



# ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ

## ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

### ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ

## Πρόγραμμα Μεταπτυχιακών Σπουδών Επιστήμη και Τεχνολογία της Πληροφορικής και των Υπολογιστών

### Ειδίκευση Δικτύων Επικοινωνιών και Κατανεμημένων Συστημάτων

#### ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Τεχνικές τεμαχισμού δικτύων (network slicing) - σύγχρονες τάσεις σε  
επίπεδο παρόχων

Εμμανουήλ Κολαρετάκης  
Α.Μ. 18036

Σταύρος Ματσουκάς  
Α.Μ. 18018

Εισηγητής: Δρ Αντώνης Μπόγρης, Καθηγητής



## **ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ**

Τεχνικές τεμαχισμού δικτύων (network slicing) - σύγχρονες τάσεις σε  
επίπεδο παρόχων

**Εμμανουήλ Κολαρετάκης**  
**A.M. 18036**

**Σταύρος Ματσουκάς**  
**A.M. 18018**

**Εισηγητής:**

**Δρ Αντώνης Μπόγρης, Καθηγητής**

**Εξεταστική Επιτροπή:**

**Αντώνης Μπόγρης, Καθηγητής**  
**Παναγιώτης Καρκαζής, Επ. Καθηγητής**  
**Νικόλαος Μυριδάκης, Επ. Καθηγητής**

**Ημερομηνία εξέτασης 8/12/2021**



## **ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΩΝ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ**

Οι κάτωθι υπογεγραμμένοι Κολαρετάκης Εμμανουήλ του Κωνσταντίνου και Ματσουκάς Σταύρος του Αθανασίου, με αριθμούς μητρώου 18036 και 18018 αντίστοιχα, φοιτητές του Προγράμματος Μεταπτυχιακών Σπουδών «Επιστήμη και Τεχνολογία της Πληροφορικής και των Υπολογιστών» του Τμήματος Μηχανικών Πληροφορικής και Υπολογιστών της Σχολής Μηχανικών του Πανεπιστημίου Δυτικής Αττικής, δηλώνουμε ότι:

«Είμαστε συγγραφείς αυτής της μεταπτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχαμε για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες κάναμε 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, βεβαιώνουμε ότι αυτή η εργασία έχει συγγραφεί από εμάς αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μας, όσο και του Πανεπιστημίου Δυτικής Αττικής.

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

Οι Δηλούντες

Κολαρετάκης Εμμανουήλ

Ματσουκάς Σταύρος



## **ΕΥΧΑΡΙΣΤΙΕΣ**

Η παρούσα διπλωματική εργασία ολοκληρώθηκε μετά από επίμονες προσπάθειες, σε ένα ενδιαφέρον γνωστικό αντικείμενο, όπως αυτό του τεμαχισμού δικτύου. Την προσπάθειά μας αυτή υποστήριξε ο επιβλέπων καθηγητής μας, τον οποίο θα θέλαμε να ευχαριστήσουμε.

Ακόμα θα θέλαμε να ευχαριστήσουμε τις οικογένειές μας που μας στήριξαν καθ' όλη τη διάρκεια των σπουδών μας.





## **ΠΕΡΙΛΗΨΗ**

Η παρούσα διπλωματική εργασία έχει ως αντικείμενο την τεχνική του τεμαχισμού δικτύων. Πρόκειται για μία τεχνική που κρίνεται απαραίτητη για την ανάπτυξη των κινητών δικτύων 5<sup>ης</sup> γενιάς. Η τεχνική αυτή επιτρέπει τη δημιουργία πολλών ανεξάρτητων λογικών δικτύων, πάνω από μία κοινή φυσική δικτυακή υποδομή. Με τον τρόπο αυτό, μπορούν σε ένα δίκτυο να φιλοξενοούνται υπηρεσίες με πολύ διαφορετικά χαρακτηριστικά και απαιτήσεις. Η τεχνική προσεγγίζεται τόσο σε θεωρητικό όσο και σε πρακτικό επίπεδο. Στο πλαίσιο του πρακτικού μέρους της διπλωματικής, παρέχονται αναλυτικές οδηγίες για τη διεξαγωγή ενός εργαστηρίου επίδειξης της τεχνικής του τεμαχισμού δικτύων.

## **ABSTRACT**

The main object of the present thesis is network slicing. Network slicing is a technique that is considered necessary for the development of 5G mobile networks. It allows the creation of many independent logical networks, over a common physical network infrastructure. This way, a network can host services with very different features and requirements. The technique is approached on both a theoretical and a practical level. The practical part of the thesis includes detailed instructions for a lab demonstration of network slicing.

Τεχνικές τεμαχισμού δικτύων (network slicing) - σύγχρονες τάσεις σε επίπεδο παρόχων

ΕΠΙΣΤΗΜΟΝΙΚΗ ΠΕΡΙΟΧΗ: Δίκτυα κινητών επικοινωνιών  
ΛΕΞΕΙΣΚΛΕΙΔΙΑ: 5G, network slicing, SDN, NFV, FlowVisor

## ΠΕΡΙΕΧΟΜΕΝΑ

<a href="#">ΕΙΣΑΓΩΓΗ</a> .....	14
<a href="#">ΚΕΦΑΛΑΙΟ 1 - Η εξέλιξη των δικτύων κινητών επικοινωνιών από το 2G έως το 5G</a> ....	17
<a href="#">1.1 Τα δίκτυα κινητών επικοινωνιών από το 2G έως το 4G</a> .....	17
<a href="#">1.2 Τα Δίκτυα Πέμπτης Γενιάς (5G)</a> .....	18
<a href="#">1.2.1 Αρχιτεκτονική των δικτύων 5G</a> .....	19
<a href="#">1.2.2 Χαρακτηριστικά τεχνολογίας 5G</a> .....	23
<a href="#">ΚΕΦΑΛΑΙΟ 2 - Αρχιτεκτονικές στα δίκτυα 5G - Δικτύωση Βάσει Λογισμικού και Εικονικοποίηση Δικτυακών Λειτουργιών</a> .....	29
<a href="#">2.1 Δικτύωση Βάσει Λογισμικού (Software-Defined Networking – SDN)</a> .....	29
<a href="#">2.2 Εικονικοποίηση Δικτυακών Λειτουργιών (NetworkFunctionVirtualization – NFV)</a> .....	32
<a href="#">ΚΕΦΑΛΑΙΟ 3 - Τεμαχισμός δικτύων 5G</a> .....	35
<a href="#">3.1 Ο Τεμαχισμός Δικτύου (NetworkSlicing)</a> .....	35
<a href="#">3.2 Η ανάγκη τεμαχισμού των δικτύων 5G</a> .....	36
<a href="#">3.3 Κατηγοριοποίηση network slicing</a> .....	38
<a href="#">3.4 Τεμαχισμός δικτύου 5G με τη χρήση SDN και NFV</a> .....	39
<a href="#">3.5 Προκλήσεις στον τεμαχισμό δικτύων</a> .....	41
<a href="#">ΚΕΦΑΛΑΙΟ 4 - Επίδειξη Network Slicing με χρήση του FlowVisor</a> .....	45
<a href="#">4.1 FlowVisor</a> .....	45
<a href="#">4.2 Mininet</a> .....	47
<a href="#">4.3 Προετοιμασία εργαστηρίου</a> .....	47
<a href="#">4.4 Διεξαγωγή εργαστηρίου</a> .....	49
<a href="#">4.5 Δημιουργία slice με βάση τις πόρτες των switch (Φυσικό Επίπεδο)</a> .....	53
<a href="#">4.6 Δημιουργία slice με βάση τη διεύθυνση IP (Επίπεδο Δικτύου)</a> .....	59
<a href="#">4.7 Ολοκλήρωση εργαστηρίου</a> .....	65
<a href="#">ΚΕΦΑΛΑΙΟ 5 - Συμπεράσματα</a> .....	66
<a href="#">ΠΑΡΑΡΤΗΜΑ Α΄</a> .....	68
<a href="#">ΒΙΒΛΙΟΓΡΑΦΙΑ</a> .....	73

## ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

<b>Σχήμα 1.1:</b> Εξέλιξη των δικτύων “G”.....	19
<b>Σχήμα 1.2:</b> Διαφορά δικτύων 4G - 5G .....	20
<b>Σχήμα 1.3:</b> Συστατικά μέρη δικτύου κορμού 5G .....	21
<b>Σχήμα 1.4:</b> Αρχιτεκτονική 5G.....	22
<b>Σχήμα 1.5:</b> Φάσμα συχνοτήτων Αρχιτεκτονικής 5G .....	24
<b>Σχήμα 1.6:</b> Beamforming.....	26
<b>Σχήμα 1.7:</b> Αρχιτεκτονική 5G υψηλού επιπέδου.....	27
<b>Σχήμα 2.1:</b> Αρχιτεκτονική SDN.....	29
<b>Σχήμα 2.2:</b> Αρχιτεκτονική NFV .....	31
<b>Σχήμα 3.1:</b> Network slicing .....	37
<b>Σχήμα 3.2:</b> Προσθήκη Ελεγκτών SDN στην αρχιτεκτονική NFV .....	39
<b>Σχήμα 4.1:</b> Το FlowVisor στην Αρχιτεκτονική SDN.....	44

## ΚΑΤΑΛΟΓΟΣ ΕΙΚΟΝΩΝ

<b>Εικόνα 4.1:</b> Ενεργοποίηση προώθησης πρωτοκόλλου X11 στο PuTTY .....	47
<b>Εικόνα 4.2:</b> Έτοιμη τοπολογία δικτύου στο miniedit.....	49
<b>Εικόνα 4.3:</b> Τεμαχισμός δικτύου με βάση τις πόρτες των switch.....	53
<b>Εικόνα 4.4:</b> Τεμαχισμός του δικτύου με βάση την IP διεύθυνση.....	59
<b>Εικόνα 4.5:</b> Προσομοίωση διακοπής σύνδεσης .....	62
<b>Εικόνα A.1:</b> Ρύθμιση 2ης κάρτας δικτύου VM .....	68

## ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

<b>Πίνακας 4.1:</b> Ιδιότητες στοιχείων δικτύου .....	50
<b>Πίνακας 4.2:</b> Πεδία κριτηρίων για το ταίριασμα πακέτων σε ροή .....	55

## ΣΥΝΤΟΜΟΓΡΑΦΙΕΣ

- 3GPP** 3rd Generation Partnership Project
- AF** Application Function
- AMF** Access and Mobility Management Function
- AUSF** Authentication Server Function
- API** Application Programmable Interface
- BSS** Business Support System
- CLI** Command Line Interface
- CPRI** Common Public Radio Interface
- DN** Data Networks
- DDoS** Distributed Denial of Service
- EDGE** Enhanced Data for GSM Evolution
- eMBB** enhanced Mobile BroadBand
- ETSI** European Telecommunication Standards Institute
- GPRS** General Packet Radio Service
- GSM** Global System for Mobile communication
- HSPA** High Speed Packet Access
- IoT** Internet of Things
- LTE** Long Term Evolution
- M2M** Machine to machine
- MANO** Management And Network Orchestration
- MEC** Multi-Access Edge Computing
- mMTC** massive Machine Type Communication
- MIMO** Multiple Input, Multiple Output
- NFV** Network Function Virtualization
- NFVI** Network Function Virtualization Infrastructure
- OFDM** Orthogonal Frequency Division Multiplexing
- OSS** Operation Support System
- PCF** Policy Control Function
- QoS** Quality of Service
- RAN** Radio Access Network
- SBA** Service-Based Architecture -
- SDN** Software-Defined Networking

**SMF** Session Management Function

**SMS** Short Message Service

**UDM** Unified Data Management

**UE** User Equipment

**UPF** User Plane Function

**URLLC** Ultra Reliable Low Latency Communication

**VIM** Virtual Infrastructure Manager

**VM** Virtual Machine

**VNF** Virtual Network Function

**W-CDMA** Wideband Code Division Multiple Access

**WiMAX** Worldwide Interoperability for Microwave Access

## ΕΙΣΑΓΩΓΗ

Με την εξέλιξη των κινητών δικτύων, έχει αλλάξει όχι μόνο ο τρόπος επικοινωνίας μας αλλά και η καθημερινότητά μας, αφού μπορούμε να είμαστε «διαθέσιμοι» αλλά και «συνδεδεμένοι» σχεδόν παντού. Ο κόσμος πλέον όχι μόνο μιλάει ή στέλνει SMS από τα κινητά του τηλέφωνα, αλλά χρησιμοποιεί όλο και πιο εξελιγμένες κινητές συσκευές και εφαρμογές από όπου επικοινωνεί, ενημερώνεται, διαχειρίζεται τα οικονομικά του, παρακολουθεί απομακρυσμένα το σπίτι του, με μια λέξη «δικτυώνεται».

Η κινητή υπολογιστική<sup>1</sup> έχει γίνει πλέον πραγματικότητα. Οι ανάγκες γίνονται πιο σύνθετες. Κάθε χρόνο η χρήση των δεδομένων αυξάνεται<sup>2</sup>. Οι συνεχώς αυξανόμενες ανάγκες έχουν εξελίξει τις τεχνολογίες της κινητής επικοινωνίας. Αμφίδρομα και παράλληλα αναπτύσσεται και η τεχνολογία των κινητών συσκευών.

Σήμερα βρισκόμαστε πια στην εποχή των δικτύων 5ης γενιάς (5G), τα οποία υπόσχονται στους χρήστες τους μια καλύτερη εμπειρία<sup>3,4</sup>. Τα συστήματα 5G ερευνούν τον τρόπο που θα ικανοποιούν τις ανάγκες των πελατών, των συσκευών, των υπηρεσιών και των επιχειρήσεων, ενώ από τα «κλειδιά» της εξέλιξης των συστημάτων αυτών είναι η υποστήριξη της βιομηχανίας σε ένα πλήθος διαφορετικών τομέων όπως αυτών της μεταποίησης, της αυτοκινητοβιομηχανίας, της υγείας, της ενέργειας των μέσων ενημέρωσης αλλά και της ψυχαγωγίας. Το 5G μπορεί υποστηρίξει ένα μεγάλο εύρος υπηρεσιών στην κοινωνία, όπως η παρακολούθηση καιρού, οι ιατρικές υπηρεσίες, οι

---

<sup>1</sup> Η κινητή υπολογιστική είναι μια νέα μορφή υπολογιστικής, στην οποία οι λειτουργίες των υπολογιστικών συστημάτων μεταφέρονται στο κινητό τηλέφωνο ή στις κινητές συσκευές, με υψηλές επεξεργαστικές δυνατότητες, παρέχοντας με αυτό τον τρόπο νέες μορφές υπηρεσιών και εφαρμογών στους χρήστες τους. – Χ Δουληγέρης (2015) Κεφάλαιο 4 Νέες Τεχνολογίες και Τεχνικές- ΚΑΛΛΙΠΟΣ - [https://repository.kallipos.gr/bitstream/11419/3973/1/01\\_chapter\\_4.pdf](https://repository.kallipos.gr/bitstream/11419/3973/1/01_chapter_4.pdf) - προσπέλαση 8/2021

<sup>2</sup> Άρθρο Κινητή τηλεφωνία: Πρωτόγνωρη αύξηση της χρήσης δεδομένων το 2020, (2021) <https://www.naftemporiki.gr/finance/story/1705801/kiniti-tilefonia-protognori-auksisi-tis-xrissi-dedomenon-to-2020> προσπέλαση 8/2021

<sup>3</sup> Άρθρο. Ξανασχεδιάζουμε τον κόσμο από την αρχή. (2021) <https://www.cosmote.gr/cs/cosmote/gr/5g.html> - προσπέλαση 8/2021

<sup>4</sup> Άρθρο Τι είναι το 5G και πώς θα επηρεάσει τη δική σας ζωή; (2021) <https://www.samsung.com/gr/explore/brand/what-is-5g-and-how-will-it-affect-your-life/> - προσπέλαση 8/2021

υπηρεσίες μεταφορών, οι εφαρμογές άμυνας και οι εφαρμογές έξυπνων πόλεων.

[1] [2]

Αυτή η γενιά κινητών δικτύων έχει οδηγήσει σε μια νέα εντελώς διαφορετική προσέγγιση όσον αφορά τη δικτύωση (networking). Οι κινητοί χρήστες αυξάνονται, όχι μόνο επειδή αυξάνεται ο αριθμός των κινητών προσωπικών συσκευών, αλλά κι επειδή υπάρχουν οι Διαμηχανικές (Machine to Machine – M2M) Επικοινωνίες καθώς και το Διαδίκτυο των Πραγμάτων (Internet of Things - IoT). Αυτό έχει ως αποτέλεσμα, να αυξάνεται ο ρυθμός δεδομένων, να αυξάνονται οι απαιτήσεις χωρητικότητας καθώς κι η ανάγκη κάλυψης.

Τα τελευταία χρόνια, το Διαδίκτυο των Πραγμάτων έχει μειώσει την ανθρώπινη παρέμβαση όσο γίνεται περισσότερο. Ένας σημαντικός αριθμός αντικειμένων μπορεί να αισθανθεί, να επικοινωνήσει και να μοιραστεί πληροφορίες (π.χ. έξυπνες οικιακές συσκευές) έτσι ώστε να δημιουργηθεί ένα περιβάλλον στο οποίο θα είναι όλα συνδεδεμένα. [3]

Αυτή η μεγάλη διασύνδεση όμως, έχει επιφέρει διάφορα ζητήματα που προκύπτουν από τον μεγάλο όγκο των δεδομένων που παράγονται κι έχουν να κάνουν με τη διαθεσιμότητα των δεδομένων, την ακρίβεια και την ασφάλεια.

Επίσης, υπάρχουν πολλές προκλήσεις, όπως: μείωση της κατανάλωσης ενέργειας σε συσκευές και σταθμούς βάσης, καλύτερη κατανομή πόρων, υψηλότεροι ρυθμοί δεδομένων, εξασφάλιση χαμηλότερων χρόνων απόκρισης, μείωση του κόστους, βελτιστοποίηση πολιτικών διαχείρισης κινητικότητας, επεκτασιμότητα, ελαστικότητα και ευελιξία.

Όλα τα παραπάνω οδηγούν στην υιοθέτηση ενός κεντρικού τρόπου ελέγχου. Μια κεντρική αρχιτεκτονική παρέχει σημαντικά οφέλη, όπως η βέλτιστη εκχώρηση συχνότητας και η αποτελεσματική πολιτική διαχείρισης της κινητικότητας. Οι υπάρχουσες αρχιτεκτονικές δεν μπορούν να υποστηρίξουν και να εξυπηρετήσουν τις νέες απαιτήσεις που παρουσιάζονται εξαιτίας του IoT, λόγω των περιορισμένων χαρακτηριστικών τους.

Οι δύο νέες αρχιτεκτονικές, οι οποίες προτείνονται για να λυθούν τα παραπάνω προβλήματα είναι η Δικτύωση Βάσει Λογισμικού (Software-Defined Networking - SDN) και η Εικονικοποίηση Δικτυακών Λειτουργιών (Network Function Virtualization - NFV), ενώ παράλληλα δοκιμάζονται πολλές τεχνικές για να επιλυθούν τα όποια ζητήματα προκύπτουν, όπως αυτή του τεμαχισμού δικτύου



(network slicing)<sup>5</sup> που αποτελεί και το κύριο αντικείμενο μελέτης της παρούσας εργασίας, τόσο σε θεωρητικό όσο και σε πρακτικό επίπεδο. Για να κατανοήσουμε πλήρως τι σημαίνει τεμαχισμός δικτύων, θα ξεκινήσουμε με μια μικρή αναδρομή στην εξέλιξη των κινητών δικτύων επικεντρώνοντας στην 5<sup>η</sup> γενιά, η οποία εξελίσσεται στις μέρες μας, αναδεικνύοντας τις αναγκαιότητες που έχουν προκύψει.

Θα μελετήσουμε τις αρχιτεκτονικές SDN και NFV, που φαίνεται να αντιμετωπίζουν τα ζητήματα που προκύπτουν από τη συνεχώς αυξανόμενη ανάγκη για δικτύωση.

Η τεχνική τεμαχισμού δικτύων (network slicing) μελετάται διεξοδικά.

Συγκεκριμένα, στο Κεφάλαιο 1 θα αναφερθούμε στα δίκτυα κινητών επικοινωνιών, κάνοντας μια μικρή αναδρομή στην εξέλιξή τους, από την εποχή των δικτύων 2ης γενιάς (2G) έως και τη σημερινή εποχή του 5G.

Στο 2ο Κεφάλαιο θα ασχοληθούμε με τις αρχιτεκτονικές Δικτύωσης Βάσει Λογισμικού (Software-Defined Networking - SDN) και Εικονικοποίησης δικτυακών λειτουργιών (Network Function Virtualization - NFV).

Το 3ο κεφάλαιο είναι όλο αφιερωμένο στην τεχνική του τεμαχισμού δικτύων (network slicing) που είναι και το κύριο αντικείμενο μελέτης της παρούσας εργασίας.

Στο 4ο κεφάλαιο, το οποίο και αποτελεί το πρακτικό μέρος της εργασίας, γίνεται παρουσίαση μιας πρότασης για την εργαστηριακή επίδειξη της τεχνικής network slicing με τη χρήση του λογισμικού FlowVisor.

Τέλος στο 5ο κεφάλαιο παρουσιάζονται τα συμπεράσματα της μελέτης μας.

---

<sup>5</sup>Network slicing – Τεμαχισμός ή Κατάτμηση Δικτύου

## **ΚΕΦΑΛΑΙΟ 1 - Η εξέλιξη των δικτύων κινητών επικοινωνιών από το 2G έως το 5G**

Η εξέλιξη των δικτύων κινητών επικοινωνιών προχωράει με γοργούς ρυθμούς και μέσα σε διάστημα 30 ετών, η πραγματικότητα τείνει να ξεπεράσει τη φαντασία. Η καθημερινότητά μας έχει αλλάξει δραματικά, σε σχέση με τον τρόπο που επικοινωνούμε και αλληλεπιδρούμε μέσω των κινητών συσκευών, ενώ η ανάπτυξη των δικτύων 5G υπόσχεται νέες εμπειρίες.

### **1.1 Τα δίκτυα κινητών επικοινωνιών από το 2G έως το 4G**

#### **Δίκτυα Δεύτερης Γενιάς (2G)**

Τα δίκτυα Δεύτερης Γενιάς (2G) εμφανίστηκαν το 1991 και παρείχαν ψηφιακή μετάδοση δεδομένων με το πρότυπο GSM. Το δίκτυο 2G, μπορούσε να εξυπηρετεί περισσότερους χρήστες ανά συχνότητα σε σχέση με το παρελθόν, ενώ παρείχε τη δυνατότητα αποστολής SMS.

Εξελίξεις των δικτύων δεύτερης γενιάς αποτελούν τα:

- 2.5G – Το πρότυπο της εξέλιξης αυτής είναι το GPRS. Το ίδιο κύκλωμα χρησιμοποιείται από διαφορετικούς χρήστες και περιλαμβάνει επικοινωνίες δεδομένων.
- 2.75G – Το πρότυπο της εξέλιξης αυτής είναι το EDGE. Με το πρότυπο αυτό, η χωρητικότητα των δικτύων GPRS τριπλασιάζεται και επιτρέπει ταχύτητες έως 384Kbps.

#### **Δίκτυα Τρίτης Γενιάς (3G)**

Τα δίκτυα Τρίτης Γενιάς (3G) εμφανίστηκαν το 1998 και χαρακτηριστικό τους ήταν η υψηλή ταχύτητα ροής δεδομένων (384 Kbps – πρότυπο W-CDMA). Στη γενιά αυτή υπάρχει η δυνατότητα πλοήγησης στο Διαδίκτυο ενώ διαθέσιμη γίνεται πλέον και η ροή βίντεο (video streaming). Τέλος παρέχεται καλύτερη ασφάλεια στην επικοινωνία σε σχέση με το παρελθόν. Στην εξέλιξη της γενιάς αυτής συναντάμε επίσης:

- Πρότυπο HSPA (High Speed Packet Access) που πιάνει ταχύτητες έως 14.4 Mbps και το
- Πρότυπο HSPA+ ή Evolved High Speed Packet Access πιάνει ταχύτητες έως 168 Mbps

### **Δίκτυα Τέταρτης Γενιάς (4G)**

Τα δίκτυα Τέταρτης Γενιάς (4G) εμφανίστηκαν το 2008, είναι η εξέλιξη του 3G και οι ταχύτητες που προσφέρουν πλέον αγγίζουν τα 100Mbps.

Η γενιά αυτή προσφέρει μεγαλύτερη ευρυζωνικότητα και στηρίζεται:

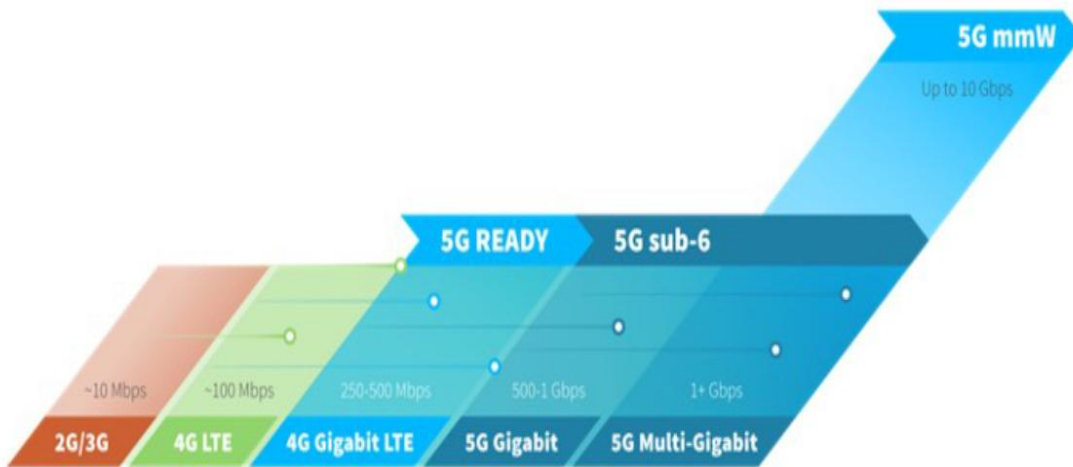
- στην τεχνολογία WiMAX, που είναι τεχνολογία ασύρματης δικτύωσης και λειτουργεί με παρεμφερή τρόπο με το Wi-Fi, η οποία όμως έχει πολύ μεγαλύτερη εμβέλεια και φθάνει τα 35 χιλιόμετρα ή και παραπάνω
- και στην τεχνολογία LTE Advanced η οποία χρησιμοποιεί τις τεχνολογίες MIMO και OFDM

### **1.2 Τα Δίκτυα Πέμπτης Γενιάς (5G)**

Τα δίκτυα Πέμπτης Γενιάς (5G) εμφανίστηκαν το 2015 και βρίσκονται σε εξέλιξη μέχρι σήμερα. Δε γνωρίζουμε ακόμα ποιες θα είναι οι πλήρεις δυνατότητές τους, γνωρίζουμε όμως τις απαιτήσεις που υπάρχουν για τα κινητά δίκτυα. Έτσι οι ανάγκες μας για δικτύωση μεταφράζονται σε απαιτήσεις για:

- 1000 φορές μεγαλύτερο όγκο δεδομένων ανά περιοχή
- 10 με 100 φορές μεγαλύτερο αριθμό συνδεδεμένων συσκευών
- 10 με 100 φορές μεγαλύτερο ρυθμό χρήσης δεδομένων
- 10 φορές μεγαλύτερη αυτονομία μπαταρίας για τις χαμηλής ενέργειας συσκευές
- 5 φορές μικρότερη End-to-End καθυστέρηση

Στο σχήμα που ακολουθεί παρουσιάζεται η εξέλιξη των δικτύων "G".



Σχήμα<sup>6</sup> 1.1: Εξέλιξη των δικτύων “G”.

Στόχος είναι τα δίκτυα 5G να προσφέρουν στους τελικούς χρήστες μέσα από πολλαπλές πλατφόρμες πρόσβασης και πολυεπίπεδα δίκτυα, γρήγορες και αξιόπιστες υπηρεσίες δεδομένων αλλά και ένα ευρύ φάσμα ασύρματων υπηρεσιών.

Στα πλεονεκτήματα των δικτύων 5G συγκαταλέγονται η διαλειτουργικότητα, η χαμηλή κατανάλωση, η καλύτερη κάλυψη, η ποιότητα υπηρεσιών (QoS) και η καλύτερη δικτύωση, ενώ στα μειονεκτήματα υπάρχουν επιφυλάξεις για τα ζητήματα της ασφάλειας και των κοινών υποδομών.

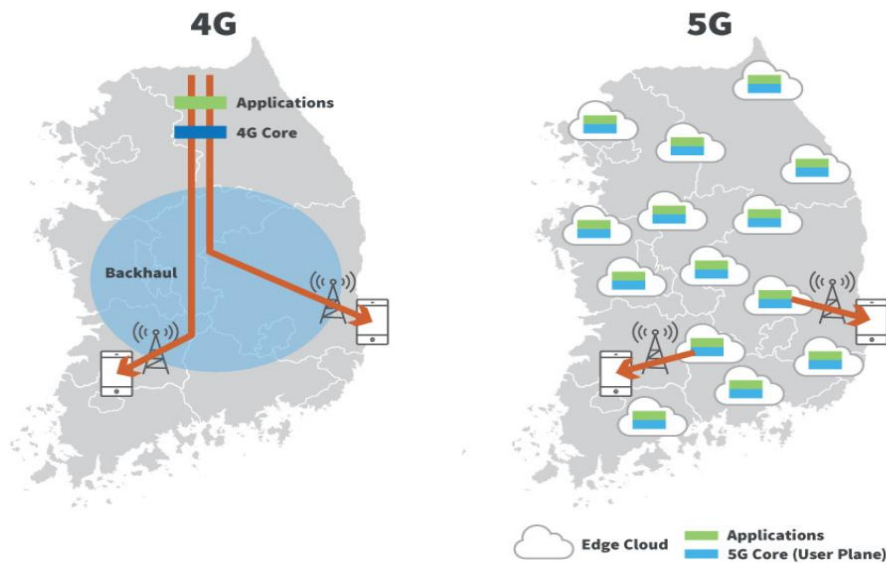
### 1.2.1 Αρχιτεκτονική των δικτύων 5G

Το δίκτυο 5G σχεδιάστηκε «από κάτω προς τα πάνω». Οι δικτυακές λειτουργίες χωριστήκαν σε υπηρεσίες και για το λόγο αυτό η αρχιτεκτονική 5G ονομάζεται και Αρχιτεκτονική Βασισμένη σε Υπηρεσίες (Service-Based Architecture – SBA). Το δίκτυο 5G είναι ουσιαστικά ένα δυναμικό, συνεκτικό και ευέλικτο πλαίσιο πολλαπλών προηγμένων τεχνολογιών που υποστηρίζουν ένα πλήθος διαφορετικών εφαρμογών.

<sup>6</sup>Πηγή: <https://www.digi.com/blog/post/5g-network-architecture> προσπέλαση 9/2021

Στην αρχιτεκτονική 4G LTE τα ραδιοδίκτυα (Radio Access Network – RAN)<sup>7</sup> και τα eNodeB<sup>8</sup> βρίσκονται κατά κανόνα κοντά, συχνά στη βάση ή δίπλα σε μία κεραία, πάνω σε εξειδικευμένο υλικό. Το 5G χρησιμοποιεί μια αρχιτεκτονική όπου τα ραδιοδίκτυα (RAN) δεν περιορίζονται πλέον από την απόσταση τους με τους σταθμούς βάσης. Στηρίζεται σε διαχωρισμένα και ευέλικτα εικονικά RAN με νέες διεπαφές που δημιουργούν πρόσθετα σημεία πρόσβασης δεδομένων.

Η αρχιτεκτονική του 5G προβλέπει ο κορμός του 5G (5G RadioCore) να είναι διαχωρισμένος και να υλοποιεί κάθε λειτουργία με τέτοιο τρόπο ώστε να μπορούν να τρέχουν ανεξάρτητα η μία από την άλλη, πάνω σε εξυπηρετητές. Αυτό επιτρέπει στους κόμβους του 5G να είναι αποκεντριοποιημένοι και ευέλικτοι. Μπορούν για παράδειγμα να βρίσκονται σε κάποιο κέντρο δεδομένων, κοντά στις εφαρμογές. Τα «μονοπάτια» λοιπόν μικραίνουν. Η επικοινωνία γίνεται έτσι πιο άμεση επιτυγχάνοντας γρηγορότερη ταχύτητα και τελικά καλύτερη εμπειρία για το χρήστη.



<sup>7</sup>Ένα ραδιοδίκτυο (Radio Access Network-RAN) είναι μέρος ενός κινητού τηλεπικοινωνιακού συστήματος. Εφαρμόζει τεχνολογία ραδιοπρόσβασης. Εννοιολογικά, βρίσκεται ανάμεσα σε μια συσκευή όπως ένα κινητό τηλέφωνο και μια τηλεπικοινωνιακή υποδομή και παρέχει σύνδεση με το κεντρικό δίκτυο.- Πηγή: <https://www.techtarget.com/searchnetworking/definition/radio-access-network-RAN>

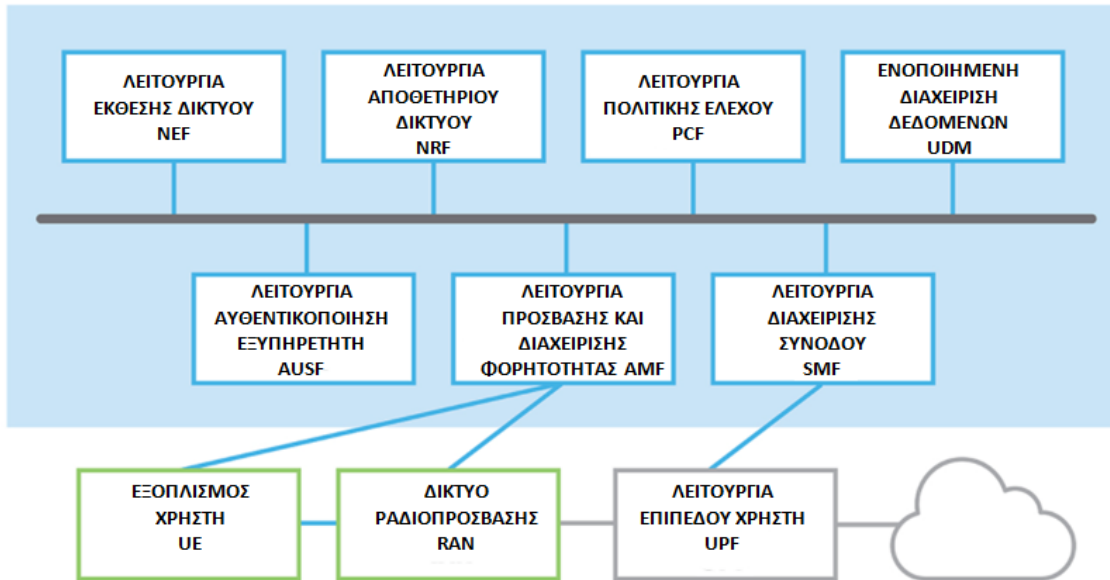
- πρόσβαση 8/2021

<sup>8</sup>eNodeB -

Υλικό που είναι συνδεδεμένο στο δίκτυο κινητής τηλεφωνίας που επικοινωνεί ασύρματα και άμεσα με τις συσκευές χρήστη όπως ένας σταθμός μετάδοσης βάσης base transceiver station (BTS) στα δίκτυα GSM

### Σχήμα 1.2: Διαφορά δικτύων 4G- 5G<sup>9</sup>

Στο διάγραμμα που ακολουθεί παρουσιάζονται τα κύρια συστατικά ενός δικτύου κορμού 5G.



Σχήμα 1.3: Συστατικά μέρη δικτύου κορμού 5G

Η λειτουργία του δικτύου είναι η εξής:

- Εξοπλισμός Χρήστη (User Equipment – UE). Οι κινητές συσκευές όπως τα έξυπνα κινητά που υποστηρίζουν 5G, συνδέονται πάνω στο Νέο Ραδιοδίκτυο (RAN) στον κορμό του 5G και στη συνέχεια στα Δίκτυα Δεδομένων (Data Networks – DN), όπως για παράδειγμα στο Διαδίκτυο.
- Η Λειτουργία Πρόσβασης και Διαχείρισης Φορητότητας (Access and Mobility Management Function – AMF) ενεργεί ως ένα μοναδικό σημείο εισόδου για τις συνδέσεις των συσκευών (UE).
- Με βάση την υπηρεσία για την οποία γίνεται το αίτημα από τη συσκευή (UE), η Λειτουργία Πρόσβασης και Διαχείρισης Φορητότητας (AMF) επιλέγει την αντίστοιχη Λειτουργία Διαχείρισης Συνόδου (Session Management Function - SMF) για να διαχειριστεί τη σύνοδο του χρήστη.

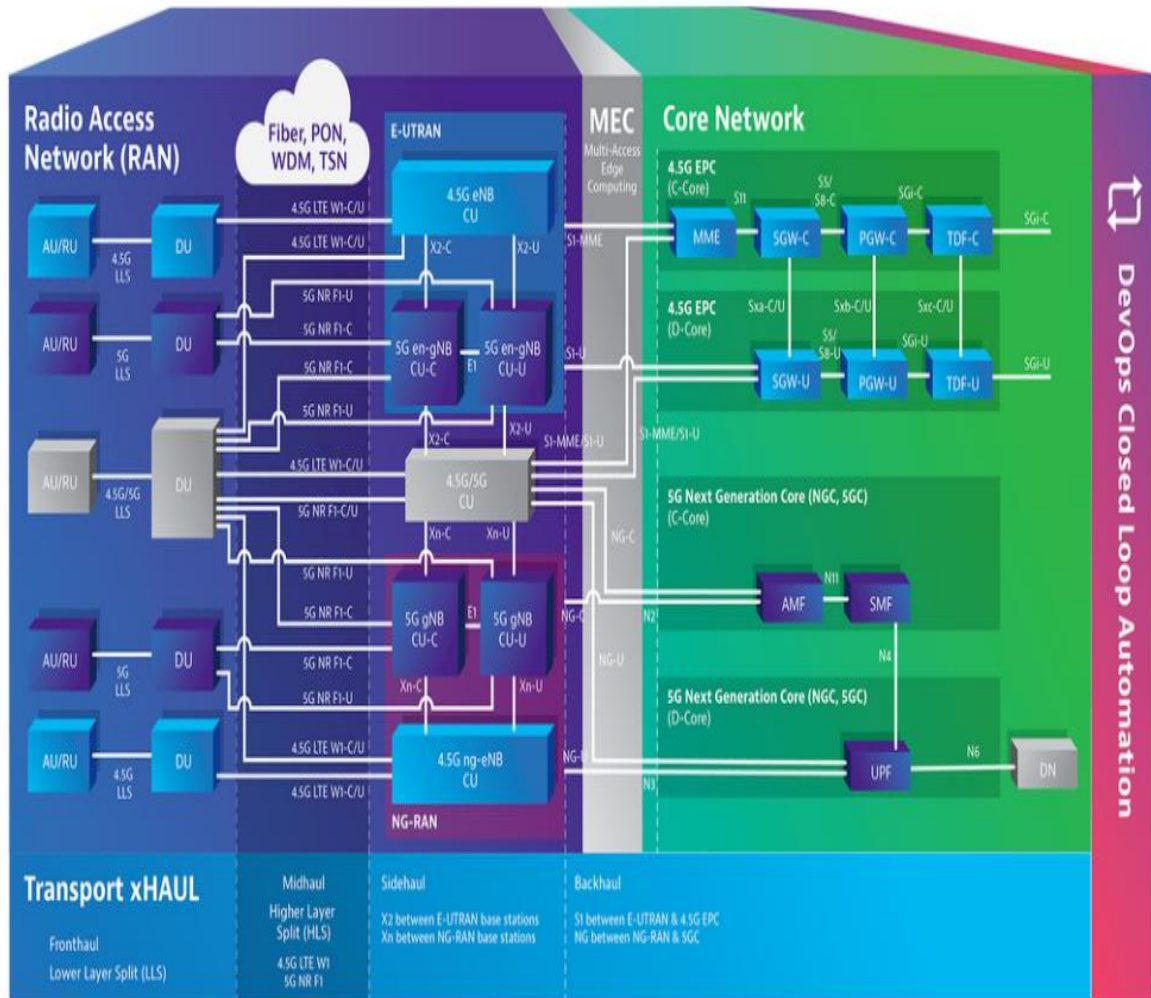
<sup>9</sup> Πηγή: <https://www.netmanias.com/en/post/blog/8256/5g-c-ran-fronthaul-kt-korea/5g-network-as-envisioned-by-kt-analysis-of-kt-s-5g-network-architecture> - προσπέλαση 8/2021

- Η Λειτουργία Επιπέδου Χρήστη (User Plane Function - UPF) μεταφέρει την IP κίνηση δεδομένων (επιπέδου χρήστη) ανάμεσα στις συσκευές (UE) και τα εξωτερικά δίκτυα.
- Η Λειτουργία Αυθεντικοποίησης Εξυπηρετητή (Authentication Server Function - AUSF) επιτρέπει στη Λειτουργία Πρόσβασης και Διαχείρισης Φορητότητας (AMF) να αυθεντικοποιεί τη συσκευή (UE), ώστε να μπορεί να αποκτήσει πρόσβαση στις υπηρεσίες του 5G.
- Άλλες λειτουργίες, όπως η Λειτουργία Διαχείρισης Συνόδου (SMF), η Λειτουργία Ελέγχου Πολιτικής (Policy Control Function - PCF), η Λειτουργία Εφαρμογής (Application Function - AF) και η Ενοποιημένη Διαχείριση Δεδομένων (Unified Data Management - UDM) παρέχουν το πλαίσιο της πολιτικής ελέγχου και διέπουν τη συμπεριφορά του δικτύου, εφαρμόζοντας αποφάσεις που σχετίζονται με την πολιτική και δίνοντας πρόσβαση σε πληροφορία «συνδρομής». [6]

Όπως μπορούμε να καταλάβουμε, η αρχιτεκτονική δικτύου 5G είναι αρκετά πολύπλοκη, όμως αυτή η πολυπλοκότητα είναι απαραίτητη ώστε οι υπηρεσίες να μπορούν να προσαρμόζονται στο μεγάλο εύρος των περιπτώσεων χρήσης του 5G. Η συνεργασία 3GPP<sup>10</sup>, παρέχει προδιαγραφές για τα δίκτυα 5G, ώστε να υπάρχει κοινός τόπος μεταξύ των κατασκευαστών. Οι προδιαγραφές αυτές ορίζουν ένα κοινό πλαίσιο για τις λειτουργίες δικτύου. Στο σχήμα που ακολουθεί παρουσιάζεται με λεπτομέρεια η αρχιτεκτονική 5G.

---

<sup>10</sup> 3rd Generation Partnership Project (3GPP)- συνεργασία ανάμεσα σε επτά οργανισμούς ανάπτυξης που αναπτύσσει προδιαγραφές συστήματος για την αρχιτεκτονική του δικτύου 5G,.Ιστότοπος: <https://www.3gpp.org/>



Σχήμα 1.4: Αρχιτεκτονική 5G<sup>11</sup>

### 1.2.2 Χαρακτηριστικά τεχνολογίας 5G

Η τεχνολογία 5G χαρακτηρίζεται από τα εξής:

- Φάσμα και συχνότητες:** Στις Νέες Ραδιοσυχνότητες (5G new radio – NR) έχει δοθεί πολλαπλό εύρος συχνοτήτων: α) το τμήμα του φάσματος των ραδιοσυχνοτήτων μεταξύ 30 GHz και 300 GHz (γνωστό ως κύμα χιλιοστών) β) οι συχνότητες μεταξύ 24 GHz και 100 GHz. και γ) οι ανεκμετάλλευτες συχνότητες UHF μεταξύ 300 MHz και 3 GHz. Αυτές οι ποικίλες συχνότητες, έχουν διαφορετικά χαρακτηριστικά και μπορούν να εξυπηρετήσουν διαφορετικές ανάγκες. Για παράδειγμα, οι συχνότητες

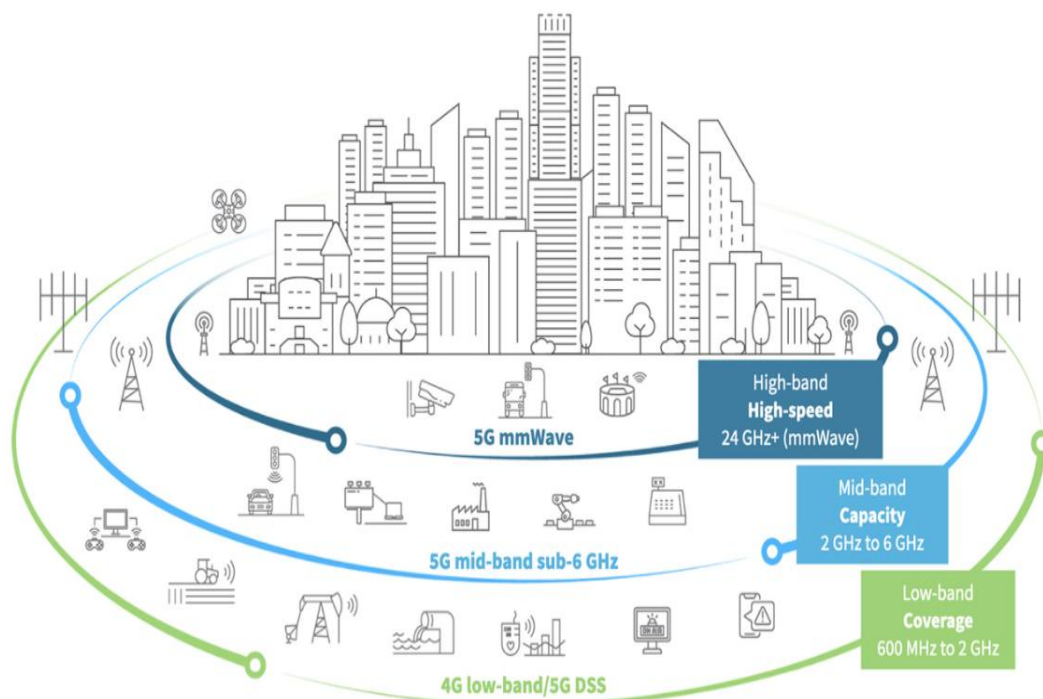
<sup>11</sup> Πηγή: <https://www.viavisolutions.com/en-us/5g-architecture> - πρόσβαση 8/2021



κυμάτων χιλιοστών είναι ιδανικές για πυκνοκατοικημένες περιοχές, αλλά αναποτελεσματικές για επικοινωνία μεγάλων αποστάσεων.

Στο κορμό του δικτύου 5G οι συχνότητες έχουν χωριστεί σε τρεις μπάντες:

- 5G high-band (mmWave) παρέχει τις υψηλότερες συχνότητες στο 5G. Από τα 24 GHz περίπου στα 100 GHz. Οι υψηλές συχνότητες δεν μπορούν εύκολα να περάσουν από εμπόδια. Έχουν μικρό εύρος από τη φύση τους και η κάλυψη που παρέχουν είναι περιορισμένη. Απαιτούνται έτσι, περισσότερες κυψελωτές υποδομές.
- 5G mid-band λειτουργεί σε εύρος 2-6 GHz και παρέχει ένα επίπεδο χωρητικότητας για αστικές περιοχές. Αυτή η μπάντα συχνοτήτων έχει τιμές αιχμής της τάξης των εκατοντάδων Mbps.
- 5G low-band λειτουργεί κάτω από τα 2 GHz και παρέχει μία ευρεία κάλυψη. Αυτή η μπάντα χρησιμοποιεί φάσμα που είναι διαθέσιμο και στο 4G LTE και ως εκ τούτου η απόδοση του low-band 5G είναι παρόμοια με αυτή του 4G LTE.



**Σχήμα 1.5:** Φάσμα συχνοτήτων Αρχιτεκτονικής 5G<sup>12</sup>

<sup>12</sup> Πηγή: <https://www.digi.com/blog/post/5g-network-architecture> - πρόσβαση 8/2021

- **Υπολογιστική Παρυφής Πολλαπλής Πρόσβασης (Multi-Access Edge Computing - MEC)** είναι ένα σημαντικό στοιχείο της αρχιτεκτονικής 5G. Είναι μια εξέλιξη στην υπολογιστική νέφους που φέρνει τις εφαρμογές από τα κέντρα δεδομένων στις «παρυφές - άκρες» του δικτύου, και άρα πιο κοντά στους χρήστες και τις συσκευές. Στην ουσία αυτό είναι μια «παράκαμψη του μεγάλου δικτυακού δρόμου» που χωρίζει το χρήστη από τους εξυπηρετητές που φιλοξενούν τις εφαρμογές. Η ανταλλαγή περιεχομένου ανάμεσα στο χρήστη και το «σταθμό φιλοξενίας» γίνεται πιο άμεσα.  
Χαρακτηριστικά της MEC είναι η χαμηλή καθυστέρηση, το υψηλό εύρος ζώνης και η πρόσβαση σε πραγματικό χρόνο σε πληροφορίες στο RAN, που διακρίνουν την αρχιτεκτονική 5G από τους προκατόχους της. Οι προδιαγραφές 5G ορίζουν τους παράγοντες ενεργοποίησης του υπολογισμού άκρων, επιτρέποντας στο MEC και το 5G να δρομολογούν συλλογικά την κίνηση.  
Τέλος, η κατανομή της υπολογιστικής ισχύος της MEC, αναμένεται να επιτρέψει το μεγάλο αριθμό συνδεδεμένων συσκευών που έχουν κληροδοτηθεί στην ανάπτυξη του 5G από την άνοδο του IoT.
- **Η Εικονικοποίηση Δικτυακών Λειτουργιών (Network function virtualization - NFV)** αποσυνδέει το λογισμικό από το υλικό αντικαθιστώντας διάφορες λειτουργίες δικτύου όπως τείχη προστασίας, εξισορροπητές φόρτου και δρομολογητές με εικονικά στιγμιότυπα που τρέχουν ως λογισμικό. Αυτό εξαλείφει την ανάγκη επένδυσης σε ακριβό υλικό και μπορεί επίσης να επιταχύνει τους χρόνους εγκατάστασης.
- **5G Radio Access Network (RAN)** Η έννοια του NFV επεκτείνεται στο RAN. Η εικονικοποίηση στοιχείων του δικτύου αποτελεί ένα μέσο για την κλιμάκωση των υπηρεσιών και τη βελτίωση της εμπειρίας του χρήστη καθώς αυξάνεται η χωρητικότητα. Τα οφέλη από την εικονικοποίηση στοιχείων του RAN, το καθιστούν πιο αποδοτικό από άποψη κόστους υλικού και λογισμικού, ειδικά για εφαρμογές IoT όπου ο αριθμός των συσκευών είναι εκατομμύρια.

- **Common Public Radio Interface- eCPRI<sup>13</sup>.** Η διαίρεση δικτύου με το διαχωρισμό των λειτουργιών φέρνει επίσης οφέλη κόστους. Ιδίως με την εισαγωγή νέων διεπαφών, όπως το eCPRI. Οι διεπαφές RF<sup>14</sup> δεν είναι οικονομικά αποδοτικές όταν αυξάνεται το πλήθος των σημάτων 5G και κατά συνέπεια, αυξάνεται κατά πολύ η ανάγκη για διεπαφές. Με τις διεπαφές eCPRI λιγότερες διεπαφές μπορούν να χρησιμοποιηθούν για τη δοκιμή πολλαπλών σημάτων 5G. Το eCPRI στοχεύει να είναι μια τυποποιημένη διεπαφή για 5G.
- **Τεμαχισμός Δικτύου (Network Slicing).** Ίσως το βασικότερο συστατικό που επιτρέπει την πλήρη αξιοποίηση των δυνατοτήτων της αρχιτεκτονικής 5G είναι ο τεμαχισμός δικτύου. Αυτή η τεχνολογία προσθέτει μια επιπλέον διάσταση στο NFV, επιτρέποντας ταυτόχρονα σε πολλαπλά λογικά δίκτυα να λειτουργούν πάνω σε μια κοινή φυσική υποδομή δικτύου. Αυτό καθιστά το network slicing αναπόσπαστο μέρος της αρχιτεκτονικής 5G, αφού δημιουργεί εικονικά δίκτυα από άκρο σε άκρο που περιλαμβάνουν τόσο λειτουργίες δικτύωσης όσο και αποθήκευσης. Οι χειριστές μπορούν να διαχειριστούν αποτελεσματικά διαφορετικές περιπτώσεις χρήσης του 5G, με διαφορετικές απαιτήσεις ταχύτητας μετάδοσης, καθυστέρησης και διαθεσιμότητας με διαίρεση πόρων δικτύου σε πολλαπλούς χρήστες ή «ενοικιαστές<sup>15</sup>». Ο τεμαχισμός δικτύου γίνεται εξαιρετικά χρήσιμος για εφαρμογές όπως το IoT όπου ο αριθμός των χρηστών μπορεί να είναι εξαιρετικά υψηλός. αλλά η συνολική ζήτηση εύρους ζώνης είναι χαμηλή.

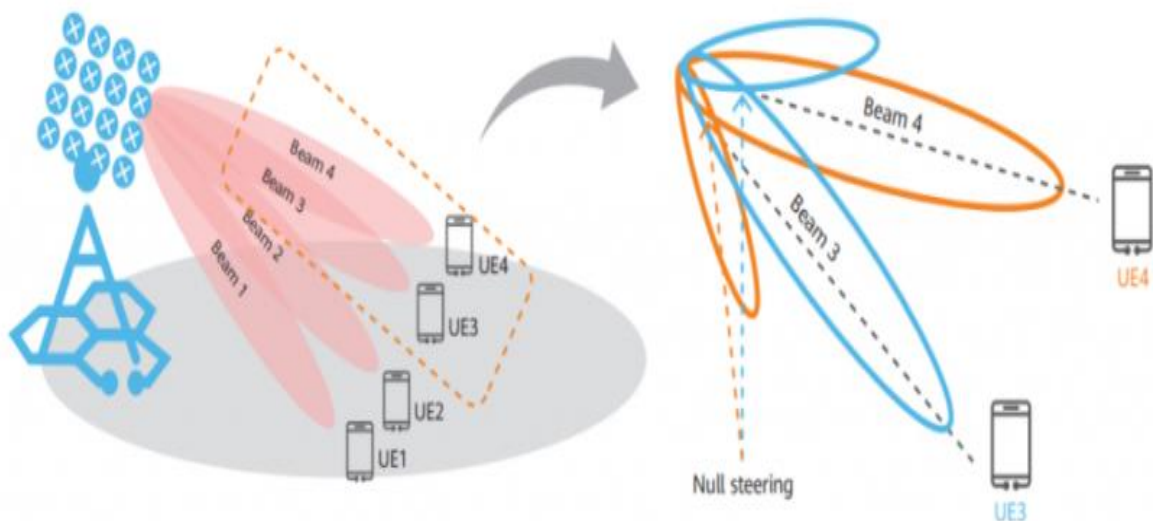
---

<sup>13</sup>eCPRI Πρότυπο που ορίζει τη διεπαφή ανάμεσα σε μία συσκευή Radio Equipment Control (REC) και μια συσκευή Radio Equipment (RE). Συχνά οι συνδέσεις CPRI χρησιμοποιούνται για τη μεταφορά δεδομένων ανάμεσα σε σημεία της κυψέλης και του σταθμού βάσης. Πηγή: [https://en.wikipedia.org/wiki/Common\\_Public\\_Radio\\_Interface](https://en.wikipedia.org/wiki/Common_Public_Radio_Interface) - Πρόσβαση 8/2021

<sup>14</sup>RF- Radio frequency

<sup>15</sup>Ενοικιαστής – tenant. Ένας εικονικός φορέας εκμετάλλευσης ή πάροχος υπηρεσιών.

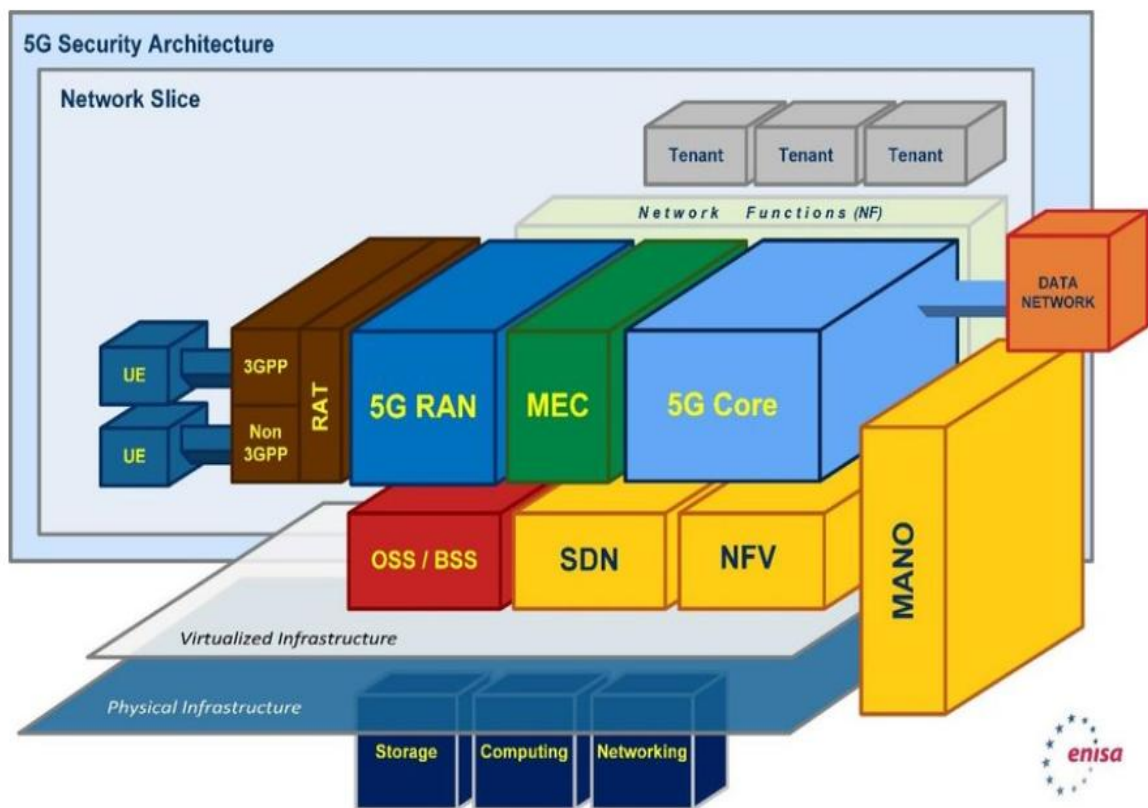
- **Διαμόρφωση δέσμης (Beamforming).** Μια ακόμα πρωτοποριακή τεχνολογία που είναι αναπόσπαστο μέρος της επιτυχίας του 5G είναι η διαμόρφωση δέσμης. Οι συμβατικοί σταθμοί βάσης μεταδίδουν σήματα σε πολλαπλές κατευθύνσεις, χωρίς να λαμβάνεται υπόψη η θέση των χρηστών ή συσκευών. Μέσω της χρήσης συστοιχιών πολλαπλής εισόδου, πολλαπλής εξόδου (MIMO), με δεκάδες μικρές κεραίες συνδυασμένες σε ένα μόνο σχηματισμό, μπορούν να χρησιμοποιηθούν αλγόριθμοι επεξεργασίας σήματος για τον προσδιορισμό της πιο αποτελεσματικής διαδρομής μετάδοσης σε κάθε χρήστη, ενώ μεμονωμένα πακέτα μπορούν να αποσταλούν σε πολλαπλές κατευθύνσεις. Τα πακέτα, κατόπιν συντονίζονται για να φτάσουν στον τελικό χρήστη με μια προκαθορισμένη ακολουθία. [8]



Σχήμα 1.6: Beamforming<sup>16</sup>

<sup>16</sup>Πηγή <https://blog.huawei.com/2020/08/17/the-wonders-of-5g-beamforming/> - προσπέλαση 8/2021

Ολοκληρώνοντας την παράγραφο 1.2 για τα δίκτυα 5G, ας δούμε το σχήμα που ακολουθεί ώστε να έχουμε κατά νου την αρχιτεκτονική των 5G σε υψηλό επίπεδο, με όλα εκείνα τα συστατικά στοιχεία που συνθέτουν μια δομή 5G, σημειώνοντας κυρίως τα σημεία που βρίσκονται τα SDN και τα NFV που παρουσιάζονται στη συνέχεια, αλλά και το μέγεθος που καταλαμβάνει το network slicing (το κύριο τμήμα της μελέτης μας, που θα δούμε αναλυτικά στο Κεφάλαιο 3)



5G High-level technical architecture

**Σχήμα 1.7** Αρχιτεκτονική 5G υψηλού επιπέδου<sup>17</sup>

<sup>17</sup>Πηγή Lourenco, Marco & Marinos, Louis. (2019). ENISA THREAT LANDSCAPE FOR 5G NETWORKS. 10.2824/49299.

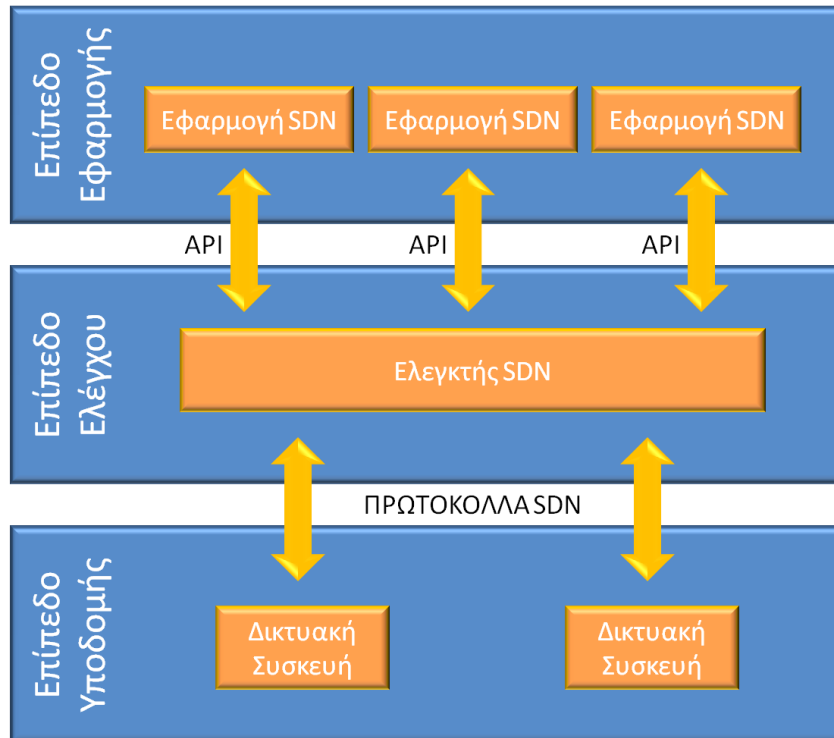
## **ΚΕΦΑΛΑΙΟ 2 - Αρχιτεκτονικές στα δίκτυα 5G - Δικτύωση Βάσει Λογισμικού και Εικονικοποίηση Δικτυακών Λειτουργιών**

Όπως είδαμε και στο κεφάλαιο 1, η ανάγκη διαχείρισης του τεράστιου όγκου δεδομένων σε συνδυασμό με τη μεγάλη διαφοροποίηση των απαιτήσεων, οδήγησαν τους επιστήμονες σε αναζήτηση λύσεων για τα ζητήματα και στην δημιουργία νέων αρχιτεκτονικών. Οι αρχιτεκτονικές Δικτύωσης Βάσει Λογισμικού (Software Defined Networking - SDN) και Εικονικοποίησης Δικτυακών Λειτουργιών (Network Function Virtualization - NFV), είναι οι λύσεις που προτείνονται για τα ζητήματα αυτά και παρουσιάζονται ακολούθως .

### **2.1 Δικτύωση Βάσει Λογισμικού (Software-Defined Networking – SDN)**

Η διαχείριση της λειτουργίας των παραδοσιακών δικτύων, προϋπέθετε την επιμέρους παραμετροποίηση των διαφόρων δικτυακών συσκευών που αποτελούσαν τη δικτυακή υποδομή. Η Δικτύωση Βάσει Λογισμικού (SDN) αποτελεί μία εναλλακτική προσέγγιση για τη λειτουργία και διαχείριση ενός δικτύου.

Η SDN διαχωρίζει το επίπεδο του ελέγχου από το επίπεδο της προώθησης των δεδομένων. Οι συσκευές του δικτύου εξακολουθούν να πραγματοποιούν την προώθηση των δεδομένων με βάση πίνακες κανόνων που διαθέτουν. Ωστόσο, η κατάρτιση των κανόνων αυτών παύει να αποτελεί ευθύνη και λειτουργία των ίδιων των συσκευών και ανατίθεται σε μία ξεχωριστή οντότητα λογισμικού, που ονομάζεται Ελεγκτής (Controller). Ο Ελεγκτής είναι κοινός για όλες τις συσκευές του δικτύου.



**Σχήμα 2.1:** Αρχιτεκτονική SDN

Στο Σχήμα 2.1 παρουσιάζεται η αρχιτεκτονική SDN, στην οποία διακρίνονται τρία επίπεδα [11]:

- Το επίπεδο εφαρμογής αποτελείται από προγράμματα τα οποία ενημερώνουν τον Ελεγκτή SDN για τις επιθυμητές συμπεριφορές του δικτύου και τους απαιτούμενους πόρους. Περιλαμβάνει εφαρμογές όπως τείχη προστασίας (firewall), συστήματα ανίχνευσης εισβολής κ.α.
- Το επίπεδο ελέγχου περιλαμβάνει τον Ελεγκτή SDN, ο οποίος λαμβάνει τα αιτήματα και τις οδηγίες των Εφαρμογών SDN, τα μεταφράζει σε συγκεκριμένους κανόνες και τα προωθεί στις δικτυακές συσκευές. Επιπλέον συλλέγει από τις συσκευές πληροφορίες για την κατάσταση και τη λειτουργία του δικτύου (π.χ. στατιστικά) και τα αναφέρει στις εφαρμογές SDN.
- Το επίπεδο υποδομής περιλαμβάνει τις δικτυακές συσκευές, οι οποίες υλοποιούν την προώθηση των πακέτων δεδομένων, με βάση τους κανόνες που έχουν καθοριστεί από τον Ελεγκτή.

Η διεπαφή μεταξύ του Ελεγκτή SDN και των εφαρμογών αναφέρεται διεθνώς ως Northbound Interface και περιλαμβάνει σχετικά API. Αντίστοιχα, η διεπαφή του Ελεγκτή με τις συσκευές αναφέρεται ως Southbound Interface και υλοποιείται με ειδικά πρωτόκολλα όπως το OpenFlow.

Η χρήση της SDN παρέχει μία σειρά από οφέλη.[12] Κατ' αρχάς, το δίκτυο καθίσταται προγραμματίσιμο, αφού η συμπεριφορά του και η λειτουργία του μπορούν να καθορίζονται από τις εφαρμογές SDN μέσω του ελεγκτή.

Επιπλέον, η παραμετροποίηση και ο έλεγχος του δικτύου μέσω του Ελεγκτή, έχει σαν αποτέλεσμα την κεντρικοποίηση της διαχείρισης. Με τον τρόπο αυτό απλουστεύονται και επιταχύνονται μία σειρά από εργασίες όπως η εφαρμογή πολιτικών και η προσθήκη νέων υπηρεσιών, ενώ το δίκτυο καθίσταται πιο ευέλικτο.

Ένα ακόμα όφελος που προκύπτει είναι η μείωση του κόστους. Από τη μία πλευρά, αυτό επιτυγχάνεται με τη δυνατότητα αξιοποίησης εφαρμογών SDN, που υποκαθιστούν συσκευές όπως τα firewall. Από την άλλη, ο διαχωρισμός του επιπέδου ελέγχου από το επίπεδο της προώθησης δεδομένων, επιτρέπει την υλοποίηση της δικτυακής υποδομής με συσκευές χαμηλότερων δυνατοτήτων και άρα με μικρότερο κόστος.

Τέλος, η χρήση ανοικτών πρωτοκόλλων (OpenFlow) και ανοικτών API στις διεπαφές της αρχιτεκτονικής SDN, διασφαλίζει τη διαλειτουργικότητα και την ανοικτότητα των δικτύων.

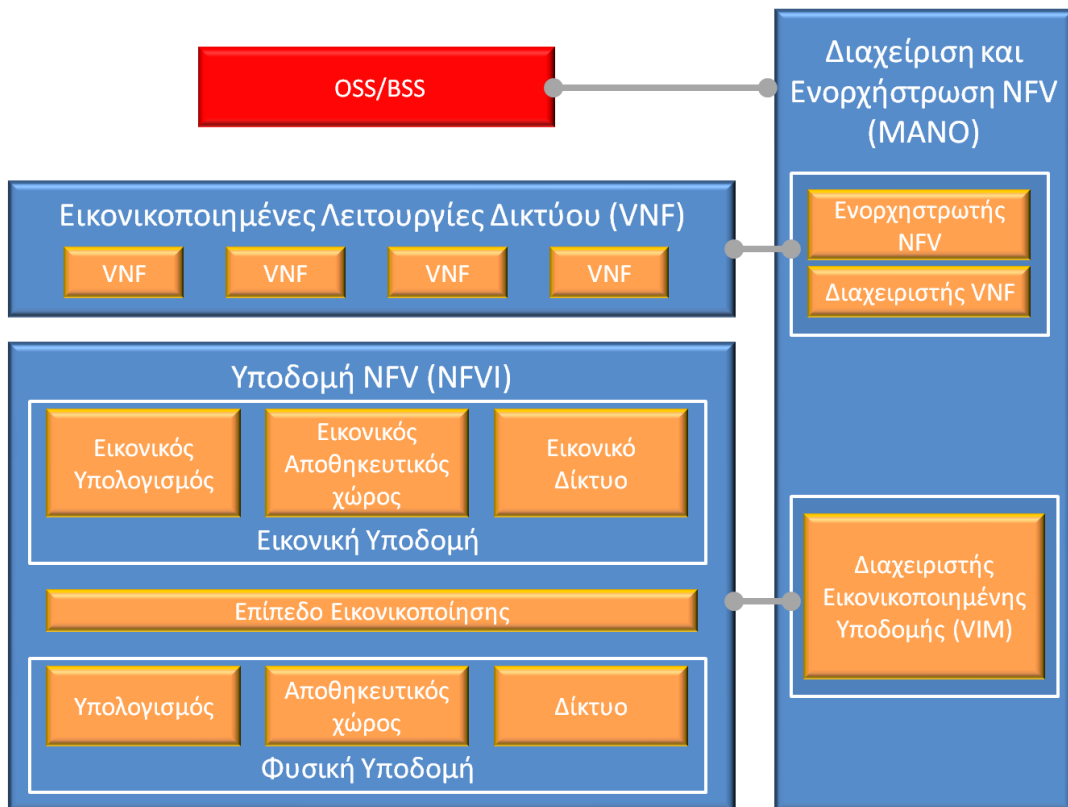
Παραδείγματα εφαρμογής της Δικτύωσης Βάσει λογισμικού συναντώνται ενδεικτικά:

- Σε δίκτυα παρόχων, τα οποία πρέπει να εξυπηρετούν πολυάριθμες εφαρμογές χρηστών με διαφορετικές απαιτήσεις.
- Σε δίκτυα κινητής τηλεφωνίας, όπου χρησιμοποιείται για την αποδοτική ενορχήστρωση των υπηρεσιών και τη δυναμική αξιοποίηση των πόρων.
- Σε εφαρμογές ροής Video, όπου διασφαλίζει την ποιότητα υπηρεσίας (QoS) μέσω της δέσμευσης χωρητικότητας.
- Σε δίκτυα DataCenter, όπου παρέχει δυνατότητες κλιμάκωσης και ευκολότερης εφαρμογής της πολιτικής ασφάλειας του δικτύου. [13],[14]



## 2.2 Εικονικοποίηση Δικτυακών Λειτουργιών (Network Function Virtualization – NFV)

Η Εικονικοποίηση Δικτυακών Λειτουργιών (NFV) είναι μία αρχιτεκτονική δικτύου, στην οποία λειτουργίες του δικτύου όπως η δρομολόγηση, το τείχος προστασίας και η εξισορρόπηση φόρτου, υλοποιούνται σε εξυπηρετητές με τη χρήση τεχνολογιών εικονικοποίησης. Με τον τρόπο αυτό, οι αφιερωμένες συσκευές υλικού που παρείχαν παραδοσιακά τις υπηρεσίες αυτές, αντικαθίστανται από τυπικούς εξυπηρετητές με εικονικές μηχανές που εκτελούν κατάλληλο λογισμικό.



Σχήμα 2.2: Αρχιτεκτονική NFV

Το Σχήμα 2.2 δείχνει τα βασικά στοιχεία της αρχιτεκτονικής NFV. Η Υποδομή Εικονικοποίησης Δικτυακών Λειτουργιών (Network Function Virtualization Infrastructure - NFVI), διαιρείται στη φυσική υποδομή και την εικονική υποδομή. Η φυσική υποδομή αποτελείται από υπολογιστές, οι οποίοι παρέχουν φυσικούς πόρους (υπολογιστική ισχύ, αποθηκευτικό χώρο κλπ.), καθώς και από δικτυακές συσκευές (π.χ. switch) και συνδέσεις, που διασυνδέουν τους υπολογιστές μεταξύ

τους. Πάνω στη φυσική υποδομή, με τη χρήση εργαλείων εικονικοποίησης, αναπτύσσεται η εικονική υποδομή. Η εικονική υποδομή παρέχει εικονικούς πόρους που μπορούν να προκύπτουν από το συνδυασμό φυσικών πόρων από πολλούς υπολογιστές ή να αποτελούν μέρος των πόρων ενός ισχυρού υπολογιστή.

Η Εικονικοποιημένη Λειτουργία Δικτύου (VirtualNetworkFunction – VNF) αποτελεί υλοποίηση μίας λειτουργίας του δικτύου (δρομολόγηση, διαμοιρασμός αρχείων, τείχος προστασίας κλπ.) με λογισμικό. Μία VNF μπορεί να εκτελείται σε μία ή περισσότερες εικονικές μηχανές (VirtualMachine – VM), οι οποίες χρησιμοποιούν τους πόρους που παρέχει η Υποδομή Εικονικοποίησης Δικτυακών Λειτουργιών και συνεργάζονται μεταξύ τους για την παροχή της υπηρεσίας κατά μήκος του δικτύου.

Η Διαχείριση και Ενορχήστρωση Δικτύου NFV (NFV Management And Network Orchestration – NFVMANO) είναι ένα πλαίσιο εργασίας που αναπτύχθηκε από το ETSI (European Telecommunications Standards Institute), για τη διαχείριση της Εικονικοποίησης Δικτυακών Λειτουργιών. Το πλαίσιο αυτό περιλαμβάνει τρεις λειτουργικές μονάδες:

- Τον Ενορχηστρωτή NFV, που είναι υπεύθυνος, για την ενσωμάτωση νέων υπηρεσιών και εικονικών λειτουργιών δικτύου, για τη διαχείριση του κύκλου ζωής των υπηρεσιών, για την καθολική διαχείριση πόρων και για την επικύρωση και εξουσιοδότηση των αιτημάτων προς την υποδομή για πόρους.
- Τον Διαχειριστή VNF, που ελέγχει τον κύκλο ζωής των Εικονικοποιημένων Λειτουργιών Δικτύου.
- Τον Διαχειριστή Εικονικοποιημένης Υποδομής (Virtual Infrastructure Manager) που ελέγχει και διαχειρίζεται τους υπολογιστικούς, αποθηκευτικούς και δικτυακούς πόρους της υποδομής NFV. [15]

Το σύστημα NFVMANO μπορεί να συνεργάζεται με ένα εξωτερικό σύστημα υποστήριξης λειτουργίας/επιχειρήσεων (OSS/BSS).

Η NFV παρέχει διάφορα πλεονεκτήματα. Οι λειτουργίες του δικτύου παύουν να εκτελούνται σε εξειδικευμένες ακριβές συσκευές κλειστής αρχιτεκτονικής και μεταφέρονται σε εξυπηρετητές. Επιπλέον, με δεδομένο ότι πάνω σε έναν υπολογιστή μπορούν να εκτελούνται περισσότερες Εικονικοποιημένες Λειτουργίες

Δικτύου, η χρήση της NFV μπορεί να οδηγήσει σε μείωση του απαιτούμενου υλικού. Με τον τρόπο αυτό μειώνεται τόσο το κόστος της προμήθειας εξοπλισμού, όσο και το κόστος λειτουργίας (μικρότεροι χώροι στέγασης, χαμηλότερη κατανάλωση ενέργειας κλπ.).

Η NFV αυξάνει επίσης την ευελιξία στα δίκτυα των παρόχων. Ενδεικτικά, η ενσωμάτωση μίας νέας υπηρεσίας δεν απαιτεί πλέον την προμήθεια εξειδικευμένου εξοπλισμού και μπορεί να πραγματοποιείται άμεσα μέσω της δημιουργίας νέων εικονικών μηχανών. Η κλιμάκωση της υποδομής γίνεται εύκολα με την προσθήκη υπολογιστών ακόμα και σε νέες τοποθεσίες. Η κλιμάκωση μίας Εικονικοποιημένης Υπηρεσίας υλοποιείται άμεσα είτε με την ανάθεση σε αυτήν πρόσθετων πόρων είτε με τη δημιουργία νέων εικονικών μηχανών. Ακόμα, δίνεται η δυνατότητα μεταφοράς υπηρεσιών από μία θέση του δικτύου σε μία άλλη, όταν κρίνεται ότι κάτι τέτοιο μπορεί να βελτιώσει την απόδοσή τους.

Παραδείγματα εφαρμογής της NFV συναντάμε:

- Σε δίκτυα τηλεπικοινωνιακών παρόχων για εικονικοποίηση του δικτύου.
- Στα δίκτυα κινητής τηλεφωνίας για υλοποίηση υπηρεσιών στα άκρα του δικτύου (edge network). Με τον τρόπο αυτό επιτυγχάνεται η μετάδοση μεγάλου όγκου δεδομένων από τερματικές συσκευές που εξυπηρετούνται π.χ. από τον ίδιο σταθμό βάσης, χωρίς να επιβαρύνεται το δίκτυο κορμού.
- Σε βιομηχανίες, όπου συσκευές παρακολούθησης της παραγωγής (βιντεοκάμερες, ενσωματωμένα συστήματα με δυνατότητες IoT κλπ.) παράγουν μεγάλο όγκο δεδομένων. Η επεξεργασία αυτών των δεδομένων κοντά στις συσκευές προέλευσης, διασφαλίζει τη χαμηλή καθυστέρηση απόκρισης και την αποφόρτιση του κεντρικού δικτύου.
- Στην ασφάλεια δικτύων, όπου η δυνατότητα κεντροποιημένου ελέγχου και κατανεμημένης επιβολής, αποτελεί σημαντικό πλεονέκτημα της χρήσης NFV. [16]

## ΚΕΦΑΛΑΙΟ 3 - Τεμαχισμός δικτύων 5G

Στις μέρες μας καταγράφονται σημαντικές εξελίξεις σε τομείς της τεχνολογίας όπως το Διαδίκτυο των Πραγμάτων, η αυτόνομη οδήγηση, και ο φορητός υπολογισμός, που σε μεγάλο βαθμό εξαρτώνται από την πρόσβασή τους σε δικτυακούς πόρους και υπηρεσίες. Τα δίκτυα 5<sup>ης</sup> γενιάς έρχονται σε αυτή τη συγκυρία, με την προσδοκία να αποτελέσουν τη δικτυακή τεχνολογία που θα στεγάσει και θα δώσει ώθηση σε όλες αυτές τις τεχνολογικές εξελίξεις. Σε αυτό το 3<sup>ο</sup> κεφάλαιο, μελετάται η τεχνική του τεμαχισμού δικτύων.

### 3.1 Ο Τεμαχισμός Δικτύου (Network Slicing)

Ο τεμαχισμός δικτύου είναι μία τεχνική που επιτρέπει τη δημιουργία πολλών ανεξάρτητων λογικών δικτύων, πάνω από μία κοινή φυσική δικτυακή υποδομή. Κάθε λογικό δίκτυο ονομάζεται τεμάχιο δικτύου (slice<sup>18</sup>) και περιλαμβάνει ένα υποσύνολο των υποκείμενων πόρων. Οι πόροι αυτοί μπορεί να αφορούν είτε πόρους υποδομής (π.χ. υπολογιστές, λογισμικό, δικτυακές συσκευές, τηλεπικοινωνιακές γραμμές κλπ.), είτε δικτυακές λειτουργίες (NF) που εκτελούνται πάνω σε πόρους υποδομής και παρέχουν συγκεκριμένες υπηρεσίες δικτύου.

Κάθε τεμάχιο έχει συγκεκριμένα χαρακτηριστικά σε όρους εύρους ζώνης, καθυστέρησης, αξιοπιστίας και ασφάλειας, ώστε να ανταποκρίνεται σε συγκεκριμένες απαιτήσεις υπηρεσίας. Βασική ιδιότητα του τεμαχισμού δικτύων είναι η απομόνωση μεταξύ των τεμαχίων. Τα τεμάχια μπορούν να χρησιμοποιούνται για την εξυπηρέτηση ομάδων χρηστών ή εφαρμογών με διαφορετικές απαιτήσεις ή ακόμα και να αποδίδονται σε διαφορετικούς εταιρικούς πελάτες.

Επιγραμματικά, τα πλεονεκτήματα της τεχνικής network slicing είναι:

- 1) Η απομόνωση τεμαχίου (Slice isolation). Η πλήρης απομόνωση των τεμαχίων επιτρέπει τον απλούστερο και πιο αποδοτικό σχεδιασμό κάθε τεμαχίου, με στόχο την κάλυψη των απαιτήσεων συγκεκριμένων κάθετων

---

<sup>18</sup>Slice- τεμάχιο ή φέτα

- εφαρμογών<sup>19</sup> και υπηρεσιών. Ακόμα, σε περίπτωση αποτυχίας, υπερφόρτωσης ή επίθεσης σε ένα τεμάχιο δεν επηρεάζεται η λειτουργία άλλων τεμαχίων στο δίκτυο.
- 2) Απλοποιημένες αλυσίδες υπηρεσιών (Simplified service chains): Σε αντίθεση με τις παραδοσιακές κινητές επικοινωνίες στις οποίες όλες οι υπηρεσίες αποτελούνται από τις ίδιες λειτουργίες, στον τεμαχισμό δικτύου κάθε υπηρεσία μπορεί να συσχετιστεί με διαφορετικό υποσύνολο λειτουργιών.
  - 3) Ευέλικτη τοποθέτηση NFV. Το NFV εισάγει έναν επιπλέον βαθμό ελευθερίας σε σχέση με την τοποθέτηση λειτουργιών στο δίκτυο. Αυτή η έξυπνη τοποθέτηση μπορεί να βελτιώσει την απόδοση του δικτύου και να μειώσει τα τηλεπικοινωνιακά κόστη.
  - 4) Διάφανη διαχείριση τεμαχίων. Υποσύνολα των φυσικών πόρων ενός δικτύου μπορεί να ανήκουν σε διαφορετικούς τομείς (domain) δικτύων (ακόμα και σε διαφορετικούς διαχειριστές). Ο τεμαχισμός δικτύων παρέχει μια «αφαίρεση» των φυσικών πόρων και κάνει τη διαχείριση των τεμαχίων διάφανη προς τους ενοικιαστές.[17]

### 3.2 Η ανάγκη τεμαχισμού των δικτύων 5G

Τα δίκτυα 5G καλούνται να εξυπηρετήσουν έναν πολύ μεγάλο και διαρκώς αυξανόμενο αριθμό χρηστών, τερματικών συσκευών και εφαρμογών, με διαφορετικές ανάγκες και απαιτήσεις από το δίκτυο. Οι χρήσεις του δικτύου μπορούν να ομαδοποιηθούν στις τρεις ακόλουθες γενικές κατηγορίες:

- Ενισχυμένη κινητή ευρυζωνικότητα (enhanced Mobile Broad Band – eMBB)
- Μαζική επικοινωνία τύπου μηχανής (massive Machine Type Communication – mMTC)
- Εξαιρετικά αξιόπιστη επικοινωνία χαμηλής καθυστέρησης (Ultra Reliable Low Latency Communication – URLLC) [18]

---

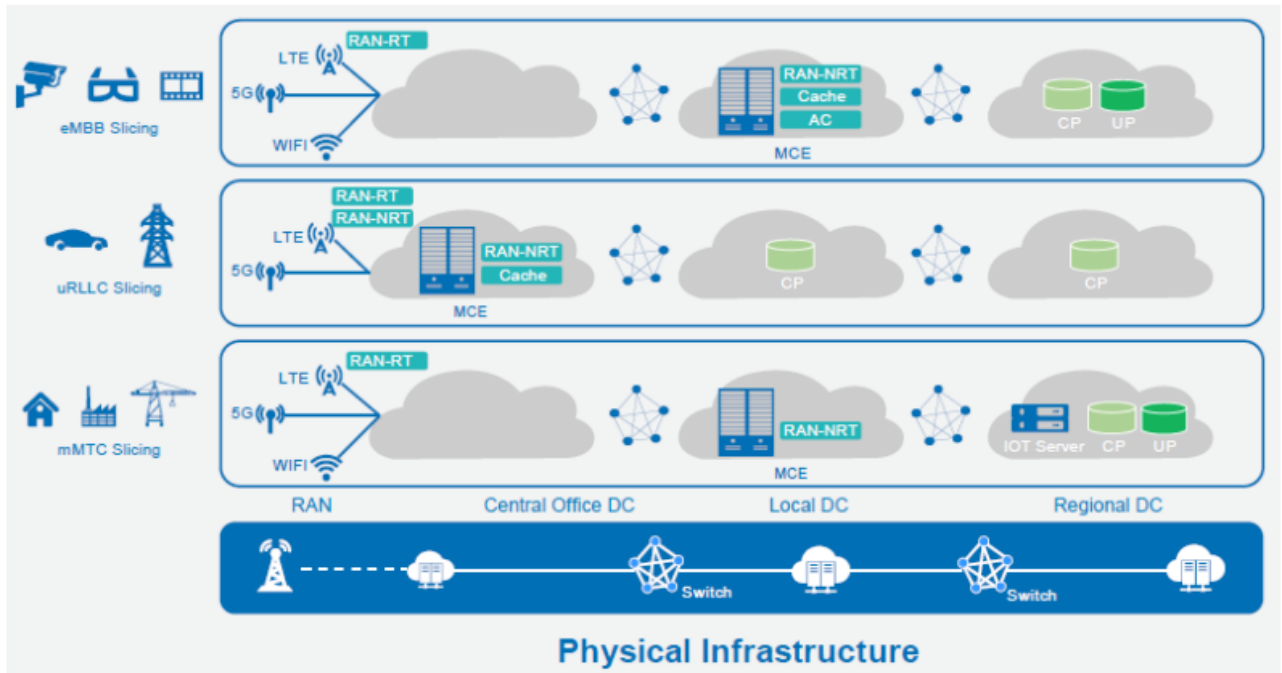
<sup>19</sup>Κάθετη εφαρμογή (vertical application) – Μια κάθετη εφαρμογή είναι λογισμικό που χειριστεί και κατασκευαστεί σύμφωνα με τις συγκεκριμένες απαιτήσεις ενός χρήστη ώστε να επιτευχθούν συγκεκριμένες λειτουργίες και διαδικασίες, μοναδικές για αυτό τον χρήστη.

Η eMBB υποστηρίζει εφαρμογές που τυπικά απαιτούν τη διακίνηση μεγάλου όγκου δεδομένων, με υψηλούς ρυθμούς μετάδοσης και με συνδέσεις που παραμένουν σταθερές για σχετικά μεγάλα χρονικά διαστήματα. Οι εφαρμογές eMBB απαιτούν από το δίκτυο υψηλό εύρος ζώνης και μέτρια αξιοπιστία. Χαρακτηριστικό παράδειγμα αυτής της κατηγορίας αποτελεί η μετάδοση video υψηλής ευκρίνειας.

Η mMTC έχει ως σκοπό την εξυπηρέτηση συσκευών του Διαδικτύου των Πραγμάτων. Οι συσκευές αυτές ενεργοποιούνται περιοδικά, για σύντομο χρονικό διάστημα και αποστέλλουν έναν σταθερό, μικρό όγκο δεδομένων. Η ευρεία διάδοση των ενσωματωμένων συστημάτων που διαθέτουν δυνατότητες IoT, θα οδηγήσει τα επόμενα χρόνια σε έναν εξαιρετικά μεγάλο αριθμό τέτοιων συσκευών. Με δεδομένο δε, ότι σε πολλές περιπτώσεις οι σχετικές εφαρμογές απαιτούν φορητότητα (π.χ. wearables) ή τοποθέτηση σε σημεία με περιορισμένες δυνατότητες συνδεσιμότητας (π.χ. δίκτυα αισθητήρων στην ύπαιθρο), τα δίκτυα 5G θα πρέπει να εξυπηρετήσουν το σημαντικότερο όγκο των συσκευών της κατηγορίας αυτής.

Η URLLC υποστηρίζει εφαρμογές όπου η υψηλή αξιοπιστία και η χαμηλή καθυστέρηση αποτελούν κρίσιμους παράγοντες. Όπως συμβαίνει και με την mMTC, η μετάδοση είναι διακοπτόμενη και ο ρυθμός των δεδομένων μικρός, αλλά στη URLLC είναι μικρότερο το πλήθος των συσκευών που εκπέμπουν. Η βασική απαίτηση της URLLC είναι η αξιοπιστία και η χαμηλή καθυστέρηση. Παραδείγματα εφαρμογών της κατηγορίας αποτελούν η αυτόνομη οδήγηση και η τηλεχειρουργική, όπου η αξιόπιστη μεταφορά των δεδομένων και η χαμηλή καθυστέρηση είναι ζωτικής σημασίας.

Από τα παραπάνω γίνεται αντιληπτό, ότι οι απαιτήσεις που έχουν από το δίκτυο οι υπηρεσίες eMBB, mMTC και URLLC, διαφοροποιούνται σημαντικά μεταξύ τους και δεν μπορούν εύκολα να συνυπάρξουν πάνω από μία κοινή δικτυακή υποδομή. Αυτός είναι ο λόγος που η τεχνική του τεμαχισμού, που επιτρέπει τη δημιουργία λογικών δικτύων, με διαφορετικά χαρακτηριστικά, ανεξάρτητη διαχείριση και λειτουργική απομόνωση, είναι ιδανική για τα δίκτυα 5ης γενιάς.



Σχήμα 3.1: Network slicing<sup>20</sup>

### 3.3 Κατηγοριοποίηση network slicing

Χωρίζουμε το Network slicing σε 2 επίπεδα ταξινόμησης ανάλογα με τα σενάρια χρήσης:

- 1) **Τεμαχισμός με βάση την ποιότητα υπηρεσίας (QoS Slicing):** Στόχος εδώ είναι η δημιουργία τεμαχίων που να προσφέρουν διαφορετικές υπηρεσίες και να εξασφαλίζεται κάποιο επίπεδο QoS μέσα στο κάθε τεμάχιο. Για παράδειγμα, μπορεί να δημιουργηθεί ένα τεμάχιο για να παρέχεται εξυπηρέτηση σε μια συγκεκριμένη ομάδα συσκευών με τις ίδιες απαιτήσεις ή ανάλογα με τον τύπο της εφαρμογής.
- 2) **Τεμαχισμός διαμοιρασμού υποδομής (Infrastructure Sharing Slicing):** Αυτή είναι η παραδοσιακή ιδέα της εικονικοποίησης δικτύου όπου υπάρχει ένας ενοικιαστής, στον οποίο δίνεται ένα τεμάχιο δικτύου. Ο ενοικιαστής έχει πλήρη έλεγχο της υποδομής δικτύου και των λειτουργιών εντός του συγκεκριμένου τεμαχίου.[19],[20]

<sup>20</sup> Πηγή: <https://moniem-tech.com/questions/why-network-slicing-is-important-for-5g/>

Μια ακόμα ταξινόμηση, που απαντά κυρίως στο μέχρι που ή σε ποιο επίπεδο εφαρμόζεται ο τεμαχισμός δικτύου έχει ταξινομήσει τον τεμαχισμό σε 3 επίπεδα:

- 1) **Τεμαχισμός σε επίπεδο φάσματος (Spectrum-level slicing):** Το φάσμα μπορεί να τεμαχιστεί με πολυπλεξία χρόνου, χώρου ή συχνότητας ή με επικάλυψη πρόσβασης. Μπορεί να θεωρηθεί ως εικονικοποίηση σύνδεσης (link virtualization).
- 2) **Τεμαχισμός σε επίπεδο υποδομής (Infrastructure-level slicing):** Είναι ο τεμαχισμός φυσικών στοιχείων δικτύου όπως: κεραιές, σταθμοί βάσης (BSs), επεξεργαστές, μνήμη. Αυτό επιτυγχάνεται κυρίως με την εικονικοποίηση.
- 3) **Τεμαχισμός σε επίπεδο δικτύου (Network-level slicing):** Πρόκειται για τον τεμαχισμό όλων των υποδομών δικτύου.

Μια ακόμα κατηγοριοποίηση που μπορούμε να κάνουμε στον τεμαχισμό δικτύου είναι με βάση τον αλγόριθμο που χρησιμοποιείται, δηλαδή τον τρόπο που γίνεται η κατάτμηση. Έτσι έχουμε:

- 1) **Στατικό τεμαχισμό δικτύων.** Οι διαχειριστές δικτύων, με βάση τις ανάγκες και τις απαιτήσεις, αλλά και τους διαθέσιμους πόρους, κάνουν την κατάτμηση χωρίς στη συνέχεια να υπάρχει βαθμός ελευθερίας. Οποιαδήποτε μεταβολή στα τεμάχια απαιτεί την εκ νέου παραμετροποίησή τους. Όπως μπορεί να γίνει εύκολα αντιληπτό, η τάση αυτή είναι περιορισμένη.
- 2) **Δυναμικό τεμαχισμό δικτύων.** Κύριος στόχος του δυναμικού τεμαχισμού δικτύων είναι να επιτρέπει στα τεμάχια να προσαρμόζονται δυναμικά ανάλογα με τις συνθήκες που επικρατούν στο δίκτυο. Ο δυναμικός τεμαχισμός δικτύων σχεδιάστηκε ώστε να υποστηρίζει την ελαστικότητα στα δίκτυα και οι αλγόριθμοι για την υλοποίησή του αποτελούν ένα από τα κύρια πεδία μελετών των ερευνητών. [17]

### 3.4 Τεμαχισμός δικτύου 5G με τη χρήση SDN και NFV

Όπως παρουσιάστηκε στην ενότητα 2.2, ο Ελεγκτής SDN παίζει το ρόλο του ενδιάμεσου ανάμεσα στις εφαρμογές και τους υποκείμενους πόρους. Στη διεπαφή του με τις εφαρμογές (northbound interface), ο Ελεγκτής λειτουργεί ως ένας

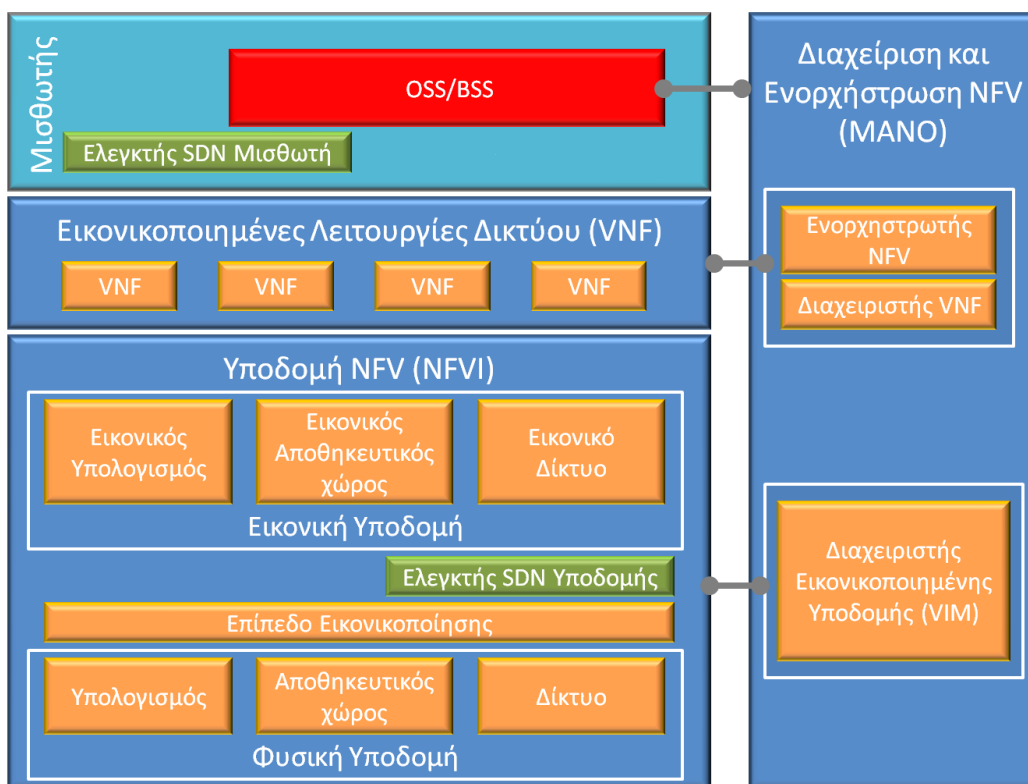


εξυπηρετητής που δέχεται αιτήματα για παροχή πόρων. Στη διεπαφή του με την υποδομή (southbound interface), λειτουργεί ως ένας πελάτης που αλληλεπιδρά με τους υποκείμενους πόρους.

Χρησιμοποιώντας εικονικοποίηση, παρέχει σε μία εφαρμογή/πελάτη ένα σύνολο πόρων, τους οποίους χρειάζεται για να επιτελέσει τη λειτουργία της. Μέσω της ενορχήστρωσης, εντάσσει με βέλτιστο τρόπο τους πόρους στα διάφορα ξεχωριστά σύνολα που παρέχει στις εφαρμογές. Έτσι καταφέρνει να εκπληρώνει τις ποικίλες απαιτήσεις υπηρεσίας των πελατών, διατηρώντας την απομόνωση μεταξύ τους. Συνεπώς, ο Ελεγκτής SDN παρέχει τις λειτουργίες επιπέδου ελέγχου, που καθιστούν εφικτή τη δημιουργία ενός τεμαχίου.

Η αρχιτεκτονική NFV από την άλλη, έρχεται να καλύψει την ανάγκη της διαχείρισης του κύκλου ζωής των τεμαχίων και των πόρων που τα αποτελούν, καθώς διαχειρίζεται τους πόρους της υποδομής και ενορχηστρώνει την ανάθεση τέτοιων πόρων που χρειάζονται για την υλοποίηση των VNF και των δικτυακών υπηρεσιών [21].

Το ETSI προτείνει την ενσωμάτωση της SDN στην NFV, μέσα από την προσθήκη δύο Ελεγκτών SDN στην αρχιτεκτονική της NFV [22]. Το Σχήμα 3.2 αποτυπώνει τη συγκεκριμένη πρόταση.



**Σχήμα 3.2:** Προσθήκη Ελεγκτών SDN στην αρχιτεκτονική NFV

Ο πρώτος Ελεγκτής τοποθετείται στο πεδίο του ενοικιαστή της υπηρεσίας και αναφέρεται ως Ελεγκτής Ενοικιαστή (Tenant Controller – TC). Ρόλος του είναι να αλληλεπιδρά με τις διάφορες χρησιμοποιούμενες VNF, ώστε να τις καθοδηγεί να ενεργούν πάνω στη δικτυακή κίνηση. Ο Ελεγκτής Ενοικιαστή μπορεί να υλοποιείται και ο ίδιος ως μία VNF.

Από την άλλη πλευρά, ο Ελεγκτής Υποδομής (Infrastructure Controller – IC), είναι υπεύθυνος για την εγκαθίδρυση της συνδεσιμότητας που απαιτείται για την επικοινωνία μεταξύ των VNF και μεταξύ των συστατικών τους στοιχείων. Η διαχείριση του Ελεγκτή Υποδομής γίνεται από τον VIM.

### 3.5 Προκλήσεις στον τεμαχισμό δικτύων

Τα δίκτυα 5G και ο τεμαχισμός δικτύου είναι νέες αναδυόμενες τεχνολογίες σε εξέλιξη και ως τέτοιες ενέχουν πολλές προκλήσεις για τους ερευνητές.

#### Ασφάλεια

Η **Ασφάλεια (Security)** είναι ένα από τα κυριότερα προβλήματα – και ίσως το σημαντικότερο – και συγκεκριμένα για το network slicing περιλαμβάνει τα παρακάτω:

- 1) **Κίνδυνος για την ιδιωτικότητα (privacy risk) στην πρόσβαση των τερματικών στο δίκτυο.** Οι πληροφορίες υποβοήθησης επιλογής τεμαχίων εκτίθενται κατά τη μετάδοση μέσω του αέρα. Έτσι, συγκεκριμένες τερματικές συσκευές μπορεί να γίνουν ευάλωτες στην παρακολούθηση ή συγκεκριμένες πληροφορίες συνδρομής των χρηστών μπορούν να εκτεθούν κατά την πρόσβαση σε ορισμένες υπηρεσίες.
- 2) **Κίνδυνος τεμαχίων στον κορμό του δικτύου.** Οι ενοικιαστές περιμένουν τα τεμάχια του δικτύου που τους έχουν ανατεθεί να συμπεριφέρονται ως αυτόνομα (standalone), πλήρως ανεξάρτητα δίκτυα κινητής τηλεφωνίας. Θα πρέπει λοιπόν, να απαγορεύεται στους ενοικιαστές η μη εξουσιοδοτημένη πρόσβαση σε άλλα τεμάχια δικτύου και η μη εξουσιοδοτημένη παρακολούθηση δεδομένων άλλων ενοικιαστών.

Όμως, ο τεμαχισμός δικτύου βασίζεται πάνω στις τεχνολογίες cloud και λογισμικού, όπου τα σφάλματα μπορούν να διαδοθούν και σε άλλα κομμάτια δικτύου μέσω του επιπέδου εικονικής αφαίρεσης.

Ως εκ τούτου, οι πάροχοι ασφάλειας απαιτείται να αναπτύξουν επαρκείς και ολοκληρωμένους αμυντικούς μηχανισμούς, για την προστασία όλων των τεμαχίων δικτύου. Αυτοί οι αμυντικοί μηχανισμοί πρέπει να λαμβάνουν υπόψη τα παραδοσιακά περιβάλλοντα φυσικού δικτύου καθώς και τα εικονικοποιημένα περιβάλλοντα που έχουν χτιστεί πάνω από αυτά.

Συγκεκριμένα οι κίνδυνοι του network slicing σε επίπεδο κορμού συνοψίζονται ως εξής:

- **Κίνδυνος διαμοιρασμού λειτουργιών δικτύου (NF) ανάμεσα στα τεμάχια:** Για να μπορέσει ένα μόνο τερματικό πρόσβασης να προσπελάσει πολλαπλά τεμάχια ταυτόχρονα, τα τεμάχια ενδέχεται να διαμοιράζονται ορισμένες λειτουργίες δικτύου. Όταν τα δεδομένα στο επίπεδο ελέγχου κάθε τεμαχίου χρησιμοποιούν το ίδιο πλαίσιο ασφαλείας, ενδέχεται να υπάρχει κίνδυνος εμπιστευτικότητας. Επιπλέον, κακόβουλα UE ενδέχεται να ξεκινήσουν επιθέσεις DoS/DDoS στα κοινόχρηστα NF, με αποτέλεσμα να διαταράσσεται η κανονική λειτουργία όλων των τεμαχίων, με την εξάντληση των κοινών πόρων.
- **Κίνδυνος απομόνωσης πόρων.** Τα τεμάχια τρέχουν σε μια ενοποιημένη φυσική υποδομή αλλά είναι εικονικά διαμοιρασμένα σε απομονωμένες λογικές λειτουργίες. Με την εμφάνιση ορισμένων ευπαθειών στην εικονικοποίηση, εμφανίστηκαν επίσης και κίνδυνοι επιθέσεων, μη εξουσιοδοτημένης χρήσης διαμοιρασμένων πόρων και μη εξουσιοδοτημένων συνδέσεων ανάμεσα σε VNF. Η αποτυχία ενός τεμαχίου ή των πόρων του μπορεί να επηρεάσει αρνητικά τη λειτουργία άλλων τεμαχίων λόγω της κοινής χρήσης φυσικής υποδομής.
- **Κίνδυνος παράνομης δια-λειτουργικότητας μεταξύ NF:** Κάποια NF που χρησιμοποιούνται για γενικές υπηρεσίες, μπορεί να επιχειρήσουν μη εξουσιοδοτημένη αλληλεπίδραση με NF σε ένα συγκεκριμένο τεμάχιο, για το οποίο θα πρέπει να έχει απαγορευτεί η πρόσβαση.

**3) Κίνδυνος διαχείρισης τεμαχισμού.** Το σύστημα διαχείρισης δικτύου για τον τεμαχισμό χρησιμοποιείται για τη διαχείριση του κύκλου ζωής των τεμαχίων και των σχέσεων μεταξύ τους. Κίνδυνοι ασφάλειας υπάρχουν σε κάθε στάδιο του κύκλου ζωής ενός τεμαχίου. Για παράδειγμα, ένας εισβολέας μπορεί να εμφυτεύσει κακόβουλο λογισμικό σε ένα πρότυπο τεμαχίου και να απειλήσει όλα τα τεμάχια δικτύου που δημιουργούνται με το πρότυπο αυτό. Ένας εισβολέας μπορεί επίσης να επιτεθεί σε τεμάχια μέσω της διεπαφής διαμόρφωσης κατά το στάδιο της διαμόρφωσης ή της λειτουργίας. Ακόμη και όταν τα τεμάχια βρίσκονται στο στάδιο της ανάκλησης, ένας εισβολέας μπορεί να λάβει εμπιστευτικά δεδομένα εάν τα δεδομένα δεν προστατεύονται σωστά. [23],[24]

### **Εγγύηση πόρων και QoS**

Για να λειτουργήσει σωστά ο τεμαχισμός δικτύου πρέπει να υπάρχουν εγγυημένοι πόροι που θα παρέχουν την κατάλληλη ποιότητα υπηρεσιών (QoS). Η κατανομή των πόρων του δικτύου μεταξύ των ενοικιαστών των τεμαχίων, πρέπει να γίνεται με τέτοιο τρόπο που να μη μένουν πόροι ανεκμετάλλετοι. Ο διαμοιρασμός των πόρων με δυναμικό τρόπο φαίνεται να είναι μια σαφώς πιο αποδοτική μέθοδος σε σχέση με τον στατικό.

### **Τυποποίηση**

Η ραγδαία εξέλιξη των δικτύων 5G και τα νέα κύματα 5G New Radio (NR) έχουν επιφέρει, όπως είδαμε και στο κεφάλαιο 1, μεγάλο βαθμό πολυπλοκότητας στην αρχιτεκτονική των κινητών δικτύων. Η τυποποίηση γύρω από το δίκτυο 5G έχει μέγιστη σημασία, ώστε να υπάρχουν κοινοί κώδικες ανάμεσα στους ερευνητές και τους κατασκευαστές, και ώστε η αρχιτεκτονική των δικτύων 5G να μπορεί να υποστηρίξει την έγκαιρη έναρξη νέων υπηρεσιών.

Μια μεγάλη πρόκληση είναι να εφαρμοστεί μία κοινά αποδεκτή, ενιαία, ολοκληρωμένη λύση λαμβάνοντας υπόψη τις νέες πτυχές των 5G New Radio, των χαρακτηριστικών των δικτύων 5G (όπως οι ξεχωριστές λειτουργίες και το Network Slicing), των υπηρεσιών Cloud και άλλων τεχνολογιών, οι οποίες μπορούν να υποστηρίξουν τις αυξημένες απαιτήσεις όλων των περιπτώσεων χρήσης των δικτύων 5G.

### **Αυτόνομη και Δυναμική ρύθμιση Παραμέτρων**

Η τεχνολογία network slicing έχει δημιουργήσει νέες απαιτήσεις για αυτόνομη και δυναμική ρύθμιση παραμέτρων δικτύου. Το συγκεκριμένο θέμα αποτελεί πεδίο εκτεταμένης έρευνας, με τους ερευνητές να αναζητούν διαρκώς νέους, βελτιωμένους αλγορίθμους, για την αποδοτικότερη αξιοποίηση των πόρων και την αυτοματοποίηση των διαδικασιών. Μεγάλο ενδιαφέρον παρουσιάζει το πώς θα μπορούσε στο μέλλον η Τεχνητή Νοημοσύνη να διαχειρίζεται τέτοια ζητήματα.

### **User Equipment Slicing**

Το δίκτυο 5G καλείται να διαφοροποιεί τη συμπεριφορά του προς τις συσκευές, ανάλογα με τα χαρακτηριστικά και τη χρήση τους. Έτσι, μία συσκευή που ανήκει σε ένα συγκεκριμένο τύπο, θα πρέπει να είναι συνδεδεμένη με ένα συγκεκριμένο τύπο network slice που θα της παρέχει το απαραίτητο QoS για την σωστή λειτουργία της. Η αντιστοίχιση αυτή υπόσχεται να φέρει μεγαλύτερη ελευθερία, προσαρμοστικότητα και ένα πλήθος διαθέσιμων εφαρμογών στους χρήστες.

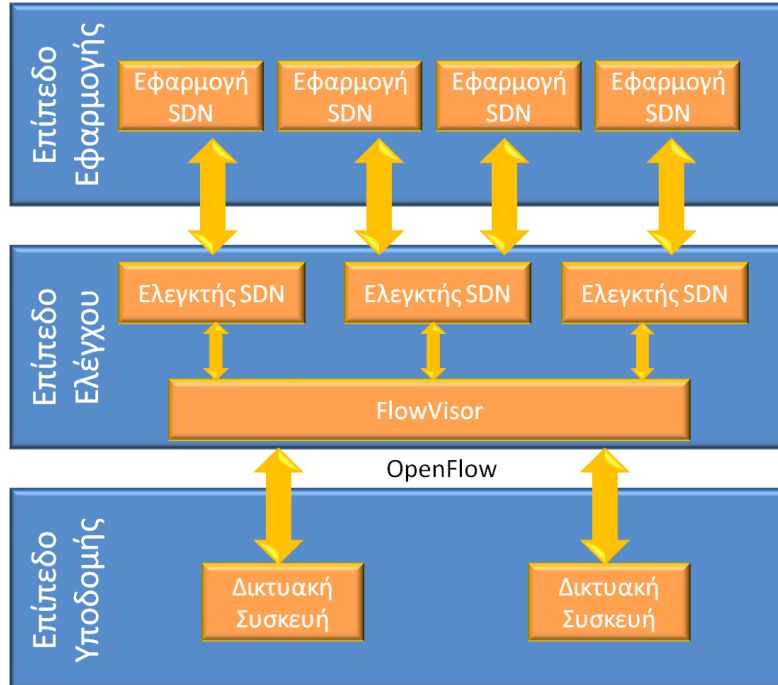
## ΚΕΦΑΛΑΙΟ 4 - Επίδειξη Network Slicing με χρήση του FlowVisor

Στόχος του Κεφαλαίου 4, που αποτελεί το πρακτικό μέρος της διπλωματικής, είναι η δημιουργία ενός lab για την παρουσίαση της τεχνικής του τεμαχισμού δικτύου. Για το σκοπό αυτό, θα δημιουργήσουμε ένα δίκτυο μέσω λογισμικού προσομοίωσης και στη συνέχεια θα το χωρίσουμε σε slice.

Το κεφάλαιο ξεκινάει με μία αναφορά στα εργαλεία λογισμικού FlowVisor και Mininet και στη συνέχεια παρουσιάζονται οι ενέργειες που απαιτούνται για την προετοιμασία και τη διεξαγωγή του εργαστηρίου.

### 4.1 FlowVisor

Το FlowVisor<sup>21</sup> είναι ένας Ελεγκτής SDN ειδικού σκοπού, που αναπτύχθηκε στο Stanford και επιτρέπει τη δημιουργία slice μέσα σε ένα δίκτυο. Στη βασική αρχιτεκτονική της SDN, λειτουργεί ως ένα ενδιάμεσο επίπεδο, που παρεμβάλλεται μεταξύ της δικτυακής υποδομής και του επιπέδου ελέγχου, παρέχοντας λειτουργίες εικονικοποίησης (Σχήμα 4.1). [25]



Σχήμα 4.1: Το FlowVisor στην Αρχιτεκτονική SDN

<sup>21</sup> Επίσημη ιστοσελίδα: <https://github.com/OPENNETWORKINGLAB/flowvisor/>

Συγκεκριμένα, στο FlowVisor ορίζονται πολιτικές ανάθεσης πόρων, με σκοπό τη δημιουργία λογικών δικτύων πάνω από την κοινή φυσική υποδομή. Κάθε λογικό δίκτυο είναι ένα slice και αποτελείται από ένα υποσύνολο των φυσικών πόρων.

Στη διεπαφή του προς το επίπεδο ελέγχου, μπορεί να επικοινωνεί με έναν ή περισσότερους Ελεγκτές SDN, παρουσιάζοντάς τους μία εικονικοποιημένη όψη του δικτύου, με βάση τις πολιτικές.

Οι Ελεγκτές SDN αγνοούν την πραγματική δικτυακή υποδομή και αντιλαμβάνονται ως επίπεδο υποδομής το slice που τους παρουσιάζει το FlowVisor. Όταν στέλνουν με το πρωτόκολλο OpenFlow μηνύματα ελέγχου για να καθορίσουν τη λειτουργία των συσκευών στο slice που τους έχει ανατεθεί, το FlowVisor λαμβάνει αυτά τα μηνύματα, τα προσαρμόζει και τα προωθεί στις φυσικές συσκευές.

Αντίστοιχα όταν μία συσκευή υποβάλει ένα ερώτημα (πάλι με το πρωτόκολλο OpenFlow) για τον χειρισμό ενός πακέτου, για το οποίο δεν υπάρχει κανόνας προώθησης, το FlowVisor λαμβάνει το ερώτημα και το προωθεί στον κατάλληλο Ελεγκτή με βάση την πολιτική ανάθεσης πόρων.

Για τον τεμαχισμό του δικτύου με το FlowVisor, αρχικά δημιουργούνται ένα ή περισσότερα slice. Για καθένα από αυτά ορίζεται το όνομά του, ο Ελεγκτής στον οποίο θα ανατεθεί και ένα mail επικοινωνίας, ενώ μπορεί να ορίζονται και κάποια όρια (π.χ. σε εύρος ζώνης).

Στη συνέχεια, δημιουργούνται μία σειρά από flowspaces που συσχετίζουν τα πακέτα δεδομένων με τα slice. Στη δημιουργία κάθε flowspace ορίζεται μεταξύ άλλων, το όνομά του, η συσκευή την οποία αφορά, ένα σύνολο κριτηρίων για το ταίριασμα πακέτων, καθώς και ένα ή περισσότερα slice με τα οποία θα αντιστοιχιστεί το flowspace.

Η δημιουργία, η διαγραφή και η τροποποίηση ενός slice, μπορούν να πραγματοποιούνται χωρίς να χρειάζεται να διακοπεί η λειτουργία των συσκευών του δικτύου.

## 4.2 Mininet

Το Mininet<sup>22</sup> είναι ένα λογισμικό προσομοίωσης δικτύου, που υποστηρίζει το πρωτόκολλο OpenFlow. Συνεπώς, μπορεί να χρησιμοποιείται για την προσομοίωση δικτύων SDN.

Βασικά στοιχεία ενός δικτύου στο Mininet αποτελούν τα OpenFlowswitch (Switch), οι Ελεγκτές SDN (Controller), οι υπολογιστές (Host) και οι συνδέσεις (NetLink). Επίσης περιλαμβάνονται δρομολογητές και switch που δεν υποστηρίζουν το OpenFlow (LegacyRouter και LegacySwitch). Οι Host υποστηρίζουν δικτυακές λειτουργίες όπως το άνοιγμα τερματικών (xterm), η εντολή ping κ.α. [27]

Η χρήση του Mininet γίνεται τυπικά από τη γραμμή εντολών, ενώ η δημιουργία μίας τοπολογίας γίνεται στη γλώσσα rython, κάνοντας χρήση ειδικού API. Ωστόσο, στη διανομή του προγράμματος περιλαμβάνεται και το εργαλείο miniedit, το οποίο επιτρέπει την οπτική σχεδίαση μίας τοπολογίας και την εκτέλεση της προσομοίωσης με το πάτημα ενός κουμπιού. Κατά τη διάρκεια της προσομοίωσης, παρέχεται η δυνατότητα εκτέλεσης εντολών στο CLI του Mininet.

Τα Switch και οι Controller ενός δικτύου SDN που προσομοιώνεται στο Mininet, μπορούν να επικοινωνούν με ένα στιγμιότυπο του FlowVisor που εκτελείται στην ίδια εικονική μηχανή. Αυτή τη δυνατότητα θα αξιοποιήσουμε στο lab που παρουσιάζεται στη συνέχεια.

## 4.3 Προετοιμασία εργαστηρίου

Για την πραγματοποίηση του εργαστηρίου έχει δημιουργηθεί ένα image εικονικής μηχανής, το οποίο περιέχει όλα τα εργαλεία λογισμικού και αρχεία, που απαιτούνται για την εκτέλεση των δραστηριοτήτων που περιγράφονται στη συνέχεια. Η διαδικασία της δημιουργίας του image παρουσιάζεται στο Παράρτημα Α.

Οι υπολογιστές του εργαστηρίου θα πρέπει να έχουν εγκατεστημένο το VirtualBox, στο οποίο θα εκτελείται η εικονική μηχανή. Επιπλέον, θα

---

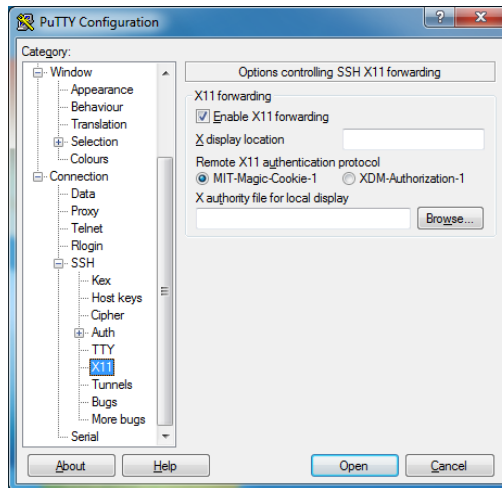
<sup>22</sup> Επίσημη ιστοσελίδα: <http://mininet.org/>



χρησιμοποιηθεί το λογισμικό PuTTY για τη σύνδεση στην εικονική μηχανή μέσω SSH, και το λογισμικό Xming που επιτρέπει την εκτέλεση παραθυρικών εφαρμογών μέσα από τη σύνδεση SSH. Αρχεία εγκατάστασης των εφαρμογών αυτών περιλαμβάνονται στο συνοδευτικό υλικό, μαζί με το image της εικονικής μηχανής.

Η εικονική μηχανή που παρέχεται βασίζεται στην έκδοση 14.04 του Ubuntu και έχει προεγκατεστημένα τα εργαλεία Mininet 2.2.2 και FlowVisor 1.4. Κάνοντας διπλό κλικ στο αρχείο image με όνομα Pada\_lab.ona ανοίγει το VirtualBox και ξεκινάει η εισαγωγή της εικονικής μηχανής. Μετά την εισαγωγή και την εκκίνηση της (με το κουμπί Εκκίνηση στο περιβάλλον του VirtualBox) η σύνδεση στην κονσόλα γίνεται με όνομα χρήστη `mininet` και κωδικό πρόσβασης `mininet`.

Για να μπορούν τα Windows να προβάλουν τις παραθυρικές εφαρμογές που θα εκτελούνται μέσω της σύνδεση SSH, θα πρέπει πριν την έναρξη του μαθήματος να έχει εκτελεστεί στους υπολογιστές το Xming. Η εκτέλεσή του δεν εμφανίζει κάποιο παράθυρο ή ενημερωτικό μήνυμα και η λειτουργία του μπορεί να επαληθευτεί μόνο μέσω τις διαχείρισης εργασιών των Windows. Τέλος, θα πρέπει να επιτραπεί η προώθηση του πρωτοκόλλου X11 πάνω από τη σύνδεση SSH. Για το λόγο αυτό, στο περιβάλλον του PuTTY θα πρέπει να ενεργοποιηθεί η σχετική ρύθμιση (Εικόνα 4.1).



**Εικόνα 4.1:** Ενεργοποίηση προώθησης πρωτοκόλλου X11 στο PuTTY

Η διεύθυνση IP που θα χρησιμοποιείται για τη σύνδεση SSH, είναι αυτή του interface `eth0` της εικονικής μηχανής. Στο αρχείο image που έχει δημιουργηθεί η

διεύθυνση αυτή είναι η 192.168.56.110. Ωστόσο, μπορεί να επαληθευτεί εκτελώντας στην κονσόλα της εικονικής μηχανής την εντολή `ifconfig -a`.

Για να μη χρειάζεται κάθε φορά να ενεργοποιείται η προώθηση του πρωτοκόλλου X11 και να δίνεται η διεύθυνση IP, προτείνεται να γίνει αποθήκευση των σχετικών ρυθμίσεων με ένα όνομα, χρησιμοποιώντας το κουμπί `save` που υπάρχει στην καρτέλα `Session` του PuTTY.

#### 4.4 Διεξαγωγή εργαστηρίου

##### Εκκίνηση εικονικής μηχανής

Αρχικά θα πρέπει να εκκινήσουμε την εικονική μηχανή που περιέχει το Mininet και το FlowVisor. Για το σκοπό αυτό, εκτελούμε το πρόγραμμα `VirtualBox`, και στη συνέχεια επιλέγουμε την εικονική μηχανή με όνομα `Pada_lab-VM` και πατάμε το κουμπί εκκίνηση (εναλλακτικά μπορούμε να κάνουμε διπλό κλικ πάνω στην εικονική μηχανή).

##### Σύνδεση στην εικονική μηχανή

Αφού ολοκληρωθεί η εκκίνηση, συνδεόμαστε στην εικονική μηχανή με SSH μέσα από το πρόγραμμα PuTTY. Αν δεν υπάρχουν αποθηκευμένες ρυθμίσεις για τη σύνδεση, θα πρέπει να εισάγουμε τη διεύθυνση IP 192.168.56.110 και να ενεργοποιήσουμε την προώθηση του πρωτοκόλλου X11 (δείτε την Εικόνα 4.1). Για να αποκτήσουμε πρόσβαση στο φλοιό, στο νέο παράθυρο που ανοίγει, δίνουμε ως όνομα χρήστη και ως κωδικό πρόσβασης τη λέξη `mininet`.

Σημείωση: Σε περίπτωση που η διεύθυνση 192.168.56.110 δε λειτουργεί, θα πρέπει να συνδεθούμε στην κονσόλα της εικονικής μηχανής με τα ίδια στοιχεία, να εκτελέσουμε την εντολή `ifconfig -a` και να εντοπίσουμε τη διεύθυνση του `interface eth0`. (Όταν κάνουμε κλικ στην κονσόλα, δεσμεύεται το ποντίκι. Για να το αποδεσμεύσουμε πρέπει να πατήσουμε το δεξί `Ctrl` στο πληκτρολόγιο).

##### Έναρξη προσομοίωσης δικτύου

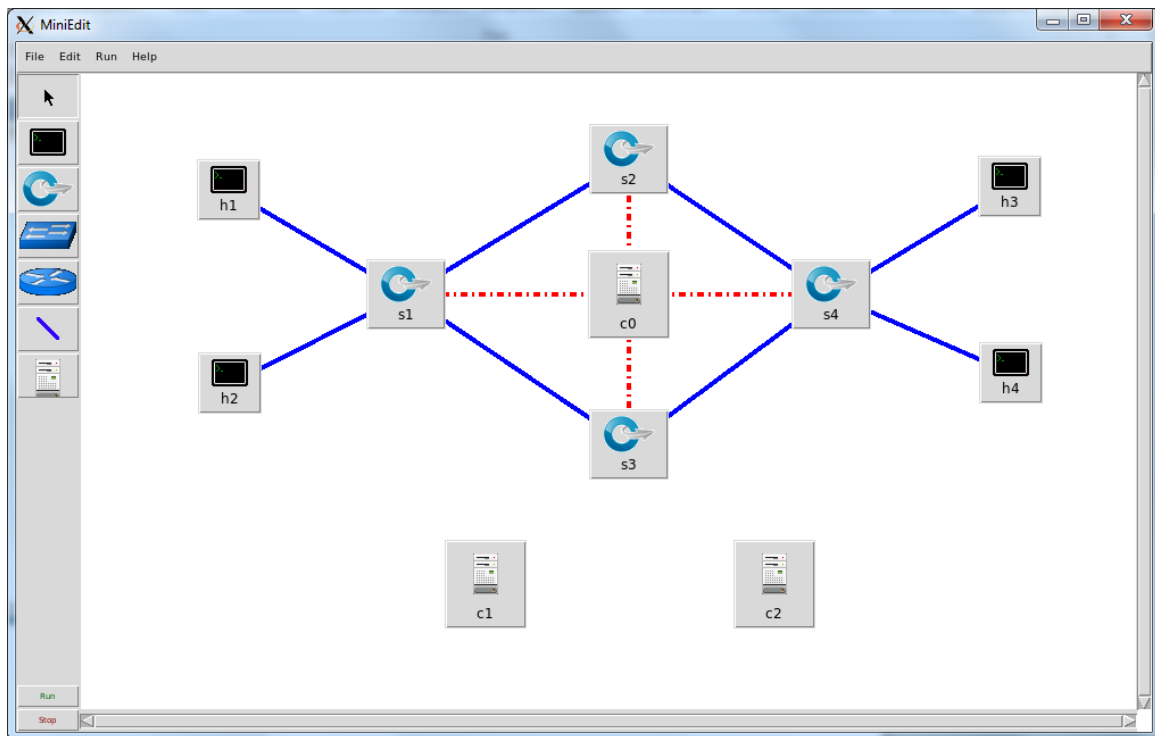
Το επόμενο βήμα είναι να ξεκινήσουμε την προσομοίωση του δικτύου στο Mininet. Για την πραγματοποίηση του εργαστηρίου έχει δημιουργηθεί μία δικτυακή τοπολογία με το οπτικό εργαλείο `mininedit`. Για να την ανοίξουμε αρχικά εκτελούμε

την εντολή:

```
sudo ~/mininet/mininet/examples/miniedit.py
```

Η εντολή αυτή ανοίγει ένα νέο παράθυρο με την εφαρμογή miniedit (με την προϋπόθεση ότι στα Windows εκτελείται το Xming και έχει γίνει σωστά η ρύθμιση της σύνδεσης στο PuTTY). Από το μενού File της εφαρμογής επιλέγουμε Open και στη συνέχεια ανοίγουμε το φάκελο pada\_lab που βρίσκεται κάτω από το φάκελο του χρήστη (/home/mininet), επιλέγουμε το αρχείο με όνομα padalab\_topo.mn και πατάμε το κουμπί Open.

Στην Εικόνα 4.2 παρουσιάζεται η τοπολογία του δικτύου όπως έχει δημιουργηθεί μέσα στο περιβάλλον του miniedit. Μπορούμε να δούμε τις ιδιότητες μίας συσκευής ή μίας σύνδεσης, κάνοντας δεξί κλικ και επιλέγοντας properties από το αναδυόμενο μενού (θα πρέπει να κρατήσουμε πατημένο το δεξί κουμπί του ποντικιού και να το αφήσουμε πάνω από την επιλογή properties). Ο Πίνακας 4.1 παρουσιάζει αναλυτικά τις ιδιότητες που έχουν οριστεί για τα στοιχεία του δικτύου (στις ιδιότητες που δεν αναφέρονται, έχουν διατηρηθεί οι προκαθορισμένες τιμές που αποδίδονται από το πρόγραμμα).



Εικόνα 4.2: Έτοιμη τοπολογία δικτύου στο miniedit

**Πίνακας 4.1:** Ιδιότητες στοιχείων δικτύου

Όνομα	Τύπος	Ιδιότητα	Τιμή
s1	Switch	DPID	1
s2	Switch	DPID	2
s3	Switch	DPID	3
s4	Switch	DPID	4
h1	Host	IP	10.0.0.1
h2	Host	IP	10.0.0.2
h3	Host	IP	10.0.0.3
h4	Host	IP	10.0.0.4
s1→s2	Link	Bandwidth	1Mbit
s1→s3	Link	Bandwidth	10Mbit
s2→s4	Link	Bandwidth	1Mbit
s3→s4	Link	Bandwidth	10Mbit
c0	Controller	Controller Type	Remote Controller
c1	Controller	Controller Port	6634
c2	Controller	Controller Port	6635

Όπως μπορούμε να δούμε, το δίκτυο περιλαμβάνει τέσσερα switch, τέσσερις υπολογιστές, και τρεις controller. Ο Controllerc0 αντιπροσωπεύει το FlowVisor που θα κάνει το slicing. Για το λόγο αυτό, ο τύπος του έχει οριστεί ως Remote Controller, χρησιμοποιεί την προκαθορισμένη πόρτα 6633 και έχει συνδεθεί με όλα τα switch. Οι Controllerc1, c2 θα είναι αυτοί οι οποίοι θα ελέγχουν τα slice που θα δημιουργηθούν με το FlowVisor. Επειδή αυτό που μας ενδιαφέρει είναι η επίδειξη του slicing, οι συγκεκριμένοι Ελεγκτές απλώς θα προωθούν την κίνηση. Έτσι, ως τύπος τους έχει διατηρηθεί ο προκαθορισμένος (OpenFlowReference), ενώ θα χρησιμοποιούν τις πόρτες 6634 και 6635 αντίστοιχα. Όσον αφορά στις συνδέσεις, στον κορμό του δικτύου υπάρχει ένα μονοπάτι με εύρος ζώνης 1 Mbps (s1→s2→s4) και ένα μονοπάτι με εύρος ζώνης 10 Mbps (s1→s3→s4).

Πατώντας το κουμπί `Run` κάτω αριστερά, ξεκινάει η προσομοίωση της τοπολογίας με το Mininet. Στο παράθυρο του PuTTY από το οποίο εκτελέστηκε το `miniedit`, εμφανίζεται η γραμμή εντολών του Mininet (το αρχείο τοπολογίας έχει ενεργοποιημένη τη ρύθμιση `StartCLI` στο μενού `Edit`→`Preferences`).

**Προσοχή:** Πριν από τον τερματισμό της προσομοίωσης (π.χ. με το κουμπί `stop`), θα πρέπει πρώτα να τερματίσουμε τη γραμμή εντολών του Mininet με την εντολή `exit`. Σε διαφορετική περίπτωση δημιουργείται πρόβλημα και δεν θα μπορεί να εκκινήσει εκ νέου η προσομοίωση. Αν συμβεί αυτό, θα πρέπει να κλείσετε το `miniedit` και τη γραμμή εντολών του Mininet, και να εκτελέσετε την εντολή `sudo mn`

-c, για να καθαρίσει το Mininet από τα δεδομένα της προσομοίωσης που δεν τερματίστηκε σωστά. Στη συνέχεια μπορείτε να εκτελέσετε εκ νέου το miniedit και να φορτώσετε την τοπολογία.

## Εκκίνηση FlowVisor

Χρησιμοποιώντας το PuTTY ανοίγουμε μία δεύτερη σύνδεση SSH με την εικονική μηχανή, χρησιμοποιώντας τις ίδιες ρυθμίσεις. Αφού συνδεθούμε με τα ίδια στοιχεία σύνδεσης εκτελούμε στο φλοιό την εντολή

```
sudo /etc/init.d/flowvisor start
```

και με τον τρόπο αυτό ξεκινάει το FlowVisor. Από αυτό το σημείο και μετά, μπορούμε να διαχειριζόμαστε το FlowVisor με την εντολή `fvctl`. Το password που έχει οριστεί για τη διαχείριση του FlowVisor είναι κενό. Συνεπώς όπου μας ζητείται μπορούμε απλώς να πατάμε Enter. Για να επαληθεύσουμε την ορθή εκκίνηση δίνουμε την εντολή

```
fvctl get-config
```

και μας επιστρέφονται οι τρέχουσες ρυθμίσεις του FlowVisor. Για να παρακάμψουμε εντελώς την εισαγωγή password, μπορούμε να χρησιμοποιούμε την εντολή `fvctl` με την παράμετρο `-f`, ώστε να διαβάζει το password από αρχείο και να του δίνουμε ως όνομα του αρχείου το `/dev/null` (αφού το password είναι κενό). Έτσι η προηγούμενη εντολή μπορεί να εκτελεστεί ως εξής:

```
fvctl -f /dev/null get-config
```

**Προσοχή:** Στα αποτελέσματα της εντολής θα πρέπει να προσέξουμε η παράμετρος `enable-topo-ctrl` να έχει τιμή `true`. Σε διαφορετική περίπτωση θα πρέπει να ενημερώσουμε την τιμή της με την εντολή

```
fvctl -f /dev/null set-config --enable-topo-ctrl
```

και στη συνέχεια να επανεκκινήσουμε το FlowVisor με την εντολή

```
sudo /etc/init.d/flowvisor restart
```

#### 4.5 Δημιουργία slice με βάση τις πόρτες των switch (Φυσικό Επίπεδο)

Σε αυτή την πρώτη δραστηριότητα, θα χωρίσουμε το δίκτυο σε δύο slice. Το πρώτο θα περιλαμβάνει το πάνω μισό του δικτύου, και το δεύτερο το κάτω μισό. Ο διαχωρισμός θα γίνει με βάση τις πόρτες των switch. Ωστόσο, στο miniedit ο αριθμός της πόρτας που χρησιμοποιείται σε κάθε σύνδεση, καθορίζεται από τη σειρά με την οποία προστίθενται οι συνδέσεις και δεν είναι ορατός στο γραφικό περιβάλλον. Για να γνωρίζουμε λοιπόν ποια πόρτα ενός switch χρησιμοποιείται σε κάθε σύνδεση, μεταβαίνουμε στο παράθυρο PuTTY όπου εκτελείται η γραμμή εντολών του Mininet και εκτελούμε την εντολή:

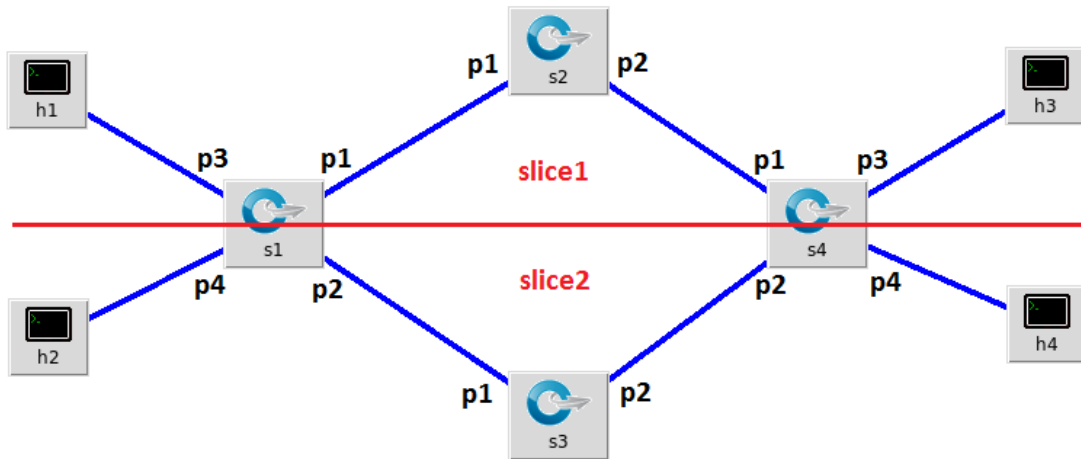
```
links
```

η οποία μας επιστρέφει πληροφορίες για όλες τις συνδέσεις της προσομοίωσης που εκτελείται. Η έξοδος της εντολής για την τοπολογία μας είναι η εξής:

```
s1-eth1<->s2-eth1 (OK OK)
s1-eth2<->s3-eth1 (OK OK)
s2-eth2<->s4-eth1 (OK OK)
s3-eth2<->s4-eth2 (OK OK)
s1-eth3<->h1-eth0 (OK OK)
s1-eth4<->h2-eth0 (OK OK)
s4-eth3<->h3-eth0 (OK OK)
s4-eth4<->h4-eth0 (OK OK)
```

Στην Εικόνα 4.3 παρουσιάζονται τα δύο slice στα οποία θα χωριστεί το δίκτυο της τοπολογίας. Με βάση τα αποτελέσματα της εντολής `links` που εκτελέστηκε στο Mininet, στην εικόνα έχουν συμπεριληφθεί και οι σχετικοί αριθμοί πόρτας των switch.

Προσοχή: Σε περίπτωση που το αποτέλεσμα της εντολής `links` στον υπολογιστή σας έχει διαφορετικούς αριθμούς πόρτας στις συνδέσεις, θα πρέπει να σχεδιάσετε ένα αντίστοιχο διάγραμμα με τις δικές σας τιμές και να προσαρμόσετε κατάλληλα τις εντολές που περιγράφονται στη συνέχεια των οδηγιών.



**Εικόνα 4.3:** Τεμαχισμός δικτύου με βάση τις πόρτες των switch

Για να χωρίσουμε το δίκτυο θα πρέπει στο FlowVisor αρχικά να ορίσουμε τα δύο slice και στη συνέχεια να ορίσουμε μία σειρά από flowspaces που θα αντιστοιχιστούν με καθένα από αυτά. Η προσθήκη ενός νέου slice στο FlowVisor γίνεται με την εντολή `fvctladd-slice`, η οποία συντάσσεται ως εξής:

```
fvctl add-slice <slicename><controller-url><admin-mail>
```

όπου `<slicename>` είναι το όνομα που θέλουμε να δώσουμε στο slice, `<controller-url>` είναι η διεύθυνση του Controller στον οποίο θα ανατεθεί το slice και έχει τη μορφή `tcp:hostname:port`, και `<admin-mail>` είναι η διεύθυνση mail του διαχειριστή του Controller, που χρησιμοποιείται σε περίπτωση που παρουσιαστεί πρόβλημα με το slice. Προκειμένου να δημιουργήσουμε το `slice1` και να το αναθέσουμε στον `Controllerc1`, ανοίγουμε το παράθυρο του PuTTY από το οποίο ξεκινήσαμε το FlowVisor και δίνουμε την εντολή:

```
fvctl -f /dev/null add-slice slice1 tcp:localhost:6634 adm@slice1
```

Κατά την εκτέλεση της εντολής εμφανίζεται προτροπή προκειμένου να ορίσουμε ένα password για το νέο slice. Για λόγους ευκολίας το αφήνουμε κενό πατώντας Enter. Στη συνέχεια εμφανίζεται μήνυμα το οποίο μας ενημερώνει ότι το slice δημιουργήθηκε με επιτυχία. Με παρόμοιο τρόπο δημιουργούμε και το `slice2`, το οποίο αναθέτουμε στον `c2`.

```
fvctl -f /dev/null add-slice slice2 tcp:localhost:6635 adm@slice2
```

Μπορούμε να επαληθεύσουμε την προσθήκη των δύο slice με την εντολή:

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

Στην έξοδο της εντολής, εκτός από τα νέα slice, εμφανίζεται και το προκαθορισμένο που ονομάζεται `fvadmin`.

Ακολουθως πρέπει να δημιουργηθούν τα `flowspace`. Η σχετική εντολή έχει την παρακάτω βασική σύνταξη:

```
fvctl add-flowspace <flowspace-name><dpid><priority><match><slice-perm>
```

όπου `<flowspace-name>` είναι ένα όνομα που ορίζουμε για το `flowspace`. Το `<dpid>` καθορίζει ένα συγκεκριμένο switch (δείτε τον Πίνακα 4.1). Η παράμετρος `<priority>` καθορίζει μία προτεραιότητα, η οποία εξετάζεται όταν ένα πακέτο ταιριάζει με περισσότερα `flowspace`. Οι τελευταίες δύο παράμετροι παρουσιάζονται αναλυτικότερα.

Η παράμετρος `<match>` περιλαμβάνει μία λίστα από κριτήρια χωρισμένα με κόμμα, τα οποία ελέγχονται για να αντιστοιχιστεί ένα πακέτο σε μία ροή. Κάθε κριτήριο έχει τη μορφή `πεδίο=τιμή`. Τα πιθανά πεδία που μπορεί να χρησιμοποιηθούν για το ταίριασμα ενός πακέτου παρουσιάζονται στον Πίνακα 4.2. Όταν ένα πεδίο παραλείπεται από τη λίστα τότε θεωρείται ότι όλες οι πιθανές τιμές του ταιριάζουν με τη ροή.



**Πίνακας 4.2:** Πεδία κριτηρίων για το ταίριασμα πακέτων σε ροή

Όνομα πεδίου	Κριτήριο
in_port	Αριθμός πόρτας του switch
dl_vlan	Τιμή ετικέτας vlan (0 – 4095, 0xffff = χωρίς ετικέτα)
dl_src	Διεύθυνση mac προέλευσης πακέτου Ethernet
dl_dst	Διεύθυνση mac προορισμού πακέτου Ethernet
dl_type	Τύπος πρωτοκόλλου Ethernet (0-65535)
nw_src	Διεύθυνση ip προέλευσης
nw_dst	Διεύθυνση ip προορισμού
nw_proto	Τύπος πρωτοκόλλου IP (0-255, π.χ. 6=TCP)
nw_tos	Τιμή πεδίου Type of Service πακέτου IP (0-255)
tp_src	Πόρτα πρωτοκόλλου μεταφοράς προέλευσης (0-65535)
tp_dst	Πόρτα πρωτοκόλλου μεταφοράς προορισμού (0-65535)

Η παράμετρος `<slice-perm>` είναι μία λίστα που περιλαμβάνει όλα τα slice που έχουν δικαιώματα σε ένα συγκεκριμένο flowspace. Τα στοιχεία της λίστας χωρίζονται με κόμμα και καθένα έχει τη μορφή `όνομα_slice=τιμή`. Όπου η τιμή μπορεί να είναι ίση με 1, 2, 4 (για δικαίωμα DELEGATE, READ και WRITE αντίστοιχα), ή με οποιοδήποτε άθροισμά τους (για συνδυασμό δικαιωμάτων).

Σύμφωνα με τα παραπάνω, δημιουργούμε ένα flowspace με όνομα `s1p3` που θα αντιστοιχίζει όλη την κίνηση στην πόρτα 3 του `s1` (σύνδεση με `h1`) στο `slice1` με την εντολή:

```
fvctl -f /dev/null add-flowspace s1p3 1 1 in_port=3 slice1=7
```

Στην προτεραιότητα έχει δοθεί τιμή 1 διότι στο συγκεκριμένο σενάριο δεν θα χρησιμοποιηθεί, ενώ στο `slice1` έχουν δοθεί πλήρη δικαιώματα (τιμή 7). Υπενθυμίζεται ότι το `s1` έχει DPID 1 (Δείτε τον Πίνακα 4.1).

Συνεχίζοντας με το πάνω τμήμα του δικτύου δημιουργούμε το flowspace `s1p1` που θα αντιστοιχίζει όλη την κίνηση στην πόρτα 1 του `s1` στο `slice1`.

```
fvctl -f /dev/null add-flowspace s1p1 1 1 in_port=1 slice1=7
```

Το `s2` ανήκει ολόκληρο στο `slice1`, συνεπώς δεν χρειάζεται να ορίσουμε κάποιο κριτήριο. Επειδή όμως η παράμετρος `<match>` είναι υποχρεωτική στη σύνταξη της εντολής, στη θέση των κριτηρίων χρησιμοποιούμε τη λέξη `any`. Δημιουργούμε το αντίστοιχο flowspace με όνομα `s2all` με την εντολή:

Τεχνικές τεμαχισμού δικτύων (network slicing) - σύγχρονες τάσεις σε επίπεδο παρόχων

```
fvctl -f /dev/null add-flowspace s2all 2 1 any slice1=7
```

Για τις πόρτες 1 και 3 του s4 που ανήκουν στο slice1, δημιουργούμε αντίστοιχα τα flowspaces με ονόματα s4p1 και s4p3 με τις ακόλουθες εντολές:

```
fvctl -f /dev/null add-flowspace s4p1 4 1 in_port=1 slice1=7
```

```
fvctl -f /dev/null add-flowspace s4p3 4 1 in_port=3 slice1=7
```

Με αντίστοιχο τρόπο, δημιουργούμε τα flowspaces s1p4, s1p2, s3all, s4p2 και s4p4, και τα αντιστοιχίζουμε στο slice2.

```
fvctl -f /dev/null add-flowspace s1p4 1 1 in_port=4 slice2=7
```

```
fvctl -f /dev/null add-flowspace s1p2 1 1 in_port=2 slice2=7
```

```
fvctl -f /dev/null add-flowspace s3all 3 1 any slice2=7
```

```
fvctl -f /dev/null add-flowspace s4p2 4 1 in_port=2 slice2=7
```

```
fvctl -f /dev/null add-flowspace s4p4 4 1 in_port=4 slice2=7
```

Μπορούμε να δούμε τη λίστα με τα flowspaces που έχουν δημιουργηθεί, με την εντολή:

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

**Σημείωση:** Σε περίπτωση που κάποιο από τα flowspaces έχει κάποιο λάθος (π.χ. λάθος δικαιώματα) μπορούμε να το διαγράψουμε με την εντολή

```
fvctl -f /dev/null remove-flowspace <flowspace-name>
```

και στη συνέχεια να το ξαναδημιουργήσουμε σωστά.

Για να επαληθεύσουμε το διαχωρισμό του δικτύου σε δύο slice, μεταφερόμαστε στο παράθυρο του PuTTY, όπου εκτελείται η γραμμή εντολών του Mininet. Ο έλεγχος της επικοινωνίας μεταξύ δύο σταθμών στην προσομοίωση, μπορεί να γίνει εύκολα κάνοντας ping από τον έναν σταθμό στον άλλον. Έτσι, για παράδειγμα με την εντολή

```
h1 ping -c3 h3
```

ο σταθμός `h1` στέλνει 3 πακέτα ICMP (το πλήθος καθορίζεται με το `-c`) στο σταθμό `h3` και αναφέρει αν έλαβε απάντηση. Για να μη χρειάζεται όμως να εκτελέσουμε την εντολή `ping` πολλές φορές, για τους διαφορετικούς συνδυασμούς σταθμών, το `Mininet` παρέχει την εντολή

```
pingall
```

η οποία ελέγχει με `ping` την αμφίδρομη συνδεσιμότητα όλων των σταθμών της τοπολογίας και μας εμφανίζει τα αποτελέσματα σε μορφή πίνακα, όπως φαίνεται παρακάτω.

```
*** Ping: testing ping reachability
h1 -> h3 X X
h3 -> h1 X X
h2 -> X X h4
h4 -> X X h2
*** Results: 66% dropped (4/12 received)
```

Όπως μπορούμε να δούμε από την έξοδο της εντολής, οι σταθμοί `h1` και `h3` μπορούν να επικοινωνήσουν μόνο μεταξύ τους και το ίδιο ισχύει για τους `h2` και `h4`. Συνεπώς επαληθεύεται ο τεμαχισμός του δικτύου.

Μετά την ολοκλήρωση και την επαλήθευση του τεμαχισμού του δικτύου με βάση τις πόρτες των `switch`, θα πρέπει να επαναφέρουμε το `FlowVisor` στην αρχική του κατάσταση, αφαιρώντας τα δύο `slice` που δημιουργήσαμε και κατ' επέκταση και τα `flowspace`. Για το σκοπό αυτό, στο τερματικό από το οποίο εκκινήσαμε το `FlowVisor`, εκτελούμε τις ακόλουθες δύο εντολές:

```
fvctl -f /dev/null remove-slice slice1
fvctl -f /dev/null remove-slice slice2
```

Εκτελώντας την εντολή:

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

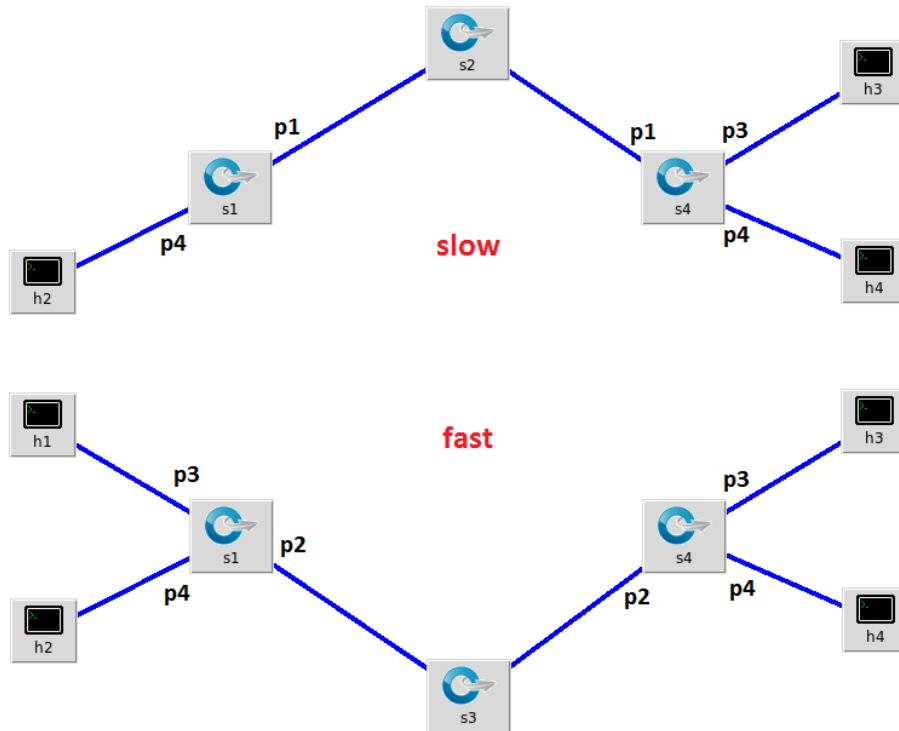
επιβεβαιώνουμε την επαναφορά του FlowVisor (θα εμφανίζεται μόνο το default slice `fvadmin`).

#### 4.6 Δημιουργία slice με βάση τη διεύθυνση IP (Επίπεδο Δικτύου)

Όπως είδαμε στον Πίνακα 4.1, το δίκτυο κορμού της τοπολογίας μας αποτελείται από δύο μονοπάτια. Ένα αργό με εύρος ζώνης 1 Mbps ( $s1 \rightarrow s2 \rightarrow s4$ ) και ένα πιο γρήγορο που λειτουργεί στα 10 Mbps ( $s1 \rightarrow s3 \rightarrow s4$ ). Στη συνέχεια του εργαστηρίου, θα δούμε πώς μπορούμε να δημιουργήσουμε slice, με βάση τις διευθύνσεις IP προέλευσης και προορισμού της κίνησης. Συγκεκριμένα, θα θεωρήσουμε ότι ο σταθμός h1 (IP διεύθυνση 10.0.0.1) είναι ένας εξυπηρετητής που είναι πολύ σημαντικός και θα του δώσουμε την αποκλειστική χρήση του γρήγορου μονοπατιού του δικτύου κορμού. Αυτό σημαίνει, ότι όλη η κίνηση IP που προέρχεται από τον h1 ή που προορίζεται για αυτόν θα αντιστοιχίζεται σε ένα slice με το όνομα `fast`, που θα περιλαμβάνει το μονοπάτι  $s1 \rightarrow s3 \rightarrow s4$ . Η κίνηση μεταξύ των υπόλοιπων σταθμών, θα αντιστοιχίζεται στο slice `slow`, το οποίο θα χρησιμοποιεί το αργό κομμάτι του δικτύου κορμού. Στο σημείο αυτό θα πρέπει να επισημάνουμε, ότι οι σταθμοί που συνδέονται πάνω στο ίδιο switch επικοινωνούν απευθείας με ρυθμό δεδομένων της τάξης των Gbps.

Στην Εικόνα 4.4 παρουσιάζονται τα δύο slice που θα δημιουργηθούν στο δίκτυο. Όπως είναι εμφανές, οι περισσότερες από τις πόρτες των ακραίων switch στις οποίες συνδέονται οι σταθμοί, θα συμμετέχουν και στα δύο slice.

Σημείωση: Στις οδηγίες που ακολουθούν, θεωρείται ότι η συγκεκριμένη δραστηριότητα θα εκτελεστεί αμέσως μετά την προηγούμενη και άρα οι συνδέσεις SSH, η προσομοίωση του δικτύου με το `miniedit`, καθώς και το FlowVisor είναι έτοιμα. Σε διαφορετική περίπτωση, πριν την έναρξη της δραστηριότητας, θα πρέπει να εκτελεστούν οι ενέργειες που περιγράφονται στην ενότητα 4.4



**Εικόνα 4.4:** Τεμαχισμός του δικτύου με βάση την IP διεύθυνση

Αρχικά θα πρέπει να δημιουργήσουμε τα δύο slice. Ανοίγουμε το παράθυρο PuTTY που χρησιμοποιούμε για το FlowVisor και δίνουμε τις παρακάτω εντολές:

```
fvctl -f /dev/null add-slice slow tcp:localhost:6634 adm@slow  
fvctl -f /dev/null add-slice fast tcp:localhost:6635 adm@fast
```

Όπως μπορούμε να δούμε από τα TCPport που χρησιμοποιούνται, η διαχείριση του slice *slow* ανατίθεται στον Ελεγκτή *c1*, ενώ του *fast* στον *c2*.

Στη συνέχεια θα πρέπει να δημιουργήσουμε τα *flowspace* και να τα αντιστοιχίσουμε με τα *slice*. Ξεκινώντας με το *s1* παρατηρούμε ότι η πόρτα 4 εμφανίζεται και στα δύο *slice*. Όταν η κίνηση στην πόρτα αυτή, έχει ως διεύθυνση IP προέλευσης ή προορισμού την IP 10.0.0.1 (σταθμός *h1*), θα αντιστοιχίζεται στο *slice fast*. Σε κάθε άλλη περίπτωση θα αντιστοιχίζεται στο *slow*.

Με την εντολή που ακολουθεί, αντιστοιχίζουμε στο *fast* τα πακέτα της πόρτας 4 του *s1* τα οποία έχουν ως προορισμό την IP 10.0.0.1. Η προτεραιότητα που δίνεται σε αυτό το *flowspace* είναι 10. (Η εντολή θα πρέπει να γραφτεί σε μία σειρά)

```
fvctl -f /dev/null add-flowspace slp4fast-src 1 10  
in_port=4,nw_src=10.0.0.1 fast=7
```

Αντίστοιχα ορίζουμε και για τα πακέτα που έχουν το 10.0.0.1 ως διεύθυνση προορισμού.

```
fvctl -f /dev/null add-flowspace slp4fast-dst 1 10  
in_port=4,nw_dst=10.0.0.1 fast=7
```

Όλα τα υπόλοιπα πακέτα στην πόρτα αυτή, θα πρέπει να αντιστοιχίζονται στο slow. Για το σκοπό αυτό, δίνουμε την εντολή

```
fvctl -f /dev/null add-flowspaceslp4slow 1 1 in_port=4 slow=7
```

η οποία έχει ως μοναδικό κριτήριο ταιριάσματος τον αριθμό της πόρτας. Συνεπώς, θα ταιριάζει και με τα πακέτα που αφορούν τον h1. Αυτός είναι ο λόγος που η οριζόμενη προτεραιότητα εδώ είναι μικρότερη (προτεραιότητα 1 έναντι 10 ώστε να υπερισχύουν τα προηγούμενα flowspaces). Από τις υπόλοιπες πόρτες του s1, η 3 συνδέεται στον h1, άρα θα ανήκει στο slice fast, η 1 στο s2 άρα θα ανήκει στο slow, και η 2 στο s3 άρα και αυτή θα πρέπει να αντιστοιχιστεί στο fast. Οι εντολές που ακολουθούν δημιουργούν τα αντίστοιχα flowspaces:

```
fvctl -f /dev/null add-flowspaceslp3fast 1 1 in_port=3 fast=7  
fvctl -f /dev/null add-flowspaceslp1slow 1 1 in_port=1 slow=7  
fvctl -f /dev/null add-flowspaceslp2fast 1 1 in_port=2 fast=7
```

Προχωρώντας στο s4, βλέπουμε ότι οι πόρτες 3 και 4 του switch, εμφανίζονται και στα δύο slice. Συνεπώς, για καθεμία από αυτές θα πρέπει να δημιουργήσουμε τρία flowspaces (όπως κάναμε και για την πόρτα 4 του s1). Ένα υψηλής προτεραιότητας για τα πακέτα με IP προέλευσης 10.0.0.1, ένα υψηλής προτεραιότητας για τα πακέτα με IP προορισμού 10.0.0.1 και ένα χαμηλής προτεραιότητας για όλα τα πακέτα της πόρτας. Οι εντολές για τη δημιουργία των flowspaces της πόρτας 3 είναι οι εξής:

```
fvctl -f /dev/null add-flowspace s4p3fast-src 4 10
in_port=3,nw_src=10.0.0.1 fast=7
fvctl -f /dev/null add-flowspace s4p3fast-dst 4 10
in_port=3,nw_dst=10.0.0.1 fast=7
fvctl -f /dev/null add-flowspace s4p3slow 4 1 in_port=3 slow=7
```

Ομοίως για την πόρτα 4 έχουμε:

```
fvctl -f /dev/null add-flowspace s4p4fast-src 4 10
in_port=4,nw_src=10.0.0.1 fast=7
fvctl -f /dev/null add-flowspace s4p4fast-dst 4 10
in_port=4,nw_dst=10.0.0.1 fast=7
fvctl -f /dev/null add-flowspace s4p4slow 4 1 in_port=4 slow=7
```

Όσον αφορά τις υπόλοιπες πόρτες του s4, η 1 συνδέεται στο s2 και άρα αποτελεί μέρος του `slow`, ενώ η 2 συνδέεται στο s3 και άρα πρέπει να αντιστοιχιστεί με το `fast`:

```
fvctl -f /dev/null add-flowspace s4p1slow 4 1 in_port=1 slow=7
fvctl -f /dev/null add-flowspace s4p2fast 4 1 in_port=2 fast=7
```

Η δημιουργία των `flowspaces` για τα `switchs2` και `s3` είναι εύκολη υπόθεση, καθώς ανήκουν εξ ολοκλήρου στο `slow` και στο `fast` αντίστοιχα:

```
fvctl -f /dev/null add-flowspace s2slow 2 1 any slow=7
fvctl -f /dev/null add-flowspace s3fast 3 1 any fast=7
```

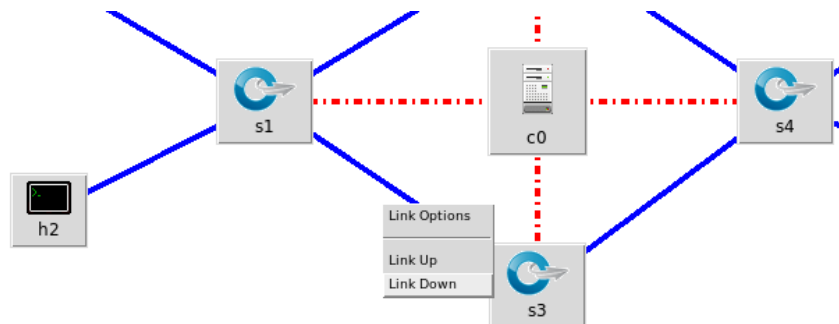
Μετά την ολοκλήρωση του ορισμού των `flowspaces`, θα πρέπει να ελέγξουμε τη λειτουργία του δικτύου. Μεταβαίνουμε στο παράθυρο του PuTTY με τη γραμμή εντολών του Mininet και δίνουμε την εντολή:

```
pingall
```

για να επαληθεύσουμε ότι κάθε σταθμός μπορεί να επικοινωνεί με όλους τους υπόλοιπους.

Προσοχή: Σε περίπτωση που η έξοδος της `pingall` δείξει πρόβλημα στην επικοινωνία μεταξύ κάποιων σταθμών, μπορεί να χρειάζεται να γίνει επανεκκίνηση της προσομοίωσης. Υπενθυμίζεται ότι πριν σταματήσετε την προσομοίωση στο `miniedit`, θα πρέπει να έχετε κλείσει τη γραμμή εντολών του `Mininet`, εκτελώντας την εντολή `exit`. Στη συνέχεια, στο περιβάλλον του `miniedit`, πατήστε το κουμπί `Stop` για να σταματήσει η προσομοίωση και μετά από λίγο πατήστε το `Start` για να την ξεκινήσετε εκ νέου.

Για να επιβεβαιώσουμε ότι τα δεδομένα διασχίζουν το δίκτυο κορμού με τον επιθυμητό τρόπο, θα αξιοποιήσουμε τη δυνατότητα που μας παρέχει το `miniedit`, να κόβουμε μία σύνδεση κατά τη διάρκεια της προσομοίωσης. Με την προσομοίωση να εκτελείται κάνουμε δεξί κλικ πάνω στη σύνδεση μεταξύ `s1` και `s3` και στο αναδυόμενο μενού επιλέγουμε `LinkDown` (Εικόνα 4.5). Η γραμμή της σύνδεσης θα αλλάξει και θα γίνει διακεκομμένη.



**Εικόνα 4.5:** Προσομοίωση διακοπής σύνδεσης

Στη γραμμή εντολών του `Miniedit` δίνουμε και πάλι την εντολή

```
pingall
```

και παίρνουμε τα παρακάτω αποτελέσματα:

```
*** Ping: testing ping reachability
h1 -> X h2 X
h3 -> X h2 h4
```



```
h2 -> h1 h3 h4
h4 -> X h3 h2
*** Results: 33% dropped (8/12 received)
```

Από την έξοδο της εντολής παρατηρούμε ότι όταν κοπεί το γρήγορο κομμάτι του δικτύου κορμού, ο σταθμός h1 μπορεί να επικοινωνεί μόνο με τον h2, ο οποίος συνδέεται στο ίδιο switch.

Στο παράθυρο του miniedit, επαναφέρουμε τη σύνδεση s1-s3 και κόβουμε τη σύνδεση s1-s2. Στη γραμμή εντολών του mininet εκτελούμε εκ νέου την pingall

η οποία μας δίνει την ακόλουθη έξοδο:

```
*** Ping: testing ping reachability
h1 -> h3 h2 h4
h3 -> h1 X h4
h2 -> h1 X X
h4 -> h1 h3 X
*** Results: 33% dropped (8/12 received)
```

Εδώ βλέπουμε ότι όταν κοπεί το αργό μονοπάτι του δικτύου κορμού, κάθε σταθμός μπορεί να επικοινωνεί μόνο με τον h1 και με το σταθμό που είναι συνδεδεμένος στο ίδιο switch.

Από τα παραπάνω βγαίνει το συμπέρασμα, ότι το κομμάτι του δικτύου κορμού το οποίο ανήκει στο slice *fast* μεταφέρει αποκλειστικά την κίνηση που αφορά τον h1, ενώ το κομμάτι του δικτύου κορμού που ανήκει στο slice *slow* μεταφέρει μόνο την κίνηση μεταξύ των υπόλοιπων σταθμών (h2-h3 ή h2-h4). Άρα ο τεμαχισμός του δικτύου λειτουργεί όπως αναμενόταν.

Αφού επαληθεύσαμε την ορθή εκτέλεση της δραστηριότητας, επαναφέρουμε το FlowVisor στην αρχική του κατάσταση διαγράφοντας τα δύο slice που δημιουργήσαμε. Στο παράθυρο του PuTTY όπου χειριζόμαστε το FlowVisor δίνουμε τις εντολές:

```
fvctl -f /dev/null remove-slice fast
fvctl -f /dev/null remove-slice slow
```

Εκτελώντας την εντολή:

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

επιβεβαιώνουμε την επαναφορά του FlowVisor (θα εμφανίζεται μόνο το default slice fvadmin).

#### 4.7 Ολοκλήρωση εργαστηρίου

Στο τέλος του εργαστηριακού μαθήματος θα πρέπει να τερματίσουμε την προσομοίωση του δικτύου, το FlowVisor, καθώς και την εικονική μηχανή. Στο παράθυρο του PuTTY με τη γραμμή εντολών του Mininet δίνουμε μία φορά την εντολή

```
exit
```

για να βγούμε από τη γραμμή εντολών. Στη συνέχεια, στο παράθυρο του miniedit με την τοπολογία, πατάμε το κουμπί “Stop” και σταματάμε την προσομοίωση. Ακολούθως ανοίγουμε το μενού “File” και πατάμε “Quit” ώστε να κλείσει το παράθυρο του miniedit. Στη συνέχεια κλείνουμε και τη σύνδεση SSH που χρησιμοποιούσαμε για το Mininet (είτε δίνοντας για δεύτερη φορά την εντολή `exit` είτε κλείνοντας το παράθυρο του PuTTY).

Στη σύνδεση SSH που χρησιμοποιήσαμε για το FlowVisor εκτελούμε την εντολή:

```
sudo /etc/init.d/flowvisor stop
```

Μετά τον τερματισμό του FlowVisor κλείνουμε και αυτό το παράθυρο του PuTTY. Στο παράθυρο με την κονσόλα της εικονικής μηχανής ανοίγουμε το μενού Αρχείο και επιλέγουμε Κλείσιμο (εναλλακτικά μπορούμε να πατήσουμε το X για να κλείσουμε το παράθυρο της κονσόλας). Στο νέο παράθυρο που ανοίγει επιλέγουμε «Τερματισμός της μηχανής» και πατάμε «Ναι». Τέλος κλείνουμε το παράθυρο του VirtualBox.

## ΚΕΦΑΛΑΙΟ 5 - Συμπεράσματα

Βρισκόμαστε σε μια εποχή, όπου οι τεχνολογίες κινητών επικοινωνιών εξελίσσονται ραγδαία. Η 5η γενιά δικτύων κινητής τηλεφωνίας έχει έρθει για να κάνει πραγματικότητα συναρπαστικές εφαρμογές, προσαρμοσμένες στις μοναδικές απαιτήσεις κάθε χρήστη. Εκμεταλλευόμενη τα νέα ραδιοκύματα (new 5G Radio Core) και τα αποκεντριοποιημένα RAN, μικραίνει τα μονοπάτια ανάμεσα σε εφαρμογές και υποδομές, με αποτέλεσμα ο χρήστης να λαμβάνει πιο γρήγορα και άμεσα υπηρεσίες.

Οι αρχιτεκτονικές SDN και NFV έρχονται για να επιλύσουν τα ζητήματα που προκύπτουν στο σχεδιασμό των δικτύων 5G, επιτρέποντας στις νέες τεχνολογίες των κινητών επικοινωνιών να αξιοποιηθούν πλήρως. Η SDN, κεντριοποιεί τον έλεγχο της λειτουργίας των δικτυακών συσκευών. Αυτό επιτυγχάνεται με το διαχωρισμό του επιπέδου ελέγχου, που υλοποιείται πλέον με λογισμικό, από το επίπεδο προώθησης δεδομένων, που εξακολουθεί να υλοποιείται στις συσκευές. Η NFV μέσω τεχνικών εικονικοποίησης επιτρέπει την υλοποίηση δικτυακών λειτουργιών, που παραδοσιακά εκτελούνταν από εξειδικευμένο υλικό, με λογισμικό που εκτελείται σε εξυπηρετητές. Με τον τρόπο αυτό, παρέχεται μεγαλύτερη ευελιξία.

Η τεχνική Network Slicing, που αποτελεί και το βασικό αντικείμενο της παρούσας, έρχεται να ολοκληρώσει τις τεχνολογίες και τις αρχιτεκτονικές του 5G, επιτρέποντας την πλήρη εκμετάλλευση των πλεονεκτημάτων τους. Για το λόγο αυτό, θεωρείται αναπόσπαστο μέρος των δικτύων 5<sup>ης</sup> Γενιάς.

Το Network Slicing επιτρέπει τη δημιουργία ανεξάρτητων λογικών δικτύων, πάνω από μία κοινή δικτυακή υποδομή, μοιράζοντας έτσι τους διαθέσιμους πόρους σε περισσότερους πελάτες. Οι πελάτες αυτοί, μπορεί να είναι διαφορετικοί τηλεπικοινωνιακοί πάροχοι, ή εφαρμογές και υπηρεσίες με διαφορετικά χαρακτηριστικά και δικτυακές απαιτήσεις.

Η υλοποίηση του διαμοιρασμού των πόρων ενός δικτύου, υλοποιείται παραδοσιακά με άλλες τεχνολογίες όπως τα VPN, οι IPAccessList κ.α. Ωστόσο, το network slicing διαθέτει συγκεκριμένα χαρακτηριστικά, όπως η κεντριοποιημένη διαχείριση και η άμεση δημιουργία και τροποποίηση των slice, που το καθιστούν μια πολύ σημαντική λύση για τις ανάγκες πραγματικών δικτύων, όπως αυτά του 5G.

Ως θεμελιώδες στοιχείο της τεχνολογίας 5G, το Network Slicing αποτελεί αντικείμενο εκτεταμένης έρευνας και η πρακτική επίδειξή του, στο πλαίσιο των μαθημάτων των κινητών επικοινωνιών, έχει μεγάλη αξία.

Το FlowVisor είναι ένα εργαλείο λογισμικού που χρησιμοποιείται για τη δημιουργία slice σε ένα δίκτυο SDN. Λειτουργεί ως ένα ενδιάμεσο επίπεδο μεταξύ του επιπέδου ελέγχου και του επιπέδου προώθησης δεδομένων. Μπορεί να ελέγχει την υφιστάμενη υποδομή και να δημιουργεί slice τα οποία αποδίδει σε Ελεγκτές SDN στο επίπεδο Ελέγχου.

Στο πρακτικό μέρος της διπλωματικής δημιουργήθηκε ένα lab επίδειξης της τεχνικής slicing με τη χρήση του FlowVisor και του προσομοιωτή SDN δικτύων, Mininet. Στην προτεινόμενη εργαστηριακή άσκηση παρουσιάζονται δύο σενάρια τεμαχισμού μίας συγκεκριμένης τοπολογίας, η οποία παρέχεται έτοιμη και έχει δημιουργηθεί με το εργαλείο miniedit.

Στο πρώτο σενάριο, γίνεται διαχωρισμός του δικτύου σε δύο τμήματα με βάση τις πόρτες των switch, λειτουργώντας στην ουσία στο φυσικό επίπεδο. Μέσα από αυτό το παράδειγμα, βλέπουμε τον τρόπο που μπορεί να γίνει η διαίρεση μιας ενιαίας δικτυακής υποδομής σε δύο ανεξάρτητα λογικά δίκτυα.

Στο δεύτερο σενάριο χρησιμοποιείται ως κριτήριο για τη δημιουργία των slice η ip διεύθυνση ενός συγκεκριμένου σταθμού, ο οποίος θεωρείται σημαντικός και του αφιερώνεται το γρήγορο τμήμα του δικτύου κορμού της τοπολογίας. Σε αυτή την περίπτωση, βλέπουμε τον τρόπο με τον οποίο το networkslicing μπορεί να χρησιμοποιηθεί για να δοθεί προτεραιότητα σε κάποια συσκευή.

Μέσα από την υλοποίηση των σεναρίων γίνεται αντιληπτό ότι το FlowVisor είναι ένα χρήσιμο εργαλείο, το οποίο μπορεί να αξιοποιηθεί τόσο για εκπαιδευτικούς όσο και για ερευνητικούς σκοπούς. Παρέχει τη δυνατότητα δημιουργίας slice με βάση κριτήρια που φτάνουν ως το επίπεδο μεταφοράς (π.χ. εφαρμογή που λειτουργεί σε συγκεκριμένο TCPPort).

Επέκταση της παρούσας διπλωματικής, θα μπορούσε να αποτελέσει η δημιουργία ποικίλων σεναρίων με διαφορετικά επίπεδα δυσκολίας και διαφορετικούς μαθησιακούς στόχους. Ενδιαφέρον παρουσιάζει ακόμα να δούμε πώς θα εξελιχθούν οι αλγόριθμοι δυναμικού τεμαχισμού δικτύων και πώς η Τεχνητή Νοημοσύνη θα συμβάλει στην ολοκλήρωση της τεχνολογίας 5G.

## ΠΑΡΑΡΤΗΜΑ Α΄

Στο παράρτημα αυτό, παρουσιάζεται η διαδικασία δημιουργίας του image της εικονικής μηχανής, που χρησιμοποιείται για την πραγματοποίηση του εργαστηρίου. Στο πλαίσιο της διαδικασίας θα χρησιμοποιηθούν τα εργαλεία λογισμικού VirtualBox, Xming και PuTTY.

Βάση για το image που θα δημιουργήσουμε, θα αποτελέσει ένα από τα έτοιμα image εικονικής μηχανής που περιέχουν το Mininet (<http://mininet.org/>) και διατίθενται στο github.

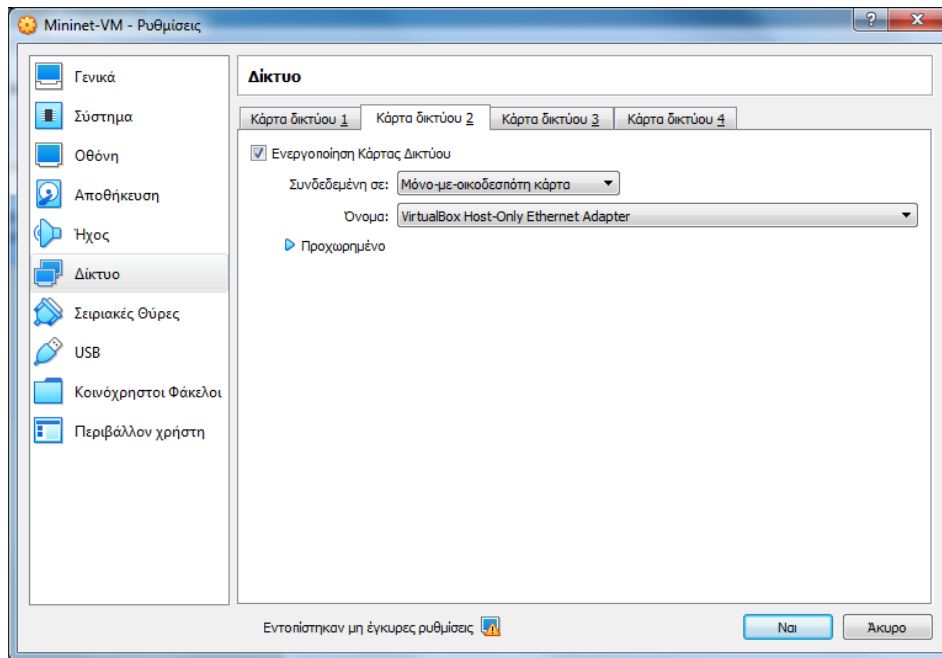
Το FlowVisor για να λειτουργήσει σωστά χρειάζεται την έκδοση 6 του openjdk, η οποία δεν είναι διαθέσιμη για τις πιο νέες εκδόσεις του Ubuntu. Για το λόγο αυτό, θα χρησιμοποιήσουμε το image που περιέχει την έκδοση 2.2.2 του Mininet, σε Ubuntu 14.04.

Μεταβαίνουμε στη διεύθυνση <https://github.com/mininet/mininet/releases/tag/2.2.2> και κατεβάζουμε το αρχείο με όνομα:

`mininet-2.2.2-170321-ubuntu-14.04.4-server-amd64.zip`ή

`mininet-2.2.2-170321-ubuntu-14.04.4-server-i386.zip` για υπολογιστές με αρχιτεκτονική 32 bit. Αποσυμπιέζουμε το αρχείο σε έναν φάκελο της επιλογής μας και κάνουμε διπλό κλικ στο αρχείο με επέκταση `.ovf`. Εφόσον το VirtualBox είναι εγκατεστημένο στον υπολογιστή, θα ανοίξει και θα εμφανίσει ένα παράθυρο για την εισαγωγή του image. Πατάμε το κουμπί «Εισαγωγή» και ξεκινάει η διαδικασία.

Μετά την εισαγωγή, θα πρέπει να προσθέσουμε στην εικονική μηχανή μία δεύτερη κάρτα δικτύου. Με επιλεγμένη τη μηχανή, πατάμε «Ρυθμίσεις» και επιλέγουμε «Δίκτυο». Ανοίγουμε την καρτέλα «Κάρτα δικτύου 2» την ενεργοποιούμε και στη ρύθμιση «Συνδεδεμένη σε» επιλέγουμε από τη λίστα το «Μόνο-με-οικοδεσπότη κάρτα» (“Host-only-network” στην αγγλική έκδοση), όπως φαίνεται στην Εικόνα Α.1.



**Εικόνα A.1:** Ρύθμιση 2<sup>ης</sup> κάρτας δικτύου VM

Στη συνέχεια εκκινούμε την εικονική μηχανή πατώντας το κουμπί «Εκκίνηση» και συνδεόμαστε στην κονσόλα με όνομα χρήστη `mininet` και κωδικό πρόσβασης `mininet`.

**Σημείωση:** Όταν κάνουμε κλικ στην κονσόλα, δεσμεύει το ποντίκι. Για να το αποδεσμεύσουμε πρέπει να πατήσουμε το δεξί `Ctrl` στο πληκτρολόγιο.

Στη γραμμή εντολών της κονσόλας δίνουμε την εντολή

```
ifconfig -a
```

και στην έξοδό της εντοπίζουμε τη διεύθυνση IP του interface `eth0`. Μπορούμε να χρησιμοποιούμε αυτή τη διεύθυνση για να συνδεόμαστε στην εικονική μηχανή από τον υπολογιστή στον οποίο εκτελείται. Επίσης παρατηρούμε ότι το interface `eth1` (η επιπλέον κάρτα δικτύου που προσθέσαμε στην εικονική μηχανή) δεν έχει λάβει ρυθμίσεις IP.

**Σημείωση:** Για μεγαλύτερη ευκολία, προτείνεται η υπόλοιπη διαδικασία να εκτελεστεί μέσα από μία σύνδεση SSH, η οποία θα πραγματοποιηθεί με το πρόγραμμα `PuTTY`.

Για να ρυθμίσουμε το `eth1` ώστε να παίρνει αυτόματα διεύθυνση IP, θα πρέπει να τροποποιήσουμε κατάλληλα το αρχείο `/etc/network/interfaces`. Ανοίγουμε το αρχείο με το συντάκτη κειμένου `vi` εκτελώντας της εντολή:

```
sudo vi /etc/network/interfaces
```

και στο τέλος του αρχείου προσθέτουμε τις ακόλουθες δύο σειρές:

```
auto eth1
iface eth1 inet dhcp
```

Στην επόμενη εκκίνηση της εικονικής μηχανής, το `eth1` θα πάρει αυτόματα διεύθυνση IP. Για να του ανατεθεί διεύθυνση στην τρέχουσα συνεδρία και να αποφύγουμε την επανεκκίνηση, εκτελούμε την εντολή:

```
sudo dhclient eth1
```

Μετά την ολοκλήρωση των ρυθμίσεων του δικτύου, μπορούμε να προχωρήσουμε με την προσθήκη του απαιτούμενου λογισμικού. Με δεδομένο ότι το Mininet είναι ήδη εγκατεστημένο στο `image`, θα πρέπει να εγκαταστήσουμε το `FlowVisor`. Ωστόσο, η σχετική διαδικασία απαιτεί την ύπαρξη στο σύστημα του `openjdk6` και του `ant`. Άρα θα πρέπει πρώτα να εγκαταστήσουμε τα δύο αυτά εργαλεία.

Με την εντολή

```
sudo apt-get update
```

το σύστημά μας ενημερώνεται για τα διαθέσιμα πακέτα λογισμικού. Στη συνέχεια εγκαθιστούμε το `openjdk 6`, δίνοντας την εντολή:

```
sudo apt-get install openjdk-6-jdk
```

Παρόμοια προσθέτουμε στο σύστημά μας και το `ant`.

Τεχνικές τεμαχισμού δικτύων (network slicing) - σύγχρονες τάσεις σε επίπεδο παρόχων

```
sudoapt-getinstallant
```

Έχοντας εγκαταστήσει τα απαραίτητα εργαλεία, κατεβάζουμε τον φάκελο με τον πηγαίο κώδικα του FlowVisor από το github με την εντολή:

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

Μόλις ολοκληρωθεί η λήψη, μπαίνουμε στο φάκελο του λογισμικού με την εντολή:

```
cdflowvisor/
```

και στη συνέχεια εγκαθιστούμε το FlowVisor από τον πηγαίο του κώδικα, δίνοντας διαδοχικά τις εντολές:

```
make
```

```
sudomakeinstall
```

Κατά τη διαδικασία της εγκατάστασης, ζητείται από το χρήστη να καθορίσει μία σειρά από παραμέτρους του προγράμματος. Αρχικά αποδεχόμαστε το προκαθορισμένο μονοπάτι εγκατάστασης (/usr/local) πατώντας Enter στη σχετική προτροπή. Στις επόμενες δύο ερωτήσεις ορίζουμε τον user και το group για την εκτέλεση του προγράμματος. Εισάγουμε και στις δύο προτροπές την τιμή mininet ώστε να μη χρειάζεται να αλλάζουμε χρήστη. Ακολούθως πατάμε Enter στην προτροπή Installtodifferentrootdirectory () για να διατηρήσουμε τον προκαθορισμένο ριζικό κατάλογο εγκατάστασης. Τέλος, για λόγους ευκολίας, αφήνουμε κενό το password για το λογαριασμό fvadmin της εφαρμογής, πατώντας και πάλι Enter.

Πριν από την πρώτη εκτέλεση του FlowVisor φορτώνουμε το αρχείο παραμετροποίησης με την εντολή:

```
sudo fvconfig load /etc/flowvisor/config.json
```



Με τις εντολές που ακολουθούν ορίζουμε τον ιδιοκτήτη και τα δικαιώματα για το φάκελο εργασίας της εφαρμογής:

```
sudo chown mininet:mininet -R /usr/local/share/db
sudo chmod -R 777 /usr/local/share/db
```

Εκκινούμε το FlowVisor με την εντολή:

```
sudo /etc/init.d/flowvisor start
```

Σημείωση: Αλλάζοντας στην προηγούμενη εντολή τη λέξη *start* με τις *stop* και *restart*, μπορούμε να τερματίζουμε και να επανεκκινούμε αντίστοιχα το *FlowVisor*.

Με την εντολή

```
fvctl set-config --enable-topo-ctrl
```

ενεργοποιούμε τον ελεγκτή τοπολογίας του FlowVisor.

Ενώ η εντολή

```
fvctl get-config
```

μας επιστρέφει τις παραμέτρους λειτουργίας του προγράμματος.

Τέλος, εάν επιθυμούμε να εκτελούμε παραθυρικές εφαρμογές μέσα από την κονσόλα της εικονικής μηχανής, μπορούμε να εγκαταστήσουμε το *xinit* και έναν διαχειριστή παραθύρων με την εντολή:

```
sudo apt-get install xinit flwm
```

## ΒΙΒΛΙΟΓΡΑΦΙΑ

- [1] J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, J.J. Ramos-Munoz, J. Lorca, J. Folgueira, «Network Slicing for 5G with SDN/NFV: Concepts, Architectures and Challenges», IEEE Communications Magazine Volume: 55, Issue: 5, May 2017
- [2] 5G-PPP, ERTICO, EFFRA, EUTC, NEM, CONTINUA and Networld2020 ETP, “5G empowering vertical industries”, White Paper, Feb. 2016.
- [3] R. Shanbhag and R. Shankarmani, "Architecture for Internet of Things to minimize human intervention," 2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2015, pp. 2348-2353, doi: 10.1109/ICACCI.2015.7275969.
- [4] S. Mattisson, "An Overview of 5G Requirements and Future Wireless Networks: Accommodating Scaling Technology," in IEEE Solid-State Circuits Magazine, vol. 10, no. 3, pp. 54-60, Summer 2018, doi: 10.1109/MSSC.2018.2844606.
- [5] Harald Remmert, “What Is 5G Network Architecture?” 2017 Ιστοσελίδα: <https://www.digi.com/blog/post/5g-network-architecture> - προσπέλαση 9/2021
- [6] Άρθρο: 5G Reference Network Architecture Ιστοσελίδα: <https://www.techplayon.com/5g-reference-network-architecture/> - προσπέλαση 8/2021
- [7] Jones Dan, Bernstein Corinne, RAN Ιστοσελίδα: <https://www.techtarget.com/searchnetworking/definition/radio-access-network-RAN> - προσπέλαση 8/2021
- [8] Άρθρο: 5GArchitecture, Ιστοσελίδα: <https://www.viavisolutions.com/en-us/5g-architecture> - προσπέλαση 8/2021
- [9] I. Stojmenovic (επιμ.) “Handbook of Wireless Networks and Mobile Computing”, τόμ. 27, John Wiley & Sons., 2003
- [10] E. Turban, D. Leidner, E. McLean και J. Wetherbe , “Information Technology For Management. Transforming Organizations in the Digital Economy”, John Wiley & Sons, 6/2008
- [11] Craven Connor, “Understanding the SDN Architecture - SDN Control Plane & SDN Data Plane”, 2015 Ιστοσελίδα: <https://www.sdxcentral.com/networking/sdn/definitions/inside-sdn-architecture/> προσπέλαση 9/2021

- [12] L. Rosencrance, J. English, J. Burke, “software-defined networking (SDN)” Ιστοσελίδα:  
<https://www.techtarget.com/searchnetworking/definition/software-defined-networking-SDN>
- [13] Purkayastha Sh., “Top 5 SDN Use Case Scenarios for Network Deployment” Ιστοσελίδα: <https://radiostud.io/top-5-sdn-use-case-scenarios-for-network-deployment/>- προσπέλαση 9/2021
- [14] Maab Saleem, “Software Defined Network: use cases from the real world” Ιστοσελίδα: <https://www.routerfreak.com/software-defined-network-use-cases-from-the-real-world/>- προσπέλαση 9/2021
- [15] Leonhardt A., “Defining The Elements of NFV Architectures” Ιστοσελίδα: <https://blog.equinix.com/blog/2019/10/17/networking-for-nerds-defining-the-elements-of-nfv-architectures/> - προσπέλαση 9/2021
- [16] Άρθρο: 5 Examples of NFV Use Cases, 2018, Ιστοσελίδα: <https://www.lanner-america.com/blog/5-examples-nfv-use-cases-2017/> - προσπέλαση 9/2021
- [17] Spyridon Vassilaras, Lazaros Gkatzikis, Nikolaos Liakopoulos, Ioannis N Stiakogiannakis, Meiyu Qi, et al.. The Algorithmic Aspects of Network Slicing. IEEE Communications Magazine, Institute of Electrical and Electronics Engineers, 2017, 55 (8), pp.112-119. [ff10.1109/MCOM.2017.1600939ff.fhal02305665f](https://doi.org/10.1109/MCOM.2017.1600939ff.fhal02305665f)
- [18] P. Popovski, K. F. Trillingsgaard, O. Simeone and G. Durisi, "5G Wireless Network Slicing for eMBB, URLLC, and mMTC: A Communication-Theoretic View" in IEEE Access, vol. 6, pp. 55765-55779, 2018, doi: 10.1109/ACCESS.2018.2872781.
- [19]  
<https://ir.lib.uth.gr/xmlui/bitstream/handle/11615/49737/18620.pdf?sequence=1>
- [20] [182]
- [21] José Antonio Ordóñez, Pablo Ameigeiras, Diego R. Lopez, Jorge Ramos, “Network Slicing for 5G with SDN/NFV: Concepts, Architectures and Challenges”, IEEE Communications Magazine · March 2017
- [22] ETSI GS NFV-EVE 005, “Network Functions Virtualisation (NFV); Ecosystem; Report on SDN Usage in NFV Architectural Framework”, V1.1.1, Dec. 2015.

- [23] Minpeng Qi, SECURITY CONSIDERATIONS FOR 5G NETWORK OPERATION, August 2021
- [24] Γεωργακόπουλος Α., “5GNetworkSlicing: Περιγραφή και Προκλήσεις”, Πτυχιακή Εργασία, ΕΚΠΑ, Νοέμβριος 2018
- [25] Sherwood, Rob & Gibb, Glen & Yap, Kok-Kiong & Appenzeller, Guido & Casado, Martin & McKeown, Nick & Parulkar, Guru. (2009). FlowVisor: A Network Virtualization Layer.
- [26] Lantz B., Handigol N., Heller B., and Jeyakumar V., “Introduction to Mininet”, Ιστοσελίδα: <https://github.com/mininet/mininet/wiki/Introduction-to-Mininet> - προσπέλαση 9/2021
- [27] Heller B., Erickson D., Handigol N., and Kazemian P., “Flowvisor Exercise”, Ιστοσελίδα: <https://github.com/onstutorial/onstutorial/wiki/Flowvisor-Exercise> - προσπέλαση 10/2021