοια κατάσταση φόρτου εργασίας. Μπορεί να γίνουν φυσικές καταστροφές όπως είναι φωτιά πλημύρες σεισμούς η διακοπή ρεύματος. Εκεί απλά θα πρέπει να υπάρχουν εφεδρικοί servers και ρεύμα με κάποια γεννήτρια άμα υπάρχει αυτή η δυνατότητα. Ο πάροχος cloud θα πρέπει να εκτελεί συνεχή συντήρηση και ενημερώσεις, έχοντας συχνά πολλά κέντρα δεδομένων σε πολλές γεωγραφικές τοποθεσίες για να προστατεύει τα δεδομένα κατά τη διάρκεια διακοπών και άλλων αστοχιών.

2.3 Μορφές υπολογιστικού νέφους

Υπάρχουν 3 μορφές υπολογιστικού νέφους. Η πρώτη είναι η Software as a Service (SaaS). Αντί να εγκατασταθεί λογισμικό στο υπολογιστή του πελάτη επιβαρύνοντάς τον με τακτικές επιδιορθώσεις, συχνές ενημερώσεις εκδόσεις κτλπ. διατίθενται μέσω του διαδικτύου για την κατανάλωση του τελικού χρήστη. Η δεύτερη είναι Platform as a Service (PaaS). Ο πελάτης δεν χρειάζεται να αγοράσει και πληρώσει τις άδειες λογισμικού για πλατφόρμες όπως και τα λειτουργικά συστήματα, τις βάσεις δεδομένων και το ενδιάμεσο λογισμικό, μπορεί να το κάνει χρησιμοποιώντας την πλατφόρμα και τα εργαλεία (όπως το Java, το .NET, Python, Ruby on Rails). Και τρίτη και τελευταία Infrastructure as a Service (IaaS). Σε αυτή την μορφή παρέχονται οι υλικές συσκευές, υπολογιστές servers, συσκευές αποθήκευσης μέσα από το διαδίκτυο με έλεγχο ταυτότητας σύνδεσης και κωδικούς πρόσβασης από οποιαδήποτε συσκευή.

2.4 Τα κέντρα δεδομένων του τώρα

Τα σύγχρονα κέντρα δεδομένων είναι πολύ διαφορετικά από ότι πριν λίγο. Η υποδομή έχει μετατοπιστεί από παραδοσιακούς εσωτερικούς φυσικούς διακομιστές σε εικονικά δίκτυα που υποστηρίζουν εφαρμογές και φόρτο εργασίας σε ομάδες φυσικών υποδομών και σε περιβάλλον πολλαπλών δυνατοτήτων. Σε αυτή την εποχή, τα δεδομένα υπάρχουν και συνδέονται σε πολλαπλά κέντρα δεδομένων, στην άκρη(edge), στα ιδιωτικά και δημοσιά clouds. Το κέντρο δεδομένων πρέπει να είναι σε θέση να επικοινωνεί μεταξύ αυτών των πολλαπλών μεριών τόσο στο εσωτερικό όσο και στο cloud. Τα κέντρα δεδομένων είναι σημαντικά για την επιχείρηση λόγω των εφαρμογών που υποστηρίζουν τα εικονικά δίκτυα. Κάποιες από αυτές είναι αλληλογραφία και διαμοιρασμό αρχείων,

εφαρμογές παραγωγικότητας, διαχείριση σχέσης πελατών (customer relationship management CRM) για την βελτίωση των επιχειρηματικών σχέσεων για την ανάπτυξη της επιχείρησης, επιχειρησιακός προγραμματισμός πόρων και βάσεις δεδομένων, μεγάλα δεδομένα(Big Data), τεχνητή νοημοσύνη και μηχανική μάθηση, εικονικά Desktop επικοινωνίες και υπηρεσίες συνεργασίας.

Ο τεμαχισμός του κέντρου δεδομένων σε εικονικά μικρότερα κέντρα δεδομένων γίνεται με την τεχνολογία δικτύωση καθορισμένη από το λογισμικό SDN (Software-defined networking) και με το πρωτόκολλο Flowvisor. Παρόλα αυτά υπάρχουν και άλλοι hypervisor που σπανέ τα δίκτυα σε εικονικά ανάλογα με την υπηρεσία. Τετοια είναι το OpenVirteX, OpenSlice, MobileVisor, RadioVisor, HyperFlex. Καθώς γίνεται ο τεμαχισμός δικτύου προκύπτουν κάποια θέματα. Αυτά είναι η ασφάλεια, ποιότητα υπηρεσίας QoS(Quality Of Service), ποιότητα εμπειρίας του χρήστη QoE, λειτουργικότητα με γνώμονα την εφαρμογή(Application-aware Functionality), Βελτιστοποίηση (Optimization).

3. Περί Δικτύων 5G

Το 5G είναι η νεότερη γενιά δικτύου κινητής επικοινωνίας. Χρησιμοποιεί κελιά όπως και το 4G. Το κάθε κελί έχει και μια κεραία. Δηλαδή η περιοχή κάλυψης χωρίζεται σε μικρές γεωγραφικές περιοχές. Μέρα με τη μέρα επεκτείνεται στον χάρτη από τους τηλεπικοινωνιακούς παρόχους και έχει φτιαχτεί για να καλύψει αυτά που δεν μπορούσε το 4G. Κάποια χαρακτηριστικά του είναι ότι προσφέρει υψηλές ταχύτητες και μικρή απόκριση, χαμηλή κατανάλωση μπαταρίας, ποιότητα υπηρεσίας και εμπειρίας χρήστη με βάση την χρέωση και μεγάλη διαθεσιμότητα, ασφάλεια και κινητικότητα. Το 5G είναι πάρα πολλές φορές πιο γρήγορο από το 4G αφού η ταχύτητα που θα πιάνει θεωρητικά είναι 10Gbps ενώ του 4G advance 300mbps στο download. Θα έχει πολύ μικρή καθυστέρηση 1ms για αυτό το καθιστά ικανότατο να υποστηρίξει υπηρεσίες μεγάλου πραγματικού χρόνου με μεγάλο bandwidth.

3.1 Εφαρμογές

Οι απαιτήσεις είναι πολλές και θα χρησιμοποιείται στην δημόσια ασφάλεια, στον παραγωγικό, εκπαιδευτικό, γεωργικό και ψυχαγωγικό τομέα. Επίσης θα υποστηρίζονται Device to Device επικοινωνίες (D2D) και Machine to Machine (M2M). Όσον αφορά για τα εργοστάσια και τις εταιρίες, το 5G θα χρησιμοποιείται για τον έλεγχο απομακρυσμένων βιομηχανικών ρομπότ και συστήματα μεταφοράς χωρίς οδηγό. Με αυτόν τον τρόπο, θα αυξηθεί η παραγωγικότητα και θα μειωθούν το κόστος και οι κίνδυνοι του προσωπικού. Θα χρησιμοποιηθεί επίσης στην ιατρική. θα μπορούν να παρακολουθούνται ασθενείς απομακρυσμένα σε πραγματικό χρόνο και ο κάθε χειρουργός θα μπορεί να χειρουργήσει τον ασθενή απομακρυσμένα με την χρήση ιατρικών ρομπότ, εάν δεν υπάρχει άλλη λύση. Τα δεδομένα θα μεταφέρονται σε πολύ γρήγορους χρόνους και οι ασθενείς θα είναι πιο ασφαλείς, αφού θα βελτιωθούν η πρόληψη, η διάγνωση, η παρακολούθηση και η θεραπεία.

Όλα αυτά έχουν ως αποτέλεσμα την βελτίωση του δημόσιου και του ιδιωτικού συστήματος υγείας.

Ένας άλλος παράγοντας είναι η εκπαίδευση και η διασκέδαση. Η εκπαίδευση σε σχολεία ή πανεπιστήμια μπορεί να χρειαστεί να γίνει εξ αποστάσεως. Θα γίνεται χωρίς πρόβλημα με το 5G αφού θα υποστηρίζονται live streaming ήχος και βίντεο χωρίς καθυστερήσεις. Στον ψυχαγωγικό τομέα τα βίντεο 4K και 8K για παράδειγμα στο YouTube θα φορτώνονται πολύ εύκολα. Θα υπάρχει η δυνατότητα για live streaming, ανταγωνιστικό gaming που χρειάζεται μικρή απόκριση και Virtual Reality (VR). Με το 5G θα δημιουργηθούν έξυπνες πόλεις, δηλαδή πολλές συσκευές IoT θα συνδέονται μεταξύ τους όπου θα μεταφέρονται δεδομένα σε πραγματικό χρόνο. Αυτό σημαίνει ότι τα αμάξια θα μπορούν να μετακινούνται χωρίς οδηγό μέσω AI και 5G, θα υπάρχει δυνατότητα παρακολούθησης των δημοσίων συγκοινωνιών και των ελευθέρων χώρων στάθμευσης, και θα παρατηρηθεί βελτιστοποίηση της κυκλοφορίας με έξυπνα φανάρια. Με αυτά τα δεδομένα θα καταπολεμηθούν ο αυξημένος συνωστισμός και η αυξημένη κυκλοφορία.

Μια άλλη σημαντική εφαρμογή είναι στη γεωργία. Με το Internet of Things (IoT) και το 5G θα αυξηθεί η παραγωγή της Γης. Αυτό θα γίνει με διάφορους αισθητήρες στις καλλιέργειες και στα ζώα διασυνδεδεμένους μεταξύ τους με 5G, όπου θα μετράνε διάφορα δεδομένα, όπως η θερμοκρασία, η υγρασία, ή τα χημικά στοιχεία του εδάφους. Μέσα από τις μετρήσεις θα βγαίνουν κάποια συμπεράσματα για να γίνουν κάποιες ενέργειες απομακρυσμένα όπως είναι το πότισμα ή το ψέκασμα μόνο όπου χρειάζεται με χρήση Drone ή άλλων τρόπων. Με το IoT η διαχείριση του νερού θα γίνει πολύ εύκολα με την χρήση έξυπνων βαλβίδων και αισθητήρων ροής, πίεσης, και θερμοκρασίας. Θα χρησιμοποιείται και στο σπίτι για ενεργοποίηση και απενεργοποίηση συσκευών όπως ο θερμοσίφωνας ή το air condition.

Μια τελευταία εφαρμογή είναι στην δημόσια ασφάλεια. Κάμερες και drones διασυνδεδεμένα μέσω 5G θα παρακολουθούν χώρους όπως μαγαζιά, εταιρίες, οικόπεδα και δρόμους για την αντιμετώπιση απρόβλεπτων καταστάσεων όπως τα αυξημένα επίπεδα ρύπανσης, οι πυρκαγιές ή οι πλημμύρες, οι σεισμοί ή οι παράνομες και επικίνδυνες καταστάσεις όπου θα χρειαστεί να επέμβουν είτε η αστυνομία ή η πυροσβεστική ή οι ομάδες αναζήτησης και διάσωσης. Θα μπορεί ένας ιδιοκτήτης σπιτιού, μαγαζιού ή οικοπέδου να παρακολουθεί απομακρυσμένα το μαγαζί του όποτε θέλει. Φυσικά το 5G λόγω των χαρακτηριστικών του ίσως θα μπορεί να προσφέρει και μελλοντικές, άγνωστες προς το παρόν, υπηρεσίες.

3.2 Επικοινωνίες Device to Device (D2D)

Πλέον με το 5G θα υποστηρίζονται οι επικοινωνίες D2D (Device to device). Οι συσκευές, ιδιαίτερα τα smartphones που θα βρίσκονται κοντά, θα μπορούν να επικοινωνούν με αυτή την τεχνολογία. Με αυτόν τον τρόπο εξοικονομείται μπαταρία, γιατί μια συσκευή θα επικοινωνεί με μια άλλη σε κοντινότερη απόσταση από ό,τι στον σταθμό

βάσης. Καλύτερεύουν το latency και η ταχύτητα δεδομένων, ενώ αποφεύγονται και οι παρεμβολές με σήματα άλλων συσκευών. Το D2D θα χρησιμοποιείται όπως και το Bluetooth, αλλά θα είναι πιο γρήγορο. Θα μεταφέρονται μεταξύ των συσκευών αρχεία, εικόνες, βίντεο πολύ γρήγορα και επίσης θα υποστηρίζονται και παιχνίδια μεταξύ των συσκευών, αφού θα υπάρχει και χαμηλό latency. Επίσης βρίσκει εφαρμογή σε περιπτώσεις έκτακτης ανάγκης, για παράδειγμα σε φυσικές καταστροφές όπως τυφώνες και σεισμοί όπου μπορεί το δίκτυο να μην λειτουργεί από αυτές τις καταστροφές. Ένα ad hoc δίκτυο μπορεί να δημιουργηθεί μέσω D2D για αυτή την περίπτωση. Άλλη μια εφαρμογή είναι το IoT. Θα βελτιωθούν κάποια δίκτυα IoT για παράδειγμα στο δίκτυο των οχημάτων (V2V) όταν ένα όχημα τρέχει με υψηλή ταχύτητα και θέλει να αλλάξει λωρίδα η επιβραδύνει θα επικοινωνεί και θα ενημερώνει τα άλλα οχήματα. Παρ' όλα αυτά πολλές συσκευές μπορεί να μην συμμετέχουν για D2D επικοινωνίες είτε γιατί δεν θα το θέλουν είτε γιατί δεν θα έχουν την δυνατότητα δηλαδή περιορισμοί πόρων όμως χαμηλή μπαταρία ή είναι υψηλό το κόστος εύρους ζώνης από φορείς δικτύων κινητής. Ένα άλλο θέμα για τα D2D είναι και η ασφάλεια. Οποιοδήποτε κόμβος ή κόμβοι του δικτύου μπορεί να επιτεθούν για να χαλάσουν την ομαλή μετάδοση δεδομένων. Για παράδειγμα, κάποιοι κόμβοι μπορεί να στείλουν μηνύματα με λανθασμένες μετρήσεις όσων αφορά το δίκτυο των οχημάτων. Αυτό μπορεί να έχει ως συνέπεια τρακαρίσματα, με αποτέλεσμα να κινδυνεύουν ζωές.

3.3 Επικοινωνίες Machine to Machine (M2M)

Στο 5G θα υποστηρίζεται και η επικοινωνία μηχανής με μηχανή (M2M). Η διαφορά με το D2D είναι ότι στο M2M μπλέκονται πολλές συσκευές διαφόρων τύπων. Τα χαρακτηριστικά των επικοινωνιών M2M περιλαμβάνουν αυτοματοποιημένα δεδομένα, παραγωγή, επεξεργασία, μεταφορά και ανταλλαγή μεταξύ ευφών μηχανών με ελάχιστη ανθρώπινη παρέμβαση. Οι συσκευές μπορεί να είναι αισθητήρες να κάνουν μετρήσεις και να καλύπτουν μια περιοχή για μια ή πολλές υπηρεσίες. Οι μετρήσεις που μπορούν να κάνουν μπορεί να είναι για παράδειγμα μετρήσεις θερμοκρασίας ή υγρασίας να στέλνονται στον σταθμό βάσης της κυψέλης και με βάση αυτές να λαμβάνεται μια απόφαση. Οι συσκευές είναι μικρές έχουν μικρά δεδομένα και κάνουν σποραδικές μεταδόσεις. Υπάρχει υψηλή αξιοπιστία, χαμηλή καθυστέρηση, και λειτουργία σε πραγματικό χρόνο. Υπάρχουν πολλές εφαρμογές. Κάποιες από αυτές είναι η βελτίωση της παραγωγής και της αποδοτικότητας σε διάφορους τομείς, όπως στη δημιουργία μηχανήματων που λειτουργούν για την κατασκευή αμαξιών και στην επικοινωνία με τους προγραμματιστές προϊόντων όταν χρειάζεται να γίνει συντήρηση σε αυτά και για ποιο λόγο. Άλλη εφαρμογή είναι η παρακολούθηση συστημάτων σε μια εταιρία παίρνοντας κάποιες μετρήσεις από έξυπνες συσκευές μέτρησης για να καταπολεμηθεί η απάτη. Άλλη μια είναι για οικιακές συσκευές. Ένα πλυντήριο με δυνατότητα M2M θα μπορούσε να στείλει ειδοποιήσεις στις έξυπνες συσκευές των κάτοχων μόλις τελειώσει το πλύσιμο ή το στέγνωμα και ένα ψυγείο θα μπορούσε να παραγγείλει αυτόματα είδη παντοπωλείου από διάφορα μαγαζιά που έχει επιλέξει ο ιδιοκτήτης μόλις εξαντληθεί το απόθεμα του. Επιπλέον εφαρμόζεται σε νοσοκομεία για την διαχείριση της υγείας και την αυτοματοποίηση των διαδικασιών για υψηλότερα επίπεδα θεραπείας. Χρησιμοποιείται και για τηλεματική δηλαδή επιτρέπει σε ιδιωτικά και εμπορικά οχήματα για την αναφορά θέσης. Αυτό βοηθάει πάρα πολύ και για τα κούριερ να μπορεί κάποιος να ξέρει την θέση του οχήματος η όταν κάποιος περιμένει ένα ταξί. Και άλλη μια τελευταία μετρητές που δείχνουν την κατανάλωση καυσίμου κάθε λίγα δευτερόλεπτα. Γενικά, είναι πάρα πολλές

οι εφαρμογές, κάποιες από τις οποίες μοιάζουν και με αυτές των IoT. Παρ' όλα αυτά όπως και στο D2D έτσι και στο M2M η ασφάλεια είναι ένα θέμα καθώς κάποιος επιτήδειος μπορεί να προκαλέσει σοβαρά προβλήματα είτε σοβαρά ή μη ανάλογα την υπηρεσία.

3.4 Θετικά 5G

Ένα μεγάλο πλεονέκτημα του 5G είναι ότι θα έχει πιο μεγάλη και πιο εύκολη διαθεσιμότητα σε σχέση με αυτή της τεχνολογίας Fiber To The Home (FTTH). Σε πολλές απομακρυσμένες κυρίως περιοχές διαφόρων χωρών το FTTH δεν είναι διαθέσιμο. Σαν προσωρινή λύση μεγάλων ταχυτήτων ώστε να καλυφθούν οι ανάγκες μπορεί να χρησιμοποιηθεί το 5G εάν είναι αυτό διαθέσιμο. Με το 5G θα μπορεί ένας χρήστης να έχει πρόσβαση οπουδήποτε υπάρχει κάλυψη 5G ενώ το FTTH θα είναι διαθέσιμο σε ένα σταθερό μέρος. Αρά μια ακόμα εφαρμογή του 5G είναι για σύνδεση στο διαδίκτυο σε σταθερούς υπολογιστές laptop tablet κτλπ. Αυτό μπορεί να γίνει μέσω ενός κινητού τηλεφώνου που υποστηρίζει 5G. Ο χρήστης μπορεί να φτιάξει ένα Hotspot που είναι εικονικό Wi-Fi ή σύνδεση με usb σε έναν υπολογιστή και μέσω αυτών των 2 τρόπων να υπάρξει πρόσβαση στο διαδίκτυο. Πέρα από αυτά ένας τρίτος τρόπος είναι με την χρήση ρούτερ και μια κεραία για 5G. Υπάρχουν ρούτερ που έχουν σχεδιαστεί παίρνοντας μια κάρτα sim να προσφέρουν σύνδεση στο διαδίκτυο μέσω κεραίας που έχει τοποθετηθεί στην ταράτσα η μπαλκόνι ενός κτηρίου που πιάνει σήμα 4G και 5G. Η κεραία δίνει ιντερνέτ στο ρούτερ και με την σειρά του αυτό στους χρήστες μέσω Wi-Fi η σύνδεση Ethernet. Αυτό έχει σαν πλεονέκτημα ότι η κεραία είναι πολύ πιο δυνατή από αυτή ενός κινητού και ο λόγος του ότι είναι σε καλύτερη τοποθεσία έχει ως αποτέλεσμα την λήψη καλύτερου σήματος αρά και πολύ καλύτερες ταχύτητες και ποιότητα σύνδεσης.

Ένα άλλο θετικό χαρακτηριστικό του 5G είναι ότι έχει φτιαχτεί για χαμηλή κατανάλωση ενέργειας. Από αυτό οφείλονται και οι χρήστες του, καθώς η μπαταρία για IoT και στις συσκευές τους είναι κάτι πάρα πολύ σημαντικό για αυτούς και για όλους. Οι εταιρίες που παρασκευάζουν π.χ. κινητά τηλέφωνα, κοιτάνε πάρα πολύ την μπαταρία, δηλαδή προσπαθούν να προσφέρουν μεγαλύτερες μπαταρίες και τα κινητά να καταναλώνουν λιγότερη μπαταρία. Χρησιμοποιούνται σταθμούς βάσης χαμηλής κατανάλωσης σε σχέση με το 4G. Λόγω του 5G θα αναπτυχθούν πολλές εφαρμογές για IoT και θα χρησιμοποιηθούν περισσότερο τα δίκτυα αισθητήρων. Στα δίκτυα αισθητήρων, η μπαταρία είναι από τα πιο σημαντικά πράγματα καθώς οι αισθητήρες έχουν τόσο χρόνο ζωής όσο και η μπαταρία τους. Δεν συμφέρει η αλλαγή μπαταρίας στον αισθητήρα στην περίπτωση που εφαρμογή και το δίκτυο αποτελούνται από πολλούς αισθητήρες γιατί απαιτείται χρόνο και κόστος για να γίνει. Στο 4G οι σταθμοί βάσης καταναλώνουν 60% με 70 % της συνολικής ενέργειας του δικτύου κινητής τηλεφωνίας και τα κινητά τηλέφωνα το 10% της συνολικής ενέργειας. Αυτό ισχύει γιατί τα κινητά για να παίξουν π.χ. ένα βίντεο καταναλώνετε ενέργεια από την φωτεινότητα της οθόνης, τον επεξεργαστή, τον ήχο, τον αποκωδικοποιητή βίντεο και την διασύνδεση δικτύου. Το 5G επιτυγχάνει χαμηλή κατανάλωση σε περιοχές όπου υπάρχουν πολλοί χρήστες χρησιμοποιώντας κόμβους μικρής κατανάλωσης και κόστους. Χρησιμοποιούνται μικρά κελιά και relays που σημαίνει ότι η κεραία λήψης και εκπομπής θα είναι κοντά με τους χρήστες. Έτσι οι χρήστες για

κάνουν μια λήψη ή εκπομπή λόγω του μικρής απόστασης της κεραίας από αυτούς θα αυτούς μικρότερη ενέργεια από το κινητό κυρίως για την αποστολή. Πέρα από αυτό έχουμε μεγαλύτερη ταχύτητα γιατί μπορούν να χρησιμοποιούν μεγάλες συχνότητες λόγω της μικρής απόστασης και μεγαλύτερη αξιοπιστία της σύνδεσης λόγω των ελάχιστων ή μηδενικών απωλειών σε σχέση με μια κεραία που θα βρισκόταν πολύ πιο μακριά και θα χρησιμοποιούσε μικρότερη συχνότητα. Λόγω της ανάγκης για κατανάλωση λιγότερης ενέργειας, έχουν αναπτυχθεί διάφορα έργα όπως Energy Aware Radio, Network technology, Green Touch, Green 5G Mobile Networks που έχουν βοηθήσει στην χαμηλότερη κατανάλωσης ενέργειας και κατά επέκταση έχουν προσφέρει καλύτερη ποιότητα εμπειρίας για τον χρήστη (QoE).

3.5 Περί συχνοτήτων 5G

Το 5G πετυχαίνει αυτές τις ταχύτητες χρησιμοποιώντας μεγαλύτερες συχνότητες από ότι το 4G. Για τις μεγάλες συχνότητες οι απώλειες είναι και μεγαλύτερες για αυτό τα κελιά που θα έχουν αυτές τις συχνότητες θα είναι και μικρότερα. Αυτό μπορούμε και να το δούμε και στο WiFi. Τα ρουτερς μπορούν να υποστηρίξουν 2,4Ghz και 5Ghz συχνότητες για το WiFi. Όταν χρησιμοποιείται τα 5Ghz που είναι μεγαλύτερη συχνότητα από αυτή των 2,4 ισχύει ότι για να έχουμε καλό σήμα και μεγαλύτερες ταχύτητες από ότι τα 2,4Ghz θα πρέπει να είμαστε πιο κοντά στο ρουτερ. Εάν υπάρχουν τοίχοι σιγουρά θα χρειαστεί ένα Repeater το οποίο θα τρέχει και αυτό στα 5Ghz. Το 5G θα λειτουργεί σε 3 ζώνες συχνοτήτων, χαμηλή, μεσαία και υψηλή. Κάθε κελί θα κάνει χρήση μια από αυτές τις 3 ζώνες ανάλογα με τις απαιτήσεις. Κάθε κελί που έχει την δικιά του ζώνη θα απαιτεί και συγκεκριμένα σχέδια κεραίας. Το κάθε κελί παρέχει διαφορετική αντιστάθμιση της ταχύτητας λήψης έναντι της απόστασης και της περιοχής εξυπηρέτησης. Για την χαμηλή ζώνη χρησιμοποιείται 600-850 MHz παρόμοιο εύρος με αυτό του 4G δίνοντας λίγο μεγαλύτερες ταχύτητες 30-250Mbps. Οι κεραίες της χαμηλής ζώνης καλύπτουν σχεδόν τα ίδια με τις κεραίες του 4G. Η μεσαία ζώνη 5G χρησιμοποιεί μικροκύματα 2,5–3,7 GHz, επιτρέποντας ταχύτητες 100–900 Mbps. Κάθε κεραία με αυτές τις συχνότητες καλύπτει αρκετά χιλιόμετρα. Αυτή η ζώνη είναι η πιο διαδεδομένη και χρησιμοποιείται στις πόλεις όπου υπάρχει αρκετός κόσμος. Η υψηλή ζώνη 5G χρησιμοποιεί συχνότητες 25–39 GHz και επιτυγχάνει ταχύτητες πάνω από 1Gbps. Μπορούν στο μέλλον να χρησιμοποιούν και μεγαλύτερες συχνότητες. Γενικά η υψηλή ζώνη έχει κάποια προβλήματα. Λόγω μεγάλης συχνότητας θα πρέπει να εφαρμοστούν πολλά μικρά κελιά αρά και πολλές κεραίες. Αυτό γίνεται γιατί έχουμε μεγάλες απώλειες όταν υπάρχουν εμπόδια. Αυτή η ζώνη προς το παρόν χρησιμοποιείται σε περιοχές όπου υπάρχουν πάρα πολλοί άνθρωποι όπως είναι αστικά κέντρα γήπεδα και συγκεντρώσεις για συνέδρια.

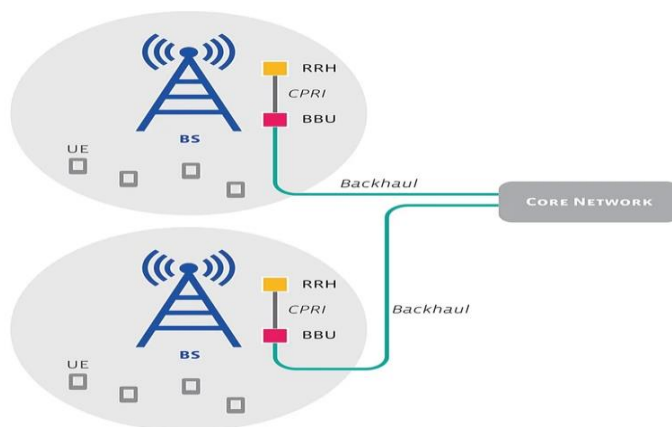
3.6 QoS και QoE στο 5G

Η ποιότητα εμπειρίας (QoE) στον τελικό χρήστη χρεώνεται ανάλογα με τις απαιτήσεις του χρήστη για εφαρμογές, δηλαδή ανάλογα ποσό ποιότητα θα επιλέξει για μια υπηρεσία. Κάθε QoE για κάθε χρήστη πρέπει να διαχειρίζονται σωστά και αυτόνομα. Παρόλα αυτά υπάρχει και η ποιότητα υπηρεσίας QoS. Ένα παράδειγμα QoE είναι premium συνδρομή IPTV. Ο χρήστης θα περιμένει καλύτερη ποιότητα υπηρεσίας. QoS σημαίνει ότι

ο χρήστης πληρώνει για να έχει προτεραιότητα και παραπάνω δικαιώματα για μια εφαρμογή. Παρόλα αυτά όταν ένας χρήστης πληρώσει για ποιότητα υπηρεσίας δεν σημαίνει ότι θα έχει και ποιότητα εμπειρίας. Για να μπορεί να προσφερθεί ποιότητα εμπειρίας στον τελικό χρήστη θα πρέπει να υπάρχει σταθερότητα στο 5G δίκτυο. Η σταθερότητα επηρεάζεται από τις διακυμάνσεις στην ποιότητα, απόδοση του δικτύου, τις διαταραχές και τις παρεμβολές. Αυτά πρέπει να είναι στο ελάχιστο επίπεδο. Έτσι το ότι ένας χρήστης πληρώνει για ποιότητα υπηρεσίας δεν σημαίνει ότι θα έχει 100% ποιότητα εμπειρίας καθώς αμα για παράδειγμα υπάρχουν παρεμβολές η πέσει μια κεραία μιας κυψέλης η γίνει κάποια επίθεση όπως άρνηση υπηρεσίας (DDOS) η κλαπούν δεδομένα θα χαθεί η ασφάλεια και δεν θα έχει κανείς υπηρεσία και αυτός που πληρώνει για QoS και αυτός που δεν πληρώνει. Οπότε για όλους θα μειώνεται η καλή εμπειρία χρήστη. Το 5G προσφέρει υψηλό επίπεδο διαφάνειας για την παροχή υπηρεσιών με υψηλό QoE κρύβοντας την πολυπλοκότητα του 5G. Κάθε υπηρεσία έχει τους δικούς της βασικούς δείκτες απόδοσης (Key Performance Indicator KPI). Τα KPI περιλαμβάνουν τα χαρακτηριστικά του 5G που αναφέραμε πιο πάνω. Δηλαδή μεγάλη κάλυψη και συνδεσιμότητα, μεγάλες ταχύτητες, χαμηλή απόκριση 1ms, εξοικονόμηση ενέργειας 90%, αξιοπιστία και διαθεσιμότητα υπηρεσιών 99,9%. Για παράδειγμα το live streaming χρειάζεται μεγάλες ταχύτητες για upload, μικρή απόκριση 1ms και εξοικονόμηση ενέργειας για να είναι όσο περισσότερο live στους χρήστες. Αντίθετα οι χρήστες που βλέπουν το live θέλουν μεγάλη ταχύτητα στο downloading και εξοικονόμηση ενέργειας. Οι απαιτήσεις της κάθε εφαρμογής που είδη ξέρουμε καλύπτονται με το 5G προσφέροντας στον χρήστη αυτά που θέλει και κατά επέκταση ωραία εμπειρία κάνοντάς το έτσι κατάλληλο σαν μια εναλλακτική λύση για FTTH.

3.7 Δίκτυο Ραδιοπρόσβασης (RAN)

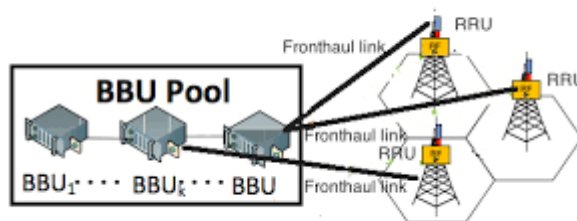
Το δίκτυο ραδιοπρόσβασης RAN είναι ένα μέρος των κινητών επικοινωνιών και συγκεκριμένα είναι οι κεραίες και το base station που χρησιμοποιούνται για να παρέχουν την απαραίτητη κάλυψη για κάθε περιοχή ανάλογα με τις εκάστοτε ανάγκες της. Το RAN είναι ένα δίκτυο πρόσβασης ραδιοφώνου που συνδέει μεμονωμένες συσκευές σε άλλα μέρη ενός δικτύου μέσω ραδιοφωνικών συνδέσεων χρησιμοποιώντας τη Τεχνολογία ραδιοπρόσβασης (RAT). Το RAN συνδέεται με το core network μέσω του backhaul link. Είναι ένα σημαντικό μέρος των σύγχρονων τηλεπικοινωνιών, με συνδέσεις δικτύου 3G, 4G και 5G για κινητά τηλέφωνα να αποτελούν παραδείγματα δικτύων ραδιοπρόσβασης. Κάποια παραδείγματα είναι το UTRAN(UMTS Radio Access Network) και το GRAN(GSM Radio Access Network).



Εικόνα 1: Αρχιτεκτονική RAN

3.8 Δίκτυο Ραδιοπρόσβασης υλοποιημένο στο νέφος (C-RAN)

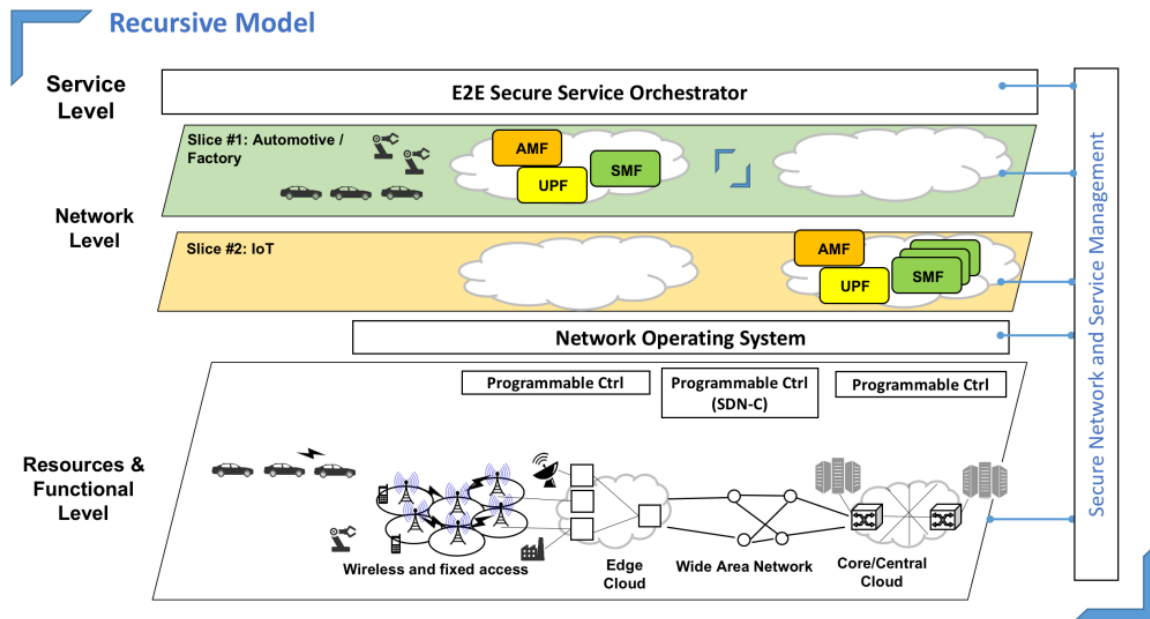
Το δίκτυο ραδιοπρόσβασης υλοποιημένο στο νέφος (C-RAN) είναι μια άλλη παραλλαγή της τεχνολογίας RAN. Υπάρχουν τρία κύρια συστατικά: Η μονάδα Βασικής Ζώνης BBU, δίκτυα απομακρυσμένης κεφαλή ραδιοεπικοινωνίας RRU και δίκτυο μεταφορών. Το pool BBU, που βρίσκεται σε κεντρικό σημείο, λειτουργεί παρόμοια με το cloud. Παρέχει στους RRU πόρους που χρειάζονται βάσει των αναγκών του δικτύου, όπως το cloud παρέχει στους υπολογιστές πόρους από απόσταση. Οι δίκτυο οιξαιρετικά αξιόπιστες και μικρής καθυστέρηση επικοινωνίες RRU συνδέει ασύρματες συσκευές στο Διαδίκτυο, όπως οι πύργοι RAN σε ένα παραδοσιακό δίκτυο ραδιοπρόσβασης RAN. Το δίκτυο μεταφορών χρησιμοποιεί οπτικές ίνες, ή ραδιοσυχνότητες κύματος χιλιοστών (mmWave) για να συνδέσει την μονάδα βασικής ζώνης BBU και την απομακρυσμένη κεφαλή ραδιοεπικοινωνίας RRUs με υψηλό εύρος ζώνης. Το C-RAN είναι αρκετά πιο φθηνό τόσο όσον αφορά το κόστος για εγκαταστάσεις όσο και το κόστος που αφορά τις λειτουργίες του. θεωρείται αρκετά αποδοτικό καθώς είναι σε θέση να συνδυάσει τις ασύρματες τεχνολογίες με τις τεχνολογίες που αφορούν τον τομέα IT (Information Technology) με το να εντάζει την τεχνολογία του cloud computing στο κλασικό RAN.



Εικόνα 2: Αρχιτεκτονική C-RAN

3.9 Αρχιτεκτονική 5G

Στο παρακάτω σχήμα βλέπουμε την αρχιτεκτονική 5G.



Εικόνα 3: Αρχιτεκτονική 5G

Στο επίπεδο **Resource & Functional Level** υπάρχουν οι φυσικοί πόροι που χρησιμεύουν για την επικοινωνία, τους υπολογισμούς και την αποθήκευση.

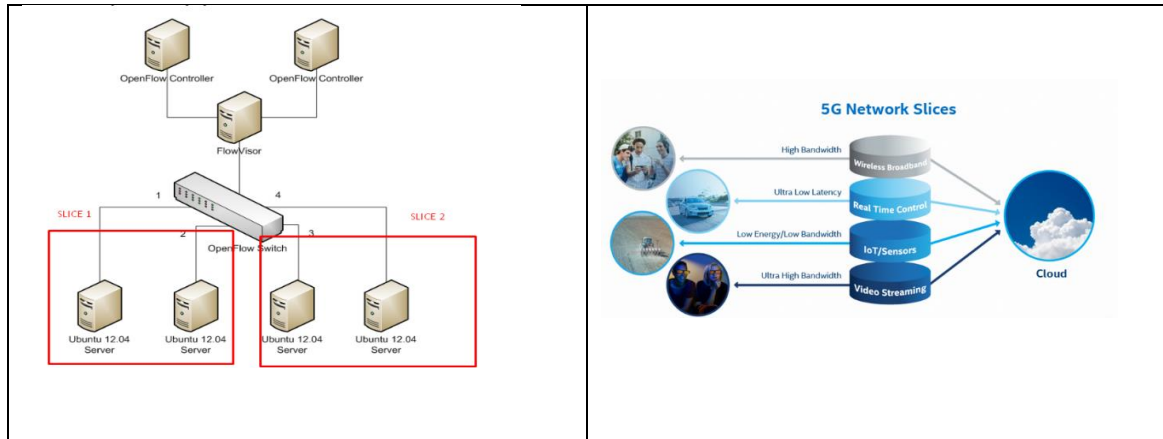
Το επίπεδο αυτό όπως βλέπουμε και στην εικόνα αποτελείται από το **Wireless and Fixed Access** το οποίο είναι υπεύθυνο για την πρόσβαση στο ιντερνέτ στα σπίτια και σε εταιρικούς πελάτες ασύρματα αντικαθιστώντας τις σταθερές γραμμές dsl κάνοντας ότι δεν μπορούσε το wimax. χρησιμοποιείται μήκη κύματος του χιλιοστού (mmWave) και έτσι παρέχονται στους καταναλωτές το εύρος ζώνης που απαιτείται για την υποστήριξη υπηρεσιών ροής υψηλής ευκρίνειας και υψηλής ταχύτητας πρόσβασης στο Διαδίκτυο. Το επίπεδο Resource & Functional Level αποτελείται επίσης και από το **edge cloud**. Το edge cloud που συχνά αναφέρεται ως Mobile Edge Computing, MEC ή Multi-Access Edge Computing, παρέχει πόρους εκτέλεσης (υπολογισμός και αποθήκευση) για εφαρμογές με δικτύωση κοντά στους τελικούς χρήστες συνήθως εντός ή στο όριο του operator network προσφέροντας υπηρεσίες με πολύ χαμηλό latency και μεγάλο throughput. Το Edge Computing μπορεί επίσης να τοποθετηθεί σε χώρους επιχειρήσεων. Ένα άλλο στοιχείο του Resource & Functional Level είναι το **Wide Area Network**. Είναι ένα σύνολο υπολογιστών που εκτείνονται σε μία ευρεία γεωγραφική περιοχή και δημιουργούν μεταξύ τους ένα δίκτυο επικοινωνίας. Τυπικά ένα WAN διασυνδέει μεταξύ τους τοπικά δίκτυα υπολογιστών. Για τη διασύνδεση αυτή χρησιμοποιούνται σχεδόν πάντα μισθωμένες δημόσιες τηλεπικοινωνιακές γραμμές ή μερικές φορές και δορυφορικές τηλεπικοινωνίες. Το γνωστότερο WAN είναι το Internet.

Το δεύτερο επίπεδο της αρχιτεκτονικής είναι το **Network level**. Εκεί γίνεται η εικονικοποίηση του φυσικού δικτύου και των πόρων δημιουργώντας εικονικά δίκτυα (slice) τα οποία είναι απομονωμένα και το καθένα εξυπηρετεί μια υπηρεσία. Κάθε slice χρησιμοποιεί διαφορετικούς πόρους (υπολογιστικούς, δικτυακούς κτλ.) για να παρέχει υπηρεσίες στους πελάτες. Η εικονικοποίηση γίνεται με το Network Operating System που είναι ένα λειτουργικό σύστημα που έχει σχεδιαστεί αποκλειστικά και μόνο για την υποστήριξη workstations, sharing βάσεων δεδομένων, sharing εφαρμογών μεταξύ διαφορετικών υπολογιστών στο δίκτυο.

Τέλος το επίπεδο **service level** είναι το επίπεδο όπου γίνεται η υποστήριξη των υπηρεσιών ταυτόχρονα με δυναμικό τρόπο. Στο service level, τα υποστηρίζονται διάφορες λειτουργίες των slices όπως δημιουργία διαγραφή και τροποποίηση.

4. Τεμαχισμός και εικονικοποίηση στα δίκτυα

Ο τεμαχισμός δικτύου επικαλύπτει πολλά εικονικά δίκτυα πάνω από ένα κοινόχρηστο δίκτυο. Κάθε τμήμα του δικτύου ελέγχει την δική του προώθηση πακέτων και μπορεί να έχει τη δική του λογική τοπολογία, κανόνες ασφαλείας και χαρακτηριστικά απόδοσης(ευρέως ζώνης, καθυστέρηση και επεξεργασία) - εντός των ορίων που επιβάλλουν τα υποκείμενα φυσικά δίκτυα. Υπάρχει ισχυρή απομόνωση μεταξύ των τμημάτων και οι ενέργειες σε ένα κομμάτι δεν υφαρπάζουν τα άλλα κομμάτια. Το SDN διαχωρίζει το επίπεδο ελέγχου του δικτύου από το επίπεδο δεδομένων χειρισμού πακέτων. Επιτρέπει στο επίπεδο ελέγχου να ορίζει εικονικά δίκτυα καθορίζοντας κανόνες χειρισμού πακέτων και ωθώντας αυτούς τους κανόνες στις συσκευές επιπέδου δεδομένων για εκτέλεση. Ο τεμαχισμός δικτύου μπορεί να χρησιμοποιεί για δοκιμές και ερευνά από ερευνητές όπως γίνεται και στις εικονικές μηχανές (virtual machines) όπου μπορείς να τρέξεις για παράδειγμα ένα πρόγραμμα να δεις συμπεριφορά ή έναν ιό χωρίς όλα αυτά να έχουν επίπτωση στο κύριο λειτουργικό σύστημα ή σε άλλες εικονικές μηχανές. Έτσι μπορεί να γίνει και στα δίκτυα για παράδειγμα κάποιος που κάνει ερευνά μπορεί να φτιάξει διάφορες εικονικές αρχιτεκτονικές δικτύου να τρέξει μια εφαρμογή και να μετρήσει την καθυστέρηση των κόμβων και άλλες μετρήσεις απόδοσης χωρίς να επηρεαστούν οι άλλες υπηρεσίες. Ο τεμαχισμός δικτύων επιτρέπει στον χειριστή του δικτύου να μεγιστοποιήσει τη χρήση των πόρων του δικτύου και την ευελιξία των υπηρεσιών. Εμείς θα ασχοληθούμε με τον τεμαχισμό δικτύου στα data centers με την τεχνολογία SDN και flowvisor και 5G με την τεχνολογία SDN και NFV.



Εικόνα 4: Τεμαχισμός Data Center & 5G

4.1 Τεμαχισμός Data Center

Οι εφαρμογές παλιά φιλοξενούνταν σε κλασσικά κέντρα δεδομένων δηλαδή σε κέντρα δεδομένων που δεν υποστηρίζονταν η εικονικοποίηση δικτύου. Υποστηρίζονταν εξειδικευμένη τοπολογία δικτύου και μηχανισμό δρομολόγησης για καλύτερη απόδοση και μειωμένα έξοδα υποδομής. Αυτά τα κέντρα δεδομένων προσφέρουν εγγυημένη επεξεργαστική συχνή (cpu), μνήμη και αποθηκευτικό χώρο σε πελάτες αλλά όχι εγγύηση εύρους ζώνης. Αυτό έχει ως αποτέλεσμα η εφαρμογές των ενοικιαστών που υποστηρίζονται από το κέντρο δεδομένων να υποφέρουν από έλλειψη εύρους ζώνης και κα επέκταση να μην λειτουργούν αποδοτικά. Η κατανομή εγγυήσεων εύρους ζώνης σε εφαρμογές στο cloud έχει γίνει περισσότερο απαιτητικό και απαραίτητο, καθώς οι εφαρμογές ανταγωνίζονται για την κοινή χρήση πόρων του δικτύου. Πλέον στα κέντρα δεδομένων υποστηρίζεται η εικονικοποίηση. Το φυσικό δίκτυο σπάει σε αλλα μικρότερα απομονωμένα εικονικά δίκτυα τα οποία φιλοξενούν το καθένα μια εφαρμογή. Έτσι κάθε ενοικιαστής μπορεί να φτιάξει το δικτύου του έτσι όπως θέλει για να είναι κατάλληλο για την εφαρμογή του και επιπλέον με την εικονικοποίηση παρέχεται και εγγυώμενο εύρος ζώνης. Η εικονικοποίηση στα κέντρα δεδομένων γίνεται με την τεχνολογία Software defined networking (SDN) και με το πρωτόκολλο flowvisor. Για να ενεργοποιηθεί η εγγύηση εύρους ζώνης στο cloud και στις εφαρμογές υπάρχουν κάποια θέματα - έννοιες στο cloud που προκύπτουν από την εικονικοποίηση που πρέπει να καλύπτονται όπως είναι η σωστή εικονικοποίηση, η ασφάλεια, ποιότητα υπηρεσίας QoS(Quality Of Service), ποιότητα εμπειρίας του χρήστη QoE, λειτουργικότητα με γνώμονα την εφαρμογή(Application-aware Functionality), και αυτο-καθορισμένη τοπολογία. Όταν όλες αυτές οι απαιτήσεις καλυφτούν τότε η εγγύηση εύρους ζώνης επιτυγχάνεται με το μοντέλο GANA[18] το οποίο υποστηρίζει δίκτυα με γνώμονα την εφαρμογή και γίνεται χαρτογράφηση του εικονικού δικτύου με το φυσικό.

Στην αυτο-καθορισμένη τοπολογία οι ενοικιαστές θα πρέπει να μπορούν να δημιουργούν τοπολογίες δικτύου όπου σε αυτές να μπορούν να αναπτυχθούν οι απαραίτητες εφαρμογές. Οι εικονικοί διακόπτες (switches) παραμένουν διασυνδεδεμένοι με παρόμοιο τρόπο όπως γίνεται και με τους φυσικούς.

4.1.1 Δικτύωση με Γνώμονα την Εφαρμογή

Καθώς περισσότερες εφαρμογές μεταβαίνουν στο cloud και με την καλύτερη δυνατή προσπάθεια (best effort) το QoS δεν είναι πλέον ικανοποιητική προσέγγιση, είναι απαραίτητη μια νέα γενιά έξυπνων δικτύων. Η δικτύωση με γνώμονα την εφαρμογή (Application-aware networking) είναι η κατάλληλη τεχνολογία για αυτό το πρόβλημα. Η δικτύωση με γνώμονα την εφαρμογή είναι η ικανότητα ενός έξυπνου δικτύου να διατηρεί τρέχουσες πληροφορίες σχετικά με εφαρμογές που συνδέονται σε αυτό και, ως εκ τούτου, βελτιστοποιεί τη λειτουργία τους, καθώς και άλλων εφαρμογών ή συστημάτων που ελέγχουν. Οι πληροφορίες που διατηρούνται περιλαμβάνουν απαιτήσεις κατάστασης εφαρμογής και πόρων. Η ικανότητα να επωφεληθούμε από την δικτύωση με γνώμονα την εφαρμογή βασίζεται σε δικτύωση που καθορίζεται από λογισμικό (SDN). Το SDN αφαιρεί το επίπεδο ελέγχου από το υλικό του δικτύου και το εφαρμόζει σε λογισμικό αντ' αυτού, το οποίο επιτρέπει δυναμικό έλεγχο και τη δυνατότητα κατανομής πόρων, ανά πάσα στιγμή, με τον καλύτερο δυνατό τρόπο, καθιστώντας τη δικτύωση με γνώμονα την εφαρμογή που βασίζεται σε VDC να είναι σημαντική και ελκυστική προσέγγιση στο κέντρο δεδομένων cloud.

4.1.2 Ποιότητα Υπηρεσίας

Η ποιότητα υπηρεσίας στο cloud είναι από τα πιο σημαντικά πράγματα. Οι εφαρμογές των ενοικιαστών που φιλοξενούνται στο cloud με την χρήση εικονικοποίησης κτλπ. χρησιμοποιούν κοινούς πόρους από το φυσικό δίκτυο. Δηλαδή ένα cluster μπορεί να επιτρέψει εργασίες από διάφορους ενοικιαστές να συνυπάρχουν. Προκύπτει και ένα θέμα της ασφάλειας που θα συζητήσουμε πιο κάτω αλλά και ένα θέμα αυτό της απόδοσης της κάθε εφαρμογής. Όταν μια εφαρμογή θέλει πόρους για παράδειγμα εύρος ζώνης για να γίνει η δουλειά μπορεί να μην υπάρχουν διαθέσιμοι πόροι τουλάχιστον όσοι χρειάζονται γιατί θα χρησιμοποιούνται από κάποια άλλη εφαρμογή. Με την ποιότητα εφαρμογής αυτό λύνεται εφόσον πληρώσει ένας ενοικιαστής για να έχει ποιότητα υπηρεσίας όταν θα χρειαστεί πόρους πχ εύρος ζώνης από το φυσικό δίκτυο θα τους έχει σε σχέση με τις άλλες εφαρμογές που δεν έχουν ποιότητα υπηρεσίας οι οποίες θα βολεύονται με τους διαθέσιμους υπολοίπους πόρους. Επίσης με το QoS ο ενοικιαστής θα έχει και τον έλεγχο της ροής του εικονικού του δικτύου.

4.1.3 Ποιότητα Εμπειρίας

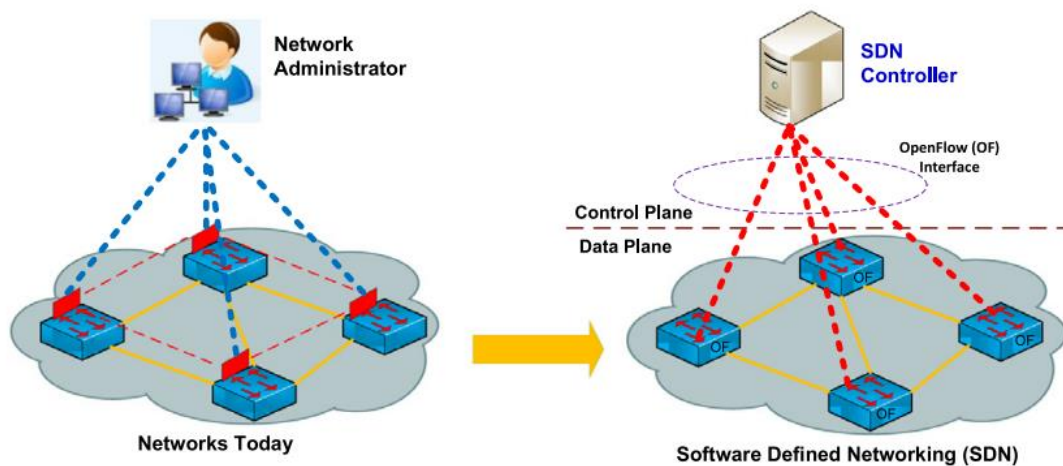
Όταν ένας ενοικιαστής ή χρήστης πληρώσει για ποιότητα υπηρεσίας δεν σημαίνει ότι θα έχει και ποιότητα εμπειρίας. Για να μπορεί να προσφερθεί ποιότητα εμπειρίας στον τελικό χρήστη θα πρέπει να υπάρχει σταθερότητα στο κέντρο δεδομένων. Η σταθερότητα επηρεάζεται από τις διακυμάνσεις στην ποιότητα, απόδοση του δικτύου, τις διαταραχές και τις κακόβουλες επίθεσης. Αυτά πρέπει να είναι στο ελάχιστο επίπεδο. Έτσι το ότι ένας χρήστης πληρώνει για ποιότητα υπηρεσίας δεν σημαίνει ότι θα έχει 100% ποιότητα εμπειρίας καθώς αμα για παράδειγμα πέσει ένας κόμβος στο κέντρο δεδομένων η γίνει κάποια επίθεση όπως άρνηση υπηρεσίας (DDOS) η κλαπούν δεδομένα θα χαθεί η ασφάλεια και δεν θα έχει κανείς υπηρεσία και αυτός που πληρώνει για QoS και αυτός που δεν πληρώνει. Οπότε για όλους θα μειώνεται η καλή εμπειρία χρήστη.

4.1.4 Ασφάλεια

[18]Όπως σε όλα τα θέματα της πληροφορικής ένα θέμα είναι η ασφάλεια έτσι και στην εικονικοποίηση στο cloud. Υπάρχουν αρκετές απειλές που μπορούν να επηρεάσουν η να παραποιήσουν την κατανομή του εύρους ζώνης σε κάθε εφαρμογή. Για την επίθεση άρνηση υπηρεσίας έχουμε μιλήσει στην εισαγωγή στο cloud όμως υπάρχει και μια άλλη επίθεση που ονομάζεται Black-Hole (B-H) όπου ένας κόμβος που παίρνει δεδομένα πέφτει η μπλοκάρει αυτά τα δεδομένα αντί να τα στείλει στον επόμενο κόμβο λήψης. Για να αντιμετωπιστεί αυτή η απειλή έχει προταθεί ένα σύστημα που αξιολογεί την εγκυρότητα ενός κόμβου με βάση την ιδιοτέλεια του. Για να ανιχνευτούν οι B-H cluster heads πρέπει να γίνει επανασύνδεση (re-clustering) για να διασφαλιστεί ότι είναι σε χρήση μόνο νόμιμοι cluster heads. Η διαδικασία επανασύνδεσης βασίζεται καθαρά σε ένα σκορ εμπιστοσύνης το οποίο είναι ο καλύτερος τρόπος διάκρισης μεταξύ κανονικών και κακόβουλων συσκευών.

4.1.5 Δίκτυο που Καθορίζεται από το Λογισμικό (SDN)

Η Δικτυώση που καθορίζεται από λογισμικό (SDN) είναι μια προσέγγιση που φέρνει νοημοσύνη ευελιξία και προγραμματισμό στα δίκτυα 5G ικανά να ενορχηστρώνουν και να ελέγχουν εφαρμογές υπηρεσίες με πιο λεπτομερή τρόπο και σε ολόκληρο το δίκτυο. Πέρα από το 5G χρησιμοποιείται και στο cloud computing, όπου διευκολύνει τη διαχείριση του δικτύου και επιτρέπει τον προγραμματισμό των ρυθμίσεων του δικτύου έτσι ώστε να έχουμε βελτιωμένη ταχύτητα και καλύτερη παρακολούθηση. Χρησιμοποιείται σε μεγάλα δίκτυα και κέντρα δεδομένων με πολλές και πολύπλοκες συσκευές όπως ρουτερς, διακόπτες κτλ όπου η διαχείριση από τους διαχειριστές δικτύου είναι δύσκολη. Είναι η γέφυρα για το network virtualization που επιδιώκει να αξιοποιήσει με τον καλύτερο δυνατό τρόπο τους δικτυακούς πόρους και να προσαρμόσει τα δίκτυα στις όλο και αυξανόμενες ανάγκες των επιχειρήσεων. Το Open Network Foundation (ONF) ορίζει τη δικτυώση που καθορίζεται από λογισμικό SDN ως τον φυσικό διαχωρισμό του επιπέδου ελέγχου δικτύου από το επίπεδο προώθησης και όπου ένα επίπεδο ελέγχου ελέγχει διάφορες συσκευές δημιουργώντας έτσι μια software-programmable υποδομή. Αυτός ο διαχωρισμός οδηγεί σε ευελιξία, συγκεντρωτικό έλεγχο και προσφέρει πλήρη εικόνα ολόκληρου του δικτύου. Το control plane είναι υπεύθυνο για την προώθηση των πακέτων του δικτύου ενώ το data plane είναι υπεύθυνο για την διαδικασία routing. Το SDN παρέχει επίσης δυνατότητες ταχείας ανταπόκρισης σε μεταβαλλόμενες συνθήκες δικτύου. Όπως φαίνεται στο παρακάτω σχήμα, η δικτυώση που καθορίζεται από λογισμικό SDN δημιουργεί ένα εικονικό επίπεδο ελέγχου που μπορεί να επιβάλει έξυπνες αποφάσεις διαχείρισης μεταξύ λειτουργιών δικτύου γεφυρώνοντας το χάσμα μεταξύ παροχής υπηρεσιών και διαχείρισης δικτύου.

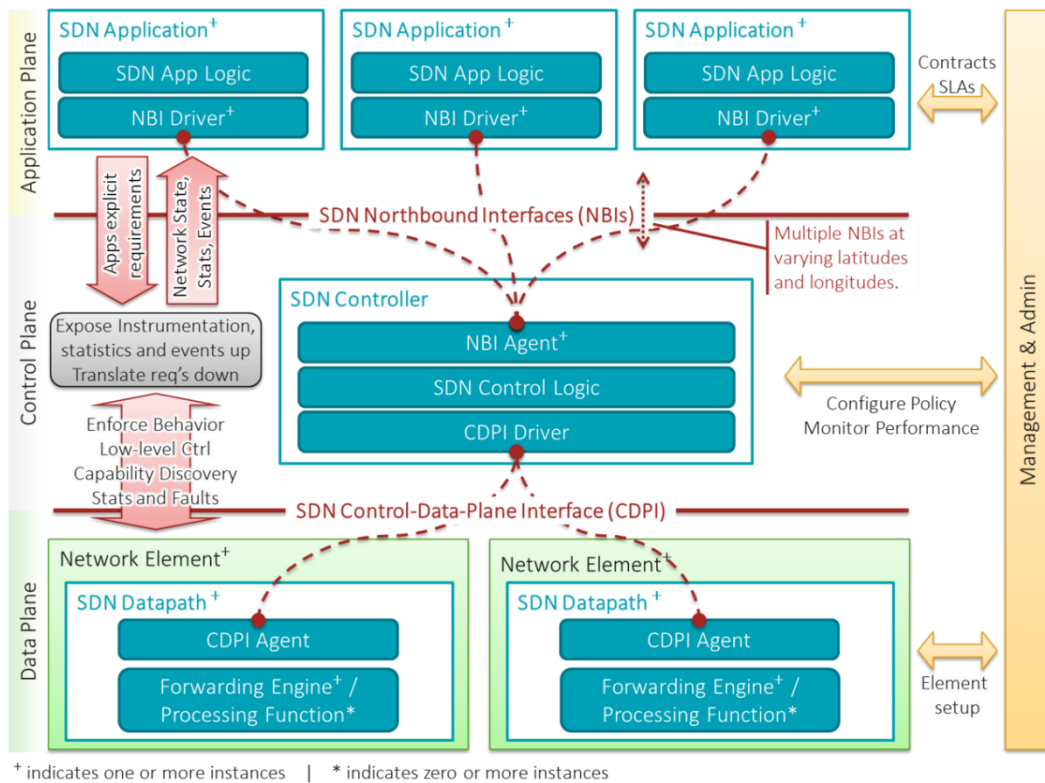


Εικόνα 5: Κλασσικά δίκτυα vs SDN

Με την δικτύωση που καθορίζεται από λογισμικό SDN, ο έλεγχος του δικτύου γίνεται άμεσα προγραμματιζόμενος χρησιμοποιώντας τυποποιημένες διεπαφές Southbound (SBI) όπως OpFlex, FoRCES και OpenFlow. Αυτά τα πρότυπα ορίζουν την επικοινωνία μεταξύ συσκευών προώθησης στο επίπεδο δεδομένων και των στοιχείων στο επίπεδο ελέγχου και διαχείρισης.

Το control plane αποτελείται από ένα ή περισσότερα controllers (ελεγκτές) που χαρακτηρίζονται ως ο “εγκέφαλος” του SDN δικτύου. Εκεί γίνονται όλες οι διαδικασίες τη διαχείρισης, ανάλυσης και αυτοματισμού του δικτύου. Τα SDN controllers παρέχουν API (Application Programming Interface) υψηλού επιπέδου στις εφαρμογές προκειμένου να γίνεται από αυτές η διαδικασία προώθησης πακέτων. Παράλληλα, οι ίδιοι οι ελεγκτές επικοινωνούν με τα στοιχεία του δικτύου μέσω API χαμηλού επιπέδου. Γι’ αυτό το σκοπό χρησιμοποιείται CLI (command line interface) ή πρωτόκολλα όπως το OpenFlow. Η δικτύωση που καθορίζεται από λογισμικό SDN χρησιμοποιείται όλο και περισσότερο προσφέρει μια πληθώρα πλεονεκτημάτων για τις επιχειρήσεις όπως διαθεσιμότητα του δικτύου εξαιτίας του μειωμένου χρόνου απόκρισης στα προβλήματα που αντιμετωπίζει το δίκτυο, μειωμένο κόστος διαχείρισης και συντήρησης λόγω της αυτοματοποιημένης φύσης του. Κάποια από τα θετικά της δικτύωσης που καθορίζεται από λογισμικό SDN είναι ότι έχει μειούμενο κόστος γιατί χρησιμοποιείται το λογισμικό για να γίνονται οι διεργασίες αντί να χρησιμοποιηθούν δικτυακές συσκευές. Η δικτύωση που καθορίζεται από λογισμικό SDN μπορεί να αξιοποιήσει κατάλληλα τα APIs ώστε εφαρμογές να μπορούν να τα εκμεταλλευτούν. Ο διαχωρισμός του control plane από το data plane και η χρήση ενός πρωτοκόλλου όπως το OpenFlow ανάμεσα τους, χαρίζει επιπλέον προσαρμοστικότητα.

Στην παρακάτω εικόνα βλέπουμε την αρχιτεκτονική SDN και τα στοιχεία που την συνθέτουν.



Εικόνα 6: Αρχιτεκτονική SDN

Το SDN Application είναι προγράμματα που επικοινωνούν κατευθείαν με το SDN controller μέσω προγραμματισμού και του μεταφέρουν τις απαιτήσεις καθώς και τη συμπεριφορά που θέλουν να έχει το δίκτυο προκειμένου να λειτουργήσουν σωστά μέσω του interface (NBI).

Ο SDN Controller είναι μια λογικά συγκεντρωτική οντότητα που είναι υπεύθυνη για τη μετάφραση-μεταφορά των απαιτήσεων από το επίπεδο SDN Application έως τα SDN Datapaths καθώς επίσης στέλνει την κατάσταση του δικτύου η οποία μπορεί να περιλαμβάνει στατιστικά και συμβάντα στο SDN application Ένας ελεγκτής SDN αποτελείται από ένα ή περισσότερα NBI, το SDN Control Logic και το πρόγραμμα οδήγησης Control to Data-Plane Interface (CDPI).

Ένα SDN Datapath περιλαμβάνει έναν driver CDPI και ένα σύνολο από έναν ή περισσότερους κινητήρες προώθησης κυκλοφορίας (πχ switches) που μετακινούν τα πακέτα δεδομένων μέσα στο δίκτυο. Αυτοί οι κινητήρες και οι λειτουργίες μπορεί να περιλαμβάνουν απλή προώθηση μεταξύ των εξωτερικών διασφών του Datapath ή των εσωτερικών λειτουργιών επεξεργασίας ή τερματισμού της κυκλοφορίας.

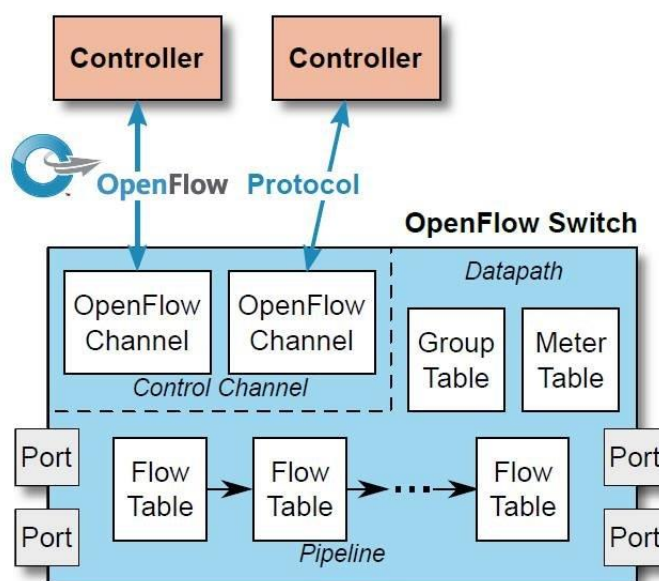
Το SDN CDPI είναι η διεπαφή που ορίζεται μεταξύ ενός SDN Controller και ενός SDN Datapath, το οποίο παρέχει προγραμματικό έλεγχο όλων των λειτουργιών προώθησης, διαφήμιση δυνατοτήτων, αναφορές στατιστικών στοιχείων και ειδοποίηση συμβάντων.

Τα SDN Northbound Interfaces (NBI) είναι διεπαφές μεταξύ του SDN Application

και SDN Controller και συνήθως παρέχουν αφηρημένες προβολές δικτύου και επιτρέπουν την άμεση έκφραση της συμπεριφοράς και των απαιτήσεων του δικτύου.

4.1.5.1 OpenFlow

Το OpenFlow είναι ένα open πρωτόκολλο επικοινωνίας που δημιουργήθηκε από το Open Networking Foundation (ONF). Παρέχει πρόσβαση στο επίπεδο προώθησης ενός διακόπτη δικτύου ή ενός δρομολογητή μέσω του δικτύου. Είναι το βασικό πρωτόκολλο που χρησιμοποιείται για την τεχνολογία SDN. Χρησιμοποιείται για την επικοινωνία των διακοπών ή των ρουτερς. Η επικοινωνία γίνεται με τα flow tables που είναι πίνακες ροής και έχουν πληροφορίες flow entries για το πως θα γίνεται η κίνηση των πακέτων. Όταν ένας ρουτερ πάρει ένα πακέτο για να το προωθήσει κοιτάει τον πίνακα ροής. Επίσης επιτρέπει στο SDN Controller την απομακρυσμένη διαχείριση των πινάκων ροής των διακοπών προσθέτοντας, τροποποιώντας και αφαιρώντας κανόνες και ενέργειες αντιστοίχισης πακέτων. Με αυτόν τον τρόπο, οι αποφάσεις δρομολόγησης μπορούν να λαμβάνονται περιοδικά από τον ελεγκτή και να μεταφράζονται σε κανόνες και ενέργειες με διαμορφώσιμη διάρκεια ζωής. Με αυτόν τον δυναμικό τρόπο ελέγχου και αποστολής των πακέτων γίνεται πολύ εύκολο στους διαχειριστές του δικτύου να έχουν μία πλήρη εικόνα για το τι γίνεται στο δίκτυο καθώς και να μπορούν ανά πάσα στιγμή να αλλάξουν τους κανόνες αναφορικά με το πως γίνεται η προώθηση (forwarding) της κίνησης.



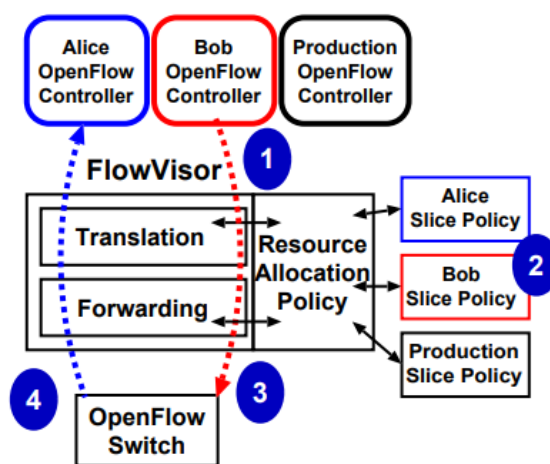
Εικόνα 7: Αρχιτεκτονική OpenFlow

Υπάρχουν 2 ειδών flow entries τα **Reactive** και τα **Proactive**. Τα Reactive είναι όταν τα πακέτα δεν ταιριάζουν με μια καταχώριση ροής αποστέλλονται στον ελεγκτή και στη συνέχεια, ο ελεγκτής δημιουργεί την απαιτούμενη καταχώριση ροής και επιστρέφει το πακέτο πίσω στον διακόπτη. Στα Proactive οι ελεγκτές προσθέτουν ροές στο διακόπτη πριν απαιτηθούν.

4.1.5.2 Flowvisor

Το FlowVisor είναι ένας πειραματικός ελεγκτής δικτύωσης (SDN) ο οποίος επιτρέπει την εικονικοποίηση του δικτύου διαιρώντας ένα φυσικό δίκτυο σε πολλά λογικά δίκτυα. Δημιουργήθηκε το 2009 από το openflow και διασφαλίζει ότι κάθε ελεγκτής αγγίζει μόνο τους διακόπτες και τους πόρους που του έχουν ανατεθεί. Διαχωρίζει επίσης το εύρος ζώνης και τους πόρους του πίνακα ροής σε κάθε διακόπτη και εκχωρεί αυτά τα διαμερίσματα σε μεμονωμένους ελεγκτές. Λειτουργεί ως ένας διαφανής ελεγκτής μεσολάβησης μεταξύ των φυσικών διακοπών ενός δικτύου OpenFlow και άλλων ελεγκτών OpenFlow και επιτρέπει σε πολλούς ελεγκτές να λειτουργούν την ίδια φυσική υποδομή, όπως ένας διακομιστής διακομιστών επιτρέπει σε πολλά λειτουργικά συστήματα να χρησιμοποιούν το ίδιο υλικό που βασίζεται σε x86. Στη συνέχεια, άλλοι τυπικοί ελεγκτές OpenFlow λειτουργούν τα δικά τους μεμονωμένα τμήματα δικτύου μέσω του διακομιστή μεσολάβησης FlowVisor. Αυτή η ρύθμιση επιτρέπει σε πολλούς ελεγκτές OpenFlow να εκτελούν εικονικά δίκτυα στην ίδια φυσική υποδομή. Τα slice μπορούν να δημιουργηθούν είτε από τον cpu του switch από την τοπολογία του δικτύου, από τα tcp/ip, από τις εφαρμογές, από τις mac διευθύνσεις, της πόρτες των πακέτων και από τα flow space και flow entries κτλπ. Στην περίπτωση που χωρίζει το δίκτυο με τους πίνακες ροής, λέμε ότι το FlowVisor περιορίζει την κυκλοφορία τεμαχίζοντας τους χώρους ροής τους διακοπών.

Στο παρακάτω σχήμα φαίνεται η λογική του flowvisor:



Εικόνα 8: Λειτουργία FlowVisor

Το FlowVisor παρεμποδίζει μηνύματα OpenFlow από ελεγκτές openflow και, χρησιμοποιώντας τα πολιτική τεμαχισμού του κάθε ελεγκτή ξαναγράφεται με διαφάνεια το μήνυμα για τον έλεγχο μόνο ενός τμήματος του δικτύου. Για να ανταλλαχτεί ένα μήνυμα που αποστέλλεται από τον ελεγκτή openflow, το FlowVisor διασφαλίζει ότι το μήνυμα ενεργεί μόνο στην κίνηση εντός των πόρων που έχουν εκχωρηθεί στον εκλεχτή. Για ένα μήνυμα προς την αντίθετη κατεύθυνση, το FlowVisor εξετάζει το περιεχόμενο του μηνύματος για να συμπεράνει σε ποιον ελεγκτή openflow πρέπει να προωθηθεί το μήνυμα.

Οι ελεγκτές επισκεπτών λαμβάνουν μόνο μηνύματα που σχετίζονται με το τμήμα δικτύου τους.

4.2 Τεμαχισμός 5G

4.2.1 Λόγοι για τεμαχισμό 5G

Ο τεμαχισμός του 5G για εφαρμογές και την υποστήριξη των απαιτήσεων τους είναι απαραίτητο για πολλούς λόγους. Αρχικά υπάρχει εκθετική ανάπτυξη των υπηρεσιών βίντεο για κινητά π.χ. YouTube και Mobile TV που απαιτούν υψηλό εύρος ζώνης. Οι εξελίξεις στο internet of things έχουν ενεργοποιήσει παγκόσμιες πρωτοβουλίες για την ανάπτυξη τα συστήματα κινητής και ασύρματης επικοινωνίας πέμπτης γενιάς (5G). Ο αυξανόμενος αριθμός έξυπνων συσκευών (π.χ. tablet) και smartphone) και ο αυξανόμενος αριθμός πεντασμένων σε εύρος ζώνης εφαρμογές για κινητές συσκευές (π.χ. ζωντανή ροή βίντεο, διαδικτυακά βιντεοπαιχνίδια) που απαιτούν υψηλότερη φασματική απόδοση από εκείνη των συστημάτων 4G θέτουν σημαντικές προκλήσεις στο 5G. Η πρόβλεψη Cisco Visual Networking Index (VNI) προβλέπει ότι η κίνηση βίντεο IP θα είναι το 82% της συνολικής κίνησης στο Διαδίκτυο για τους καταναλωτές έως το 2022, από 75% του 2017. Μόνο το βίντεο για τα κινητά θα αντιπροσωπεύει το 78% της παγκόσμιας κίνησης δεδομένων κινητής τηλεφωνίας. Ενώ η επισκεψιμότητα για εικονική επαυξημένη πραγματικότητα (VR / AR) θα αυξηθεί 82% μεταξύ 2017 και 2022. Οι ρυθμοί αύξησης της κυκλοφορίας των τηλεοράσεων, Τα tablet, τα smartphone και οι μονάδες M2M θα είναι 21%, 29%, 49% και 49%, αντίστοιχα. Μια τέτοια τεράστια ανάπτυξη θα είναι το αποτέλεσμα του 12,3 δισεκατομμύρια συνδεδεμένες με κινητές συσκευές συσκευές, οι οποίες αναμένονται να υπερβούν τον προβλεπόμενο πληθυσμό των 8 δισεκατομμυρίων στον κόσμο έως το 2022. Για αυτούς τους λόγους λοιπόν το 5G και ο τεμαχισμός είναι πολύ σημαντικά. Το 5G προσφέρει τα χαρακτηριστικά όπως το εύρος ζώνης, την χαμηλή καθυστέρηση την καλύτερη κάλυψη και την εξοικονόμηση ενέργειας. Με τον τεμαχισμό θα μπορούμε να εφαρμόσουμε για κάθε εφαρμογή κάποια από αυτά τα παραπάνω χαρακτηριστικά που χρειάζονται για να καλυφτούν οι απαιτήσεις τους και να τρέχουν αποδοτικά.

4.2.2 Περί τεμαχισμού 5G

Όπως και στα κέντρα δεδομένων έτσι και στο 5G Ο τεμαχισμός του δικτύου χρησιμοποιεί μια έννοια που είναι γνωστή ως virtualization. Το δίκτυο σπάει σε αλλα εικονικά δίκτυα που το καθένα έχει φτιαχτεί και έχει δικούς τους πόρους για να εξυπηρετεί υπηρεσίες. Εκτελούνται στην ίδια φυσική υποδομή όπως και στο κέντρο δεδομένων. Τα slices είναι απομονωμένα και αμα γίνει κάτι στο ένα όπως μια επίθεση δεν θα έχει επίπτωση στα υπόλοιπα. Κάθε slice έχει τους δικούς του μηχανισμούς ασφάλειας και πρέπει να φέρει εγγύηση για την σωστή λειτουργία του, για την ασφάλεια, και την μη πρόφαση από μη εξουσιοδοτημένες οντότητες. Επίσης κάθε slice πρέπει να μπορεί να προσφέρει τους πόρους για να τρέξουν σωστά οι εφαρμογές. Ο τεμαχισμός γίνεται με τα SDN και NFV και

με την βοήθεια αυτών μπορούν να σχεδιαστούν, να διαμοιραστούν, να οργανωθούν και να βελτιστοποιηθούν οι πόροι σε κάθε slice. Η ανάπτυξη του network slicing αποτελείται από δύο φάσεις Creation (δημιουργία) και Runtime (χρόνος εκτέλεσης). Κατά την δημιουργία του slice ο χρήστης ζητάει ένα slice και ο πάροχος των slices του δίνει αυτό το κομμάτι. Στην δεύτερη φάση διαφορετικά NFVs παρέχουν ακριβώς αυτές τις υπηρεσίες τις οποίες απαιτεί ο χρήστης μέσω των slices.

Ένα θετικό του τεμαχισμού του 5G είναι πως ο διαχειριστής του θα μπορεί να τρέχει πολλές εφαρμογές σε μια κοινόχρηστη υποδομή χωρίς να χρειαστεί να αγοράσει άλλες υποδομές και έτσι έχουμε μείωση στις δαπάνες κεφαλαίου CAPEX και εξοικονόμηση χρόνου. Τα slices εκτελούνται όπως είπαμε σε μια κοινόχρηστη υποδομή η οποία αποτελείται από ειδικό hardware(στοιχεία δικτύου στο RAN) και διαμοιραζόμενο hardware όπως πόροι από το NFVI δηλαδή από servers οπου τρέχουν τα NFVs.

Υπάρχουν 2 σενάρια slicing για το 5G. Slicing με QoS και slicing χωρίς QoS σε κοινή χρήση υποδομών. Όπως και στα κέντρα δεδομένων υπάρχει το QoS και QoE έτσι και στο τεμαχισμό του 5G για τον τεμαχισμό και των μοιραστό των πόρων. Κάθε slice προσφέρει διαφορετικό τύπο υπηρεσιών και έχει συγκεκριμένο QoS και μέσα από αυτό εξασφαλίζει τα χαρακτηριστικά του που χρειάζεται για να εκτελεστεί μια υπηρεσία με τέτοιο τρόπο ώστε να καλυφθούν οι απαιτήσεις των χρηστών. Τα μεμονωμένα slice θα έχουν διαφορετικά χαρακτηριστικά, συμπεριλαμβανομένου του QoS και του latency και μεμονωμένες συσκευές θα μπορούν να έχουν πρόσβαση σε πολλά slices ταυτόχρονα. Για παράδειγμα μια υπηρεσία με QoS είναι οι αισθητήρες στο IoT που κάνουν κάποια δουλειά και έχουν εφαρμοστεί κάπου και χρειάζονται ένα συγκεκριμένο QoS ώστε να εξασφαλίζεται η εξοικονόμηση ενέργειας και μπαταρίας χωρίς να τους νοιάζει πχ το μεγάλο bandwidth εφόσον ανταλλάζουν - μεταδίδουν πχ απλά στατιστικά. Αν όμως κάτι δεν πάει καλά στο 5G πχ χαλάσει το QoS η γίνει μια επίθεση η μια παρεμβολή η τότε χαλάει η εμπειρία του χρήστη (QoE). Το άλλο σενάριο slicing είναι για σκοπούς της κοινής χρήσης υποδομών. Εδώ ο ενοικιαστής ενοικιάζει ένα slice από τον κάτοχο με βάση μια συμφωνία και ο ενοικιαστής μετά έχει πλήρη έλεγχο του slice των λειτουργιών και της υποδομής του.

4.2.3 Αρχές 5G slicing

Υπάρχουν και κάποιες αρχές στις οποίες βασίζετε το slicing για να λειτουργήσει αποδοτικά. Πρώτα είναι η απομόνωση. Όπως είπαμε το κάθε slice είναι απομονωμένο και το ένα δεν βλέπει το άλλο και δεν ασχολείται τι κάνει, δεν υπάρχει πρόσβαση και αμα γίνεται μια επίθεση σε ένα slice τα αλλα δεν θα επηρεαστούν. Δεύτερον είναι οι πόροι που θα τεθούν σε ένα slice να είναι αρκετοί και να χρησιμοποιούνται αποδοτικά ώστε να τρέξει μια υπηρεσία και κατά επέκταση να καλυφθούν οι ανάγκες του πελάτη. Τρίτον είναι η ελαστικότητα του slice δηλαδή η προσαρμογή των πόρων της εφαρμογής προς τα πάνω η προς τα κάτω ανάλογα με την συνολική ζήτηση που θα υπάρχει η οποία θα έχει οριστεί με βάση μετρήσεων και στατιστικών στοιχείων. Τέταρτων προγραμματισιμότητα που επιτρέπει σε τρίτους να ελέγχουν και επεξεργάζονται τους πόρους που έχουν δεσμευτεί για

το εκάστοτε slice. Και τέλος End-to-end αρχη που είναι η τεχνολογία που εγγυάται την μετάδοση των δεδομένων από τον πάροχο στον τελικό χρήστη.

4.2.4 Εφαρμογές τεμαχισμού 5G

Θα ξανά αναφέρουμε τις βασικές εφαρμογές που είχαμε πει στην αρχη συνοπτικά. Παρόλα αυτά δεν είναι μόνο αυτές. Αυτές είναι οι βασικές και στον χρόνο με το 5G θα δημιουργηθούν και άλλες που δεν είχαν δημιουργηθεί λόγω του ότι δεν μπορούσαν να υποστηριχθούν από το 4G οποτε δεν είχαμε μπει στον κόπο να σκεφτούμε και να τις παράγουμε. Πέρα από αυτό κάποιες εφαρμογές βγαίνουν από άλλες εφαρμογές, οποτε το μόνο σίγουρο είναι ότι στο μέλλον θα έχουμε πολύ περισσότερες εφαρμογές από όσο νομίζαμε.

Οι απομακρυσμένες χειρουργικές επεμβάσεις, ειδικότερα, είναι μια από τις πιο σημαντικές εφαρμογές του 5G. Μικροσκοπικά ρομπότ που εκτελούν χειρουργικές επεμβάσεις υψηλού κινδύνου, όλα ελέγχονται από ειδικούς χειρουργούς που μπορεί να βρίσκονται στη μέση του πλανήτη. Μια χειρουργική επέμβαση με το 5G θα έχει καθυστέρηση 0,01 δευτερόλεπτα, σε σύγκριση με την περίοδο καθυστέρησης 0,27 δευτερολέπτων με τα ασύρματα δίκτυα 4G που κυριαρχούν επί του παρόντος στις αναπτυσσόμενες χώρες. Αν πρόκειται να γίνει χειρουργική επέμβαση με εξ αποστάσεως βοήθεια, θα πρέπει να γίνει λες και ο χειρουργός είναι σχεδόν αυτοπροσώπως. Δεν μπορεί να υπάρξει καθυστέρηση άνω των δύο χιλιοστών του δευτερολέπτου. Και εκεί έρχεται η τεχνολογία 5G.

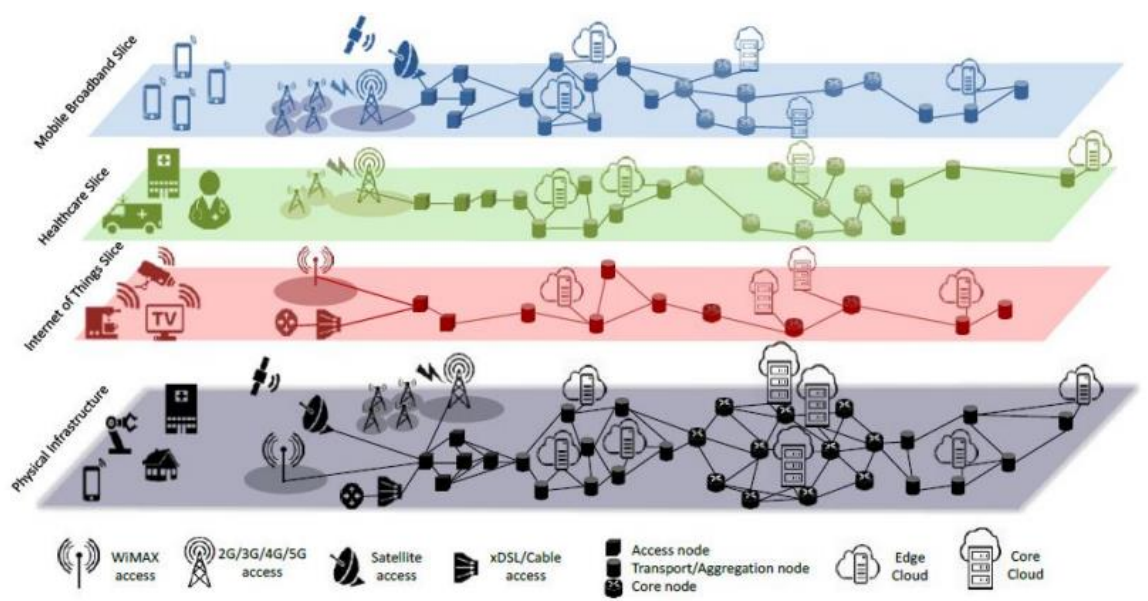
Το παιχνίδι είναι άλλη μια σίγουρη εφαρμογή και κομμάτι του 5G. Το gaming δεν υπάρχει μόνο στους υπολογιστές αλλά και στα κινητά και όχι απλό gaming αλλά και ανταγωνιστικό που σημαίνει ότι θα πρέπει να μην υπάρχει καθόλου καθυστέρηση για να οδηγηθεί ένας gamer που κάνει 1vs1 στην νίκη. Το Mobile Gaming δεν θεωρείται πλέον ως δραστηριότητα για νέους εφήβους. Έχει εξελιχθεί σε έναν τρόπο ζωής για όλες τις ηλικιακές ομάδες. Επειδή αυτός ο τρόπος ζωής είναι διαδικτυακός, ένα ειδικό τμήμα δικτύου πρέπει να είναι ένα σταθερό θεμέλιο.

Άλλη μια βασική εφαρμογή είναι τα αυτόματα αμάξια. Περίπου το 40% των ενήλικων Αμερικανών οδηγών κλίνουν περισσότερο στην αγορά αυτοκινούμενων αυτοκινήτων. Αυτή η αύξηση της δημοτικότητας ενθαρρύνει μεγάλες πολυεθνικές όπως η General Motors Co, η Uber Technologies Inc και η Apple Inc να επενδύσουν σε μεγάλο βαθμό σε οχήματα που μπορούν να οδηγηθούν αυτόνομα. Αν και τώρα χρησιμοποιούνται και πωλούνται όμως πολύς κόσμος δεν τα εμπιστεύεται και τα θεωρεί ότι δεν είναι ασφαλή. Το 5G είναι απαραίτητο για αυτή την εφαρμογή γιατί προσφέρει ασφάλεια από τυχόν επιθέσεις, εγγυημένη χαμηλή καθυστέρηση και διαθεσιμότητα.

Ο αθλητισμός είναι μια άλλη εφαρμογή που θα καλύπτετε γρήγορα από το 5G προς όφελός της. Η μετάδοση αγώνων θα γίνεται πολύ πιο ευκολα. Οι κάμερες με δυνατότητα 5G εξαλείφουν την ανάγκη χρήσης καλωδίων, διευκολύνοντας την live μετάδοση των σπορ που πραγματοποιούνται σε διάφορες και απομακρυσμένες περιοχές. Θα υπάρχει καλύτερο live streaming. Το 5G θα μεταμορφώσει επίσης την εμπειρία των τελικών χρηστών, επιτρέποντας live streaming υψηλής ποιότητας, πιο αξιόπιστες ροές. Αυτό θα επιταχύνει τις μεταβαλλόμενες συνήθειες των χρηστών και θα διαταράξει τα παραδοσιακά μοντέλα

εκπομπών που αποτέλεσαν το θεμέλιο της ανάπτυξης του αθλητισμού σε μια μεγάλη βιομηχανία. Η σύνδεση μέσα στο γήπεδο από τους χιλιάδες οπαδούς θα καλυτερέψει. Σε αυτή την περίπτωση θα χρησιμοποιηθεί η μεγάλη μπάνα συχνότητων του 5G εφόσον πρόκειται για μέρος χωρίς εμπόδια και απώλειες και υπάρχει πολύς κόσμος. Οι οπαδοί την ώρα που βλέπουν των αγώνα ανεβάζουν στα μέσα κοινωνικής δικτύωσης βίντεο με τις στιγμές και άλλα πράγματα, και θέλουν να έχουν πρόσβαση σε πρόσθετες πληροφορίες, να παρακολουθούν στιγμιότυπα βίντεο με αποτέλεσμα να καταναλώνουν πολλά GB. Ορισμένοι αθλητικοί οργανισμοί φοβούνται ότι ορισμένοι θεατές ενδέχεται να μείνουν στο σπίτι τους εάν δεν μπορούν να συνδεθούν στο internet. Ωστόσο, τα υπάρχοντα δίκτυα κινητής τηλεφωνίας και Wi-Fi δεν διαθέτουν την ικανότητα για τέτοια πυκνοκατοικημένα περιβάλλοντα, γι' αυτό οι χώροι και οι φορείς εκμετάλλευσης είναι τόσο ενθουσιασμένοι για το 5G. Τέλος μπορεί να υποστηριχθεί η εξ αποστάσεως εκπαίδευση των αθλητών σε πραγματικό χρόνο. Η εξαιρετικά χαμηλή καθυστέρηση του 5G σημαίνει ότι οι επίδοξοι αθλητές μπορούν να μάθουν από προπονητές μέσω εικονικής πραγματικότητας (VR) ή ολογραφικής τεχνολογίας.

Τέλος ο τεμαχισμός του δικτύου θα προσφερθεί και για το IoT. Το 5G θα μπορεί να εξυπηρετήσει εκατομμύρια συσκευές όπως κινητά τηλέφωνα, αισθητήρες, έξυπνα, ρολόγια, κάμερες, οικιακές συσκευές όπως πλυντήρια air-condition όπου όλα αυτά θα μπορείς να τα ελέγχεις απομακρυσμένα



Εικόνα 9: Εφαρμογές 5G Slicing

4.2.5 Εικονικοποίηση Λειτουργίας Δικτύου (NFV)

Το Network Function Virtualization (NFV) έχει στόχο την υλοποίηση των λειτουργιών του δικτύου στο λογισμικό. Κάνει αντικατάσταση λειτουργιών δικτύου όπως δρομολογητές, συσκευές για εξισορρόπηση φορτίου και τείχη προστασίας κτλπ. μέσω λογισμικού. Χρησιμοποιεί τις τεχνολογίες της εικονικοποίησης για να εικονικοποιήσει

όλες τις κατηγορίες λειτουργιών κόμβου δικτύου σε δομικά στοιχεία που μπορούν να συνδεθούν για να δημιουργήσουν υπηρεσίες επικοινωνίας. Αυτό σημαίνει ότι μία λειτουργία π.χ. ένα firewall μπορεί να δοθεί σε μία εταιρία ως software. Με αυτό τον τρόπο μπορούμε να έχουμε μία πληθώρα εικονικών λειτουργιών που τις ονομάζουμε VNF (Virtual Network Functions) που μπορούν να τρέχουν σε έναν σερβερ. Έτσι δεν υπάρχει η ανάγκη για αγορά και εγκατάσταση επιπλέον υλικού. Το NFV διαφέρει από την εικονικοποίηση ενός server σε άλλους μικρότερους εικονικούς server μέσω ενός λογισμικού. Μια λειτουργία ενός NFV μπορεί να αποτελείται από ένα ή περισσότερα εικονικά μηχανήματα (VM) που εκτελούν διαφορετικές διεργασίες το καθένα καθώς και διακομιστές υψηλής χωρητικότητας, switches, συσκευές αποθήκευσης όπως επίσης και cloud computing συσκευές.

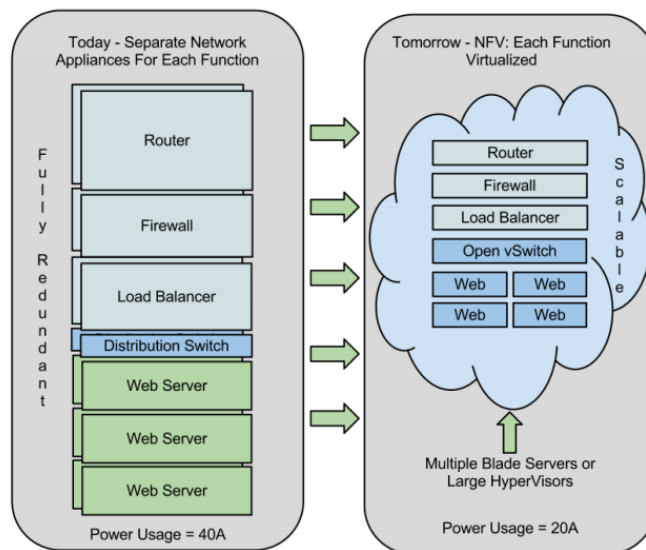
Ο σκοπός της NFV είναι να μεταμορφώσει τον τρόπο κατασκευής των δικτύων και την παροχή υπηρεσιών. Με το NFV, οποιαδήποτε επιχείρηση μπορεί να απλοποιήσει ένα ευρύ φάσμα λειτουργιών δικτύου, καθώς και να μεγιστοποιήσει την αποδοτικότητα και να εισαγάγει νέες υπηρεσίες που δημιουργούν έσοδα γρηγορότερα και ευκολότερα. Το NFV προσφέρει ευελιξία στις υπηρεσίες με μεγαλύτερους ρυθμούς μετάδοσης των δεδομένων. Μειώνονται οι δαπάνες κεφαλαίου CapEx και οι δαπάνες λειτουργίας OpEx καθώς δεν χρειάζεται να προμηθευτούν καινούργιο εξοπλισμό δικτύου και να γίνονται περιττά έξοδα. Πέρα από αυτό έχουμε και μείωση των δαπανών λειτουργίας OpEx καθώς δεν θα χρειάζονται η συνεχή αλλαγή και βελτίωση των ικανοτήτων που διαθέτουν οι τεχνικοί των δικτύων ώστε να μπορούν να ανταπεξέλθουν αποτελεσματικά σε ένα σενάριο με πολύ περίπλοκο δικτυακό εξοπλισμό. Επίσης μια εταιρία το να πάρει δικτυακό εξοπλισμό είναι επικίνδυνο και έχει μεγάλο ρίσκο και μη κερδοφόρο καθώς δεν ξέρει αμα θα έχει αρκετούς συνδρομητές για να ξεχρεώσει.

Για να επιτευχθούν τα παραπάνω οφέλη πρέπει να γίνουν κάποιες αλλαγές σε σχέση με το πως είναι τώρα τα πράγματα. Πρώτα από όλα πρέπει να γίνει διαχωρισμός του software από το hardware για να μπορεί το ένα να εξελιχθεί ανεξάρτητα από το άλλο. Δεύτερον το ότι έχει γίνει διαχωρισμός αυτών των δυο μπορεί πάνω από μια φυσική υποδομή να τρέχουν δικτυακές λειτουργίες ταυτόχρονα και γρηγορά. Έτσι το δίκτυο μπορεί να παρέχει τις υπηρεσίες του ταχύτερα μέσα από την ίδια φυσική υποδομή. Η τελευταία αλλαγή είναι η δυναμική κλιμάκωση των πόρων σε κάθε εφαρμογή. Δηλαδή κάθε εφαρμογή να έχει μεταβλητούς πόρους, όσους πόρους χρειαστείτε εκείνη την στιγμή.

Στο 5G, το NFV θα επιτρέψει τον τεμαχισμό δικτύου μια πτυχή αρχιτεκτονικής εικονικού δικτύου που επιτρέπει τη δημιουργία πολλαπλών εικονικών δικτύων πάνω σε μια κοινή φυσική υποδομή. Τα εικονικά δίκτυα μπορούν στη συνέχεια να προσαρμοστούν για να καλύψουν τις ανάγκες εφαρμογών, υπηρεσιών, συσκευών και πελατών. Στο 5G, το NFV θα επιτρέψει επίσης το καταναμημένο cloud, βοηθώντας στη δημιουργία ευέλικτων και προγραμματιζόμενων δικτύων για τις ανάγκες του αύριο. Το NFV επιτρέπει την εικονικοποίηση 5G, ώστε το φυσικό δίκτυο να μπορεί να χωριστεί σε πολλαπλά εικονικά δίκτυα που μπορούν να υποστηρίξουν διαφορετικά δίκτυα πρόσβασης ραδιοφώνου (RAN) ή διάφορους τύπους υπηρεσιών για συγκεκριμένα τμήματα πελατών. Τα τμήματα δικτύου θα απομονωθούν το ένα από το άλλο στο επίπεδο ελέγχου και στο επίπεδο χρήστη, οπότε η εμπειρία χρήστη θα είναι η ίδια σαν να ήταν ένα φυσικά ξεχωριστό δίκτυο. Τα μελλοντικά δίκτυα 5G θα προσφέρουν στους χειριστές δικτύων την ευελιξία να κατανέμουν ταχύτητα,

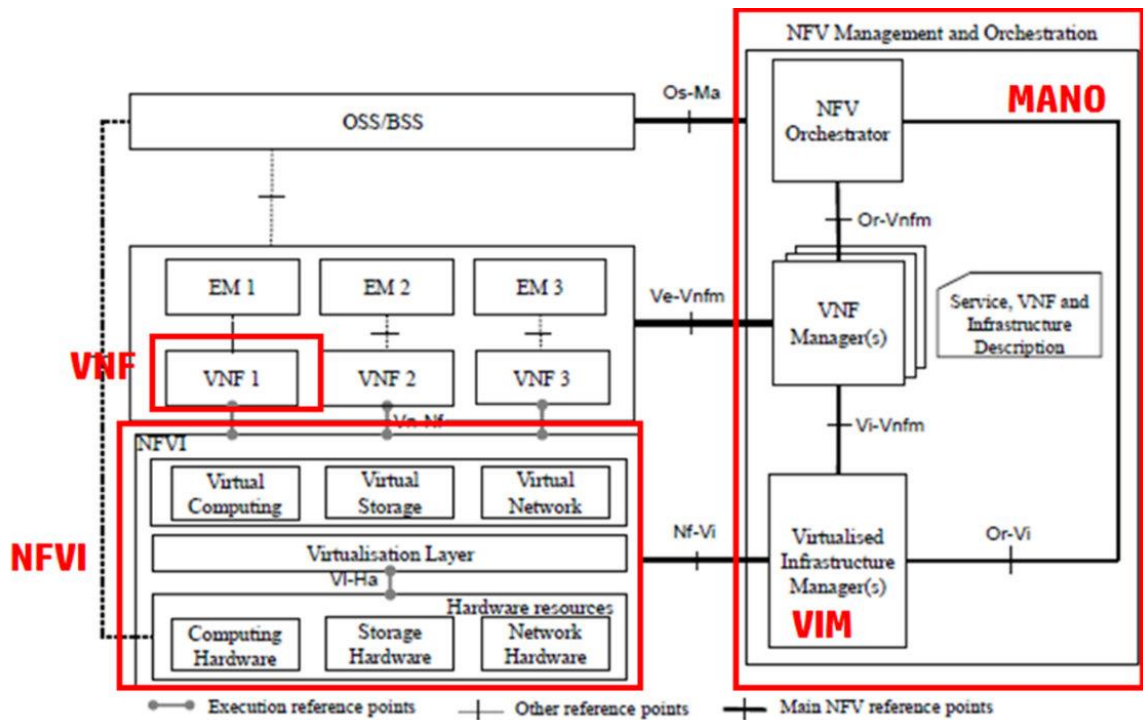
χωρητικότητα και κάλυψη σε λογικά κομμάτια σύμφωνα με τις απαιτήσεις κάθε περίπτωσης χρήσης.

Στο παρακάτω σχήμα φαίνεται η βασική ιδέα του NFV



Εικόνα 10: Βασική ιδέα NFV

Παρακάτω απεικονίζεται η αρχιτεκτονική: European Telecommunication Standards Institute (ETSI)



Εικόνα 11: Αρχιτεκτονική ETSI NFV

Η αρχιτεκτονική ETSI ISG NFV αποτελείται από 3 κυρία στοιχεία: NFVI (NFV Infrastructure), τα VNFs και τέλος τις λειτουργίες NFV MANO (Management and Orchestration).

Το NFVI είναι ο συνδυασμός πόρων του λογισμικού και του υλικού όπου αναπτύσσονται τα VNFs. Οι φυσικοί πόροι είναι πχ αποθηκευτικός χώρος και μία υποδομή δικτύου που παρέχει την κατάλληλη σύνδεση και επεξεργαστική ισχύ στα VNF. Οι εικονικοί πόροι είναι οι αποθηκευτικοί και οι δικτυακοί πόροι. Για την εικονικοποίηση χρησιμοποιείται ένα Layer που διαχωρίζει τους εικονικούς πόρους από τους φυσικούς.

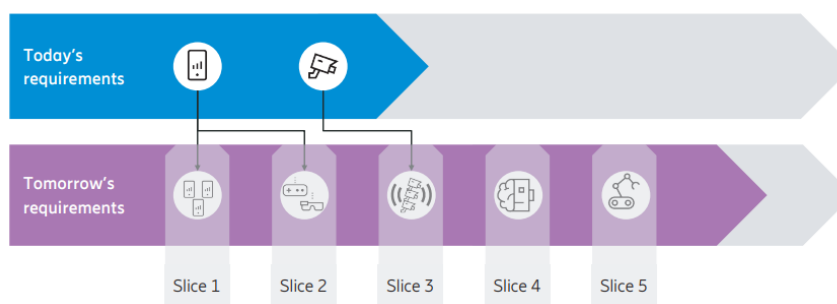
Τα VNFs είναι οι δικτυακές λειτουργίες όπως routers, firewalls κτλ που προσφέρονται μέσα από λογισμικά ως εφαρμογές. Ένα VNF είναι μια η και παραπάνω δικτυακές λειτουργίες (NFs) που αναπτύχθηκε χρησιμοποιώντας ιδεατούς πόρους. Τα NFs τρέχουν μέσα από εικονικές μηχανές (VMs). Ο χρήστης δεν μπορεί να παρατηρήσει κάποια σημαντική διαφορά στις υπηρεσίες που τους παρέχονται των οποίων οι λειτουργίες τρέχουν πάνω σε μία φυσική υποδομή και αυτών που οι λειτουργίες τους τρέχουν πάνω σε ένα VM.

Το NFV MANO έχει να κάνει με το virtualization. Ασχολείται με το orchestration πως θα διαμοιράζονται οι πόροι, κατανέμει και διαμορφώνει τα VNF και παρέχει τις δομές που τρέχουν VNF. Αποτελείτε από το VNF managers, Virtualized infrastructure managers και orchestration τα οποία συνδέονται μεταξύ τους και δημιουργούν το NFV MANO.

4.2.6 Ericsson 5G Slicing

[52]Η Ericsson βλέπει το 5G Slicing όπως το περιγράψαμε από πάνω. Δηλαδή πολλά 5G εικονικά δίκτυα τα οποία είναι απομονωμένα και το καθένα έχει τα δικά του χαρακτηριστικά για να φιλοξενήσει μια υπηρεσία. Η Ericsson συνεργάστηκε με τον Arthur D. Little για τη διεξαγωγή έρευνας αγοράς σχετικά με τον τεμαχισμό δικτύου για τον προσδιορισμό μελλοντικών ευκαιριών αγοράς.

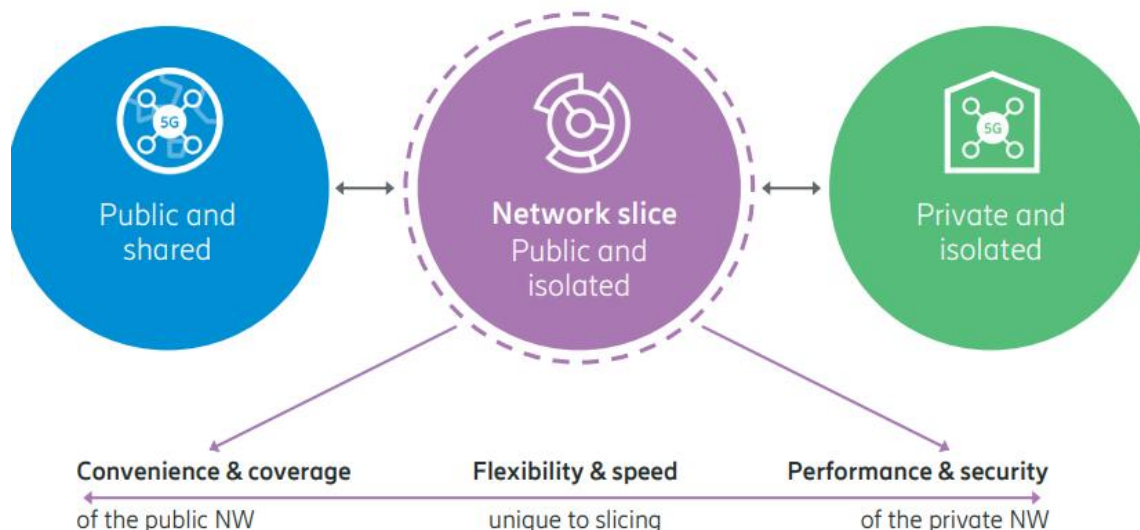
Η τεχνολογική πρόοδος σε μεγάλες βιομηχανίες αυξάνει την ζήτηση για υψηλής απόδοσης, ευέλικτες υπηρεσίες επικοινωνιών. Ο τεμαχισμός δικτύου εμφανίζεται ως ένας κρίσιμος τρόπος για να αντιμετωπιστεί το χάσμα υπηρεσιών μεταξύ δημόσιων δικτύων που δεν μπορούν να ικανοποιήσουν αυτές τις απαιτήσεις και εξειδικευμένων ιδιωτικών δικτύων, κάτι που απαιτεί υψηλότερες επενδύσεις. Όσον αφορά τα ασύρματα κυψελοειδή δεδομένα, ένα κοινό δίκτυο ήταν ο κανόνας. Οι επιχειρήσεις βασίστηκαν σε αυτό το δίκτυο για τις περισσότερες μη κρίσιμες εργασίες, όπως κλήσεις διασκέψεων, συστήματα κρατήσεων, εφεδρικές κάμερες ασφαλείας, ψηφιακές πληρωμές, Intranet και βίντεο κατ'απαίτηση. Ωστόσο, είναι σαφές ότι το κοινόχρηστο δημόσιο δίκτυο δεν μπορεί να καλύψει τις ανάγκες των αναδύομενων και προηγμένων περιπτώσεων χρήσης κινητής συνδεσιμότητας, οι οποίες έχουν ένα ευρύ φάσμα τεχνικών λειτουργιών και απαιτήσεων ασφάλειας. Η ανάπτυξη στο Διαδίκτυο των πραγμάτων (IoT), οι βελτιωμένες ευρυζωνικές κινητές συσκευές και οι κρίσιμες επικοινωνίες τύπου μηχανικής ανοίγουν νέες ροές εσόδων, επιχειρηματικές συνεργασίες και περιπτώσεις χρήσης. Αυτές οι περιπτώσεις χρήσης έχουν υψηλότερες απαιτήσεις για την απόδοση του δικτύου, και εάν αυτές δεν είναι εφικτές, οι περιπτώσεις χρήσης δεν θα λειτουργούν. Η ανάπτυξη νέων φυσικών δικτύων για όλες τις υπηρεσίες και τοποθεσίες ή η αναδιάρθρωση υπαρχόντων για συγκεκριμένες περιπτώσεις χρήσης δεν αποτελεί βιώσιμη λύση σε αυτήν την πρόκληση. Κάτι τέτοιο θα ήταν απαγορευτικά δαπανηρό και περιορίζει την ευελιξία για νέες υπηρεσίες ή περιπτώσεις χρήσης - ουσιαστικά, αυτό θα δημιουργούσε ακριβώς το ίδιο πρόβλημα πέντε χρόνια στο μέλλον, ενώ ταυτόχρονα θα εμπόδιζε την καινοτομία με ένα άκαμπτο δίκτυο. Ρίχνοντας μια πιο προσεκτική ματιά στα τρέχοντα δημόσια δίκτυα, το τρέχον επίπεδο των πόρων του δικτύου δεν μπορεί να ταιριάζει με την αυξανόμενη ποικιλία των απαιτήσεων με την πάροδο του χρόνου. Και ενώ αυτά τα δίκτυα επεκτείνονται, όπως με την τρέχουσα διάθεση 5G, ακόμη και τότε, η επέκταση δεν θα ικανοποιήσει πλήρως κάθε περίπτωση χρήσης με την εξαιρετικά υψηλή αξιοπιστία, την ασφάλεια, την εξαιρετικά χαμηλή καθυστέρηση και άλλες απαιτήσεις που απαιτούν πολλές περιπτώσεις χρήσης.



Εικόνα 12: Ericsson 5G Slicing

Ο τεμαχισμός δικτύου είναι ένα παράδειγμα όπου οι CSP (communications service providers) δημιουργούν λογικά δίκτυα ή διαμερίσματα με την κατάλληλη απομόνωση τους, τους κατάλληλους πόρους και με την βελτιστοποιημένη τοπολογία για να παρέχουν μια υπηρεσία που να ανταποκρίνεται στις μοναδικές απαιτήσεις μιας συγκεκριμένης

περίπτωσης χρήσης. Διατηρεί πολύτιμους πόρους δικτύου από μη κρίσιμες περιπτώσεις χρήσης και δραστηριότητες, ώστε να μπορούν να αναπτυχθούν όπου χρειάζεται και όπου κάποιος είναι πρόθυμος να πληρώσει για αυτό. Ως αποτέλεσμα, το slicing παρέχει τα οφέλη τόσο των δημόσιων όσο και των ιδιωτικών αυτόνομων δικτύων, μαζί με ορισμένα μοναδικά χαρακτηριστικά του.



Εικόνα 13: Public & Private δίκτυα

Τα θετικά της απομόνωσης των slices είναι πολλά. Πρώτον, αυξάνει την ανθεκτικότητα, επειδή οι βλάβες ή οι διακοπές λειτουργίας σε ένα κομμάτι δεν επηρεάζουν άλλα κομμάτια. Επιπλέον, ο χρόνος αγοράς μπορεί να είναι μικρότερος, επειδή υπάρχουν λιγότερες εξαρτήσεις από άλλες λειτουργίες δικτύου. Αλλά μπορεί να έχει ακόμη μεγαλύτερα οφέλη για την ασφάλεια, τα οποία μπορούν να προσαρμοστούν ανά slice για να πληρούν μοναδικές απαιτήσεις ασφαλείας. Επιπλέον, εάν μια επίθεση είναι επιτυχής, θα περιέχεται στο slice και δεν θα μπορεί να μετακινηθεί πλευρικά σε ολόκληρο το δίκτυο. Και όταν εξελίσσεται η επίθεση, η απομόνωση δεδομένων μεταξύ πελατών slice είναι πολύ πιο εύκολο να διατηρηθεί.

Υπάρχουν επίσης τεχνικά ζητήματα. Τα CSP θα πρέπει να καθιερώσουν συντονισμό μεταξύ τομέων, να επιτρέψουν εγγυήσεις απόδοσης και απομόνωση δικτύου, να διεξάγουν διαχείριση slicing και εννοχρήστρωση end to - end και να βεβαιωθούν ότι διαθέτουν τους απαραίτητους πόρους και απαιτήσεις τεμαχισμού.

Καθώς το 5G και ο τεμαχισμός εξαπλώνονται και οι πάροχοι υπηρεσιών μοιράζονται πόρους δικτύου, αυξάνεται η πολυπλοκότητα, η οποία μπορεί με τη σειρά της να αμφισβητήσει κανονισμούς που διέπουν τους κλάδους συγκεκριμένων πελατών, ειδικά για περιπτώσεις κρίσιμης σημασίας χρήσης.

Ο τεμαχισμός δικτύου ανοίγει για νέα επιχειρηματικά μοντέλα καθώς το δίκτυο γίνεται πλατφόρμα για άλλες επιχειρήσεις. Αυτό θα οδηγήσει σε νέες συνεργασίες και μοντέλα μετάβασης στην αγορά.

Στον τομέα των επιχειρήσεων προς τους καταναλωτές (B2C), το CSP χρεώνει ένα ασφάλιστρο απευθείας στον καταναλωτή για υψηλότερη ποιότητα ή αποκλειστική πρόσβαση σε περιεχόμενο που παραδίδεται με τον τεμαχισμό. Για παράδειγμα ένας

πελάτης αγοράζει πρόσβαση σε παιχνίδια κινητής τηλεφωνίας χαμηλού λανθάνοντος χρόνου smartphone ή συσκευή παιχνιδιών. Το CSP προσφέρει σταθερή ασύρματη πρόσβαση Fixed Wireless Access (FWA) με βάση ένα ειδικό τμήμα δικτύου.

Στην επιχείρηση-επιχείρηση ή στην κυβέρνηση (B2B / B2G), ο «αγοραστής slice» είναι ο τελικός πελάτης, συνήθως μια κρατική οντότητα ή επιχείρηση που χρησιμοποιεί το slice για να πραγματοποιήσει μια περίπτωση χρήσης για εσωτερικές λειτουργίες. Για παράδειγμα ένας κατασκευαστής αγοράζει μια υπηρεσία που βασίζεται σε ένα τμήμα δικτύου για να πραγματοποιήσει μια περίπτωση χρήσης ρομποτικής σε μια γραμμή παραγωγής.

Τέλος B2B2C. Εδώ, ο αγοραστής slice χρησιμοποιεί το slice για να πραγματοποιήσει μια περίπτωση χρήσης για έναν πελάτη. Η αλυσίδα θα μπορούσε να είναι μεγάλη με τον δεύτερο πελάτη που παρέχει υπηρεσίες με δυνατότητα slice σε άλλη οντότητα. Για παράδειγμα ένας πάροχος υπηρεσιών cloud αγοράζει ένα κομμάτι για να παρέχει αποκλειστική ασύρματη συνδεσιμότητα υψηλής τεχνολογίας για μια εταιρεία πλατφόρμας παιχνιδιών που στη συνέχεια χρησιμοποιεί το συνδυασμένο πακέτο για να τροφοδοτήσει μια premium, υψηλής απόδοσης συνδρομή παιχνιδιού για τους καταναλωτές.

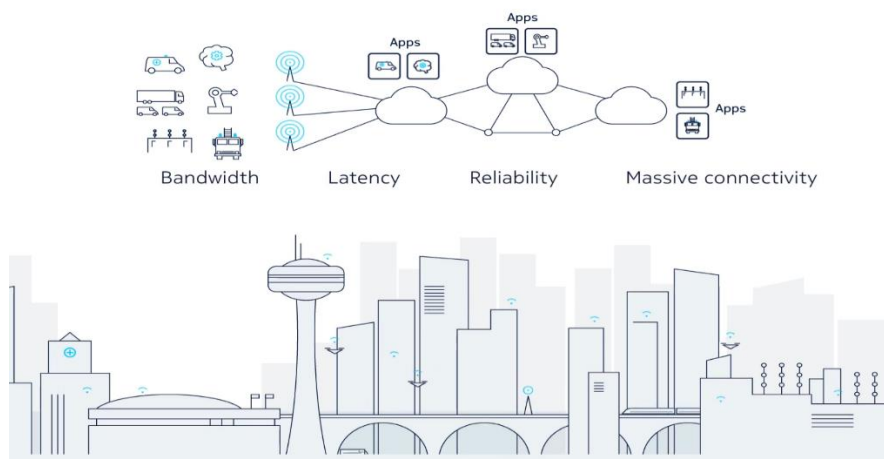
Οι δέκα μεγαλύτερες περιπτώσεις χρήσης σύμφωνα με την Ericsson είναι:

- [53] Αυτοκινητοβιομηχανία (Αυτόματος οδηγός).
- Υγεία(νοσοκομεία, μεταφορά δεδομένων, απομακρυσμένες εγχειρήσεις με ρομπότ)
- Παραγωγή και μετάδοση ενέργειας (Απομακρυσμένη κάλυψη, αξιοπιστία, ασφάλεια)
- Δημόσιο τομέα(Εξυπνη παρακολούθηση σε πραγματικό χρόνο, τεράστια αποστολή κριτικής IoT).
- Κυβερνητικές υπηρεσίες έκτακτης ανάγκης (Κρίσιμες αποστολές push to talk, ρομπότ που καταστρέφουν φορβές drones και αλλα που απαιτούν αξιόπιστη, χαμηλή καθυστέρηση, συνδεσιμότητα υψηλού εύρους ζώνης.)
- Broadcasting & streaming.
- Κατασκευή – παραγωγή (AR που επιτρέπουν την ποιοτική επιθεώρηση και διάγνωση για εργαζόμενους συντήρησης, τεχνικούς και χειριστές σε ολόκληρο το εργοστάσιο, απομακρυσμένος έλεγχος ρομπότ όπως ανεμογεννήτριες, τρισδιάστατη αλληλεπίδραση μέσω βίντεο μεταξύ συνεργατικών ρομπότ και ανθρώπων, καθώς και βελτιστοποίηση διαδικασιών μέσα στο εργοστάσιο)
- Εφοδιαστική αλυσίδα (Supply chain) (Απομακρυσμένη ποιότητας ελέγχου ή διαγνωστικών, παρακολούθηση προϊόντων σε πραγματικό χρόνο απόδοσης, παραλλαγών ποιότητας και μεταβαλλόμενων παραγόντων στο περιβάλλον, διαχείριση εμπορευμάτων).
- Gaming (VR cloud gaming, e sports gaming, computer- console gaming).
- Σιδηροδρομικός(αισθητήρες που προβλέπουν μελλοντική συντήρηση, οδήγηση απομακρυσμένα)

4.2.7 Nokia 5G Slicing

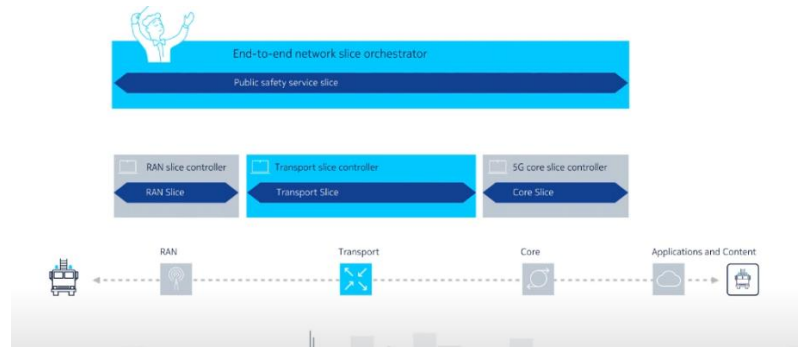
[54] Η Νokia βλέπει το 5G slicing όπως και οι άλλοι. Τεμαχίζει το δίκτυο ραδιοπρόσβασης (RAN), Transport και core network. Το 5G σπάει σε αλλα εικονικά 5G δίκτυα και το καθένα εξυπηρετεί μια εφαρμογή. Το κάθε 5G δίκτυο έχει συγκεκριμένα χαρακτηριστικά για που χρειάζεται η εφαρμογή ώστε να εκτελεστεί αποδοτικά. Κάποια από αυτά είναι Bandwidth, low latency, μεγάλος αριθμός συνδεδεμένων συσκευών και αξιοπιστία.

Η διαδικασία έχει ως εξής, ένας πελάτης για παράδειγμα η πυροσβεστική θέλει να τρέξει διάφορες εφαρμογές. Για παράδειγμα critical voice, μεταφορά μεγάλων δεδομένων, έλεγχος drone απομακρυσμένα, sensors που θα ανιχνεύουν την φωτιά κ.α. Όλες αυτές οι εφαρμογές έχουν διαφορετικές απαιτήσεις – χαρακτηριστικά, για παράδειγμα το critical voice θέλει low bandwidth και low latency. Όλες αυτές οι εφαρμογές με τις απαιτήσεις αποτελούν το SLA.(Service level agreement) μεταξύ του πελάτη και του CSP. Για να μπορεί ο πελάτης αυτός να τρέξει αυτές τις εφαρμογές ο CSP θα φτιάξει ένα slice που θα φιλοξενούνται οι εφαρμογές κάθε μια με το δικό της SLA.



Εικόνα 14: Nokia 5G slicing apps

Ο service orchestrator δουλεύει με controllers στο δίκτυο ραδιοπρόσβασης (RAN), Transport και Core network για να προσδιορίζονται οι πόροι του κάθε slice με βάση το SLA από τον end user μέχρι το data center που φιλοξενείται η εφαρμογή.



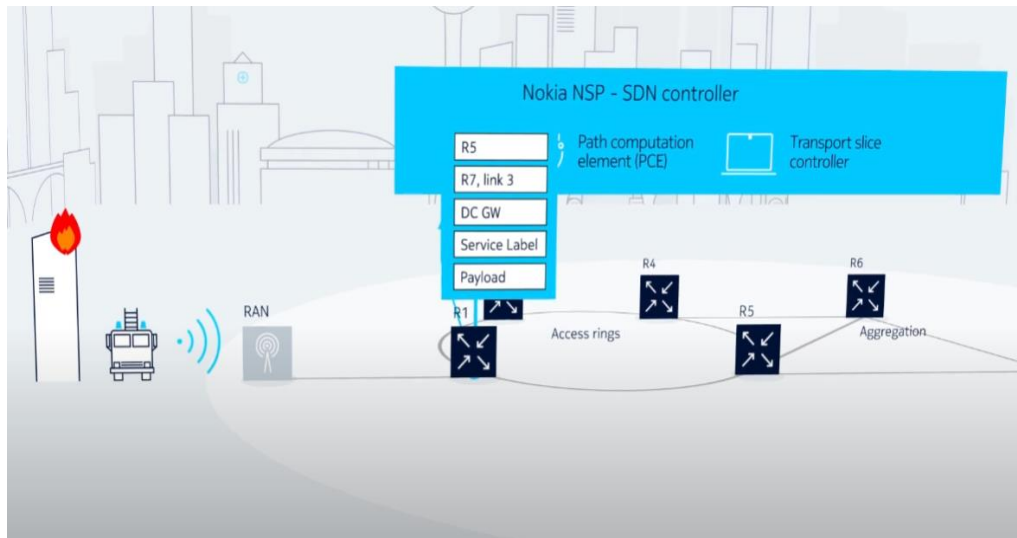
Εικόνα 15: Nokia End to end network slice orchestrator

Εστιάζοντας στο IP routing στο δίκτυο μεταφοράς η Νοκία χρησιμοποιεί έναν controller NSP-SDN οπύ χωρίζει το επίπεδο μεταφοράς για κάθε slice, στην συγκεκριμένη περίπτωση να συνδέσει τις εφαρμογές της πυροσβεστικής από το RAN στο Core δίκτυο με βάση τις απαιτήσεις της κάθε εφαρμογής. Το κάνει αυτό βρίσκοντας μονοπάτια η δημιουργώντας services tunnels με την βοήθεια του path computation element (PCE) . Οι ρουτερς τον μονομανιών αυτών θα παρέχουν πόρους στην εφαρμογή για να δημιουργηθεί το transport section από οπύ θα περάσει η εφαρμογή. Κάθε εφαρμογή έχει το δικό της κόστος (CoS). Η προτεραιότητα το εγγυημένο bandwidth και καθυστέρηση κάθε εφαρμογής προσδιορίζονται στο δίκτυο μεταφοράς από τους ρουτερς.



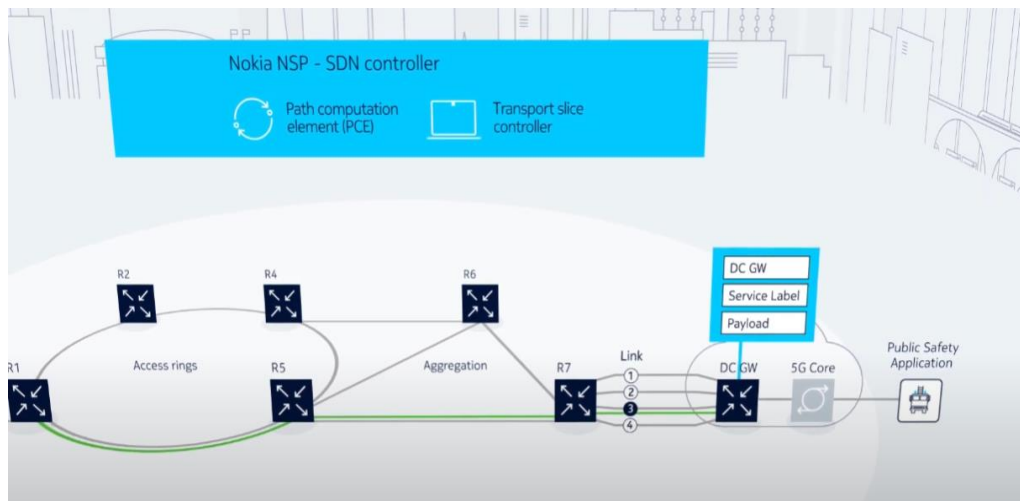
Εικόνα 16: Nokia Slice vs Slice at Transport Network

Για κάθε από τα μονοπάτια που βρίσκονται από το Nokia NSP το PCE κατεβάζει ένα service label και αλλα routing labels στον ingress router(R1). Το service label προσδιορίζει ότι είναι μια από τις εφαρμογές της πυροσβεστικής.



Εικόνα 17: Nokia Ετικέτα πακέτου δρομολόγησης

Αυτά τα label μπορεί να είναι γενικά η ειδικά αμα υπάρχουν απαιτήσεις από load balancing ή latency. Στην παραπάνω φωτογραφία δείχνει ένα κουτί στον ingress router με διαφορά labels μέσα. Τα 2 πρώτα λένε που να προχωρήσει το πακέτο δηλαδή στον ρουτερς 5 και στον ρουτερς 7 μέσω του συνδέσμου 3.



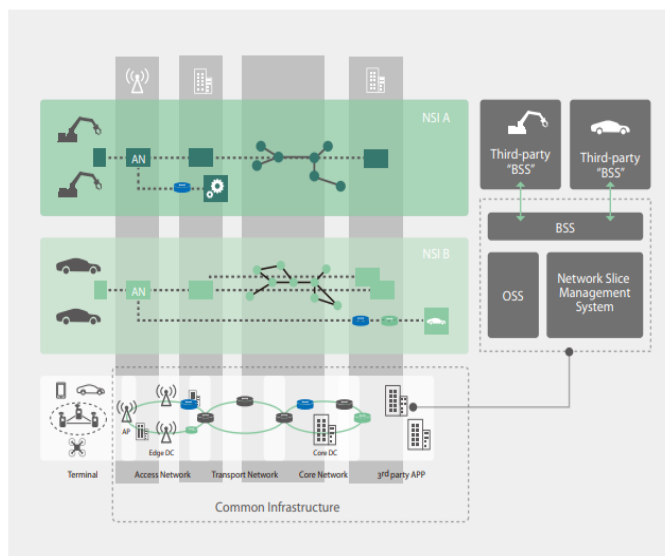
Εικόνα 18: Nokia Δρομολόγηση πακέτου μέσω ετικέτας

Μόλις το πακέτο φτάσει στον προορισμό του, ο Direct current gateway router (DC GW router) αφαιρεί το DC GW label, διαβάζει το service label και επεξεργάζεται το payload προορίζοντας το στην εφαρμογή της πυροσβεστικής (Public safety Application). Αν στο δίκτυο μεταφοράς πέσει κάποιος ρουτερ, οι ρουτερς θα το καταλάβουν αμέσως και θα ενημερώσουν τον Nokia NSP controller για αλλαγές και προβλήματα και έτσι θα δημιουργηθεί νέο μονοπάτι οπού θα υποστηρίζει το SLA των εφαρμογών και θα

ενημερωθεί ο ingress router για να γίνει σωστά η δρομολόγηση. Οι Nokia ip ρουτερς μαζεύουν μετρήσεις και στατιστικά από την υποδομή με μετρητές που μετρούν την απόδοση του δικτύου μεταφοράς όπως την καθυστέρηση, jitter και packet drops και τα αναφέρουν στον NSP. Έτσι ο NSP controller που έχει πλήρη γνώση του δικτύου μεταφοράς αμα χρειαστεί θα αλλάξει μονοπάτια ώστε να μπορεί να υποστηρίζεται το SLA.

4.2.8 Huawei 5G Slicing

[55] Όπως φαίνεται στο παρακάτω σχήμα, η συνολική αρχιτεκτονική αποτελείται από τρία θεμελιώδη επίπεδα: το επίπεδο υποδομής, το επίπεδο slice δικτύου και το επίπεδο διαχείρισης δικτύου. Το επίπεδο υποδομής παρέχει τους φυσικούς και εικονικοποιημένους πόρους, για παράδειγμα, πόρους υπολογιστών, πόρους αποθήκευσης και συνδεσιμότητα χρηστών και συσκευών. Το επίπεδο slice δικτύου τρέχει πάνω από το επίπεδο υποδομής και παρέχει τις απαραίτητες λειτουργίες, εργαλεία και μηχανισμούς δικτύου για τη δημιουργία λογικών δικτύων end-to-end (E2E) μέσω NSI. Το επίπεδο διαχείρισης δικτύου περιέχει το γενικό σύστημα διαχείρισης slice δικτύου (NSM) BSS / OSS και το οποίο σχεδιάζει και διαχειρίζεται τον τεμαχισμό δικτύου. Επιπλέον, επίσης διασφαλίζει τις απαιτήσεις SLA.



Εικόνα 19: Huawei 5G Slicing Αρχιτεκτονική

Τα βασικά χαρακτηριστικά είναι:

- Κοινή υποδομή: Όντας διαφορετικός από την αποκλειστική λύση δικτύου που χρησιμοποιεί φυσικά απομονωμένα και στατικά δίκτυα για την υποστήριξη

ενοικιαστών, ο τεμαχισμός του δικτύου προωθεί τη χρήση μιας κοινής υποδομής μεταξύ ενοικιαστών από τον ίδιο χειριστή. Βοηθά στην επίτευξη υψηλότερης αποδοτικότητας χρήσης πόρων.

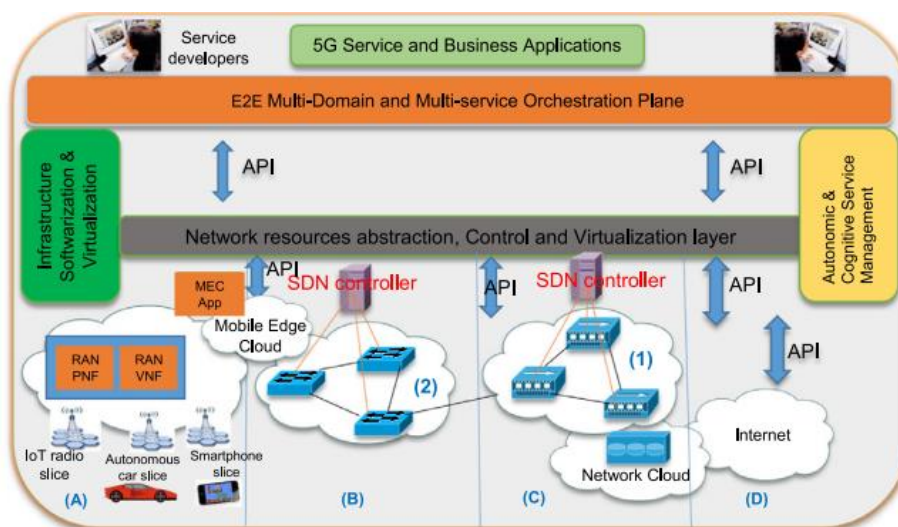
- Προσαρμογή και απαίτηση: Κάθε τεχνικός τομέας σε ένα NSI έχει διαφορετικές δυνατότητες προσαρμογής, οι οποίες συντονίζονται μέσω του συστήματος NSM κατά τη διάρκεια της διαδικασίας σχεδιασμού προτύπου slice δικτύου και ανάπτυξης NSI και O&M. Κάθε τεχνικός τομέας μπορεί να εκτελέσει μια ανεξάρτητη διαδικασία προσαρμογής όσον αφορά τα σχέδια σχεδιασμού για να επιτύχει μια αποτελεσματική ισορροπία μεταξύ της απλότητας που απαιτείται από την εμπορική πρακτική και της αρχιτεκτονικής πολυπλοκότητας
- Απομόνωση: Η συνολική αρχιτεκτονική υποστηρίζει την απομόνωση των NSI, συμπεριλαμβανομένης της απομόνωσης πόρων, της απομόνωσης των λειτουργιών και συντήρησης (O&M) και της απομόνωσης ασφαλείας. Τα NSI μπορούν να απομονωθούν είτε φυσικά είτε λογικά σε διαφορετικά επίπεδα.
- Εγγυημένη απόδοση: Με τον τεμαχισμό δικτύου μπορούν να φτιαχτούν τοπολογίες και δίκτυα 5G καταλληλά ώστε να ικανοποιηθούν και να διασφαλιστούν προδιαγραφές απόδοσης 5G που καθορίζονται από τη βιομηχανία και να ανταποκρίνεται στις κάθετες απαιτήσεις της βιομηχανίας.
- Επεκτασιμότητα: Λόγω της εικονικοποίησης, η οποία είναι μια από τις βασικές τεχνολογίες ενεργοποίησης για την κοπή δικτύου, οι πόροι που καταλαμβάνει ένα NSI μπορούν να αλλάξουν δυναμικά, π.χ. scale in/out .

Το σύστημα NSM παίζει σημαντικό ρόλο σε ολόκληρη την αρχιτεκτονική του συστήματος. Παρέχει τις ακόλουθες υπηρεσίες:

- Σχεδίαση: σχεδίαση προτύπων slice δικτύου σύμφωνα με τις δυνατότητες δικτύου και τις απαιτήσεις SLA.
- Παροχή: περιλάβετε slice instantiation, διαμόρφωση και ενεργοποίηση.
- Διασφάλιση χρόνου εκτέλεσης: Δυνατότητα παρατήρησης της κατάστασης της λειτουργίας των NSI και εξασφάλιση SLA.
- Παροπλισμός: διαγραφή ενός NSI όταν οι υπηρεσίες του δεν χρησιμοποιούνται πλέον.

4.2.9 Λογισμηκοποίηση (Softwarization) 5G

Η εικονικοποίηση δικτύου του 5G σχεδιάζεται, υλοποιείται, αναπτύσσεται με την χρήση προγράμματος με το οποίο γίνεται και η διαχείριση και συντήρηση του εξοπλισμού. Η εικονικοποίηση του δικτύου στοχεύει στην παροχή υπηρεσιών και εφαρμογών 5G με μεγαλύτερη ευελιξία και χαμηλό κόστος. Μαζί με την υλοποίηση των απαιτήσεων δικτύου 5G όπως δυνατότητα προγραμματισμού, ευελιξία, και προσαρμοστικότητα, το λογισμικό εικονικοποίησης είναι έτοιμο να παρέχει διαχείριση υπηρεσιών E2E (exchange-to-exchange) και να βελτιώσει το QoE του τελικού χρήστη. Ο τεμαχισμός δικτύου ως υπηρεσία (Network slicing as-a-service) και η συνολική ενοποίηση της πλατφόρμας υπηρεσιών 5G E2E θα πραγματοποιηθεί με τη εικονικοποίηση του δικτύου χρησιμοποιώντας τεχνολογίες SDN, NFV και cloud computing. Η δύναμη των τεχνολογιών softwarization και virtualization είναι οι κύριοι μοχλοί καινοτομιών στην εποχή 5G όπου οι προγραμματιστές και οι χειριστές μπορούν να δημιουργήσουν γρήγορα δίκτυα με γνώμονα την εφαρμογή και εφαρμογές με γνώμονα το δίκτυο, ώστε να ανταποκρίνονται στις απαιτήσεις της επιχείρησής τους. Προκειμένου να επιτευχθούν οι στόχοι της softwarization του δικτύου, απαιτείται νέος σχεδιασμός και υλοποίηση σε διαφορετικά τμήματα δικτύου 5G (e.g., RAN, transport networks, core networks, mobile-edge networks, and network clouds). Αυτό συμβαίνει επειδή κάθε τμήμα έχει διαφορετικές απαιτήσεις ή τεχνικά χαρακτηριστικά και επίπεδο softwarization. Το σχήμα 4 απεικονίζει τις τεχνολογίες δικτύου λογισμικού που εφαρμόζονται σε τμήματα δικτύου 5G (RAN, δίκτυα κινητής τηλεφωνίας, δίκτυα μεταφοράς, δίκτυα πυρήνα).



Εικόνα 20: Softwarezation 5G

Το Mobile edge network στοχεύει να μεταφέρει τα περιεχόμενα, τις λειτουργίες δικτύου και τους πόρους πιο κοντά στον τελικό χρήστη, επεκτείνοντας το συμβατικό κέντρο δεδομένων στην άκρη των δικτύων 5G. Η λογισμηκοποίηση σε δίκτυα κινητής τηλεφωνίας θα εφαρμοστεί με βάση την εικονικοποιημένη πλατφόρμα που αξιοποιεί SDN, NFV. Το Multi-access Edge Computing (MEC) χαρακτηρίζεται από υψηλό εύρος ζώνης, χαμηλό λανθάνοντα χρόνο (low latency) και επίγνωση θέσης. Το MEC παρέχει δυνατότητες

υπολογιστικού νέφους για την ικανοποίηση απαιτητικών απαιτήσεων 5G, όπως η απόδοση και βελτιωμένο QoE για τους τελικούς χρήστες. Μέσω της προσωρινής αποθήκευσης περιεχομένων στο διακομιστή MEC η λογισμηκοποίηση του MEC στο 5G υπόσχεται να μειώσει τον όγκο των δεδομένων που μεταδίδονται στο κεντρικό δίκτυο 5G για επεξεργασία, επιτρέποντας την αποτελεσματική χρήση των διαθέσιμων πόρων και να τρέχουν οι εφαρμογές σε πραγματικό χρόνο.

Ο σχεδιασμός των περισσότερων core δικτύων και λειτουργιών επιπέδου εξυπηρέτησης στην εποχή του δικτύου 5G αναμένεται να εφαρμοστούν ως Virtual Network Functions (VNFs) σύμφωνα με τις προβλεπόμενες αρχιτεκτονικές αρχές SDN / NFV. Τα VNFs είναι εικονικές υπηρεσίες δικτύου που εκτελούνται σε ανοιχτές πλατφόρμες υπολογιστών που προηγουμένως εκτελούνταν από αποκλειστική τεχνολογία υλικού. Τα VNF περιλαμβάνουν εικονικοποιημένους δρομολογητές, τείχη προστασίας, βελτιστοποίηση WAN και υπηρεσίες μετάφρασης διευθύνσεων δικτύου (NAT). Τα περισσότερα VNF εκτελούνται σε εικονικές μηχανές (VM) σε κοινό λογισμικό υποδομής εικονικοποίησης, όπως VMWare. Τα VNF μπορούν να βοηθήσουν στην αύξηση της επεκτασιμότητας και της ευελιξίας του δικτύου, ενώ ταυτόχρονα επιτρέπει την καλύτερη χρήση των πόρων υποδομής δικτύου. Άλλα οφέλη περιλαμβάνουν τη μείωση της κατανάλωσης ενέργειας και την αύξηση της ασφάλειας και του διαθέσιμου φυσικού χώρου, καθώς τα VNF αντικαθιστούν το φυσικό υλικό. Αυτό οδηγεί επίσης σε μειωμένες λειτουργικές και κεφαλαιουχικές δαπάνες. Στο 5G θα λειτουργούν σε Virtual Machines (VMs) δυνητικά πάνω από τυπικούς διακομιστές ενεργοποιημένους σε περιβάλλοντα Fog / Cloud Computing.

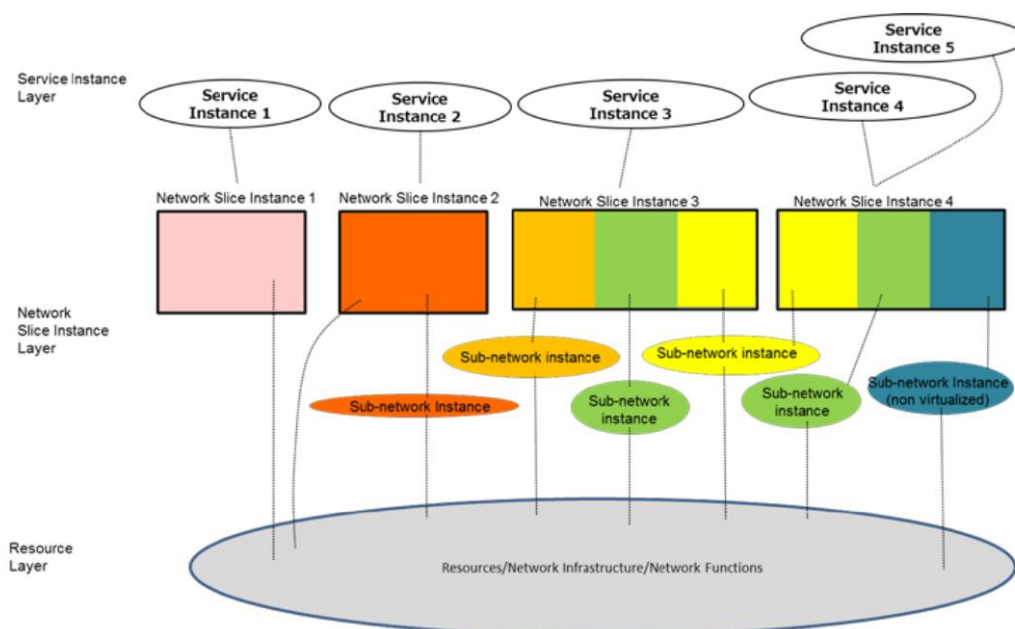
Για να προσαρμοστούν στις ανάγκες των 5G Radio Access Networks (RANs), τα μελλοντικά προγραμματιζόμενα δίκτυα μεταφορών (transport networks) θα πρέπει να εφαρμοστούν ως πλατφόρμα όπου μπορούν να φιλοξενηθούν διάφορες υπηρεσίες χρήστη και δικτύου. Ο σχεδιασμός ενός τέτοιου λογισμηκοποιημένου δικτύου μεταφοράς μπορεί να γίνει χρησιμοποιώντας κατάλληλα διασυνδέσεις- διεπαφές (interfaces) σε υποδομές SDN / NFV. Με αυτόν τον τρόπο, οι μηχανισμοί ανακάλυψης πόρων και βελτιστοποίησης μπορούν εύκολα να εφαρμοστούν στο επίπεδο ελέγχου 5G. Είναι σημαντικό να αναφερθεί ότι, ένα λογισμηκοποιημένο δίκτυο μεταφοράς 5G θα επιτρέπει στενά συνδεδεμένες αλληλεπιδράσεις με το δίκτυο ραδιοπρόσβασης RAN όπου πτυχές όπως η κινητικότητα και η εξισορρόπηση φορτίου μπορούν να συντονιστούν αποτελεσματικά.

Η δυνατότητα προγραμματισμού δικτύου είναι μια έννοια που περιλαμβάνει τη λογισμηκοποίηση του δικτύου και την εικονικοποίηση χρησιμοποιώντας υποδομή της δικτύωσης που καθορίζεται από λογισμικό SDN / NFV. Η δυνατότητα προγραμματισμού του 5G χρειάζεται συστηματικό διαχωρισμό των NFs για την αντιμετώπιση των αναδυόμενων αναγκών της αποτελεσματικότητας του δικτύου 5G και την αξιοπιστία, ευελιξία και ασφάλεια υπηρεσιών. Η δυνατότητα προγραμματισμού 5G ενισχύει τη γρήγορη, ευέλικτη και δυναμική ανάπτυξη νέων υπηρεσιών δικτύου και διαχείρισης που μπορούν να εκτελεστούν ως ομάδες VM σε όλα τα τμήματα του δικτύου (επίπεδο ελέγχου και διαχείρισης). Η δυνατότητα προγραμματισμού 5G θα διευκολύνει τη δημιουργία 5G οικοσυστημάτων που θα μπορούσαν να ωφελήσουν σε διαφορετικά επίπεδα ελέγχου και διαχείρισης διαισθητικά σε όλο το δίκτυο, χρησιμοποιώντας open Application Programming Interface (API) and Software Development Kit (SDK).

4.2.10 Δίκτυο Κινητής Τηλεφωνίας Επομένης γενιάς (NGMN)

Ο τεμαχισμός δικτύου 5G δημιουργήθηκε και πρωτοεμφανίστηκε από το Δίκτυο κινητής τηλεφωνίας επόμενης γενιάς Next Generation Mobile Network (NGMN). Όπως ορίζεται από το NGMN, ένα slice δικτύου είναι ένα λογικό δίκτυο που εκτελείται σε μια κοινή υποκείμενη (φυσική ή εικονική) υποδομή, απομονωμένη, με ανεξάρτητο έλεγχο και διαχείριση που μπορεί να δημιουργηθεί κατ' απαίτηση. Τα slice δικτύου είναι επομένως αυτόνομα, απομονωμένα, διαχειρίσιμα και υποστηρίζουν πολλαπλές υπηρεσίες και λειτουργίες.

Η αρχιτεκτονική network slicing ορίζεται από την NGMN (Next Generation Mobile Networks) και αποτελείται από 3 επίπεδα όπως απεικονίζεται στην παρακάτω εικόνα:



Εικόνα 21: Αρχιτεκτονική NGMN

Το Service Instance layer είναι υπεύθυνο για την οργάνωση και διατήρηση των εφαρμογών στους τελικούς χρήστες, οι οποίες υποστηρίζονται από το δίκτυο. Κάθε υπηρεσία αντιπροσωπεύεται από ένα Service Instance.

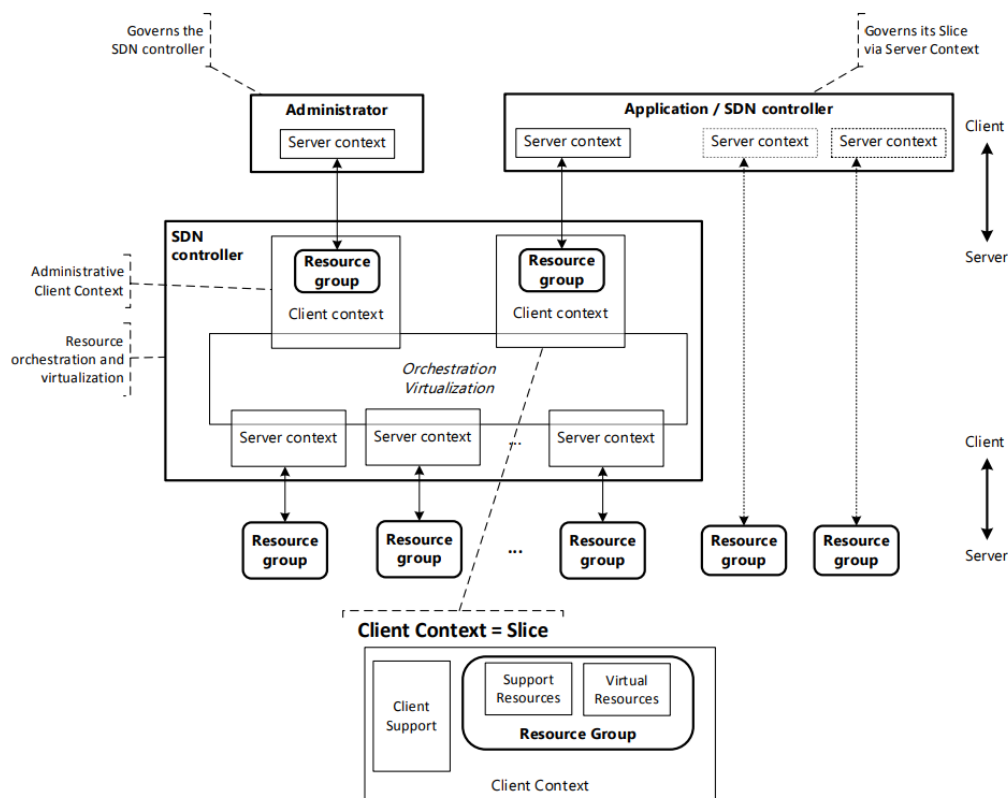
Το Network Slice instance layer είναι υπεύθυνο για την δικτυακή υποδομή δηλαδή τους πόρους που θα χρησιμοποιεί μια εφαρμογή. Σε αυτό το επίπεδο δημιουργούνται τα network slice instance με ένα blueprint. Ένα instance μπορεί να χωριστεί σε sub-network instances τα οποία θα παίρνουν πόρους από ένα instance η και παραπάνω. Ένα instance περιλαμβάνει φυσικούς και λογικούς πόρους και είναι απομονωμένο από τα άλλα instance. Για να φτιαχτεί ένα instance πρέπει να γίνει με κάποιες πολιτικές. Το blueprint δημιουργεί

το slice παρέχει ακριβώς αυτά τα χαρακτηριστικά τα οποία απαιτούνται από κάποια υπηρεσία.

Τέλος το Resource Layer περιέχει τους φυσικούς και εικονικούς πόρους (δικτυακούς επεξεργασία μνήμη αποθήκευση και λειτουργίες δικτύων) ώστε να υλοποιηθεί ένα network slice instance. Σε αυτό το layer η διαχείριση του slice γίνεται από τον διαχειριστή των πόρων του δικτύου ο οποίος αποτελείται από τον NFV Orchestrator (NFVO) όπως επίσης και από εφαρμογές που διαμορφώνουν τους πόρους του δικτύου.

4.2.11 Open Network Foundation (ONF)

Στο παρακάτω σχήμα φαίνεται η αρχιτεκτονική ONF (Open Network Foundation) SDN.



Εικόνα 22: Αρχιτεκτονική ONF

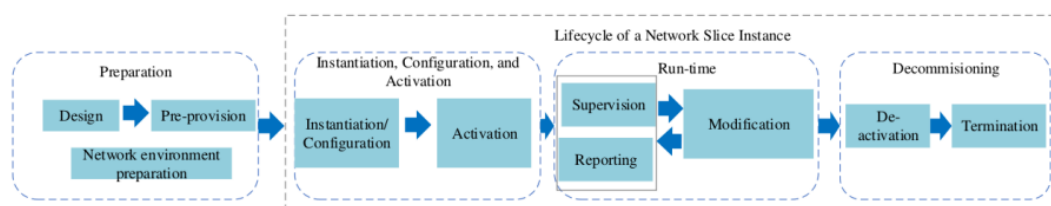
Αν το δούμε από κάτω προς τα πάνω, ο sdn ελεγκτής στην μέση επικοινωνεί με τους πόρους (Resource group) ως client-server και μετά επικοινωνεί από πάνω με τις εφαρμογές ως server-client. Ο sdn ελεγκτής στην μέση λειτουργεί ως διαμεσολαβητής μεταξύ των αιτημάτων των clients(που έρχονται από πάνω από τον sdn) και των διαθέσιμων πόρων που

υπάρχουν εκείνη τη στιγμή(κάτω από τον SDN) και αλληλοεπιδρά με τους clients μέσω του client context και με τους πόρους μέσω server context.

Ο client context αντιπροσωπεύει όλες τις πληροφορίες που χρειάζεται κάποιος controller για να επικοινωνήσει με κάποιον client. Το client context είναι το slice που αποτελείται από ένα σύνολο πόρων (Resource Group) που διαχειρίζονται, ελέγχονται και προσφέρονται από έναν ελεγκτή (Application / SDN controller) σε έναν πελάτη. Οι πόροι αυτοί καθορίζονται από τον Administrator που ορίζει πολιτικές στον SDN controller όσον αφορά τους πόρους κάθε slice. Το Client support περιέχει όλα αυτά τα στοιχεία που είναι απαραίτητα ώστε να πραγματοποιηθούν οι ενέργειες του client. Ο SDN controller μέσω του server context ζητά τους πόρους κάθε slice και γίνεται η εντοπιστική. Ο server context περιέχει όλες τις πληροφορίες που χρειάζεται το controller για να αλληλοεπιδράσει με ένα σύνολο πόρων που βρίσκονται σε ένα Resource Group. Πολλοί από τους πόρους που χρησιμοποιούνται από το SDN ενδεχομένως να έχουν προμηθευτεί από το NFV. Το SDN και το NFV αλληλοσυμπληρώνονται επιτρέποντας μία καλύτερη διαμόρφωση του δικτύου στην επιθυμητή εικόνα.

4.2.12 Κύκλος ζωής του Slice

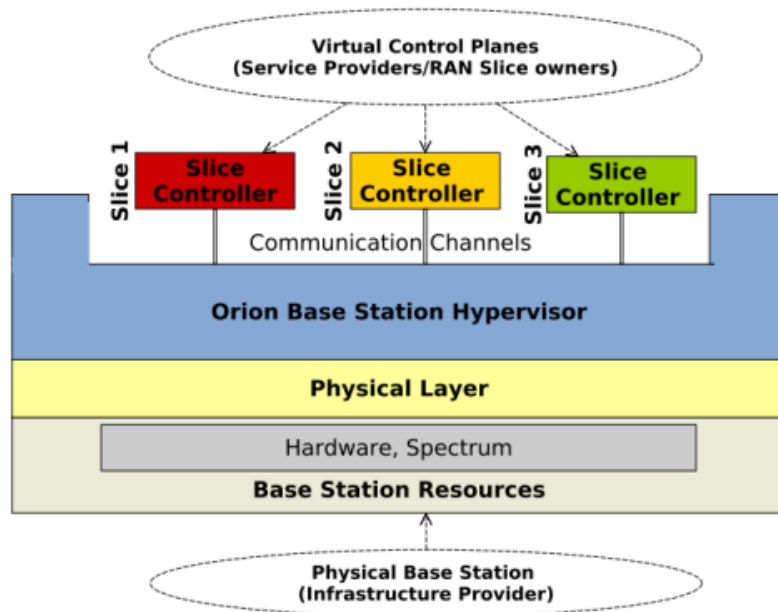
[39]Κάθε slice που δημιουργείται πέρα από τα χαρακτηριστικά όπως το QoS εύρος ζώνης και την καθυστέρηση έχει ένα κύκλο ζωής. Ο κύκλος αυτός εξαρτάται ανάλογα με το ποσό χρήσιμο είναι το slice. Ένα slice έχει το Network Slice life-cycle management που περιέχει τις διαδικασίες του κύκλου ζωής του όπως είναι δημιουργία τρέξιμο και καταστροφή κτλ. Και το δεύτερο είναι το Network Slice instances level.



Εικόνα 23: Επίπεδο Network Slice life-cycle management

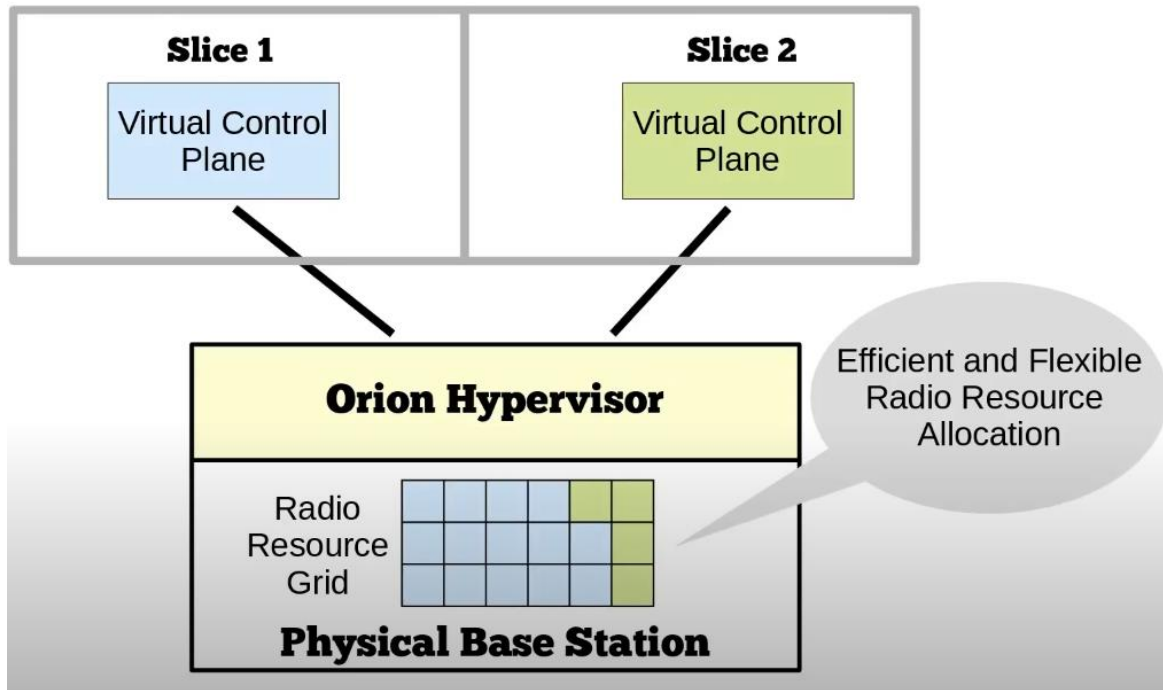
4.2.13 Τεμαχισμός Δίκτυου Ραδιοπρόσβασης (RAN Slicing)

Το Orion πρόκειται για ένα σύστημα RAN slicing το οποίο ανταποκρίνεται επαρκώς στις απαιτήσεις για cost-effective αρχιτεκτονική δικτύου. Η σχεδίαση του Orion μας διευκολύνει να ξεχωρίσουμε το base station (εξοπλισμός radio, μνήμη φάσμα κτλ). Κάθε base station στην αρχιτεκτονική του Orion υποστηρίζει την τεχνολογία ραδιοπρόσβασης (RAT) που σημαίνει πως όλοι οι πόροι (radio και φάσματος) μπορούν να αξιοποιηθούν μέσω ενός διαμοιραζόμενου physical layer.



Εικόνα 24: Αρχιτεκτονική τεμαχισμού RAN Orion

Ο BSH (Base Station Hypervisor) είναι τοποθετημένος πάνω από το physical χρησιμοποιείται για να διαχειριστεί και να απομονώσει τα Ran Slices. Συνδέει τα απομονωμένα slices με την φυσική υποδομή επιτρέποντας τους να έχουν μία οπτική της υποκείμενων ραδιοπόρων. Ένα Ran Slice είναι και ένα base station και βρίσκεται πάνω από τον Hypervisor. Κάθε virtual base station αποτελείται από ένα virtual control plane που είναι υπεύθυνο για τη διαχείριση της κατάστασης του data plane. Το virtual control plane ενός slice είναι ουσιαστικά ένα controller που τρέχει ως ξεχωριστή διεργασία και η δουλειά του είναι να διαχειριστεί τους πόρους που θα δεσμευτούν για τα UE(user equipment). Η επικοινωνία των virtual control planes των slices με τον Hypervisor γίνεται με μηνύματα μέσω ανεξάρτητων physical/virtual καναλιών επικοινωνίας. Αυτή η προσέγγιση επιτρέπει την ανάπτυξη των slices στο ίδιο μηχάνημα που ανήκει ο Hypervisor ή και σε διαφορετικό. Στο παρακάτω σχήμα βλέπουμε ότι ο Orion Hypervisor δίνει πόρους στα εικονικά base stations ανάλογα τις απαιτήσεις της υπηρεσίας.

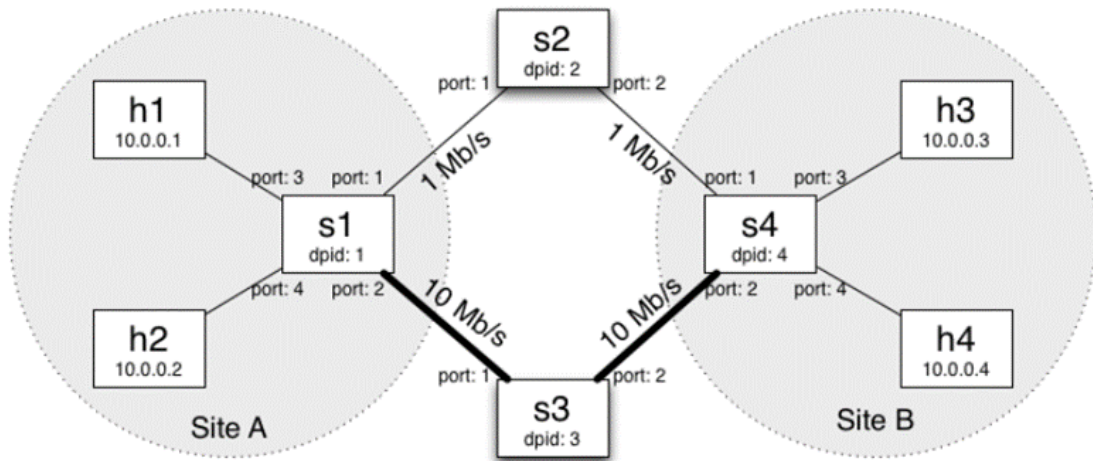


Εικόνα 25: Ευελιξία πόρων για κάθε slice

4.3 Παραδείγματα τεμαχισμού δικτύου

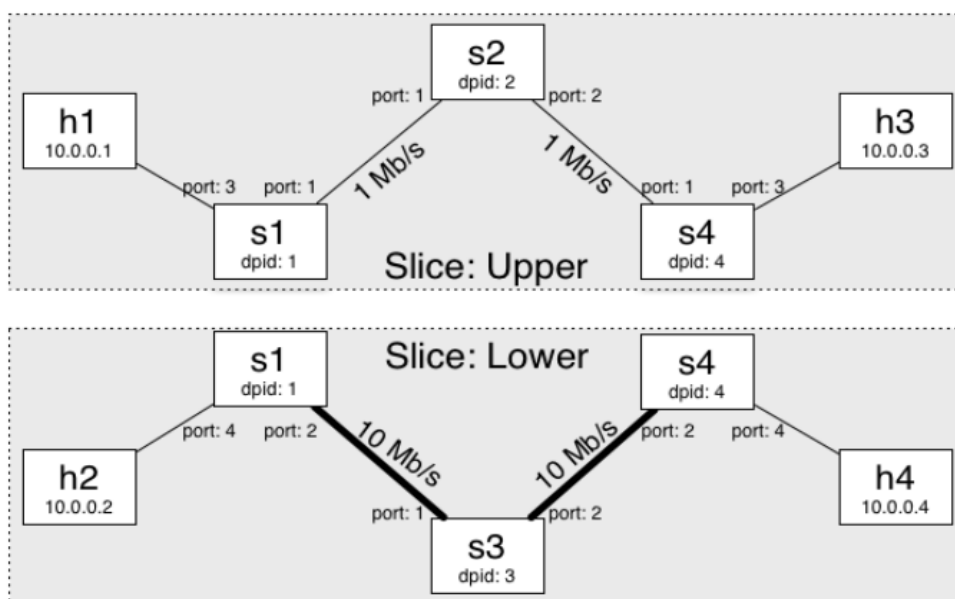
4.3.1 Παράδειγμα 1

Στην παρακάτω τοπολογία βλέπουμε 4 χρήστες **h1,h2,h3,h4** και 4 switches **S1,S2,S3,S4**. Για την επικοινωνία S1 και S4 υπάρχουν 2 διαδρομές, οι S1-S2-S4 και S1-S3-S4. Στην πρώτη το bandwidth είναι 1mbps και στο δεύτερο 10mbps.



Εικόνα 26: Τοπολογία παραδείγματος 1

Θα χρησιμοποιήσουμε το Flowvisor για να χωρίσουμε την τοπολογία σε 2 κομμάτια με βάση τις πόρτες όπως φαίνεται στο παρακάτω σχήμα.



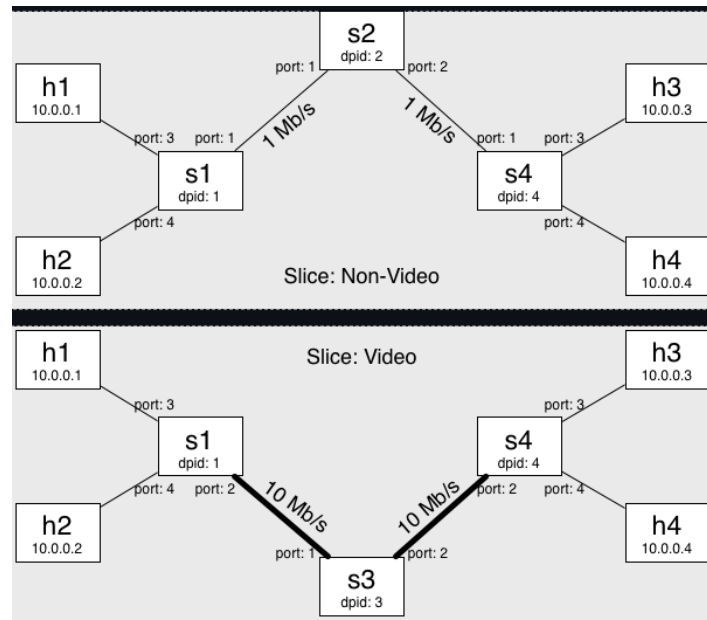
Εικόνα 27: Τεμαχισμός τοπολογίας παραδείγματος 1

Έτσι ο h1 θα μπορεί να επικοινωνήσει μόνο με τον h3 και αντίστροφα με bandwidth **1mbps** και ο h2 μόνο με τον h4 και αντίστροφα με bandwidth **10mbps**

Αυτό το παράδειγμα θα λυθεί στην πειραματική ενασχόληση όπου θα εξηγηθεί επιπλέον το configuration δηλαδή τα εργαλεία και την παραμετροποίηση για την λειτουργία του σε περιβάλλον Linux.

4.3.2 Παράδειγμα 2

Σε αυτό το παράδειγμα έχουμε την ίδια τοπολογία με το παράδειγμα 1 όμως τα slices θα δημιουργηθούν με βάση την εφαρμογή. Παρατηρούμε τις 2 διαδρομές S1-S2-S4 και S1-S3-S4 με bandwidth 1mbps και 10mbps αντίστοιχα. Η πρώτη διαδρομή θέλουμε να χρησιμοποιείται για βίντεο και η δεύτερη διαδρομή για οτιδήποτε άλλο.



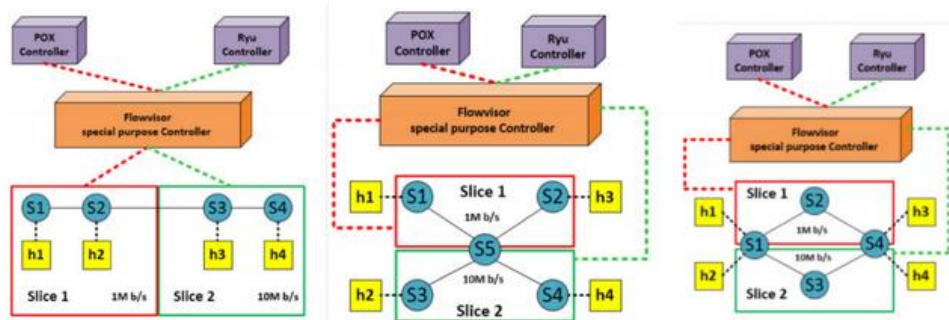
Εικόνα 28: Τοπολογία παραδείγματος 2

Στο παράδειγμα αυτό δεν έχουμε σκοπό να αποκόψουμε τους χρήστες όπως κάναμε στο πρώτο παράδειγμα. Όλοι οι χρήστες θα μπορούν να επικοινωνήσουν μεταξύ τους απλά θα γίνει ένας διαχωρισμός στην επικοινωνία τους σε βίντεο και οτιδήποτε άλλο όπου αυτά τα 2 θα μεταφέρονται σε 2 διαφορετικές διαδρομές ξεχωριστά το καθένα με το κατάλληλο bandwidth. Έτσι θα δημιουργηθούν 2 slices με βάση την εφαρμογή. Αυτό θα γίνει ελέγχοντας στα switches s1 και s4 τα πακέτα που έρχονται από τους χρήστες τους και ανάλογα το πακέτο θα σταλεί στην κατάλληλη πόρτα που αντιστοιχεί στην σωστή διαδρομή. Οποτε τα UDP πακέτα με πόρτα 9999 αντιστοιχούν σε βίντεο και τα άλλα πακέτα στο “οτιδήποτε άλλο”.

4.3.3 Παράδειγμα 3

Σε αυτό το παράδειγμα θα μετρήσουμε το delay, RTT και jitter σε διάφορες περιπτώσεις όπως διαφορετικούς controllers και με διαφορετικό bandwidth 1 ή 10 Mbps.

Έχουμε σε κάθε περίπτωση 4 χρήστες h1, h2, h3, h4 και switches 4 ή 5 ανάλογα την τοπολογία.



Εικόνα 29: Τοπολογίες παραδείγματος 3

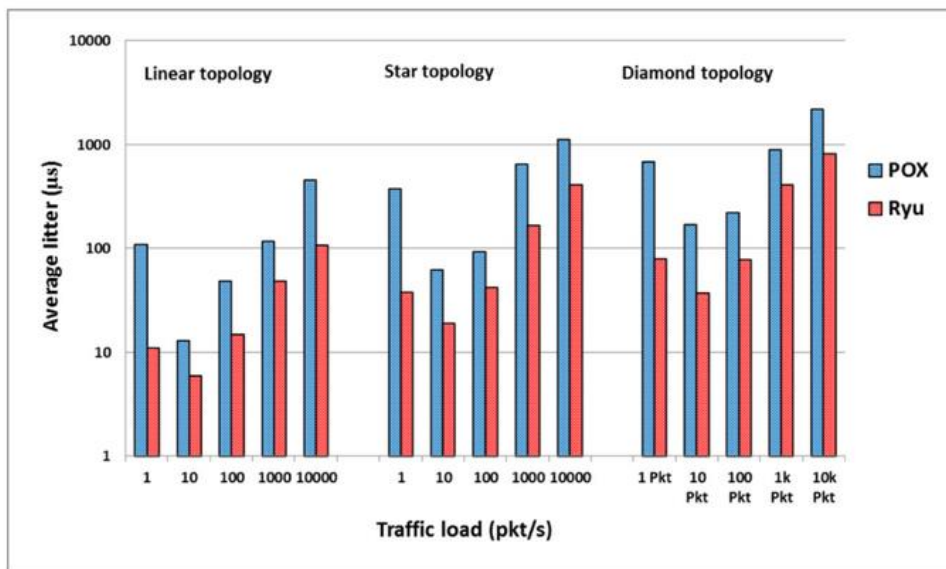
Όπως φαίνεται από κάτω στο στιγμιότυπο έχουμε:

- Αριστερά τοπολογία δαυλού
- Μέση τοπολογία αστέρα
- Δεξιά τοπολογία διαμαντιού

Εδώ σπάμε και τις 3 τοπολογίες σε 2 slices που σημαίνει ότι θα έχουμε 2 controllers. Θα χρησιμοποιήσουμε 2 controllers τον POX και Ryu για το πρώτο και το δεύτερο slice αντίστοιχα. Ο POX χρησιμοποιείται συνήθως για έλεγχο δεδομένων και ο Ryu για ήχο και βίντεο.

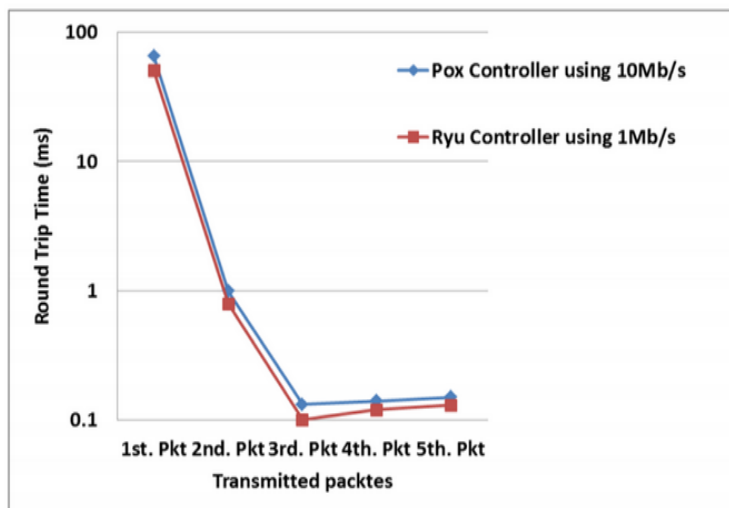
Για το test latency, RTT και jitter θα χρησιμοποιήσουμε 3 διαφορετικά σενάρια. 1 Mbps και 10 Mbps, 1 Mbps και 1 Mbps, 10 Mbps και 1 Mbps αντίστοιχα για τους controllers. Για τον έλεγχο latency και jitter έχει χρησιμοποιηθεί η εντολή ring και το πρόγραμμα D-ITG με το οποίο μπορούμε να μετρήσουμε το μέσο όρο latency και jitter.

Στο παρακάτω σχήμα βλέπουμε την μέτρηση jitter στις 3 τοπολογίες. Βλέπουμε η linear τοπολογία έχει χαμηλότερο jitter και στους 2 controllers.

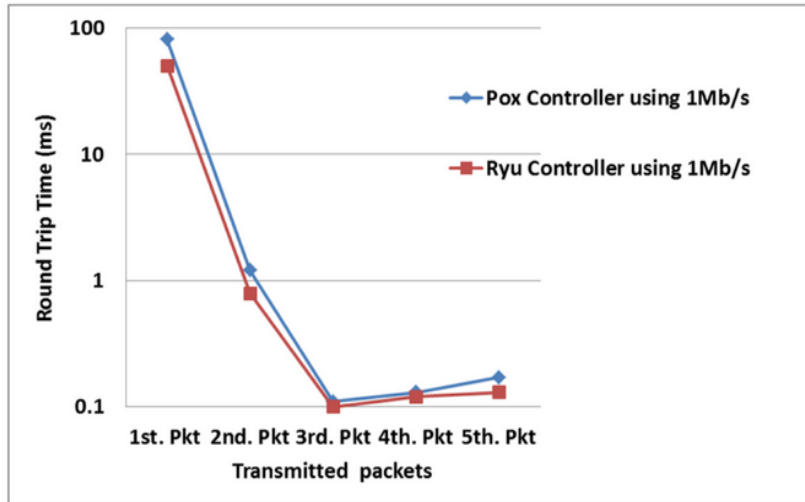


Εικόνα 30: Μέτρηση jitter των 3 τοπολογιών

Στα παρακάτω σχήματα έχει γίνει μέτρηση RTT στην τοπολογία διαμάντι βλέπουμε ότι ο Ryu έχει χαμηλότερο RTT και στις 3 περιπτώσεις bandwidth

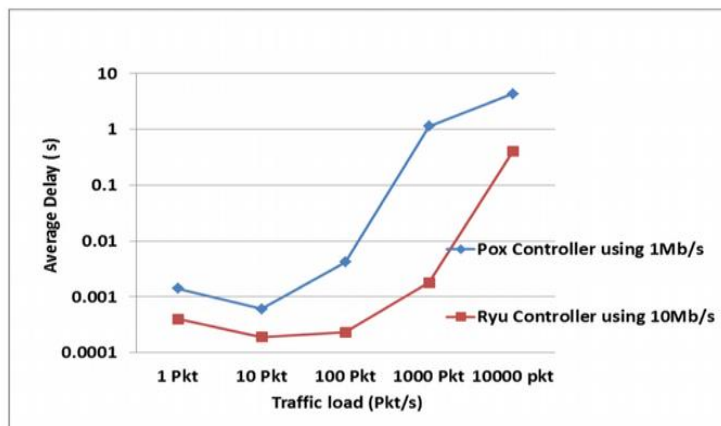


Εικόνα 31: Μέτρηση RTT στην τοπολογία διαμάντι 10mb/s - 1mb/s

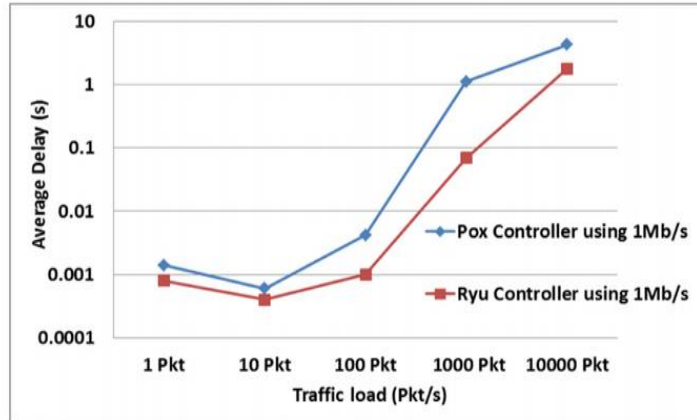


Εικόνα 32: Μέτρηση RTT στην τοπολογία διαμάντι 1mb/s - 1mb/s

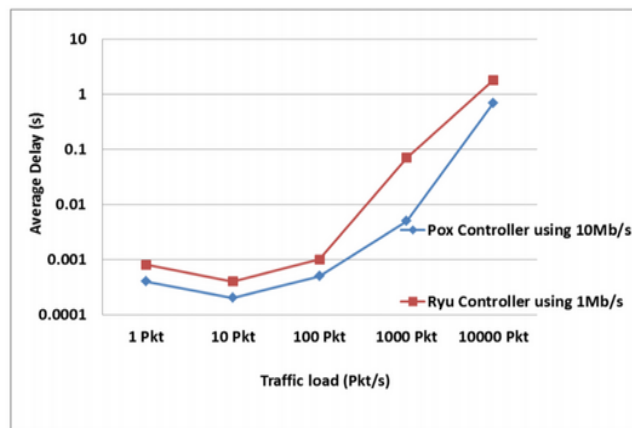
Στα παρακάτω σχήματα βλέπουμε το delay. Ο Ryu έχει το χαμηλότερο delay από το μεσαίο στιγμιότυπο που χρησιμοποιεί 1mbps και στους 2 controllers. Χάνει μόνο όταν ο POX έχει bandwidth 10mbps στο δεξί στιγμιότυπο. Στο αριστερό στιγμιότυπο που ο Ryu έχει 10mbps εκεί κερδίζει κατά πολύ τον POX. Και στις 3 περιπτώσεις bandwidth βλέπουμε ότι όσο περισσότερα πακέτα στείλουμε τόσο μεγαλώνει και το delay και αυτό είναι λογικό γιατί όσο περισσότερο φόρτο εργασίας τόσο μεγαλύτερο και το delay.



Εικόνα 33: Μέτρηση delay στην τοπολογία διαμάντι 1mb/s - 10mb/s

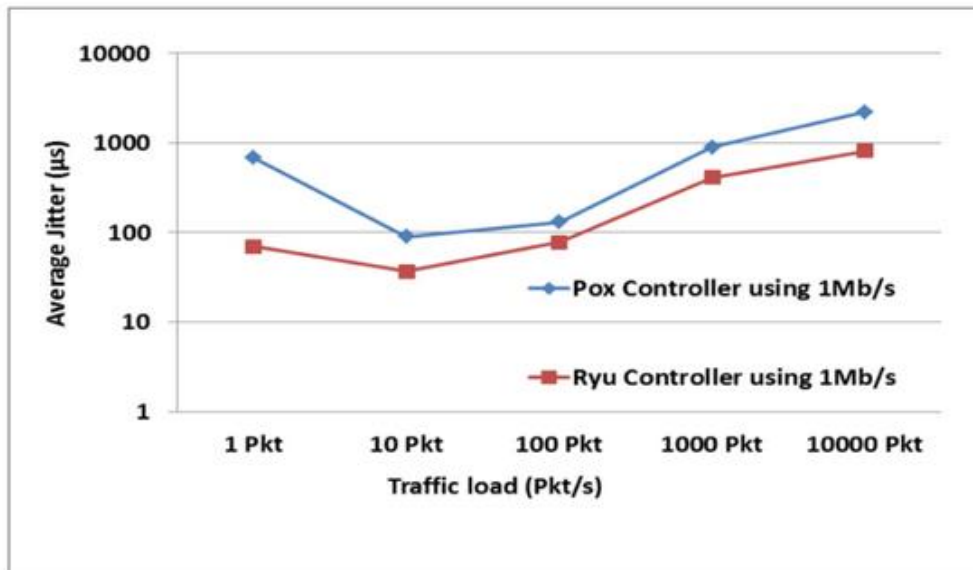


Εικόνα 34: Μέτρηση delay στην τοπολογία διαμάντι 1mb/s - 1mb/s



Εικόνα 35: Μέτρηση delay στην τοπολογία διαμάντι 10mb/s - 1mb/s

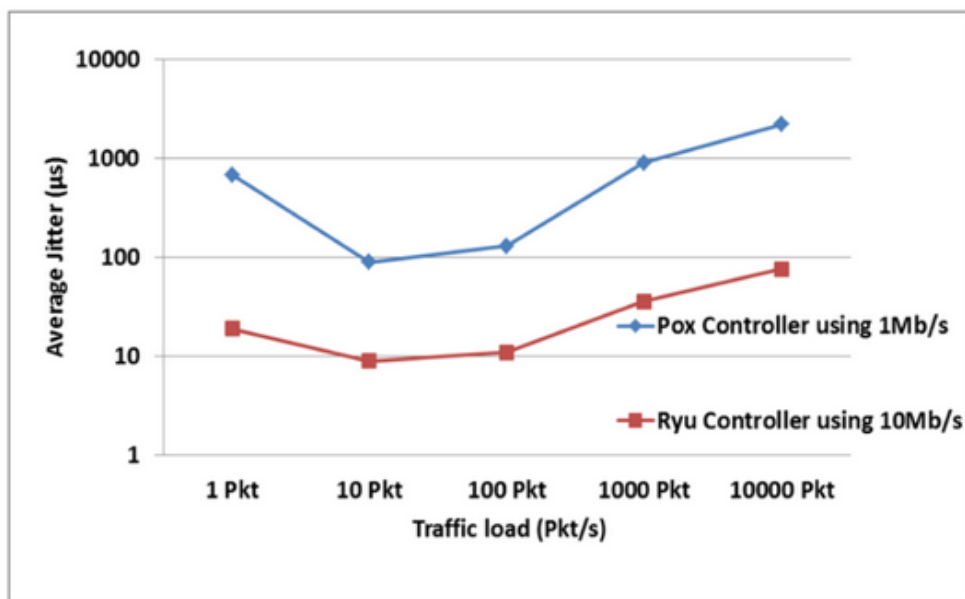
Στα παρακάτω σχήματα συγκρίνουμε το jitter των controllers με όλες τις περιπτώσεις bandwidth. Βλέπουμε ότι ο Ryu έχει το χαμηλότερο jitter που χρησιμοποιεί 1mbps και στους 2 controllers.



Εικόνα 36: Μέτρηση jitter στην τοπολογία διαμάντι 1mb/s - 1mb/s

Χάνει μόνο όταν ο POX έχει bandwidth 10mbps

Στο στο παρακάτω στιγμιότυπο που ο Ryu έχει 10mbps εκεί κερδίζει κατά πολύ τον POX.

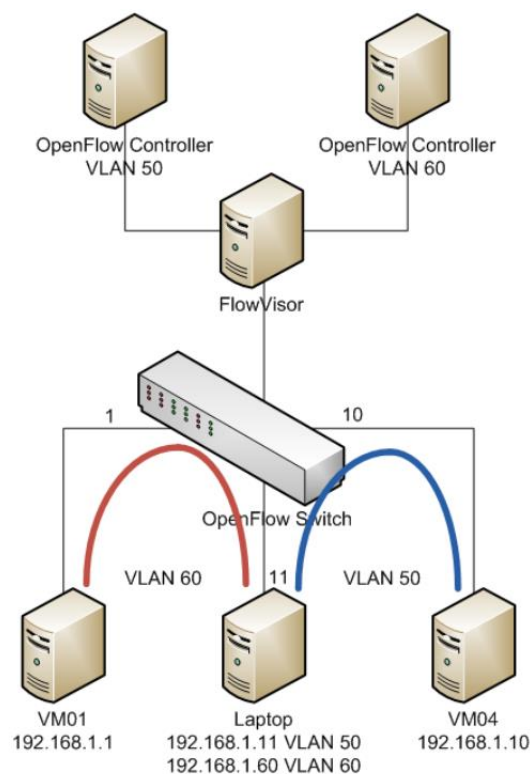


Εικόνα 37: Μέτρηση jitter στην τοπολογία διαμάντι 1mb/s - 10mb/s

Σε όλες τις περιπτώσεις bandwidth βλέπουμε ότι όσο περισσότερα πακέτα στείλουμε τόσο μεγαλώνει και το και αυτό είναι λογικό γιατί όσο περισσότερο φόρτο εργασίας τόσο μεγαλύτερο και το jitter.

4.3.4 Παράδειγμα 4

Σε αυτό το παράδειγμα η τοπολογία χωρίζεται σε 2 slices το πρώτο για τον χρήστη vm01 και το δεύτερο για τον vm04. Θα χρησιμοποιήσουμε την τεχνολογία vlan για την μεταφορά δεδομένων από τους 2 χρήστες που ανήκουν σε 2 διαφορετικά slices στο laptop και αντίστροφα μέσω της πόρτας 11 του switch.



Εικόνα 38: Τοπολογία παραδείγματος 4

Για να γίνει αυτό αντιστοιχούμε την τιμή vlan 60 στο πρώτο slice και την τιμή 50 στο δεύτερο slice. Οποτε όταν ένα πακέτο έρχεται στο switch απο την πόρτα 1 η 10, το switch το σημαδεύει με την κατάλληλη τιμή vlan και το στέλνει στην πόρτα 11. Αντίστροφα όταν το switch δέχεται ένα πακέτο από την πόρτα 11 ψάχνει στο πακέτο την τιμή vlan και ανάλογα την τιμή το στέλνει στην κατάλληλη πόρτα

Οι ροές φαίνονται στο παρακάτω πίνακα.

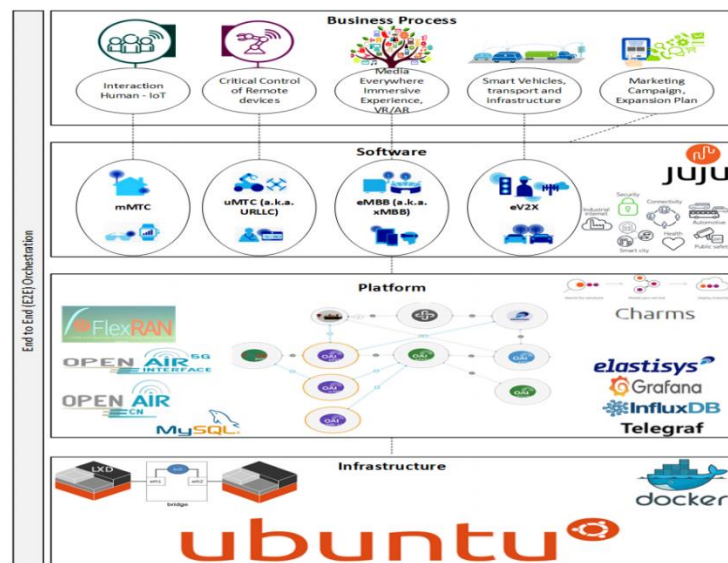
Controller	Match	Action
floodlight2	in_port 11,vlan-id:50	out_port 10
floodlight1	in_port 11,vlan-id:60	out_port 1
floodlight2	in_port 10	set-vlan-id=50 out_port 11
floodlight1	in_port 1	set-vlan-id=60 out_port 11

Εικόνα 39: Πίνακας αντιστοίχισης πακέτων με ενέργεια

4.3.5 Παράδειγμα 5 Αντιμετώπιση Ελαστικότητας

[51] Για να τα πούμε συνοπτικά όπως έχουμε ήδη πει το 5G Slicing γίνεται με την χρήση του SDN και NFV και γίνεται εικονικά σε server σε εικονικές μνήμες (VMs) με τους φυσικούς του πόρους επεξεργαστής, μνήμη, αποθήκευση κτλπ. Όπως έχουμε επίσης είδη πει για το δίκτυο Ραδιοπρόσβασης υλοποιημένο στο νέφος C-RAN ότι αποτελείται από την μονάδα Βασικής Ζώνης BBU και την απομακρυσμένη κεφαλή ραδιοεπικοινωνίας RRH. Τα BBU δείχνουν πόρους στα RRH μέσω του δικτύου μεταφοράς που δεν είναι άλλο από οπτικές ίνες. Όλα αυτά οδηγούν στο Core Network του 5G. Επίσης όλα αυτά εικονικοποιημένα με τα SDN και NFV και τρέχουν σε server.

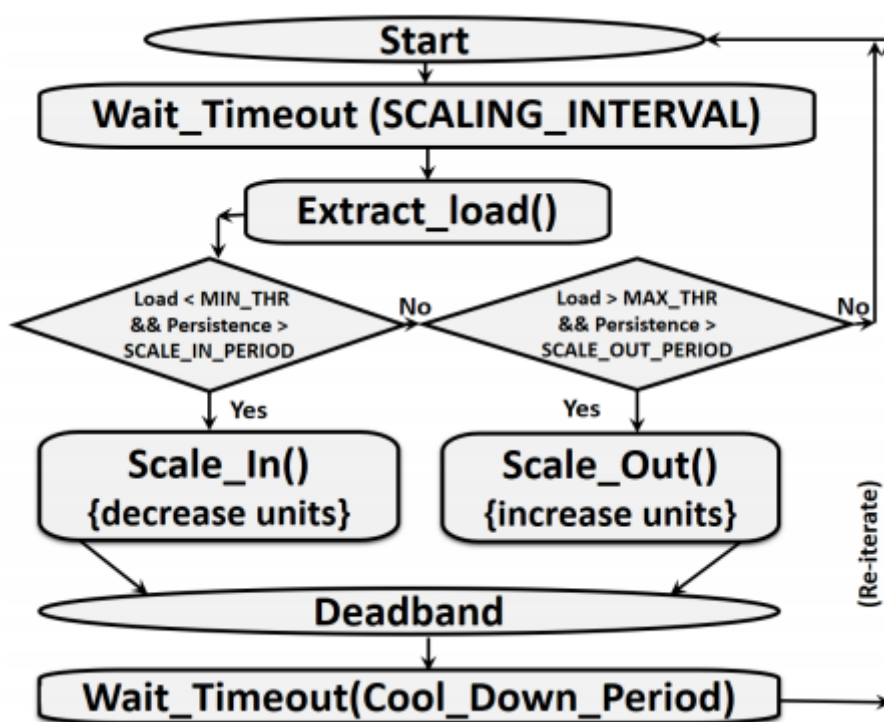
Το θέμα που προκύπτει είναι το θέμα της αποδοτικά χρησιμοποίησης των εικονικών πόρων και την ελαστικότητα τους στα slices. Αρχικά οι VMs χρησιμοποιούν περισσότερους πόρους από ότι τα Containers για να κάνουν την δουλειά τους. Τα container κάνουν παρόμοια και καλύτερη δουλειά με τα VMs όμως έχουν τελείως διαφορετική αρχιτεκτονική από πίσω. Επίσης με τα container μπορούμε να λύσουμε πιο ευκολα το θέμα της ελαστικότητας εφαρμόζοντας έναν αλγόριθμο που κάνει αυτόματα scale out/in πόρων στην μονάδα Βασικής Ζώνης BBU ή εφαρμόζοντας έναν αλγόριθμο εισπνοής και εκπνοής πόρων στο BBU. Τα Containers τρέχουν σε Linux και θα χρειαστεί να γίνει εικονικοποίηση των NFVs που τρέχουν στις VMs σε Containers μέσω των Juju Charms. Όταν γίνει αυτό προκύπτει ένα νέο σχέδιο επίπεδων ενορχήστρωσης που φέρνεται από παρακάτω.



Εικόνα 40: Αρχιτεκτονική ενορχήστρωσης σε επίπεδο στρωμάτων υπηρεσίας

[51] Όπως φαίνεται στο σχήμα γίνεται αντιστοίχιση των υπηρεσιών (πρώτο στρώμα) με τα χαρακτηριστικά (δεύτερο στρώμα) ενός slice. Για παράδειγμα το IoT αντιστοιχίζεται με εξαιρετικά αξιόπιστες και μικρής καθυστέρηση επικοινωνίες εξαιρετικά αξιόπιστες και μικρής καθυστέρηση επικοινωνίες mMTC ανάλογα με την αξιοπιστία και την καθυστέρηση έναντι της πολυπλοκότητας ελέγχου ταυτότητας και των απαιτήσεων ισχύος. Στο τρίτο στρώμα είναι η πλατφόρμα όπου εκεί αναπτύσσονται τα NFVs από το δίκτυο κατάστημα (Juju Charms Store) όπου και ελέγχονται. Στο τελευταίο στρώμα υπάρχουν οι φυσικοί πόροι όπως είναι και στον server.

Όπως είπαμε παραπάνω η αντιμετώπιση της ελαστικότητας γίνεται σε 2 σενάρια, στο σενάριο όπου γίνεται scale out/in και στο σενάριο “εισπνοής και εκπνοής πόρων” μεταξύ των φετών. Στο πρώτο σενάριο λοιπόν έχουμε μια απομακρυσμένη κεφαλή ραδιοεπικοινωνίας (RRH) που ζητάει πολλούς πόρους από το BBU τότε το BBU θα έχει μεγάλο φορτίο load. Αν το load ξεπεράσει ένα κατώφλι πχ 80% θα εκτελεστεί ένας αλγόριθμος αυτόματα όπου θα γίνει scale out και θα φύγουν πόροι από ένα buffer στο BBU με αποτέλεσμα το BBU εφόσον θα έχει περισσότερους πόρους να πέσει το load του και να μπορεί το RRH να εξυπηρετήσει περισσότερο κόσμο ασύρματα. Όταν σταματήσει η ζήτηση από το RRH και πέσει το load BBU κάτω από ένα κατώφλι πχ 20% τότε αυτόματα γίνεται scale in και φεύγουν πόροι από το BBU στο buffer. Στην παρακάτω εικόνα φαίνεται ο αλγόριθμος.



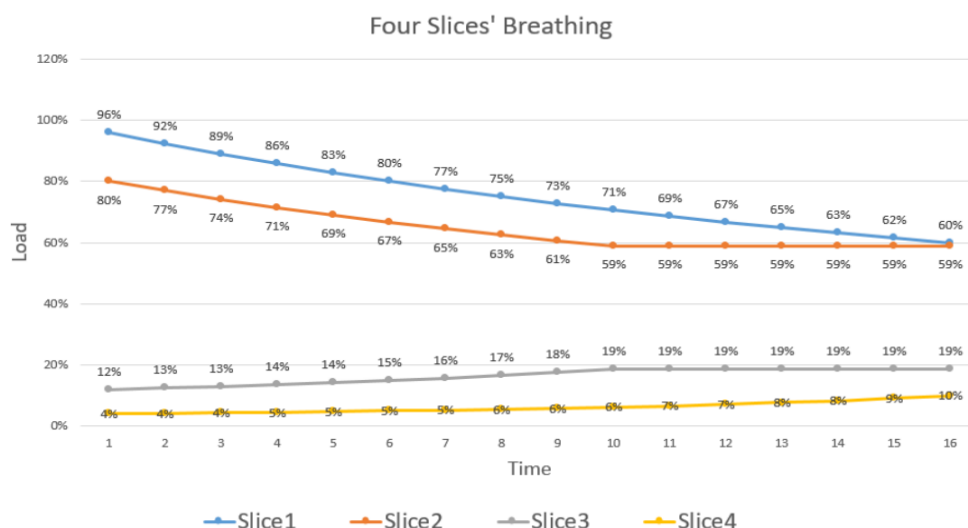
Εικόνα 41: Αλγόριθμος auto scale out/in

Στην παρακάτω εικόνα φέρνεται η εφαρμογή του αλγορίθμου όπου κάνει scale out δίνει πόρους στο BBU και πέφτει το load του.



Εικόνα 42: Αλγόριθμος auto scale out/in

Στο δεύτερο σενάριο είναι να μην γίνει καθόλου scale out/in αλλά εισπονή πόρων άλλου BBU που έχει χαμηλό load και εκπονή πόρων στο BBU που έχει μεγάλο load. Έτσι το αποτέλεσμα θα είναι να χαμηλωθεί το load που ήταν μεγάλο στο BBU που υπάρχει αυξημένη ζήτηση και να αυξηθεί το load στο BBU που είχε χαμηλό load. Όταν όμως όλα τα BBU έχουν αυξημένο load δεν μπορεί να εφαρμοστεί το σενάριο αυτό οπότε το σενάριο 1 που γίνεται scale in/out είναι μονόδρομος. Στην παρακάτω εικόνα φαίνεται το σενάριο 2 όπου τα slice 1 και 2 παίρνουν πόρους από τα slice 3 και 4. Βλέπουμε ότι τα slice 1 και 2 πέφτει το load γιατί παίρνουν πόρους και τα slice 3 και 4 αυξάνεται το load γιατί χάνουν πόρους που ήταν idle.



Εικόνα 43: Αλγόριθμος auto εισπολής/εκπολής.

Και πιο κάτω φαίνεται ο αλγόριθμος του σεναρίου 2 εισπολής εκπολής.

Algorithm 1 Breathe algorithm

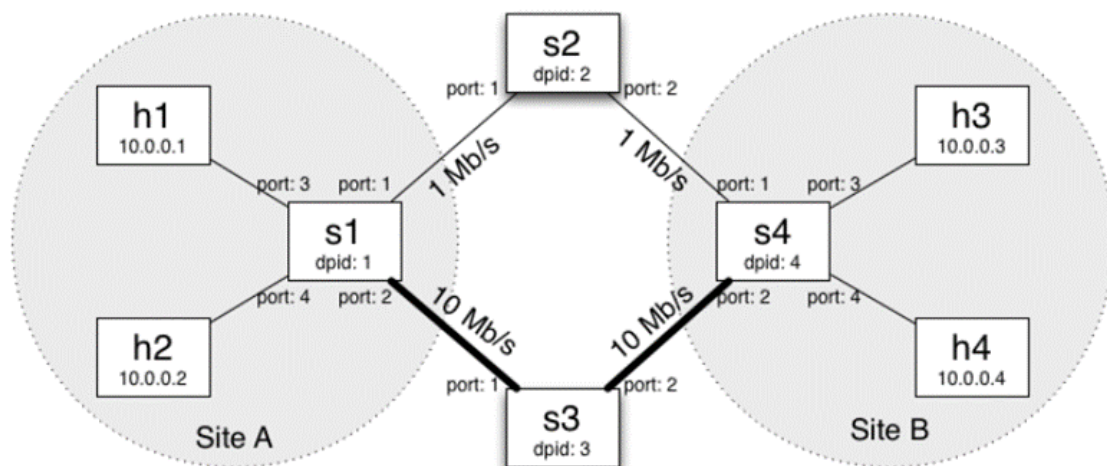
```
1: procedure Inhale-Exhale(slices)
2:   Initialize threshold_h;
3:   while (not all load(slice) <= threshold_h) do
4:     for each load(slice_i) > threshold_h do
5:       slice_j=find_min_load_min_degrad_slice();
6:       portion_i=offload(slice_i);
7:       slice_j=add_load(portion_i);
8:     end for
9:   end while
10: end procedure
```

Εικόνα 44: Αλγόριθμος αυτο εισπνοής/εκπνοής.

5. Πειραματική ενασχόληση

5.1 Παράδειγμα 1 SDN

[46] Στην παρακάτω τοπολογία βλέπουμε 4 χρήστες **h1,h2,h3,h4** και 4 switches **S1,S2,S3,S4**. Για την επικοινωνία S1 και S4 υπάρχουν 2 διαδρομές, οι S1-S2-S4 και S1-S3-S4. Στην πρώτη το bandwidth είναι 1mbps και στο δεύτερο 10mbps.



Εικόνα 45: Τοπολογία παραδείγματος 1

Θα χρησιμοποιήσουμε το flowvisor για να χωρίσουμε την τοπολογία σε 2 κομμάτια με βάση τις πόρτες όπως φαίνεται στο παρακάτω σχήμα.

Έτσι ο h1 θα μπορεί να επικοινωνήσει μόνο με τον h3 και αντίστροφα με bandwidth **1mbps** και ο h2 μόνο με τον h4 και αντίστροφα με bandwidth **10mbps**.

Το παράδειγμα αυτό εκτελέστηκε με το mininet 2.3.0d6 και το openjdk-6-jdk στο λειτουργικό σύστημα Ubuntu 14.04.6 LTS 64bit. Υπήρξαν πολλά προβλήματα ασυμβατότητας των version του mininet, javajdk και Ubuntu με αποτέλεσμα να μην μπορούσαν να εκτελεστούν κάποιες εντολές και να μην μπορεί να τρέξει το παράδειγμα. Μετα από πολύ ψάξιμο και πειραματισμό το παράδειγμα έτρεξε σε αυτές τις versions. Για άλλα παραδείγματα πιο σύνθετα με περισσότερους χρήστες και συσκευές ενδέχεται να χρειαστούν άλλες versions. Τα προβλήματα ασυμβατότητας ίσως έχουν να κάνουν με την μνήμη που χρησιμοποιεί το mininet από το λειτουργικό σύστημα για να υποστηρίξει την τοπολογία και ίσως για κάθε version mininet να χρειαστεί και την κατάλληλη version openjdk. Τα errors έρχονταν με την εντολή fvctl.

[47]Το Mininet είναι ένας emulator δικτύου που δημιουργεί ένα δίκτυο εικονικών κεντρικών υπολογιστών, διακοπών, ελεγκτών και συνδέσμων. Το Mininet εκτελείται σε Linux και υποστηρίζει το OpenFlow και το Software-Defined Networking. Το Mininet χρησιμοποιείται για έρευνα, ανάπτυξη, μάθηση, πρωτοτυπία, τον έλεγχο, τον εντοπισμό σφαλμάτων και οποιεσδήποτε άλλες εργασίες που θα μπορούσαν να επωφεληθούν από την ύπαρξη πλήρους πειραματικού δικτύου σε φορητό υπολογιστή ή άλλο υπολογιστή.

Αφού έχουμε κάνει εγκατάσταση το mininet και το openjdk εκτελούμε αυτές τις τρεις εντολές

- `sudo apt-get install git`
- `sudo apt-get install build-essential`
- `sudo apt-get install ant`

Επιπλέον επειδή οι ελεγκτές τις τοπολογίας είναι αρχιτεκτονικής 32 bit μπορεί να μην τους αναγνωρίζει το σύστημα ως εκτελέσιμα σε αυτή τη περίπτωση κάνουμε:

- `sudo apt-get update`
- `sudo apt-get install libc6:i386 libncurses5:i386 libstdc++6:i386`
- `sudo dpkg --add-architecture i386`

Μετά κάνουμε clone τα αρχεία από το git:

- `git clone git://github.com/OPENNETWORKINGLAB/flowvisor.git`

Στη συνέχεια αφού μετάβουμε στο φάκελο του FlowVisor (`cd flowvisor`) κάνουμε:

- `make`

Μετά δημιουργούμε τον user:

- `sudo adduser flowvisor`

Και ενώ αφού είμαστε ακόμα στο φάκελο του FlowVisor και με δικαιώματα διαχειριστή εκτελούμε:

- `sudo make fvuser= flowvisor fvgroup= flowvisor install`

Μετα συνεχίζουμε να εκτελούμε τις εντολές που γράφονται στο [46]. Εκτελούμε την εντολή:

- `sudo mn --custom ~/onstutorial/flowvisor_scripts/flowvisor_topo.py --topo fvtopo --link tc --controller remote --mac --arp`

για να ξεκινήσει η τοπολογία (`flowvisor_topo.py`) η οποία έχει κατεβεί όταν κάναμε `clone` τα αρχεία. Συνεχίζουμε με διάφορες εντολές του [46] για το ξεκίνημα τον έλεγχο του `flowvisor` και της τοπολογίας όπως:

- `sudo -u flowvisor fvconfig generate /etc/flowvisor/config.json`
- `sudo /etc/init.d/flowvisor start`
- `fvctl -f /dev/null set-config --enable-topo-ctrl`
- `sudo /etc/init.d/flowvisor restart`
- `fvctl -f /dev/null get-config`

Θα πρέπει να βγει κάτι τέτοιο.

```
$ fvctl -f /dev/null get-config
{
  "enable-topo-ctrl": true,
  "flood-perm": {
    "dpid": "all",
    "slice-name": "fvadmin"
  },
  "flow-stats-cache": 30,
  "flowmod-limit": {
    "fvadmin": {
      "00:00:00:00:00:00:01": -1,
      "00:00:00:00:00:00:02": -1,
      "00:00:00:00:00:00:03": -1,
      "00:00:00:00:00:00:04": -1,
      "any": null
    }
  },
  "stats-desc": false,
  "track-flows": false
}
```

Εικόνα 46: Αποτελέσματα 1

- `fvctl -f /dev/null list-slices` (λίστα με slices) θα πρέπει να βγει κάτι τέτοιο:

```
$ fvctl -f /dev/null list-slices
Configured slices:
fvadmin          --> enabled
```

Εικόνα 47: Αποτελέσματα 2

- `fvctl -f /dev/null list-flowspace` (λίστα με flowspaces) θα πρέπει να βγει κάτι τέτοιο:

```
$ fvctl -f /dev/null list-flowspace
Configured Flow entries:
None
```

Εικόνα 48: Αποτελέσματα 3

- `fvctl -f /dev/null list-datapaths` (θα πρέπει να βγει κάτι τέτοιο)

```
$ fvctl -f /dev/null list-datapaths
Connected switches:
 1 : 00:00:00:00:00:00:00:01
 2 : 00:00:00:00:00:00:00:02
 3 : 00:00:00:00:00:00:00:03
 4 : 00:00:00:00:00:00:00:04
```

Εικόνα 49: Αποτελέσματα 4

- `fvctl -f /dev/null list-links` θα πρέπει να βγει κάτι τέτοιο.

```
$ fvctl -f /dev/null list-links
[
  {
    "dstDPID": "00:00:00:00:00:00:00:01",
    "dstPort": "1",
    "srcDPID": "00:00:00:00:00:00:00:02",
    "srcPort": "1"
  },
  {
    "dstDPID": "00:00:00:00:00:00:00:02",
    "dstPort": "1",
    "srcDPID": "00:00:00:00:00:00:00:01",
    "srcPort": "1"
  },
  {
    "dstDPID": "00:00:00:00:00:00:00:04",
    "dstPort": "1",
    "srcDPID": "00:00:00:00:00:00:00:02",
    "srcPort": "2"
  },
  {
    "dstDPID": "00:00:00:00:00:00:00:03",
    "dstPort": "2",
    "srcDPID": "00:00:00:00:00:00:00:04",
    "srcPort": "2"
  },
  {
    "dstDPID": "00:00:00:00:00:00:00:01",
    "dstPort": "2",
    "srcDPID": "00:00:00:00:00:00:00:03",
    "srcPort": "1"
  },
  {
    "dstDPID": "00:00:00:00:00:00:00:04",
    "dstPort": "2",
    "srcDPID": "00:00:00:00:00:00:00:03",
    "srcPort": "2"
  },
  {
    "dstDPID": "00:00:00:00:00:00:00:02",
    "dstPort": "2",
    "srcDPID": "00:00:00:00:00:00:00:04",
    "srcPort": "1"
  },
  {
    "dstDPID": "00:00:00:00:00:00:00:03",
    "dstPort": "1",
    "srcDPID": "00:00:00:00:00:00:00:01",
    "srcPort": "2"
  }
]
```

Εικόνα 50: Αποτελέσματα 5

Αφού όλα είναι οκ προχωράμε στο configuration του παραδείγματος. Πρώτα εκτελούμε την εντολή:

- `fvctl -f /dev/null add-slice upper tcp:localhost:10001 admin@upperslice`

Για να φτιάξουμε το πάνω slice με έναν controller που ακούει στην `tcp:localhost:10001` με email `admin@upperslice` σε περίπτωση που συμβεί κάτι με το slice να γίνει επικοινωνία με αυτό το email (Τίποτα το ιδιαίτερο) Αν ζητηθεί κωδικός τον αφήνουμε κενό δηλαδή πατάμε `enter`.

Μετα φτιάχνουμε το κάτω slice με την εντολή:

- `fvctl -f /dev/null add-slice lower tcp:localhost:10002 admin@lowerslice`

Μετα φτιάχνουμε τα `flowspaces`. Τα `flowspaces` συσχετίζουν τα πακέτα ενός συγκεκριμένου τύπου στο δίκτυο με συγκεκριμένα `slices`. Η μορφή της εντολής για να εισάγουμε ένα `flowspace` είναι:

```
●fvctl add-flowspace [options] <flowspace-name> <dpid> <priority> <match>
<slice-perm>
```

Το `flowspace-name` είναι το όνομα του `flowspace`, το `dpid` είναι το switch, το `priority` η προτεραιότητα του `flowspaces`, το `match` είναι το interface του switch, το `slice-perm` είναι τα δικαιώματα που έχει το slice (`DELEGATE=1`, `READ=2`, `WRITE=4`)

Για το switch 1 έχουμε τις εξής εντολές:

- `fvctl -f /dev/null add-flowspace dpid1-port1 1 1 in_port=1 upper=7`
- `fvctl -f /dev/null add-flowspace dpid1-port3 1 1 in_port=3 upper=7`

Για το switch s2 επειδη ανήκει ολόκληρο στο slice upper για να μην εκτελούμε μια εντολή για κάθε interface του μπορούμε να χρησιμοποιήσουμε το `any` αντί για το `in_port`.

- `fvctl -f /dev/null add-flowspace dpid2 2 1 any upper=7`

Για το switch 4 έχουμε:

- `fvctl -f /dev/null add-flowspace dpid4-port1 4 1 in_port=1 upper=7`
- `fvctl -f /dev/null add-flowspace dpid4-port3 4 1 in_port=3 upper=7`

Τελειώσαμε για το πάνω slice. Τώρα θα εκτελέσουμε αυτές τις εντολές για το lower slice.

- `fvctl -f /dev/null add-flowspace dpid1-port2 1 1 in_port=2 lower=7`
- `fvctl -f /dev/null add-flowspace dpid1-port4 1 1 in_port=4 lower=7`
- `fvctl -f /dev/null add-flowspace dpid3 3 1 any lower=7`
- `fvctl -f /dev/null add-flowspace dpid4-port2 4 1 in_port=2 lower=7`
- `fvctl -f /dev/null add-flowspace dpid4-port4 4 1 in_port=4 lower=7`

Ελέγχουμε τα flowspace:

- `fvctl -f /dev/null list-flowspace`

Μετα εκτελούμε αυτές τις τελευταίες εντολές σε 2 νέα τερματικά

- `cd ~/onstutorial/beacon-fvexercise-controller1`
- `./beacon`

- `cd ~/onstutorial/beacon-fvexercise-controller2`
- `./beacon`

Για να βρούμε τους controllers και να κανουμε beacon παμε στο link [50] γιατί δεν υπάρχουν στο λειτουργικό σύστημα. Προσέχουμε στο path ότι το όνομα του φακέλου δεν είναι onstutorial αλλά onstutorial-master σύμφωνα με το link.

Μετα από αυτά μπορούμε να κανουμε διάφορα ping από το mininet για να δούμε αμα λειτουργεί το παράδειγμα.

- `mininet> h1 ping -c1 h3`
- `mininet> h1 ping -c1 -W1 h2`
- `mininet> h1 ping -c1 -W1 h4`

- `mininet> h2 ping -c1 h4`
- `mininet> h2 ping -c1 -W1 h1`
- `mininet> h2 ping -c1 -W1 h3`

Στο πρώτο στιγμιότυπο βλέπουμε την επιτυχή επικοινωνία μεταξύ h1 και h3. Ενώ στα αλλα 2 στιγμιότυπα σωστά την μη επικοινωνία μεταξύ h1 με h2 h4.

```
mininet> h1 ping -c1 h3
PING 10.0.0.3 (10.0.0.3) 56(84) bytes of data.
64 bytes from 10.0.0.3: icmp_seq=1 ttl=64 time=11.2 ms

--- 10.0.0.3 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 11.210/11.210/11.210/0.000 ms
```

Εικόνα 51: Αποτελέσματα 6 ping h1-h3

```
mininet> h1 ping -c1 -w1 h2  
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.  
  
--- 10.0.0.2 ping statistics ---  
1 packets transmitted, 0 received, 100% packet loss, time 0ms
```

Εικόνα 52: Αποτελέσματα 7 ping h1-h2

```
mininet> h1 ping -c1 -w1 h4  
PING 10.0.0.4 (10.0.0.4) 56(84) bytes of data.  
  
--- 10.0.0.4 ping statistics ---  
2 packets transmitted, 0 received, 100% packet loss, time 999ms
```

Εικόνα 53: Αποτελέσματα 8 ping h1-h4

Στο πρώτο στιγμιότυπο βλέπουμε την επιτυχή επικοινωνία μεταξύ h2 και h4. Ενώ στα άλλα 2 στιγμιότυπα σωστά την μη επικοινωνία μεταξύ h2 με h1 h3.

```
mininet> h2 ping -c1 h4  
PING 10.0.0.4 (10.0.0.4) 56(84) bytes of data.  
64 bytes from 10.0.0.4: icmp_seq=1 ttl=64 time=10.3 ms  
  
--- 10.0.0.4 ping statistics ---  
1 packets transmitted, 1 received, 0% packet loss, time 0ms  
rtt min/avg/max/mdev = 10.305/10.305/10.305/0.000 ms
```

Εικόνα 54: Αποτελέσματα 9 ping h2-h4

```
mininet> h2 ping -c1 -w1 h1  
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.  
  
--- 10.0.0.1 ping statistics ---  
1 packets transmitted, 0 received, 100% packet loss, time 0ms
```

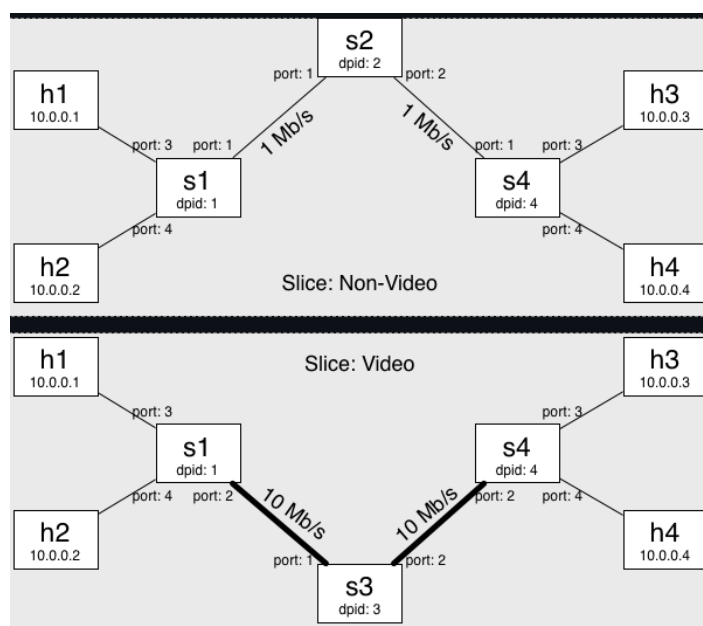
Εικόνα 55: Αποτελέσματα 10 ping h2-h1

```
mininet> h2 ping -c1 -w1 h3  
PING 10.0.0.3 (10.0.0.3) 56(84) bytes of data.  
  
--- 10.0.0.3 ping statistics ---  
1 packets transmitted, 0 received, 100% packet loss, time 0ms
```

Εικόνα 56: Αποτελέσματα 11 ping h2-h3

5.2 Παράδειγμα 2 SDN

Σε αυτό το παράδειγμα έχουμε την ίδια τοπολογία με το παράδειγμα 1 όμως τα slices θα δημιουργηθούν με βάση την εφαρμογή. Παρατηρούμε τις 2 διαδρομές S1-S2-S4 και S1-S3-S4 με bandwidth 1mbps και 10mbps αντίστοιχα. Η πρώτη διαδρομή θέλουμε να χρησιμοποιείται για βίντεο και η δεύτερη διαδρομή για οτιδήποτε άλλο.



Εικόνα 57: Τοπολογία παραδείγματος 2

Στο παράδειγμα αυτό δεν έχουμε σκοπό να αποκόψουμε τους χρήστες όπως κάναμε στο πρώτο παράδειγμα. Όλοι οι χρήστες θα μπορούν να επικοινωνήσουν μεταξύ τους απλά θα γίνει ένας διαχωρισμός στην επικοινωνία τους σε βίντεο και οτιδήποτε άλλο όπου αυτά τα 2 θα μεταφέρονται σε 2 διαφορετικές διαδρομές ξεχωριστά το καθένα με το κατάλληλο bandwidth. Έτσι θα δημιουργηθούν 2 slices με βάση την εφαρμογή. Αυτό θα γίνει ελέγχοντας στα switches s1 και s4 τα πακέτα που έρχονται από τους χρήστες τους και ανάλογα το πακέτο θα σταλεί στην κατάλληλη πόρτα που αντιστοιχεί στην σωστή διαδρομή. Οποτε τα UDP πακέτα με πόρτα 9999 αντιστοιχούν σε βίντεο και τα άλλα πακέτα στο “οτιδήποτε άλλο”.

Για το configuration του παραδείγματος 2 έχουμε:

Φτιάχνουμε τα 2 slices:

- `fvctl -f /dev/null add-slice video tcp:localhost:10001 admin@videoslice`
- `fvctl -f /dev/null add-slice non-video tcp:localhost:10002 admin@nonvideoslice`
-

Ελέγχουμε τα 2 slices:

- `fvctl -f /dev/null list-slices`

Και από εδώ και πέρα προσθέτουμε τα εξωτερικά flowspaces βάζοντας μεγαλύτερη προτεραιότητα στα πακέτα του video καθώς υπάρχουν πακέτα που γίνονται match και από τα 2 slices.

Για το interface 3 του s1 έχουμε:

- `fvctl -f /dev/null add-flowspace dpid1-port3-video-src 1 100 in_port=3,dl_type=0x0800,nw_proto=6,tp_src=9999 video=7`
- `fvctl -f /dev/null add-flowspace dpid1-port3-video-dst 1 100 in_port=3,dl_type=0x0800,nw_proto=6,tp_dst=9999 video=7`
- `fvctl -f /dev/null add-flowspace dpid1-port3-non-video 1 1 in_port=3 non-video=7`

Για το interface 4 του s1 έχουμε:

- `fvctl -f /dev/null add-flowspace dpid1-port4-video-src 1 100 in_port=4,dl_type=0x0800,nw_proto=6,tp_src=9999 video=7`
- `fvctl -f /dev/null add-flowspace dpid1-port4-video-dst 1 100 in_port=4,dl_type=0x0800,nw_proto=6,tp_dst=9999 video=7`
- `fvctl -f /dev/null add-flowspace dpid1-port4-non-video 1 1 in_port=4 non-video=7`

Για το interface 3 του s4 έχουμε:

- `fvctl -f /dev/null add-flowspace dpid4-port3-video-src 4 100 in_port=3,dl_type=0x0800,nw_proto=6,tp_src=9999 video=7`
- `fvctl -f /dev/null add-flowspace dpid4-port3-video-dst 4 100 in_port=3,dl_type=0x0800,nw_proto=6,tp_dst=9999 video=7`
- `fvctl -f /dev/null add-flowspace dpid4-port3-non-video 4 1 in_port=3 non-video=7`

Για το interface 4 του s4 έχουμε:

- `fvctl -f /dev/null add-flowspace dpid4-port4-video-src 4 100 in_port=4,dl_type=0x0800,nw_proto=6,tp_src=9999 video=7`
- `fvctl -f /dev/null add-flowspace dpid4-port4-video-dst 4 100 in_port=4,dl_type=0x0800,nw_proto=6,tp_dst=9999 video=7`
- `fvctl -f /dev/null add-flowspace dpid4-port4-non-video 4 1 in_port=4 non-video=7`

Και τώρα πάμε στα εσωτερικά interfaces των switches.

Για το interface 2 του s1 έχουμε:

- `fvctl -f /dev/null add-flowspace dpid1-port2-video 1 100 in_port=2 video=7`

Για όλα τα interfaces του s3 έχουμε:

- `fvctl -f /dev/null add-flowspace dpid3-video 3 100 any video=7`

Για το interface 2 του s4 έχουμε:

- `fvctl -f /dev/null add-flowspace dpid4-port2-video 4 100 in_port=2 video=7`

Για το interface 1 του s1 έχουμε:

- `fvctl -f /dev/null add-flowspace dpid1-port1-non-video 1 1 in_port=1 non-video=7`

Για όλα τα interfaces του s2 έχουμε:

- `fvctl -f /dev/null add-flowspace dpid2-non-video 2 1 any non-video=7`

Για το interface 1 του s4 έχουμε:

- `fvctl -f /dev/null add-flowspace dpid4-port1-non-video 4 1 in_port=1 non-video=7`

Ελέγχουμε ότι υπάρχουν 18 flowspaces που μόλις βάλαμε.

- `fvctl -f /dev/null list-flowspace`

Τρέχουμε τους 2 controllers σε 2 διαφορετικά τερματικά περιμένοντας λίγα δευτερόλεπτα να συνδεθούν ο καθένας στο slice του. Όπως και στο παράδειγμα 1 έτσι και εδώ οι controllers μάλλον δεν υπάρχουν στο λειτουργικό σύστημα οπότε πάμε στο link [50] προσέχοντας στο path ότι το όνομα του φακέλου δεν είναι onstutorial αλλά onstutorial-master σύμφωνα με το link.

- `cd ~/onstutorial/beacon-fvexercise-controller1`
- `./beacon`
- `cd ~/onstutorial/beacon-fvexercise-controller2`
- `./beacon`

Κάνοντας pingall στο mininet θα δημιουργηθούν ICMP πακέτα που αντιστοιχούν στο slice που δεν είναι για βίντεο. Στο παρακάτω σχήμα βλέπουμε ότι όλοι η χρήστες μπορούν να επικοινωνήσουν μεταξύ τους. Και είναι λογικό γιατί δεν χωρίσαμε την τοπολογία με βάση

τα interfaces, δηλαδή δεν σπάσαμε την τοπολογία. Μπορούν όλοι να επικοινωνήσουν απλά το μονοπάτι θα διαλέγετε με βάση την πόρτα των πακέτων.

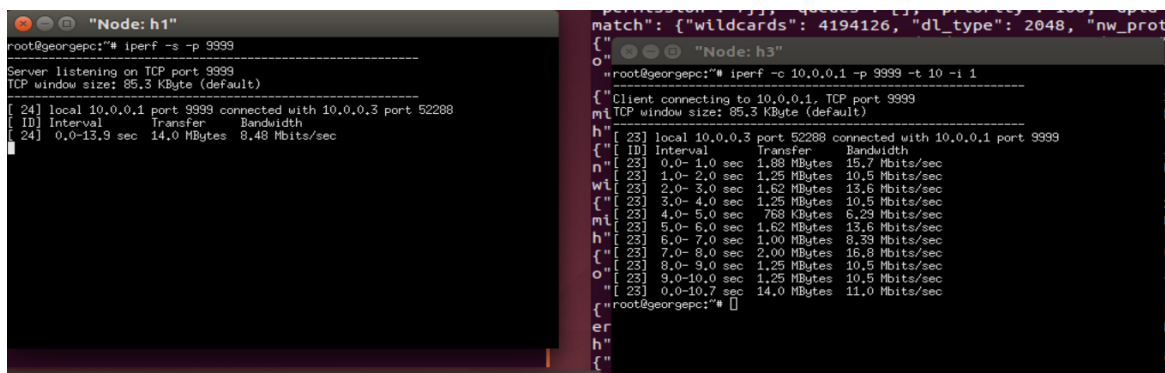
```
mininet> pingall
*** Ping: testing ping reachability
h1 -> h2 h3 h4
h2 -> h1 h3 h4
h3 -> h1 h2 h4
h4 -> h1 h2 h3
*** Results: 0% dropped (12/12 received)
```

Εικόνα 58: Έλεγχος λειτουργίας παραδείγματος 2

Τώρα όσον αφορά το βίντεο χρησιμοποιήσουμε την εντολή iperf για να μετρήσουμε το bandwidth. Θα στείλουμε πακέτα βίντεο από τον h1 στον h3 με 10mbps UDP κυκλοφορία και προορισμό πόρτα 9999. Αυτό σημαίνει ότι τα πακέτα αυτά θα πρέπει να περάσουν από την πρώτη διαδρομή δηλαδή από το πρώτο slice.

- Xterm h1 h3
- Iperf -s -u -p 9999 -b 10M (Για τον receiver)
- Iperf -c 10.0.0.1 -p 9999 -t 10 -i 1 (Για τον sender)

Σε αυτό το στιγμιότυπο ο αποδέκτης είναι ο h1(server) και ο h3 ο αποστολέας. Βλέπουμε ότι το bandwidth είναι 8,48Mbps που σημαίνει ότι τα πακέτα έχουν περάσει από την διαδρομή S1-S3-S4 10Mbps



The image shows two terminal windows side-by-side. The left window is titled "Node: h1" and shows the server side of an iperf test. The right window is titled "Node: h3" and shows the client side of the same test. Both windows display connection details and a table of performance metrics over time.

```
root@georgepc1~# iperf -s -p 9999
Server listening on TCP port 9999
TCP window size: 85.3 KByte (default)
[ 24] local 10.0.0.1 port 9999 connected with 10.0.0.3 port 52288
[ ID] Interval      Transfer      Bandwidth
[ 24] 0.0-15.9 sec  14.0 MBytes  8.48 Mbits/sec

root@georgepc1~# iperf -c 10.0.0.1 -p 9999 -t 10 -i 1
Client connecting to 10.0.0.1, TCP port 9999
TCP window size: 85.3 KByte (default)
[ ID] Interval      Transfer      Bandwidth
[ 23] 0.0- 1.0 sec  1.88 MBytes  15.7 Mbits/sec
[ 23] 1.0- 2.0 sec  1.25 MBytes  10.5 Mbits/sec
[ 23] 2.0- 3.0 sec  1.62 MBytes  13.6 Mbits/sec
[ 23] 3.0- 4.0 sec  1.25 MBytes  10.5 Mbits/sec
[ 23] 4.0- 5.0 sec  758 KBytes   6.29 Mbits/sec
[ 23] 5.0- 6.0 sec  1.62 MBytes  13.6 Mbits/sec
[ 23] 6.0- 7.0 sec  1.00 MBytes  8.39 Mbits/sec
[ 23] 7.0- 8.0 sec  2.00 MBytes  16.8 Mbits/sec
[ 23] 8.0- 9.0 sec  1.25 MBytes  10.5 Mbits/sec
[ 23] 9.0-10.0 sec  1.25 MBytes  10.5 Mbits/sec
[ 23] 0.0-10.7 sec  14.0 MBytes  11.0 Mbits/sec
```

Εικόνα 59: Έλεγχος λειτουργίας παραδείγματος

Σε αυτό το στιγμιότυπο ο αποδέκτης είναι ο h1(server) και ο h4 ο αποστολέας. Βλέπουμε ότι το bandwidth είναι 8,41Mbps που σημαίνει ότι τα πακέτα έχουν περάσει από την

διαδρομή S1-S3-S4 10Mbps. Σε σχέση με το προηγούμενο παράδειγμα(1) αυτοί οι χρήστες δεν μπορούσαν να επικοινωνήσουν που σημαίνει ότι με αυτό μαζί με το pingall είναι απόδειξη ότι το network slicing λειτουργεί σωστά.

```

"Node: h1"
root@georgepc:~# iperf -s -p 9999
Server listening on TCP port 9999
TCP window size: 85.3 KByte (default)

[ 24] local 10.0.0.1 port 9999 connected with 10.0.0.4 port 47538
[ ID] Interval      Transfer     Bandwidth
[ 24] 0.0-12.7 sec  12.8 MBytes  8.41 Mbits/sec

"Node: h4"
root@georgepc:~# iperf -s -p 9999
Server listening on TCP port 9999
TCP window size: 85.3 KByte (default)

root@georgepc:~# iperf -c 10.0.0.1 -p 9999 -t 10 -i 1
Client connecting to 10.0.0.1, TCP port 9999
TCP window size: 85.3 KByte (default)

[ 23] local 10.0.0.4 port 47538 connected with 10.0.0.1 port 9999
[ ID] Interval      Transfer     Bandwidth
[ 23] 0.0- 1.0 sec  1.62 MBytes  13.6 Mbits/sec
[ 23] 1.0- 2.0 sec  1.12 MBytes  9.44 Mbits/sec
[ 23] 2.0- 3.0 sec  1.50 MBytes  12.6 Mbits/sec
[ 23] 3.0- 4.0 sec  512 KBytes  4.19 Mbits/sec
[ 23] 4.0- 5.0 sec  1.50 MBytes  12.6 Mbits/sec
[ 23] 5.0- 6.0 sec  640 KBytes  5.24 Mbits/sec
[ 23] 6.0- 7.0 sec  1.88 MBytes  15.7 Mbits/sec
[ 23] 7.0- 8.0 sec  1.88 MBytes  15.7 Mbits/sec
[ 23] 8.0- 9.0 sec  1.00 MBytes  8.39 Mbits/sec
[ 23] 9.0-10.0 sec  1.00 MBytes  8.39 Mbits/sec
[ 23] 0.0-10.3 sec  12.8 MBytes  9.83 Mbits/sec
root@georgepc:~#
  
```

Εικόνα 60: Έλεγχος λειτουργίας παραδείγματος 2

Για non video κυκλοφορία πατάμε στο mininet> Xterm h2 h4 και στον χρήστη h2 που είναι ο server γράφουμε iperf -s -p 8888. Η πόρτα είναι 8888 και όχι 9999 οπότε θα ακολουθήσει το μονοπάτι s1-s2-s4 που είναι το μονοπάτι του 1mbrs. Και όντως όπως φαίνεται στο παρακάτω στιγμιότυπο το bandwidth είναι 915kbrs κατά μέσο όρο περίπου 1mbrs.

```

"Node: h2"
root@georgepc:~# iperf -s -p 8888
Server listening on TCP port 8888
TCP window size: 85.3 KByte (default)

[ 24] local 10.0.0.2 port 8888 connected with 10.0.0.4 port 58724
[ ID] Interval      Transfer     Bandwidth
[ 24] 0.0-22.9 sec  2.50 MBytes  915 Kbits/sec

"Node: h4"
root@georgepc:~# iperf -c 10.0.0.2 -p 8888 -t 10 -i 1
Client connecting to 10.0.0.2, TCP port 8888
TCP window size: 85.3 KByte (default)

[ 23] local 10.0.0.4 port 58724 connected with 10.0.0.2 port 8888
[ ID] Interval      Transfer     Bandwidth
[ 23] 0.0- 1.0 sec   324 KBytes  2.15 Mbits/sec
[ 23] 1.0- 2.0 sec   128 KBytes  1.05 Mbits/sec
[ 23] 2.0- 3.0 sec    0.00 Bytes  0.00 bits/sec
[ 23] 3.0- 4.0 sec   256 KBytes  2.10 Mbits/sec
[ 23] 4.0- 5.0 sec   128 KBytes  1.05 Mbits/sec
[ 23] 5.0- 6.0 sec   256 KBytes  2.10 Mbits/sec
[ 23] 6.0- 7.0 sec   384 KBytes  3.15 Mbits/sec
[ 23] 7.0- 8.0 sec   384 KBytes  3.15 Mbits/sec
[ 23] 8.0- 9.0 sec    0.00 Bytes  0.00 bits/sec
[ 23] 9.0-10.0 sec   512 KBytes  4.19 Mbits/sec
[ 23] 0.0-10.8 sec  2.50 MBytes  1.34 Mbits/sec
root@georgepc:~#
  
```

Εικόνα 61: Έλεγχος λειτουργίας παραδείγματος 2

Ίδια και με τους χρήστες h2-h3.

```

"Node: h2"
root@georgepc:~# iperf -s -p 8888
Server listening on TCP port 8888
TCP window size: 85.3 KByte (default)

[ 24] local 10.0.0.2 port 8888 connected with 10.0.0.3 port 40208
[ ID] Interval      Transfer     Bandwidth
[ 24] 0.0-24.1 sec  2.75 MBytes  355 Kbits/sec

"Node: h3"
root@georgepc:~# iperf -c 10.0.0.2 -p 8888 -t 10 -i 1
Client connecting to 10.0.0.2, TCP port 8888
TCP window size: 85.3 KByte (default)

[ 23] local 10.0.0.3 port 40208 connected with 10.0.0.2 port 8888
[ ID] Interval      Transfer     Bandwidth
[ 23] 0.0- 1.0 sec   384 KBytes  3.15 Mbits/sec
[ 23] 1.0- 2.0 sec   128 KBytes  1.05 Mbits/sec
[ 23] 2.0- 3.0 sec   128 KBytes  1.05 Mbits/sec
[ 23] 3.0- 4.0 sec   256 KBytes  2.10 Mbits/sec
[ 23] 4.0- 5.0 sec   128 KBytes  1.05 Mbits/sec
[ 23] 5.0- 6.0 sec   256 KBytes  2.10 Mbits/sec
[ 23] 6.0- 7.0 sec   384 KBytes  3.15 Mbits/sec
[ 23] 7.0- 8.0 sec   384 KBytes  3.15 Mbits/sec
[ 23] 8.0- 9.0 sec   640 KBytes  5.24 Mbits/sec
[ 23] 9.0-10.0 sec   0.00 Bytes  0.00 bits/sec
[ 23] 0.0-10.7 sec  2.75 MBytes  2.17 Mbits/sec
root@georgepc:~#
  
```

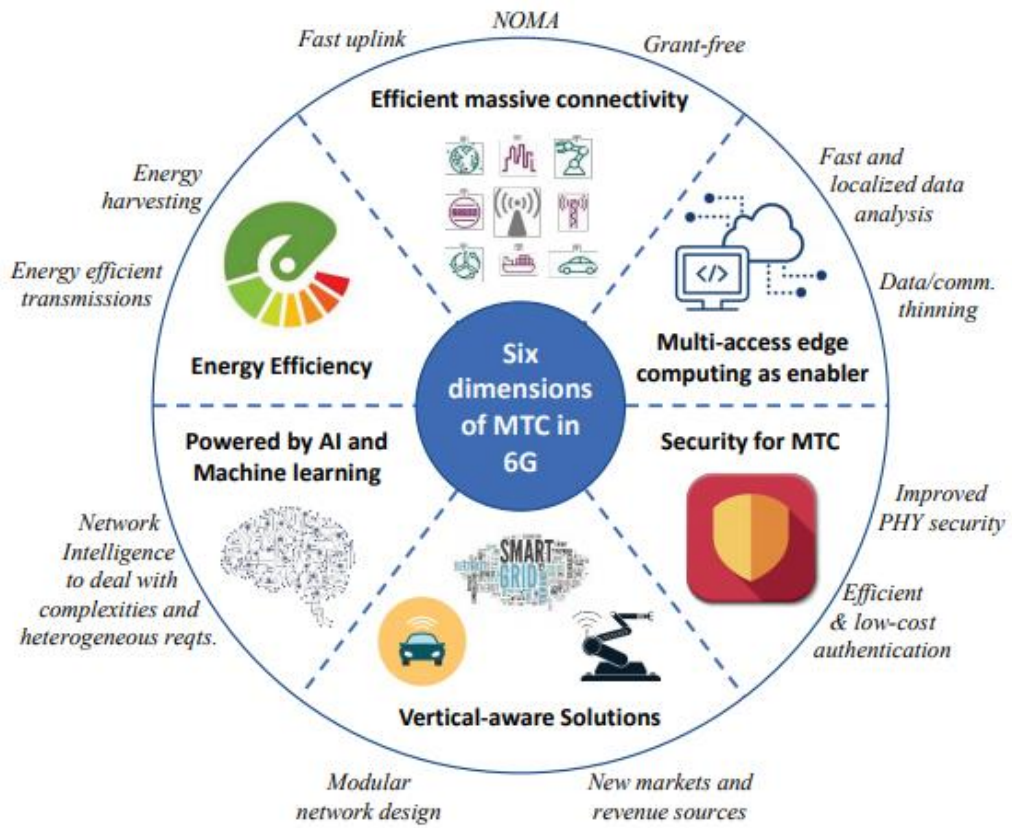
Εικόνα 62: Έλεγχος λειτουργίας παραδείγματος 2

6. Προκλήσεις και μελλοντικές εξελίξεις

Στο network slicing υπάρχουν κάποιες προκλήσεις που πρέπει να προσέχονται και να αντιμετωπιστούν. Η πρώτη πρόκληση είναι η ασφάλεια και στα κέντρα δεδομένων και στο 5G. Τα κέντρα δεδομένων καλούνται να αντιμετωπίσουν επιθέσεις και κενά ασφάλειας τα οποία τα εκμεταλλεύονται διάφοροι επιτήδριοι είτε είναι μέσα στο δίκτυο είτε έξω για να δημιουργούν προβλήματα. Επιθέσεις όπως DDOS, black hole ή εκμετάλλευση των κοινών πόρων των slice και σιγουρά τα μελλοντικά bugs, κενά ασφάλειας κτλπ. πρέπει να αποκρούονται και να αντιμετωπίζονται π.χ. με firewalls κτλπ. Διαφορετικά οι χρήστες μπορεί να μην μπορούν να εξυπηρετηθούν να μην είναι διαθέσιμες οι υπηρεσίες ή κάποιες δυνατότητες ανάλογα την ζημιά και έτσι να χαθεί το QoE. Άλλη πρόκληση είναι η σωστή απομόνωση, η δυναμική δημιουργία, ο σωστός διαμοιρασμός των πόρων των slice και το σωστό QoS ανάλογα με τις απαιτήσεις. Αυτές οι προκλήσεις έχουν να κάνουν και με την ασφάλεια. Σε κάθε slice πρέπει να εξασφαλίζεται ότι έχει εγγυημένους πόρους για να τρέξει η εφαρμογή και ότι αμα ένα slice δεχθεί επίθεση δεν θα επηρεαστούν τα υπόλοιπα.

[48] Η μελλοντική εξέλιξη του 5G είναι το 6G που φημίζεται να γίνεται διαθέσιμο παγκόσμιος το 2030. Το 6G θα είναι 100 φορές πιο γρήγορο από το 5G. Το 5G είναι ακόμη στην αρχή του υποστηρίζεται ότι οι ταχύτητες gigabits ανά δευτερόλεπτο μπορεί να υπολείπονται για την υποστήριξη πολλών αναδυόμενων εφαρμογών, όπως τα παιχνίδια 3D και η εκτεταμένη πραγματικότητα. Τέτοιες εφαρμογές θα απαιτούν αρκετές εκατοντάδες gigabits ανά δευτερόλεπτο έως αρκετά terabits ανά δευτερόλεπτο ρυθμούς δεδομένων με χαμηλό λανθάνοντα χρόνο και υψηλή αξιοπιστία, οι οποίοι αναμένεται να είναι οι σχεδιαστικοί στόχοι των συστημάτων επικοινωνίας επόμενης γενιάς 6G. Δεδομένης της δυνατότητας των συστημάτων επικοινωνιών terahertz (THz) να παρέχουν τέτοιους ρυθμούς δεδομένων σε μικρές αποστάσεις, θεωρούνται ευρέως ως τα επόμενα σύνορα για την έρευνα ασύρματων επικοινωνιών. Το 6G θα χρησιμοποιεί μέχρι και 10 THz. Συγκεκριμένα, οι συχνότητες THz υπόσχονται να υποστηρίξουν άφθονο φάσμα, τεράστια συνδεσιμότητα, πυκνότερα δίκτυα και εξαιρετικά ασφαλείς μεταδόσεις.

Στο 6G έχουν εισαχθεί νέες κατηγορίες υπηρεσιών που στοχεύουν σε εξαιρετικά αξιόπιστη επικοινωνία χαμηλού λανθάνοντος χρόνου (targeting ultrareliable low-latency communication URLLC) και machine type communication (MTC) παράλληλα με το αναβαθμισμένο σύστημα ευρυζωνικής κινητής πρόσβασης (enhanced mobile broadband eMBB). Το URLLC αντιμετωπίζει κρίσιμες εφαρμογές σε διαφορετικές βιομηχανίες ενώ το MTC έχει να κάνει με την παροχή ενεργειακής και φασματικά αποδοτικής συνδεσιμότητας σε μεγάλο αριθμό συσκευών Internet of Things (IoT). Κάποια άλλα χαρακτηριστικά είναι ότι θα έχει καλύτερη ασφάλεια, καλύτερη εξοικονόμηση ενέργειας, πιο γρήγορο uplink, χαμηλός κόστος ελέγχου ταυτότητας και εξουσιοδότησης (Improved physical layer security techniques), βελτιωμένες τεχνικές ασφαλείας φυσικού επιπέδου κτλπ. Μια εικόνα με τα χαρακτηριστικά του 6G απεικονίζεται παρακάτω.



Εικόνα 63: Χαρακτηριστικά 6G

7. Επίλογος

Από ό,τι φαίνεται οι τεχνολογίες των τηλεπικοινωνιών έχουν μπει για τα καλά στην ζωή μας. Το 5G είναι μια μεγάλη αλλαγή στον τομέα των τηλεπικοινωνιών και για τουλάχιστον 10 χρονιά από τώρα θα είναι το μέλλον για κόσμο και τις επιχειρήσεις. Το 5G θα βοηθήσει στην ανάπτυξη νέων εφαρμογών και υπηρεσιών. Και αυτό γιατί το νέο 5G δίκτυο θα είναι σε θέση να μας παρέχει εξαιρετικά μεγάλες ταχύτητες, μικρή καθυστέρηση και απόλυτη ασφάλεια. Για την κατανόηση του θέματος, έγινε λόγος για τα Data centers, το 5G, την αρχιτεκτονική 5G, τα RAN και τα C-RAN. Στην συνέχεια αναλύθηκε το SDN (Software Defined Networking) και την αρχιτεκτονική του καθώς και το πιο γνωστό πρωτόκολλο που είναι το OpenFlow. Δόθηκε η ανάλογη εστίαση στο πρωτόκολλο flowvisor για την κοπή των δικτύων των κέντρων δεδομένων. Το Network Function Virtualization που είναι απαραίτητο ώστε να γίνονται οι λειτουργίες του δικτύου με βάση το λογισμικό και όχι σε υποδομές, πράγμα που θα ελαφρύνει αρκετά το δικτυακό hardware και θα συμβάλλει στην εξοικονόμηση εσόδων. Στον τεμαχισμό του 5G είδαμε και αναλύσαμε τις αρχιτεκτονικές κάποιων οργανισμών όπως NGMN και ONF. Επίσης είδαμε την ζωή κύκλου ενός slice και το Ran Slicing. Τέλος, είπαμε 2 λόγια για τις προκλήσεις και τα προβλήματα που έχουμε να αντιμετωπίσουμε με το Network Slicing και γενικά με το 5G και το data center και τις μελλοντικές εξελίξεις όπως το 6G το οποίο με λίγα λόγια θα κάνει ότι δεν θα μπορέσει να κάνει το 5G και ότι κάνει το 5G θα το κάνει καλύτερα.

ΑΡΚΤΙΚΟΛΕΞΑ – ΑΚΡΩΝΥΜΙΑ

5G	5th Generation of Cellular Mobile Communications	5η γενιά κινητών επικοινωνιών κινητής τηλεφωνίας
API	Application Programming Interface	Διεπαφή προγραμματισμού εφαρμογών
BBU	Baseband Unit	Μονάδα Βασικής Ζώνης
BS	Base Station	Σταθμός βάσης
BSH	Base Station Hypervisor	Hypervisor Σταθμού βάσης
BSS	Business Support System	Σύστημα Υποστήριξης Επιχειρήσεων
B2B	Business-to- Business	Επιχείρηση προς Επιχείρηση
B2C	Business-to-consumer	Επιχείρηση προς καταναλωτή
B2G	Business-to-Government	Επιχείρηση-προς-κυβέρνηση
CapEx	Capital Expenditures	Δαπάνες Κεφαλαίου
CSP	Communications Service Providers	Πάροχοι υπηρεσιών επικοινωνιών
CoS	Cost of Service	Κόστος υπηρεσίας
CRAN	Cloud Radio Access Network	Δίκτυο Ραδιοπρόσβασης υλοποιημένο στο νέφος
DC	Data Center	Κέντρο Δεδομένων

DC-GW router	Direct current gateway Router	Δρομολογητής πύλης συνεχούς ρεύματος
E2E	End-to-end	Από άκρη σε άκρη
eMBB	Enhanced Mobile Broadband	Αναβαθμισμένο Σύστημα Ευρυζωνικής Κινητής Πρόσβασης
FWA	Fixed Wireless Access	Σταθερή ασύρματη πρόσβαση
SLL	Secure Sockets Layer	Ασφαλές επίπεδο υλοποίησης sockets
IaaS	Infrastructure as a Service	Υποδομή ως υπηρεσία
IoT	Internet of Things	Το διαδίκτυο των πραγμάτων
LTE	Long-Term Evolution	Μακροπρόθεσμη εξέλιξη
MANO	Management and Orchestration	Διαχείριση και εντοπισμός
MVNO	Mobile Virtual Network Operator	Διαχειριστής εικονικού δικτύου κινητής τηλεφωνίας
mMTC	Massive Machine Type Communications	Ογκώδης επικοινωνία τύπου μηχανών
NaaS	Network as a Service	Δίκτυο ως υπηρεσία
NBI	Northbound Interface	Διεπαφή Northbound
NF	Network Function	Λειτουργία δικτύου
NFV	Network Functions Virtualization	Εικονικοποίηση λειτουργιών δικτύου
NFVI	Network Functions Virtualization Infrastructure	Υποδομή εικονικοποίησης λειτουργιών δικτύου
NFVO	Network Functions Virtualization Orchestrator	Ενορχηστρωτής εικονικοποίησης λειτουργιών δικτύου
NGMN	Next Generation Mobile Network	Δίκτυο κινητής τηλεφωνίας επόμενης γενιάς
NSI	Network Slice Infrastructure	Υποδομή δικτύου Slice
NSP	Nokia Network Services Platform	Πλατφόρμα υπηρεσιών δικτύου Nokia
NSM	Network Slice Management System	Σύστημα διαχείρισης κομματιών του δικτύου
O&M	Operations and Maintenance	Λειτουργίες και Συντήρηση
ONF	Open Network Foundation	Ίδρυμα ανοιχτού δικτύου

OpEx	Operating Expenses	Δαπάνες λειτουργίας
OSS	Orchestration System	Σύστημα ενορχήστρωσης
PCE	Path Computation Element	Στοιχείο υπολογισμού διαδρομής
PN	Physical Network	Φυσικό Δίκτυο
PNF	Physical Network Function	Λειτουργία φυσικού δικτύου
QoE	Quality of Experience	Ποιότητα εμπειρίας
QoS	Quality of Service	Ποιότητα εξυπηρέτησης
RAN	Radio Access Network	Δίκτυο ραδιοπρόσβασης
RAT	Radio Access Technology	Τεχνολογία ραδιοπρόσβασης
RRH	Remote Radio Head	Απομακρυσμένη κεφαλή ραδιοεπικοινωνίας
SDN	Software-Defined Networking	Δικτύωση που ορίζεται από λογισμικό
SLA	Service Level Agreements	Συμφωνίες επιπέδου υπηρεσίας
URLLC	Ultra-reliable and low-latency communications	Εξαιρετικά αξιόπιστες και μικρής καθυστέρησης επικοινωνίες
VDC	Virtual Data Center	Εικονικό κέντρο δεδομένων
VIM	Virtualized Infrastructure Management	Εικονικοποιημένη διαχείριση υποδομής
VM	Virtual Machine	Εικονική μηχανή
VN	Virtual Network	Εικονικό Δίκτυο
VNF	Virtual Network Function	Λειτουργία εικονικού δικτύου

Βιβλιογραφία

1. Dusit Niyato, Nguyen Cong Luong, Ping Wang, Zhu Han(2020). Auction Theory for Computer Networks. United Kindom: Tj International, Padstow Cornwall.ruo
2. Kris Jamsa(2012).Cloud Computing: SaaS, PaaS, IaaS, Virtualization, Business Models, Mobile, Security, and More.United States of America :Lawrence J.Goodrich.
3. Chen, L., (2016).Security, Privacy, And Digital Forensics In Cloud And Big Data Era. John Wiley & Sons.
4. NIST Cloud Security Framework.
5. Marinescu D. (2019).Cloud computing: Theory and Practice, MA: Morgan Kaufmann.
6. T.-T. Nguyen, C. Bonnet, J. Harri (2016).SDN-Based Distributed mobility management for 5G networks. Doha, Qatar :IEEE.
7. J. Heinonen, P. Korja, T. Partti, H. Flinck, P. Pöyhönen (2016), Mobility management enhancements for 5G low latency services.Kuala Lumpur, Malaysia :IEEE.
8. G. Fabio, C. Luca, B. Carlos J(2015).Distributed mobility management for future 5G networks.0163-6804:IEEE.
9. A.A. Barakabitze, L. Sun, I.-H. Mkwawa, E. Ifeachor(2018).A novel QoE-Centric SDNbased multipath routing approach of mutimedia services over 5G networks.Kansas City, MO:IEEE.
10. D. Fang, Y. Qian, R.Q. Hu(2017).Security for 5G mobile wireless networks.2169-3536:IEEE.
11. M. Iwamura(2015).NGMN View on 5G architecture.Glasgow UK:IEEE
12. A.D. Domenico, E.C. Strinati, A. Capone(2014).Enabling green cellular networks: a survey and outlook.Italy:computer communications.
13. M. Gruber, O. Blume, D. Ferling, D. Zeller, M.A. Imran, E.C. Strinati,(2009)EARTH – Energy Aware radio and network technologies.Tokyo, Japan:IEEE
14. M. Olsson, C. Cavdar, P. Frenger, S. Tombaz, D. Sabella, R. Jantti,(2013).5GrEen:towards green 5G mobile networks.:9th IEEE International Conference on Wireless and Mobile Computing Networks.
15. M. Agiwal, A. Roy, N. Saxena(2016).Next generation 5G wireless networks:a comprehensive survey.IEEE Communications Surveys & Tutorials
16. F. Boccardi, R. W. Heath, A. Lozano, T. L. Marzetta, and P. Popovski(2014).“Five disruptive technology directions for 5G,”.IEEE Commun.

17. Vijay Laxmi Kalyani, Deeksha Sharma(2015).IoT: Machine to Machine (M2M), Device to Device (D2D) Internet of Everything (IoE) and Human to Human (H2H): Future of Communication.Volume -2, Issue- 6,ISSN: 2394 – 8124
18. Saleem Karmoshi, Shuo Wang, Naji Alhusaini, Jing Li, Ming Zhu and Ammar Hawbani(2019).GANA-VDC: Application-Aware with Bandwidth Guarantee in Cloud Datacenters. China:Electronics MDPI
19. Alcardo Alex Barakabitzea, Arslan Ahmadb, Rashid Mijumbi c, Andrew Hines(2020).5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges.Computer NetworksVolume 167, 11 February 2020, 106984
20. Mudigonda, J., Yalagandula, P., Mogul, J., Stiekes, B., Pouffary, Y. NetLord: (2011). A scalable multi-tenant network architecture for virtualized datacenters. ACM SIGCOMM Comput. Commun. Rev. 41, 62–73.
21. Aloqaily, M., Otoum, S., Al Ridhawi, I., Jararweh, Y, (2019). An Intrusion Detection System for Connected Vehicles in Smart Cities. Ad Hoc Netw.
22. Otoum, S.; Kantarci, B.; Mouftah, H.T. (2017).Hierarchical trust-based black-hole detection in WSN-based smartgrid monitoring.Paris, France:In Proceedings of the 2017 IEEE International Conference on Communications (ICC)
23. MultiPath TCP. Available online: <http://www.multipath-tcp.org/> (accessed on 25 February 2019).
24. Mudigonda, J.; Yalagandula, P.; Mogul, J.; Stiekes, B.; Pouffary, Y. (2011). NetLord: A scalable multi-tenant network architecture for virtualized datacenters. ACM SIGCOMM Comput. Commun. Rev. 2011, 41, 62–73.
25. Soliman, M.; Nandy, B.; Lambadaris, I.; Ashwood-Smith, P.(2014). Exploring source routed forwarding in SDN-based WANs. In Proceedings of the 2014 IEEE International Conference on Communications (ICC), Sydney, Australia, 10–14 June; pp. 3070–3075.
26. Guo, C.; Lu, G.; Wang, H.J.; Yang, S.; Kong, C.; Sun, P.P.; Wu, W.; Zhang, Y.(2010) Secondnet: A data center network virtualization architecture with bandwidth guarantees. In Proceedings of the 6th International Conference, Graz, Austria, 1–3; p. 15.
27. Aguiar, R.; Collares-Pereira, M. (1992)TAG: A time-dependent, autoregressive, Gaussian model for generating synthetic hourly radiation. Sol. Energy , 49, 167–174.
28. Mysore, R.N., Mysore, R.N., Farrington, N., Farrington, N., Miri, P., Radhakrishnan, S., Subramanya, V., Vahdat, A.(2009)Portland: A scalable fault-tolerant layer 2 data center network fabric. ACM SIGCOMM Comput.Commun. Rev. , 39, 39–50.
29. Cisco Visual Networking Index: Forecast and Trends, (2017–2022) - White Paper, February, 2019, [Online]. Available: <https://www.cisco.com/>

c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.pdf.

30. Alison McCabe(2019). Five 5G network slicing use cases.Opennet
<https://www.openet.com/blog/five-5g-network-slicing-use-cases-2-2/>
31. View on 5G Architecture:5G PPP Architecture Working Group, (<https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-5G-Architecture-WP-For-public-consultation.pdf>). [Online: accessed 20-March-2019].
32. https://en.wikipedia.org/wiki/Software-defined_networking
33. 5G ARCHITECTURE 5G PPP Public Private Partnership (2017)
https://bscw.5g-ppp.eu/pub/bscw.cgi/d230105/flyer-archt-MWC18_v1.1.pdf
34. Rob Sherwood , Glen Gibb , Kok-Kiong Yap , Guido Appenzeller , Martin Casado , Nick McKeown† , Guru Parulkar (2009). FlowVisor: A Network Virtualization Layer. Deutsche Telekom Inc. R&D Lab, Stanford University Nicira Networks: OPENFLOW-TR
35. NFV 5G
https://en.wikipedia.org/wiki/Network_function_virtualization
36. ONF TR-526, Applying SDN Architecture to 5G Slicing(2016).
https://opennetworking.org/wp-content/uploads/2014/10/Applying_SDN_Architecture_to_5G_Slicing_TR-526.pdf
37. <https://www.techopedia.com/definition/9089/radio-access-network-ran>
38. <https://www.sdxcentral.com/5g/ran/definitions/radio-access-network/>
39. 5G PPP 5G Architecture White Paper Revision 2.0 <https://5g-ppp.eu/wp-content/uploads/2018/01/5GPPP-5G-Architecture-White-Paper-Jan-2018-v2.0.pdf>
40. <https://www.etsi.org/technologies/nfv>
41. https://www.ngmn.org/wp-content/uploads/160113_NGMN_Network_Slicing_v1_0.pdf
42. <https://github.com/onstutorial/onstutorial/wiki/Flowvisor-Exercise>
43. <https://books.google.gr/books?id=oXLnDwAAQBAJ&pg=PA273&dq=flowvisor+example&hl=el&sa=X&ved=2ahUKEwiy4PXwjv3sAhWikhQKHTRRBrEQ6AEwAHoECAYQAg#v=onepage&q&f=false>
44. https://books.google.gr/books?id=9CL3DwAAQBAJ&pg=PA3&dq=flowvisor+mininet&hl=el&sa=X&ved=2ahUKEwi_2qqAmf3sAhXP-KQKHWTRBEgQ6AEwAXoECAAQAg#v=onepage&q=flowvisor%20mininet&f=false
45. <https://delaat.net/rp/2012-2013/p28/report.pdf>

46. <https://github.com/onstutorial/onstutorial/wiki/Flowvisor-Exercise>
47. <http://mininet.org/overview/>
48. Nurul Huda Mahmood; Hirley Alves; Onel Alcaraz López; Mohammad Shehab; Diana P. Moya Osorio; Matti Latva-Aho (2020). Six Key Features of Machine Type Communication in 6G. Levi, Finland: IEEE.
49. X. Foukas, M. K. Marina, K. Kontovasilis, "Orion: RAN Slicing for a Flexible and Cost-Effective MultiService Mobile Network Architecture", the 23rd Annual International Conference, October 2017
50. <https://github.com/onstutorial/onstutorial>
51. Nazih Salhab; Salah El Falou; Rana Rahim; Salah Eddine El Ayoubi; Rami Langar(2018). Optimization of the implementation of network slicing in 5G RANJounieh, Lebanon: IEEE.
52. <https://www.ericsson.com/assets/local/digital-services/network-slicing/network-slicing-value-potential.pdf>
53. <https://www.ericsson.com/assets/local/digital-services/network-slicing/top-network-slicing-use-cases.pdf>
54. <https://www.nokia.com/networks/solutions/network-slicing/#solutions>
55. <https://www-file.huawei.com/-/media/corporate/pdf/white%20paper/5g-service-guaranteed-network-slicing-whitepaper.pdf?la=en>