ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Network Slicing και SDN: Ανάλυση και Εφαρμογές σε Σύγχρονα Δίκτυα

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

του

Μπουτσικούδη Νικολάου

Επιβλέπων: Αν. Καθηγητής Σκούτας Δημήτριος

Μέλη εξεταστικής επιτροπής: Καθηγητής Σκιάνης Χαράλαμπος,
Καθηγητής Κορμέντζας Γεώργιος

Σάμος, Σεπτέμβριος 2026

Η σελίδα αυτή είναι σκόπιμα λευκή.

Δήλωση Συγγραφέα

Είμαι συγγραφέας αυτής της διπλωματικής εργασίας και δηλώνω ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, έχω αναφέρει τις πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης, βεβαιώνω ότι αυτή η εργασία προετοιμάστηκε από εμένα προσωπικά ειδικά για τη συγκεκριμένη διπλωματική εργασία.

Πρόλογος και ευχαριστίες

Η παρούσα διπλωματική εργασία εκπονήθηκε με αντικείμενο τη μελέτη του Network Slicing και του Software-Defined Networking (SDN), δύο τεχνολογικών προσεγγίσεων που συνδέονται άμεσα με την εξέλιξη των σύγχρονων τηλεπικοινωνιακών δικτύων. Η συνεχής αύξηση των απαιτήσεων σε χωρητικότητα, αξιοπιστία, ασφάλεια και ποιότητα υπηρεσίας καθιστά αναγκαία τη μετάβαση από στατικές και δύσκαμπτες αρχιτεκτονικές σε πιο ευέλικτα, προγραμματιζόμενα και αποδοτικά μοντέλα διαχείρισης δικτυακών πόρων.

Στο πλαίσιο αυτό, το SDN προσφέρει τη δυνατότητα κεντρικού και προγραμματιζόμενου ελέγχου του δικτύου, διαχωρίζοντας το επίπεδο ελέγχου από το επίπεδο προώθησης. Παράλληλα, το Network Slicing επιτρέπει τη δημιουργία πολλαπλών λογικών τμημάτων πάνω στην ίδια φυσική υποδομή, έτσι ώστε διαφορετικές υπηρεσίες να εξυπηρετούνται με διαφορετικές απαιτήσεις ως προς την καθυστέρηση, το εύρος ζώνης, την ασφάλεια και την αξιοπιστία. Η συνδυαστική αξιοποίηση των δύο αυτών τεχνολογιών αποτελεί βασικό άξονα για τα δίκτυα 5G, τις υποδομές νέφους, το Διαδίκτυο των Πραγμάτων και τα περιβάλλοντα υπολογιστικής στο άκρο.

Η εργασία οργανώθηκε με στόχο να παρουσιαστεί τόσο το θεωρητικό υπόβαθρο όσο και η πρακτική διάσταση των αρχιτεκτονικών αυτών. Για τον σκοπό αυτό εξετάζονται βασικές έννοιες, όπως η ποιότητα υπηρεσίας, η απομόνωση μεταξύ τμημάτων δικτύου, η ασφάλεια, η ενορχήστρωση, η διαχείριση κύκλου ζωής και η δυναμική κατανομή πόρων. Παράλληλα, αξιοποιούνται εργαλεία προσομοίωσης, όπως το Cisco Packet Tracer, το GNS3 και το Mininet, ώστε οι θεωρητικές αρχές να συνδεθούν με ρεαλιστικά σενάρια υλοποίησης και αξιολόγησης.

Η επιλογή του συγκεκριμένου θέματος απορρέει από τη σημασία που έχουν σήμερα τα προγραμματιζόμενα δίκτυα και η λογική διαμέριση πόρων για την υποστήριξη ετερογενών υπηρεσιών. Η εργασία επιχειρεί να αναδείξει ότι η αποτελεσματική λειτουργία των σύγχρονων δικτύων δεν εξαρτάται μόνο από την αύξηση της φυσικής χωρητικότητας, αλλά κυρίως από την έξυπνη οργάνωση, την αυτοματοποίηση, την παρακολούθηση και την προσαρμοστική διαχείριση των διαθέσιμων πόρων.

Θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες στον επιβλέποντα καθηγητή κ. Δημήτριο Σκούτα για την καθοδήγηση, την υποστήριξη και τις ουσιαστικές παρατηρήσεις του κατά τη διάρκεια εκπόνησης της παρούσας διπλωματικής εργασίας. Ευχαριστώ επίσης την οικογένειά μου για την αμέριστη στήριξη, την υπομονή και την εμπιστοσύνη της σε όλη τη διάρκεια των σπουδών μου, καθώς η συμβολή της υπήρξε καθοριστική για την ολοκλήρωση αυτής της προσπάθειας.

© 2026
του
ΜΠΟΥΤΣΙΚΟΥΔΗ ΝΙΚΟΛΑΟΥ
Τμήμα Μηχανικών Πληροφοριακών και Επικοινωνιακών Συστημάτων
ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΙΓΑΙΟΥ

Η σελίδα αυτή είναι σκόπιμα λευκή.

Πίνακας περιεχομένων

1 Εισαγωγή 1
1.1 Σύγχρονα δικτυακά περιβάλλοντα και προκλήσεις πολυπλοκότητας 1
1.2 Αντικείμενο διπλωματικής 3
1.2.1 Αντικείμενο, στόχοι και ερευνητικά ερωτήματα της διπλωματικής εργασίας 4
1.2.2 Network Slicing και Software-Defined Networking (SDN) στον χώρο των σύγχρονων δικτύων 5
1.3 Μεθοδολογία προσέγγισης και εργαλεία προσομοίωσης (Cisco Packet Tracer, GNS3/Mininet) 7
1.4 Δομή της διπλωματικής 8
2 Θεωρητικό υπόβαθρο SDN και Network Slicing 9
2.1 Παραδοσιακές αρχιτεκτονικές δικτύων και περιορισμοί στη διαχείριση πόρων 9
2.2 Αρχές Software-Defined Networking: διαχωρισμός control/data plane και βασικά πρωτόκολλα 10
2.3 Έννοια και αρχιτεκτονική του Network Slicing σε δίκτυα 5G, Cloud και IoT 13
2.4 Μηχανισμοί QoS, ασφάλειας και απομόνωσης μεταξύ slices 16
2.5 Εφαρμογές SDN/Network Slicing σε σύγχρονα δίκτυα 20
2.6 Ενορχήστρωση και διαχείριση κύκλου ζωής διαμερίσεων δικτύου 23
2.7 Εργαλεία υλοποίησης που απαιτούνται για τα πειράματα 25
2.8 Δυναμική διαχείριση πόρων και αυτοματοποίηση με Python 25
2.9 Αρχές πειραματικής αξιολόγησης, baseline και αναπαραγωγιμότητας 26
3 Πειραματική εφαρμογή και συγκριτική αξιολόγηση SDN και Network Slicing 27
3.1 Πειραματικός σχεδιασμός: baseline, εφαρμογή και άμεση αξιολόγηση 27
3.2 Υλοποίηση Network Slicing με χρήση VLANs, ACLs, QoS και routing σε Cisco Packet Tracer 27
3.2.1 Ελαττωματικό πρότυπο αναφοράς χωρίς Network Slicing 28
3.2.2 Διορθωτική διαμόρφωση με λογική Network Slicing 28
3.2.3 Συγκριτική επαλήθευση: χωρίς και με Network Slicing 31
3.2.4 Στιγμιότυπα εκτέλεσης Packet Tracer και Mininet 33
3.3 Προγραμματιζόμενη προώθηση με Mininet/OVS και OpenDaylight: χωρίς και με ενεργή πολιτική SDN 48
3.3.1 Ελαττωματικό πρότυπο αναφοράς: συνδεδεμένος controller χωρίς κανόνες προώθησης 48
3.3.2 Διορθωτική παρέμβαση: εγκατάσταση κανόνων OpenFlow από τον controller 51
3.3.3 Λειτουργική επαλήθευση και αξιολόγηση 52
3.4 Δυναμική διαχείριση πόρων με Python: στατική έναντι προσαρμοστικής πολιτικής 53
3.4.1 Ελαττωματικό πρότυπο αναφοράς: σταθερή κατανομή πόρων 53
3.4.2 Διορθωτική παρέμβαση: βρόχος ελέγχου με βάση SLA και χρήση CPU 54
3.4.3 Λειτουργική επαλήθευση και αξιολόγηση της πολιτικής 54
3.5 Συνολική συγκριτική αξιολόγηση των εφαρμογών του Κεφαλαίου 3 55
4 Μελλοντικά σενάρια εφαρμογής αρχιτεκτονικών SDN και Network Slicing 57
4.1 Πλαίσιο σχεδιασμού και παραδοχές των μελλοντικών σεναρίων 57
4.2 Μελλοντικό σενάριο 1 Δυναμική διαμέριση δικτύου για έξυπνο νοσοκομείο 59
4.3 Μελλοντικό σενάριο 2 Προγραμματιζόμενος έλεγχος για συνεργατική αυτόνομη κινητικότητα 61
4.4 Μελλοντικό σενάριο 3 Προγνωστική διαχείριση πόρων σε βιομηχανικό Edge 63
4.5 Μελλοντικό σενάριο 4 Ενοποιημένη αρχιτεκτονική 6G και Edge για αντιμετώπιση καταστροφών 65
4.6 Συγκριτικό πρωτόκολλο αξιολόγησης των σεναρίων 67
4.7 Προϋποθέσεις υλοποίησης και ερευνητικός οδικός χάρτης 70
Συμπεράσματα εργασίας 73
Βιβλιογραφία 75
Παράρτημα Ι: Συμπληρωματικό υλικό προσομοιώσεων και ενδεικτικές ρυθμίσεις 81

Λίστα Σχημάτων

Εικόνα 1: Η ιδέα της διαμέρισης δικτύου και οι προκλήσεις του end-to-end Network Slicing 21
Εικόνα 2: Υψηλού επιπέδου σχήμα διαχείρισης και ενορχήστρωσης διαμερίσεων 24
Εικόνα 3: Τοπολογίες βασικού, δύο και τεσσάρων δομικών στοιχείων 26
Εικόνα 4: Κοινή φυσική τοπολογία για τις καταστάσεις B0 και S1 27
Εικόνα 5: Διαμόρφωση switch με trunk και access ports στα VLAN 11, 110 και 210 28
Εικόνα 6: Έλεγχος VLANs με show vlan brief και αντιστοίχιση θυρών 29
Εικόνα 7: Εφαρμογή ACL Deny_Subnet και ρυθμίσεις δρομολόγησης OSPF 29
Εικόνα 8: Ορισμός ACL για απομόνωση υποδικτύου και αναγνώριση κρίσιμης κίνησης 30
Εικόνα 9: Προβολή ACLs και πίνακα δρομολόγησης 30
Εικόνα 10: Διαμόρφωση QoS με class-map και policy-map 31
Εικόνα 11: Εκτέλεση τοπολογίας στο Cisco Packet Tracer 33
Εικόνα 12: Έλεγχος IP configuration του PC0 μέσω της εντολής ipconfig 34
Εικόνα 13: Έλεγχος IP configuration του PC6 μέσω της εντολής ipconfig 35
Εικόνα 14: Έλεγχος επικοινωνίας μέσω της εντολής ping 36
Εικόνα 15: Παρουσίαση της ACL Deny_Subnet στον router R1 36
Εικόνα 16: Παρουσίαση τμήματος της διαμόρφωσης του router R1 και του πρωτοκόλλου OSPF 37
Εικόνα 17: Παρουσίαση της διαμόρφωσης των VLANs στο switch S1 38
Εικόνα 18: Παρουσίαση της trunk διαμόρφωσης στο switch S1 39
Εικόνα 19: Έλεγχος IP configuration του PC5 μέσω της εντολής ipconfig 40
Εικόνα 20: Αποτυχημένη επικοινωνία μεταξύ PC5 και PC0 μέσω της εντολής ping 41
Εικόνα 21: Παρουσίαση των μετρητών της ACL Deny_Subnet στον router R1 42
Εικόνα 22: Παρουσίαση της πολιτικής WAN_QOS στον router R1 43
Εικόνα 23: Παρουσίαση της διαμόρφωσης της πολιτικής WAN_QOS στον router R1 44
Εικόνα 24: Παρουσίαση του πίνακα δρομολόγησης του router R1 45
Εικόνα 25: Έλεγχος εφαρμογής της πολιτικής WAN_QOS στον router R1 46
Εικόνα 26: Απόρριψη ICMP πακέτου από την ACL στον router R1 47
Εικόνα 27: Τοπολογία του πειράματος με τρεις διαμερίσεις 49
Εικόνα 28: Σύνδεση των μεταγωγέων με τον OpenDaylight στην κατάσταση M0 50
Εικόνα 29: Πίνακας ροών και pingall στην κατάσταση M0 50
Εικόνα 30: Εγκατάσταση της πολιτικής M1 μέσω RESTCONF 51
Εικόνα 31: Πίνακας επικοινωνίας του pingall στην κατάσταση M1 52
Εικόνα 32: Μετρητές του πίνακα ροών του s2 στην κατάσταση M1 53

Λίστα Πινάκων

Πίνακας 1: Αντιστοίχιση λειτουργικών ενοτήτων σε ρόλους διαχείρισης και ενορχήστρωσης διαμερίσεων 24
Πίνακας 2: Σύγκριση ελαττωματικού προτύπου B0 και διαμόρφωσης S1 31
Πίνακας 3: Ελεγχόμενη επαλήθευση της στατικής P0 και της προσαρμοστικής P1 πολιτικής 52
Πίνακας 4: Σύγκριση baseline, παρέμβασης, αποτελέσματος και περιορισμών των τριών εφαρμογών 53
Πίνακας 5: Αντιστοίχιση μελλοντικών σεναρίων, αρχιτεκτονικών και βασικών δεικτών αξιολόγησης 66
Πίνακας 6: Οικογένειες δεικτών του κοινού πρωτοκόλλου αξιολόγησης των σεναρίων 67

Ακρωνύμια

ACL	Access Control List
AI	Artificial Intelligence
APIs	Application Programming Interfaces
ARMA	Autoregressive Moving Average
BSS	Business Support Systems
CPU	Central Processing Unit
eMBB	enhanced Mobile Broadband
FCAPS	Fault, Configuration, Accounting, Performance, Security
GNS3	Graphical Network Simulator-3
GPS	Global Positioning System
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IoT	Internet of Things
ITU	International Telecommunication Union
KPI	Key Performance Indicator
LSTM	Long Short-Term Memory
ML	Machine Learning
MR	Machine Reasoning
mMTC	massive Machine-Type Communications
NETCONF	Network Configuration Protocol
NFV	Network Functions Virtualization
NLP	Natural Language Processing
NTN	Non-Terrestrial Network
OSPF	Open Shortest Path First
OSS	Operations Support Systems
OVS	Open vSwitch
QoS	Quality of Service
RAM	Random Access Memory
REST	Representational State Transfer
RESTCONF	REST-based Network Configuration Protocol
SDN	Software-Defined Networking
SLAs	Service Level Agreements
URLLC	Ultra-Reliable Low-Latency Communications
VLAN	Virtual Local Area Network

Περίληψη

Η παρούσα διπλωματική εργασία εξετάζει τη διαμέριση δικτύου (Network Slicing) και τη δικτύωση οριζόμενη από λογισμικό (Software-Defined Networking-SDN) ως δύο βασικές τεχνολογικές κατευθύνσεις για τη σχεδίαση, τη διαχείριση και τη βελτιστοποίηση σύγχρονων δικτυακών υποδομών. Αφετηρία της μελέτης αποτελεί η διαπίστωση ότι τα σημερινά δίκτυα καλούνται να εξυπηρετήσουν ετερογενείς υπηρεσίες με διαφορετικές και συχνά αντικρουόμενες απαιτήσεις, όπως υψηλό εύρος ζώνης, χαμηλή καθυστέρηση, αξιοπιστία, ασφάλεια και δυνατότητα δυναμικής προσαρμογής. Σε αυτό το πλαίσιο, οι παραδοσιακές αρχιτεκτονικές δικτύων εμφανίζουν περιορισμούς, καθώς βασίζονται σε στατικές ρυθμίσεις και σε κατανεμημένη λογική ελέγχου που δυσκολεύει την αυτοματοποίηση και την ευέλικτη αξιοποίηση των πόρων.

Στο θεωρητικό μέρος της εργασίας αναλύονται οι αρχές του SDN, με έμφαση στον διαχωρισμό του επιπέδου ελέγχου από το επίπεδο προώθησης, στον ρόλο του ελεγκτή SDN και στη χρήση πρωτοκόλλων όπως το OpenFlow. Παράλληλα, παρουσιάζεται η έννοια της διαμέρισης δικτύου, δηλαδή η δυνατότητα δημιουργίας πολλαπλών λογικών διαμερίσεων δικτύου πάνω στην ίδια φυσική υποδομή, καθένα από τα οποία μπορεί να εξυπηρετεί διαφορετικές κατηγορίες υπηρεσιών. Ιδιαίτερη έμφαση δίνεται στους μηχανισμούς ποιότητας υπηρεσίας, στην απομόνωση μεταξύ των διαμερίσεων, στην ασφάλεια, στην αξιοπιστία και στην ενορχήστρωση του κύκλου ζωής των διαμερίσεων δικτύου.

Η εφαρμοσμένη μεθοδολογία οργανώνεται ως σύγκριση κατάστασης αναφοράς (baseline)–παρέμβασης–αξιολόγησης. Στο Cisco Packet Tracer συγκρίνεται η ίδια τοπολογία χωρίς και με λογική διαμέριση μέσω VLAN(Virtual Local Area Network), ACL(Access Control List) και QoS(Quality of Service). Στο Mininet/OVS (Open vSwitch) εξετάζεται αρχικά μια τοπολογία με συνδεδεμένο ελεγκτή OpenDaylight αλλά χωρίς χρήσιμους κανόνες προώθησης και στη συνέχεια η ίδια τοπολογία μετά την εγκατάσταση OpenFlow ροών. Επιπλέον, με Python ελέγχεται ένας ντετερμινιστικός μηχανισμός προσαρμογής πόρων βάσει ορίου SLA (Service Level Agreement) και χρήσης CPU (Central Processing Unit). Η αξιολόγηση βασίζεται σε πραγματικά λειτουργικά τεκμήρια, όπως η εφαρμογή πολιτικών, η συνδεσιμότητα, οι εγκατεστημένες ροές και οι μετρητές τους, καθώς και σε ελεγχόμενες δοκιμές της λογικής κλιμάκωσης, χωρίς να παρουσιάζονται ως μετρημένες αριθμητικές βελτιώσεις τιμές που δεν προέκυψαν από το πείραμα.

Τα αποτελέσματα δείχνουν με λειτουργικό τρόπο ποια δυνατότητα προσθέτει κάθε παρέμβαση. Η λογική διαμέριση επιβάλλει διακριτά όρια υπηρεσιών, ελεγχόμενη πρόσβαση και προτεραιοποίηση, ενώ η παρέμβαση μέσω SDN μετατρέπει ένα συνδεδεμένο αλλά χωρίς χρήσιμη πολιτική επίπεδο προώθησης σε δίκτυο με κεντρικά εγκατεστημένους και επαληθεύσιμους κανόνες ροής. Ο μηχανισμός Python δείχνει πώς οι μετρικές μπορούν να μετατραπούν σε σαφή απόφαση κλιμάκωσης. Παράλληλα, καταγράφονται οι περιορισμοί των εργαλείων και διαχωρίζονται οι λειτουργικές επαληθεύσεις από τις ποσοτικές μετρήσεις επιδόσεων, οι οποίες δεν μπορούν να εκτιμηθούν αξιόπιστα σε περιβάλλον εξομοίωσης.

Λέξεις-κλειδιά: Διαμέριση δικτύου (Network Slicing), δικτύωση οριζόμενη από λογισμικό (Software-Defined Networking, SDN), 5G δίκτυα, ποιότητα υπηρεσίας, εικονικοποίηση δικτύου, δυναμική διαχείριση πόρων, αυτοματοποίηση δικτύων.

Abstract

This diploma thesis examines Network Slicing and Software-Defined Networking (SDN) as two key technological directions for the design, management, and optimization of modern network infrastructures. The study begins from the observation that today's networks are required to support heterogeneous services with different and often conflicting requirements, such as high bandwidth, low latency, reliability, security, and the ability to adapt dynamically. In this context, traditional network architectures present significant limitations, as they rely on static configurations and distributed control logic, which make automation and flexible resource utilization more difficult.

The theoretical part of the thesis analyses the principles of SDN, with emphasis on the separation of the control plane from the forwarding plane, the role of the SDN controller, and the use of protocols such as OpenFlow. At the same time, the concept of Network Slicing is presented, namely the ability to create multiple logical network segments over the same physical infrastructure, each of which can serve different categories of services. Particular emphasis is placed on quality-of-service mechanisms, isolation between slices, security, reliability, and the orchestration of the lifecycle of network slices.

The applied methodology is organized as a baseline–intervention–evaluation comparison. In Cisco Packet Tracer, the same topology is examined without and with logical slicing based on VLANs (Virtual Local Area Networks), ACLs (Access Control Lists), and QoS (Quality of Service). In Mininet/OVS (Open vSwitch), a topology with an attached OpenDaylight controller but no useful forwarding rules is compared with the same topology after OpenFlow rules are installed. In addition, a deterministic Python resource-scaling policy is tested using an SLA (Service Level Agreement) latency threshold and CPU utilization. The evaluation relies on actual functional evidence, including enforced policies, connectivity, installed flows and counters, and controlled test vectors for the scaling logic, while avoiding numerical performance claims that were not measured in the experiment.

The results demonstrate, at a functional level, the specific capability added by each intervention. Logical slicing introduces explicit service boundaries, controlled isolation, and differentiated priority, whereas the SDN intervention turns a connected but policy-less forwarding plane into a network with centrally installed and verifiable flow rules. The Python mechanism shows how monitored values can be converted into a deterministic scaling decision. The limitations of the tools are stated explicitly, and functional verification is kept distinct from quantitative performance measurement that would require a more production-like experimental environment.

Keywords: Network Slicing, Software-Defined Networking, SDN, 5G networks, Quality of Service, network virtualization, dynamic resource management, network automation.

1 Εισαγωγή

1.1 Σύγχρονα δικτυακά περιβάλλοντα και προκλήσεις πολυπλοκότητας

Τα δίκτυα επόμενης γενιάς αναμένεται να είναι ολοένα και πιο πολύπλοκα και αλληλένδετα, εμπλέκοντας πολύ μεγάλο αριθμό συσκευών, υποσυστημάτων και ετερογενών τεχνολογιών. Σε τέτοια περιβάλλοντα, οι απαιτήσεις για διαθεσιμότητα, αξιοπιστία, ευελιξία και ασφάλεια αυξάνονται συνεχώς, ενώ ταυτόχρονα οι πάροχοι καλούνται να υποστηρίξουν δυναμικά μεταβαλλόμενα πρότυπα κίνησης και υπηρεσιών. Ως συνέπεια, τα πλαίσια και τα εργαλεία διαχείρισης δικτύων αποκτούν κρίσιμη σημασία, ώστε να διασφαλίζεται η αποτελεσματική και ασφαλής λειτουργία αυτών των πολύπλοκων υποδομών [5],[6],[11].

Στο παρόν υποκεφάλαιο παρέχεται μια παρουσίαση του χώρου στον οποίο εντάσσεται η διπλωματική εργασία. Αρχικά περιγράφονται τα βασικά χαρακτηριστικά των σύγχρονων δικτυακών περιβαλλόντων και ο τρόπος με τον οποίο η συνεχής εξέλιξή τους οδηγεί σε αυξημένη πολυπλοκότητα, ανάγκη για αυτοματοποίηση της διαχείρισης και αυστηρότερες απαιτήσεις ως προς την ποιότητα υπηρεσίας. Στη συνέχεια αναδεικνύονται τα κύρια προβλήματα που προκύπτουν από αυτές τις συνθήκες, με στόχο να προετοιμαστεί ο αναγνώστης για τα ζητήματα που θα εξεταστούν στα επόμενα κεφάλαια, χωρίς όμως σε αυτό το σημείο να γίνεται ακόμα αναφορά σε συγκεκριμένες τεχνικές λύσεις ή στη λεπτομερή στόχευση της διπλωματικής.

Ένα από τα πιο διαδεδομένα και διαχρονικά πλαίσια διαχείρισης δικτύου είναι το κλασικό μοντέλο για τη διαχείριση δικτύων FCAPS (Fault, Configuration, Accounting, Performance, Security), το οποίο εισήχθη από τον International Organization for Standardization (ISO) ήδη από το 1977 [7]. Το πλαίσιο αυτό οργανώνει τη διαχείριση δικτύων σε πέντε βασικούς άξονες: διαχείριση βλαβών (Fault), διαχείριση διαμόρφωσης (Configuration), διαχείριση λογιστικής/χρέωσης (Accounting), διαχείριση απόδοσης (Performance) και διαχείριση ασφάλειας (Security). Η διαχείριση βλαβών αφορά τον έγκαιρο εντοπισμό και τη διόρθωση προβλημάτων στο δίκτυο, ώστε οι υπηρεσίες να επανέρχονται γρήγορα σε κανονική λειτουργία.

Η διαχείριση διαμόρφωσης σχετίζεται με τις ρυθμίσεις, τις αλλαγές και τη γενικότερη συντήρηση των συσκευών και των υπηρεσιών του δικτύου. Η διαχείριση λογιστικής έχει ως στόχο να καταγράφει πόροι και υπηρεσίες που χρησιμοποιούνται, ώστε να υποστηρίζονται η χρέωση και η συλλογή στατιστικών στοιχείων. Η διαχείριση απόδοσης ασχολείται με τον συνεχή έλεγχο και τη

βελτίωση της ποιότητας λειτουργίας του δικτύου, ενώ η διαχείριση ασφάλειας επικεντρώνεται στην προστασία από μη εξουσιοδοτημένη πρόσβαση, επιθέσεις και άλλες απειλές. Με τη συστηματική εφαρμογή του πλαισίου FCAPS, οι διαχειριστές μπορούν να αντιμετωπίζουν πιο οργανωμένα τα ζητήματα λειτουργίας, σταθερότητας και ασφάλειας σε σύγχρονα, μεγάλης κλίμακας δίκτυα [7].

Η συνεχής αύξηση της πολυπλοκότητας των δικτύων τα τελευταία χρόνια έχει οδηγήσει στην έντονη διερεύνηση μεθόδων διαχείρισης που βασίζονται στην Τεχνητή Νοημοσύνη (AI – Artificial Intelligence) στο πλαίσιο του FCAPS. Οι προσεγγίσεις αυτές χωρίζονται, σε γενικές γραμμές, σε δύο βασικές κατηγορίες: στη Μηχανική Μάθηση (ML – Machine Learning) και στη Μηχανική Συλλογιστική (MR – Machine Reasoning) [7].

Αν και οι δύο αποτελούν βασικά συστατικά της AI, επιτελούν διαφορετικούς ρόλους στη μοντελοποίηση πολύπλοκων φαινομένων και στη λήψη αποφάσεων. Η ML επικεντρώνεται στην ανάπτυξη αλγορίθμων και στατιστικών μοντέλων που επιτρέπουν σε ένα σύστημα να «μαθαίνει» από δεδομένα, να αναγνωρίζει πρότυπα και να βελτιώνει την απόδοσή του σε συγκεκριμένες εργασίες χωρίς ρητό προγραμματισμό. Μέσα από την ανάλυση πολύ μεγάλων όγκων δεδομένων, ένα μοντέλο ML μπορεί να πραγματοποιεί προβλέψεις, να ταξινομεί γεγονότα και να εντοπίζει κρυφές δομές, κάτι που το έχει καταστήσει ιδιαίτερα χρήσιμο σε τομείς όπως η όραση υπολογιστών, η ιατρική διάγνωση, οι μηχανές αναζήτησης, η αναγνώριση ομιλίας και η Επεξεργασία Φυσικής Γλώσσας (NLP– Natural Language Processing).

Η Μηχανική Συλλογιστική (MR), από την άλλη πλευρά, στοχεύει στη δημιουργία συστημάτων AI που βασίζονται σε ρητά μοντελοποιημένη γνώση και δομημένες διαδικασίες συμπερασμού. Τα συστήματα αυτά αξιοποιούν διαφορετικά είδη γνώσης, όπως λογικούς κανόνες, γράφους γνώσης, στοιχεία κοινής λογικής και πληροφορία από κείμενα, και στη συνέχεια χρησιμοποιούν κατάλληλους μηχανισμούς συλλογιστικής ώστε να αντιμετωπίζουν συγκεκριμένα προβλήματα μέσα στα εκάστοτε όρια και περιορισμούς. Ένα βασικό χαρακτηριστικό των μεθόδων MR είναι η δυνατότητά τους να παράγουν αναγώγιμες και κατανοητές εξηγήσεις για τα συμπεράσματά τους, βελτιώνοντας έτσι την ερμηνευσιμότητα και την εμπιστοσύνη στα αποτελέσματα. Σε αντίθεση με πολλές «μαύρου κουτιού» προσεγγίσεις ML, οι MR μέθοδοι δίνουν έμφαση στη δυνατότητα ερμηνείας και αιτιολόγησης των αποφάσεων.

Παρότι η κλασική μηχανική μάθηση (ML) έχει αποδειχθεί ιδιαίτερα ισχυρή σε πληθώρα εφαρμογών, παρουσιάζει σημαντικές προκλήσεις όταν καλείται να λειτουργήσει σε περιβάλλοντα με συχνές αλλαγές ή σε σενάρια που δεν έχουν εμφανιστεί στα δεδομένα εκπαίδευσης. Τα πιο πρόσφατα μοντέλα που βασίζονται σε βαθιά νευρωνικά δίκτυα (deep learning) κάνουν δύσκολη την εξήγηση του πώς και γιατί κατέληξαν σε ένα συγκεκριμένο αποτέλεσμα. Αυτό δημιουργεί πρόβλημα όταν θέλουμε να τα χρησιμοποιήσουμε για τη διαχείριση δικτύων, όπου είναι σημαντικό ο διαχειριστής να μπορεί να ελέγχει και να κατανοεί τις αποφάσεις του συστήματος [14].

Για τους λόγους αυτούς, αυξάνεται το ενδιαφέρον για προσεγγίσεις MR στο πλαίσιο της διαχείρισης σύγχρονων δικτύων. Οι MR μέθοδοι, χάρη στην ικανότητά τους να γενικεύουν και να εξάγουν λογικά συμπεράσματα σε νέα σενάρια, είναι περισσότερο κατάλληλες για περιβάλλοντα όπου οι συνθήκες αλλάζουν γρήγορα και απαιτείται συνδυασμός δεδομένων, γνώσης και κανόνων. Επιπλέον, επειδή είναι εγγενώς επεξηγηματικές, διευκολύνουν την κατανόηση και τον έλεγχο των αποφάσεων από ανθρώπινους διαχειριστές, κάτι ιδιαίτερα σημαντικό όταν η διαχείριση αφορά σύνθετα δίκτυα 5G/6G με αυστηρές απαιτήσεις ποιότητας υπηρεσίας και ασφάλειας. Πρόσφατες

έρευνες δείχνουν ότι οι MR προσεγγίσεις μπορούν να ξεπεράσουν σε αρκετές περιπτώσεις τις καθαρά ML λύσεις τόσο ως προς την ακρίβεια όσο και ως προς την ερμηνευσιμότητα, όταν εφαρμόζονται σε σενάρια διαχείρισης βλαβών, διαμόρφωσης, απόδοσης και ασφάλειας σε σύγχρονες τηλεπικοινωνιακές υποδομές [7].

Η είσοδος της MR στον χώρο των τηλεπικοινωνιών έχει συμβάλει σε μια νέα γενιά «έξυπνων» πλαισίων διαχείρισης δικτύου, εντός και πέραν του κλασικού FCAPS. Η ανάλυση μεγάλων ποσοτήτων λειτουργικών δεδομένων δικτύου επιτρέπει σε MR αλγορίθμους να εντοπίζουν σύνθετα πρότυπα συμπεριφοράς, να προτείνουν βέλτιστες διαμορφώσεις και να υποστηρίζουν την προληπτική συντήρηση μέσω πρόβλεψης πιθανών αστοχιών. Παράλληλα, η δυνατότητα προσαρμογής των παρεχόμενων υπηρεσιών στις ανάγκες και στις προτιμήσεις των χρηστών, η ενίσχυση της ασφάλειας μέσα από έγκαιρη ανίχνευση ανωμαλιών και κυβερνοαπειλών, καθώς και η βελτιστοποίηση της κατανομής πόρων με βάση πρότυπα ζήτησης και προβλέψεις κίνησης, αναδεικνύουν τη MR ως έναν πολλά υποσχόμενο μηχανισμό αντιμετώπισης της πολυπλοκότητας στα σύγχρονα δικτυακά περιβάλλοντα [7].

1.2 Αντικείμενο διπλωματικής

Η παρούσα εργασία έχει ως αντικείμενο τη μελέτη, την ανάλυση και την αξιολόγηση αρχιτεκτονικών που συνδυάζουν την διαμέριση δικτύου (Network Slicing), με δικτύωση οριζόμενη από λογισμικό (SDN - Software-Defined Networking) σε σύγχρονα δικτυακά περιβάλλοντα. Η εργασία εστιάζει στο πώς μια κοινή φυσική υποδομή μπορεί να υποστηρίξει πολλαπλές λογικές υπηρεσίες με διαφορετικές απαιτήσεις, όπως υψηλό εύρος ζώνης, χαμηλή καθυστέρηση, αυξημένη αξιοπιστία, ασφάλεια και απομόνωση της κίνησης. Το βασικό ζήτημα που εξετάζεται είναι ότι τα παραδοσιακά δίκτυα, τα οποία στηρίζονται σε στατικές ρυθμίσεις και αποκεντρωμένη λήψη αποφάσεων ανά συσκευή, δυσκολεύονται να ανταποκριθούν στις ανάγκες των δικτύων 5G, των υποδομών νέφους (cloud), του Διαδικτύου των Πραγμάτων (Internet of Things) και των εφαρμογών πραγματικού χρόνου.

Το πρόβλημα που επιχειρεί να αντιμετωπίσει η διπλωματική αφορά την αδυναμία των συμβατικών αρχιτεκτονικών να παρέχουν ευέλικτη και αποδοτική διαχείριση πόρων, συνεπή εφαρμογή πολιτικών ποιότητας υπηρεσίας και σαφή διαχωρισμό μεταξύ διαφορετικών κατηγοριών υπηρεσιών. Σε ένα σύγχρονο δίκτυο μπορεί να συνυπάρχουν εφαρμογές βίντεο υψηλής ανάλυσης, υπηρεσίες βιομηχανικού ελέγχου, εφαρμογές χαμηλής καθυστέρησης και μαζικές συνδέσεις αισθητήρων. Οι υπηρεσίες αυτές δεν έχουν τις ίδιες τεχνικές απαιτήσεις και, επομένως, δεν μπορούν να εξυπηρετούνται αποτελεσματικά με ενιαία και στατική λογική διαχείρισης. Η εργασία εξετάζει πώς η διαμέριση δικτύου μπορεί να δημιουργήσει ξεχωριστές λογικές διαμερίσεις, ενώ το SDN μπορεί να αναλάβει τον κεντρικό, προγραμματιζόμενο και δυναμικό έλεγχο αυτών των διαμερίσεων.

Η προσέγγιση της εργασίας δεν περιορίζεται στη θεωρητική παρουσίαση των δύο τεχνολογιών, αλλά επεκτείνεται στη σχεδίαση και προσομοίωση αντιπροσωπευτικών δικτυακών σεναρίων. Για τον σκοπό αυτό αξιοποιούνται εργαλεία όπως το Cisco Packet Tracer, το Graphical Network Simulator-3 (GNS3) και το Mininet, ώστε να εξεταστούν διαφορετικοί μηχανισμοί υλοποίησης, όπως VLANs (Virtual Local Area Networks), ACLs (Access Control Lists), QoS (Quality of

Service), δρομολόγηση (routing), OpenFlow, εικονικοί μεταγωγείς και ελεγκτές SDN (SDN controllers). Μέσα από τα σενάρια αυτά διερευνάται ο τρόπος με τον οποίο μπορούν να διαχωριστούν οι ροές κίνησης, να απομονωθούν υπηρεσίες, να εφαρμοστούν κανόνες προτεραιότητας και να αξιολογηθεί η επίδραση των επιλογών σχεδίασης στην απόδοση και στη σταθερότητα του δικτύου.

Ιδιαίτερη βαρύτητα δίνεται στις τεχνικές δυσκολίες που συνοδεύουν την πρακτική αξιοποίηση των SDN και της διαμέρισης δικτύου. Η δημιουργία μιας λογικής διαμέρισης δεν αρκεί από μόνη της, εάν δεν συνοδεύεται από σωστή κατανομή πόρων, έλεγχο συμφόρησης, τήρηση συμφωνιών επιπέδου υπηρεσίας, ασφάλεια του επιπέδου ελέγχου και μηχανισμούς παρακολούθησης της κατάστασης του δικτύου. Για τον λόγο αυτό, η εργασία εξετάζει μετρικές όπως καθυστέρηση, απώλεια πακέτων, διεκπεραιωτική ικανότητα, αξιοποίηση συνδέσεων, χρόνος εγκατάστασης κανόνων ροής και συμπεριφορά σε συνθήκες συμφόρησης ή αποτυχίας. Με αυτόν τον τρόπο, ο αναγνώστης μπορεί να κατανοήσει τόσο τον σκοπό της διπλωματικής όσο και τις βασικές τεχνικές προκλήσεις που ανακύπτουν κατά την εφαρμογή των προτεινόμενων αρχιτεκτονικών.

1.2.1 Αντικείμενο, στόχοι και ερευνητικά ερωτήματα της διπλωματικής εργασίας

Το αντικείμενο της διπλωματικής εργασίας είναι η συστηματική διερεύνηση του τρόπου με τον οποίο το SDN μπορεί να υποστηρίξει τη διαμέριση δικτύου και να καταστήσει δυνατή τη λειτουργία πολλαπλών, ανεξάρτητων και προσαρμόσιμων λογικών δικτύων πάνω στην ίδια φυσική υποδομή. Η εργασία αντιμετωπίζει την διαμέριση δικτύου ως μηχανισμό οργάνωσης υπηρεσιών με διαφορετικές απαιτήσεις και το SDN ως τεχνολογικό υπόβαθρο που επιτρέπει την κεντρική επιβολή πολιτικών, τη δυναμική δρομολόγηση και την αυτοματοποίηση της διαχείρισης. Με αυτόν τον τρόπο, το αντικείμενο της μελέτης συνδέει την αρχιτεκτονική θεώρηση με την πρακτική υλοποίηση και αξιολόγηση σε περιβάλλον προσομοίωσης.

Οι βασικοί στόχοι της εργασίας είναι η αποσαφήνιση των αρχών λειτουργίας του SDN και της διαμέρισης δικτύου, η ανάδειξη των πλεονεκτημάτων τους σε σχέση με τις παραδοσιακές αρχιτεκτονικές δικτύων και η εξέταση του τρόπου με τον οποίο οι δύο προσεγγίσεις μπορούν να λειτουργήσουν συμπληρωματικά. Παράλληλα, επιδιώκεται η σχεδίαση ρεαλιστικών σεναρίων προσομοίωσης, η εφαρμογή τεχνικών απομόνωσης και ποιότητας υπηρεσίας, η μέτρηση κρίσιμων δεικτών απόδοσης και η αξιολόγηση της συμπεριφοράς του δικτύου σε συνθήκες κανονικής λειτουργίας, αυξημένου φόρτου και πιθανών αστοχιών.

Η διπλωματική θέτει ως κεντρικό ερευνητικό ερώτημα το κατά πόσο ο συνδυασμός διαμέρισης δικτύου και SDN μπορεί να βελτιώσει τη διαχείριση πόρων, την ποιότητα υπηρεσίας και την ευελιξία σε σύγχρονα δίκτυα. Από το ερώτημα αυτό προκύπτουν επιμέρους ερωτήματα: πώς μπορούν να δημιουργηθούν και να διαχειριστούν ξεχωριστές διαμερίσεις δικτύου με διαφορετικές απαιτήσεις, ποιοι μηχανισμοί είναι κατάλληλοι για την απομόνωση της κίνησης, πώς επηρεάζεται η απόδοση όταν εφαρμόζονται πολιτικές QoS και ποιος είναι ο ρόλος του ελεγκτή SDN στην παρακολούθηση και προσαρμογή της λειτουργίας του δικτύου.

Επιπλέον, η εργασία εξετάζει εάν τα εργαλεία προσομοίωσης μπορούν να χρησιμοποιηθούν αποτελεσματικά για την αξιολόγηση τέτοιων αρχιτεκτονικών πριν από την υλοποίησή τους σε πραγματικό εξοπλισμό. Στο πλαίσιο αυτό διερευνάται ποια πλεονεκτήματα προσφέρει το Cisco Packet Tracer για τη βασική δικτυακή σχεδίαση, ποια πρόσθετη ρεαλιστικότητα παρέχουν το GNS3

και το Mininet, και πως μπορούν να αξιοποιηθούν τεχνικές αυτοματοποίησης ή μηχανικής μάθησης για τη δυναμική διαχείριση πόρων. Έτσι, η εργασία συνδέει τη θεωρητική γνώση με μια πειραματική διαδικασία που επιτρέπει συγκρίσεις, επαναληψιμότητα και τεκμηριωμένη εξαγωγή συμπερασμάτων.

Η αναμενόμενη συμβολή της διπλωματικής είναι η διαμόρφωση μιας ολοκληρωμένης εικόνας για τον σχεδιασμό, την υλοποίηση και την αξιολόγηση της διαμέρισης δικτύου βασισμένη σε SDN σε σύγχρονα δίκτυα. Η εργασία δεν αντιμετωπίζει τις τεχνολογίες αυτές ως μεμονωμένες έννοιες, αλλά ως μέρος ενός ευρύτερου πλαισίου διαχείρισης, όπου η απόδοση, η ασφάλεια, η απομόνωση, η αξιοπιστία και η αυτοματοποίηση πρέπει να εξετάζονται ταυτόχρονα. Με αυτόν τον τρόπο παρέχεται ένα σαφές υπόβαθρο για περαιτέρω μελέτη σε δίκτυα 5G, edge computing, υποδομές νέφους και μελλοντικές αρχιτεκτονικές 6G.

1.2.2 Network Slicing και Software-Defined Networking (SDN) στον χώρο των σύγχρονων δικτύων

Το παρόν υποκεφάλαιο παρουσιάζει το ρόλο της διαμέρισης δικτύου και της δικτύωσης που ορίζεται από λογισμικό (SDN) στα σύγχρονα τηλεπικοινωνιακά περιβάλλοντα. Η διαμέριση δικτύου και το SDN αποτελούν δύο αλληλένδετες τεχνολογικές κατευθύνσεις που απαντούν στις προκλήσεις πολυπλοκότητας, ετερογένειας και απαιτήσεων ποιότητας υπηρεσίας που αναλύθηκαν στις προηγούμενες υποενότητες. Παράλληλα, η κατανόησή τους είναι απαραίτητη προϋπόθεση για την ερμηνεία των σεναρίων προσομοίωσης και των αποτελεσμάτων που παρουσιάζονται στα επόμενα κεφάλαια της διπλωματικής, καθώς αποτελούν το θεωρητικό υπόβαθρο πάνω στο οποίο δομείται το σύνολο της εργασίας.

Η διαμέριση δικτύου αποτελεί μία από τις σημαντικότερες εξελίξεις στην αρχιτεκτονική των 5G και 6G υποδομών και έχει ως στόχο τη δημιουργία πολλαπλών λογικών δικτύων επάνω στην ίδια φυσική υποδομή, καθένα από τα οποία διαθέτει συγκεκριμένες προδιαγραφές ως προς την ποιότητα υπηρεσίας, την καθυστέρηση, την ασφάλεια και τη διαχείριση πόρων [1]. Σε αντίθεση με κλασικές τεχνικές διαχωρισμού, όπως οι VLANs ή οι απλοί μηχανισμοί QoS, η διαμέριση δικτύου εισάγει την έννοια του πλήρως απομονωμένου λογικού δικτύου, με δική του αρχιτεκτονική, πολιτικές διαχείρισης, μηχανισμούς ελέγχου και διαδικασίες λειτουργίας [3],[10],[11].

Με τον τρόπο αυτό, οι πάροχοι μπορούν να εξυπηρετούν ταυτόχρονα εντελώς διαφορετικές υπηρεσίες, από εφαρμογές υψηλής χωρητικότητας που εντάσσονται στην κατηγορία της εξελιγμένης κινητής ευρυζωνικότητας (eMBB – enhanced Mobile Broadband)[1], μέχρι υπηρεσίες εξαιρετικά υψηλής αξιοπιστίας και χαμηλής καθυστέρησης (URLLC – Ultra-Reliable Low-Latency Communications)[2] και υπηρεσίες μαζικής διασύνδεσης συσκευών, ή αλλιώς μαζικών μηχανικού

[1] Η κατηγορία enhanced Mobile Broadband (eMBB) αφορά υπηρεσίες πολύ υψηλού ρυθμού μετάδοσης και μεγάλης χωρητικότητας, όπως video streaming υψηλής ανάλυσης, εφαρμογές εικονικής/επαυξημένης πραγματικότητας κ.λ.π.

[2] Η κατηγορία Ultra-Reliable Low-Latency Communications (URLLC) αφορά υπηρεσίες με εξαιρετικά υψηλή αξιοπιστία και πολύ χαμηλή καθυστέρηση, κατάλληλες για βιομηχανικό έλεγχο, κρίσιμες εφαρμογές αυτοματισμού, απομακρυσμένη ιατρική κ.λ.π.

τύπου επικοινωνιών (mMTC– massive Machine-Type Communications)[3], χωρίς να απαιτείται η δημιουργία ξεχωριστών φυσικών δικτύων [3],[10],[11].

Η βασική ιδέα πίσω από τη διαμέριση δικτύου είναι ότι κάθε διαμέριση υλοποιεί ένα "εικονικό δίκτυο από άκρο σε άκρο", το οποίο εκτείνεται από τη συσκευή του τελικού χρήστη μέχρι τον πυρήνα και τις υποδομές νέφους και edge computing. Κάθε τέτοια διαμέριση μπορεί να σχεδιάζεται, να παραμετροποιείται και να διαχειρίζεται με βάση συγκεκριμένα επιχειρησιακά σενάρια, όπως για παράδειγμα για υπηρεσίες βιομηχανικού αυτοματισμού, υπηρεσίες υγείας ή εφαρμογές ψυχαγωγίας με υψηλές απαιτήσεις εύρους ζώνης [2]. Στο πλαίσιο αυτό, οι συμφωνίες επιπέδου υπηρεσίας (SLAs – Service Level Agreements) μεταφράζονται σε συγκεκριμένες τεχνικές παραμέτρους (μέγιστη καθυστέρηση, ρυθμοί μετάδοσης, επίπεδα απωλειών, απαιτήσεις διαθεσιμότητας) που πρέπει να ικανοποιούνται συνεχώς κατά τη διάρκεια ζωής της διαμέρισης [5],[6].

Για να υλοποιηθεί αποδοτικά αυτή η λογική διαμέριση, απαιτείται η ύπαρξη μηχανισμών ευέλικτης διαχείρισης πόρων και δυναμικής προσαρμογής της υποδομής, ιδίως σε περιβάλλοντα όπου οι απαιτήσεις των εφαρμογών μεταβάλλονται γρήγορα ή παρουσιάζουν έντονη εποχικότητα. Εδώ αναδεικνύεται ο κρίσιμος ρόλος του SDN, το οποίο εισάγει μια θεμελιώδη αρχιτεκτονική αλλαγή, διαχωρίζοντας το επίπεδο ελέγχου από το επίπεδο προώθησης (control και data plane), έτσι ώστε οι αποφάσεις δρομολόγησης και πολιτικής να λαμβάνονται κεντρικά από έναν ή περισσότερους ελεγκτές SDN [4], οι οποίοι διαθέτουν μια σφαιρική, λογικά κεντρικοποιημένη εικόνα του δικτύου και μπορούν να εφαρμόζουν κανόνες σε επίπεδο ροών (flows) σε πληθώρα συσκευών, ανεξάρτητα από τον κατασκευαστή ή την συγκεκριμένη τεχνολογία υλοποίησης [58].

Η προσέγγιση αυτή προσφέρει πολλαπλά πλεονεκτήματα για την υποστήριξη της διαμέρισης δικτύου. Πρώτον, επιτρέπει την ταχεία δημιουργία, τροποποίηση και διαγραφή διαμερίσεων, αφού οι αλλαγές δεν απαιτούν χειροκίνητη παραμετροποίηση κάθε επιμέρους συσκευής αλλά επιβάλλονται κεντρικά μέσω κατάλληλων APIs (Application Programming Interfaces) και πρωτοκόλλων, όπως π.χ. OpenFlow [4]. Δεύτερον, διευκολύνει την αυτοματοποίηση της διαχείρισης, καθώς οι πολιτικές που αφορούν την διαβάθμιση της κίνησης, την εφαρμογή μηχανισμών QoS ή την απομόνωση μεταξύ διαμερίσεων μπορούν να ενσωματωθούν σε λογισμικό και να εκτελούνται δυναμικά. Τρίτον, καθιστά πιο απλή την ενσωμάτωση τεχνικών μηχανικής μάθησης και αναλυτικής δεδομένων στο επίπεδο ελέγχου, επιτρέποντας τη λήψη αποφάσεων βάσει μετρήσεων και προβλέψεων κίνησης [1],[14].

Η σύζευξη της διαμέρισης δικτύου και του SDN, η οποία αποτελεί κεντρικό άξονα της παρούσας διπλωματικής, δίνει τη δυνατότητα υλοποίησης σύνθετων σεναρίων στα οποία οι ανάγκες των εφαρμογών μεταβάλλονται δυναμικά, τόσο σε επίπεδο ζήτησης πόρων όσο και σε επίπεδο απαιτήσεων αξιοπιστίας και ασφάλειας [1],[3]. Μια διαμέριση που εξυπηρετεί εφαρμογές χαμηλής καθυστέρησης, όπως βιομηχανικό έλεγχο, μπορεί να αναδιαμορφώνει την πορεία της κίνησης έτσι ώστε να αποφεύγονται συμφορήσεις, ενώ μια διαμέριση για υπηρεσίες υψηλής χωρητικότητας, όπως συνεχής μετάδοση βίντεο (video streaming) υψηλής ανάλυσης, μπορεί να προσαρμόζει δυναμικά το διαθέσιμο εύρος ζώνης ανάλογα με τις αιχμές κίνησης. Ο ελεγκτής SDN

[3] Η κατηγορία massive Machine-Type Communications (mMTC) αφορά υπηρεσίες μαζικής διασύνδεσης μεγάλου αριθμού συσκευών μικρής κατανάλωσης, όπως αισθητήρες και συσκευές IoT, με σχετικά μικρούς ρυθμούς μετάδοσης αλλά υψηλή πυκνότητα ανά περιοχή.

λειτουργεί ως ενορχηστρωτής όλων των προαναφερόμενων αλλαγών, παρακολουθώντας διαρκώς την κατάσταση του δικτύου και εφαρμόζοντας τις κατάλληλες πολιτικές δρομολόγησης/διαχείρισης στο επίπεδο κάθε διαμέρισης [5],[6].

Ένα επιπλέον πλεονέκτημα της συνδυαστικής αυτής προσέγγισης είναι η δυνατότητα αυστηρής απομόνωσης μεταξύ διαμερίσεων, τόσο σε επίπεδο απόδοσης όσο και σε επίπεδο ασφάλειας. Η λογική διαχωριστική γραμμή που παρέχει η διαμέριση δικτύου μπορεί να ενισχυθεί από τους μηχανισμούς ελέγχου του SDN, ώστε να περιορίζεται η διάδοση επιθέσεων ή η ακούσια παρεμβολή κίνησης μεταξύ διαφορετικών υπηρεσιών [3]. Επιπρόσθετα, η ύπαρξη κεντρικού σημείου ελέγχου διευκολύνει την παρακολούθηση δεικτών απόδοσης (KPIs) και την εξαγωγή συμπερασμάτων για την τήρηση των SLAs, ενώ δημιουργεί τις προϋποθέσεις για υλοποίηση αυτορρυθμιζόμενων (self-healing - αυτοαποκατάσταση, self-optimizing - αυτοβελτιστοποίηση) δικτύων, όπου οι διαμερίσεις προσαρμόζονται αυτόματα με βάση τη ζήτηση και τις συνθήκες λειτουργίας του δικτύου [2],[6],[23].

Παρά τα οφέλη, η υλοποίηση της διαμέρισης δικτύου πάνω από υποδομές βασισμένες σε SDN συνοδεύεται από σημαντικές προκλήσεις, οι οποίες αποτελούν αντικείμενο εντατικής ερευνητικής δραστηριότητας [1],[3]. Η σύνθετη αλληλεπίδραση μεταξύ φυσικής υποδομής, επιπέδου ελέγχου και πολλαπλών διαμερίσεων δημιουργεί ζητήματα κλιμακωσιμότητας, ανθεκτικότητας και διαλειτουργικότητας μεταξύ διαφορετικών πλατφορμών και προτύπων. Επιπλέον, η ανάγκη για ακριβή παρακολούθηση της κατάστασης κάθε διαμέρισης, σε συνδυασμό με τις απαιτήσεις σε πραγματικό χρόνο, καθιστά αναγκαία την ανάπτυξη αποδοτικών μηχανισμών συλλογής και επεξεργασίας μετρήσεων. Θέματα όπως η ασφάλεια του ελεγκτή SDN, η προστασία από κακόβουλες ή εσφαλμένες πολιτικές ελέγχου, καθώς και η διασφάλιση της ιδιωτικότητας των δεδομένων εντός των διαμερίσεων, αποτελούν επίσης κρίσιμους παράγοντες που δεν μπορούν να αγνοηθούν [4],[12],[15].

Σε αυτό το πλαίσιο, η παρούσα διπλωματική εστιάζει στην καλύτερη κατανόηση και αξιολόγηση των αρχιτεκτονικών SDN και διαμέρισης δικτύου μέσω σχεδίασης και προσομοίωσης αντιπροσωπευτικών σεναρίων. Οι έννοιες που μελετήθηκαν εδώ, λειτουργούν προπαρασκευαστικά για την προσέγγιση και τα εργαλεία προσομοίωσης (Cisco Packet Tracer, GNS3/Mininet) που θα αξιοποιηθούν στα επόμενα κεφάλαια, όπου το SDN και η διαμέριση δικτύου θα μελετηθούν σε ρεαλιστικά πειραματικά περιβάλλοντα, με έμφαση στη διαχείριση πόρων, την ποιότητα υπηρεσίας και την ασφάλεια των σύγχρονων δικτυακών υποδομών.

1.3 Μεθοδολογία προσέγγισης και εργαλεία προσομοίωσης (Cisco Packet Tracer, GNS3/Mininet)

Η μεθοδολογία βασίζεται σε ελεγχόμενες συγκρίσεις της ίδιας λογικής υποδομής πριν και μετά την εφαρμογή ενός μηχανισμού. Για κάθε σενάριο ορίζονται η κατάσταση αναφοράς, η διορθωτική παρέμβαση και το τεκμήριο που χρησιμοποιείται για την επαλήθευση του αποτελέσματος. Η προσέγγιση αυτή επιτρέπει να αποδίδεται η παρατηρούμενη αλλαγή στον εξεταζόμενο μηχανισμό και όχι σε αλλαγή της τοπολογίας ή των αρχικών συνθηκών [27].

Το Cisco Packet Tracer χρησιμοποιείται για το σενάριο λογικής διαμέρισης με VLAN, ACL και QoS, ενώ το Mininet με Open vSwitch και OpenDaylight χρησιμοποιείται για τη σύγκριση προώθησης χωρίς και με εγκατεστημένη πολιτική SDN. Η Python χρησιμοποιείται σε ξεχωριστό σενάριο για να ελεγχθεί ένας απλός βρόχος προσαρμογής πόρων βάσει SLA. Οι τεχνικές λεπτομέρειες των εργαλείων παρουσιάζονται μία φορά στο Κεφάλαιο 2 και στο Κεφάλαιο 3 αναφέρονται μόνο όσα απαιτούνται για την εκτέλεση και την ερμηνεία κάθε εφαρμογής [18],[27], [32].

Η αξιολόγηση προσαρμόζεται στις δυνατότητες κάθε εργαλείου. Όπου υπάρχουν πραγματικά λειτουργικά τεκμήρια, όπως ACL, πίνακες ροών (flow tables), μετρητές ή αποτέλεσμα συνδεσιμότητας, χρησιμοποιούνται άμεσα. Όπου δεν υπάρχουν πραγματικές μετρήσεις, δεν εισάγονται τεχνητές αριθμητικές τιμές. Με αυτόν τον τρόπο διατηρείται σαφής διάκριση ανάμεσα σε λειτουργική επαλήθευση, ελεγχόμενο unit test και ποσοτική μέτρηση [27].

1.4 Δομή διπλωματικής

Η διπλωματική εργασία οργανώνεται σε τέσσερα κύρια κεφάλαια. Στο Κεφάλαιο 1 παρουσιάζονται το γενικό πλαίσιο, το αντικείμενο και η μεθοδολογική κατεύθυνση της μελέτης. Στο Κεφάλαιο 2 συγκεντρώνεται το θεωρητικό υπόβαθρο του SDN και διαμέρισης δικτύου (Network slicing), μαζί με τις απολύτως αναγκαίες έννοιες για τα εργαλεία υλοποίησης, τη δυναμική διαχείριση πόρων και την πειραματική αξιολόγηση, ώστε να αποφεύγεται η επανάληψη θεωρίας στα επόμενα κεφάλαια. Στο Κεφάλαιο 3 η έμφαση μεταφέρεται στην εφαρμογή: για κάθε βασικό μηχανισμό ορίζεται πρώτα ένα πρότυπο αναφοράς χωρίς την εξεταζόμενη λειτουργία, παρουσιάζεται η διορθωτική διαμόρφωση και αξιολογείται άμεσα τι αλλάζει στη συμπεριφορά του ίδιου δικτύου. Ειδικότερα εξετάζονται η λογική διαμέριση στο Cisco Packet Tracer, η προγραμματιζόμενη προώθηση με Mininet/ Open vSwitch (OVS) και OpenDaylight και ένας μηχανισμός προσαρμοστικής διαχείρισης πόρων με Python. Στο Κεφάλαιο 4 γίνεται συνθετική αποτίμηση των ευρημάτων ως προς την αξιοποίηση πόρων, την ποιότητα υπηρεσίας, την ασφάλεια, την αξιοπιστία και την απόδοση του επιπέδου ελέγχου. Τέλος, ακολουθούν η βιβλιογραφία και το παράρτημα με συμπληρωματικό τεχνικό υλικό.

2 Θεωρητικό υπόβαθρο SDN και Network Slicing

2.1 Παραδοσιακές αρχιτεκτονικές δικτύων και περιορισμοί στη διαχείριση πόρων

Οι παραδοσιακές αρχιτεκτονικές δικτύων στηρίζονται σε συσκευές όπως δρομολογητές και μεταγωγείς, οι οποίες παίρνουν μόνες τους αποφάσεις για το πώς θα προωθήσουν την κίνηση, με βάση τους τοπικούς πίνακες τους και τις ρυθμίσεις που έχει ορίσει ο διαχειριστής. Κάθε συσκευή έχει μέσα της και το μέρος που παίρνει τις αποφάσεις και το μέρος που στέλνει τα πακέτα, οπότε η συνολική εικόνα του δικτύου είναι το άθροισμα πολλών ανεξάρτητων κινήσεων. Σε μικρά δίκτυα αυτό μπορεί να δουλεύει ικανοποιητικά, όμως όταν ο αριθμός των συσκευών και των υπηρεσιών μεγαλώνει, η συμπεριφορά του δικτύου γίνεται δύσκολο να κατανοηθεί και η διαχείριση κουραστική και επιρρεπής σε λάθη [19] .

Στις κλασικές υλοποιήσεις, η διαχείριση των πόρων βασίζεται κυρίως σε στατικές ρυθμίσεις. Ο διαχειριστής ορίζει χειροκίνητα πίνακες δρομολόγησης, κανόνες για την προτεραιότητα της κίνησης και διάφορα φίλτρα, συνήθως με βάση την εμπειρία του και κάποιες γενικές προβλέψεις για το αναμενόμενο φορτίο. Για λόγους ασφάλειας ο διαχειριστής επιλέγει να υπολογίζει το δίκτυο με βάση τις πιο δύσκολες συνθήκες λειτουργίας, λαμβάνοντας υπόψη το μεγαλύτερο δυνατό φορτίο, κάτι που έχει ως αποτέλεσμα τις περισσότερες ώρες της ημέρας να μένουν πόροι που δεν αξιοποιούνται. Από την άλλη πλευρά, σε περιόδους έντονης κίνησης δεν υπάρχουν πάντα εργαλεία για γρήγορη ανακατανομή της κίνησης, με αποτέλεσμα συμφόρηση, αυξημένη καθυστέρηση και απώλειες πακέτων, ιδίως αν η κίνηση προέρχεται από πολλές και διαφορετικές εφαρμογές [19].

Ένα σοβαρό μειονέκτημα είναι ότι σχεδόν κάθε αλλαγή απαιτεί χειροκίνητη παρέμβαση σε πολλές συσκευές. Αν πρέπει να προστεθεί μια νέα υπηρεσία, να αλλάξει η τοπολογία, να γίνει αναβάθμιση σε μια σύνδεση ή να εφαρμοστεί μια νέα πολιτική πρόσβασης, ο διαχειριστής καλείται να συνδεθεί σε πολλές κονσόλες, να πληκτρολογήσει εντολές και να φροντίσει να μην ξεχάσει κανένα ενδιάμεσο βήμα. Αυτό παίρνει χρόνο, αυξάνει το λειτουργικό κόστος και δημιουργεί μεγάλη εξάρτηση από λίγα άτομα που γνωρίζουν τις λεπτομέρειες του κάθε κατασκευαστή. Αν προστεθούν και οι ιδιαιτερότητες κάθε πλατφόρμας, η εικόνα γίνεται ακόμη πιο σύνθετη και η πιθανότητα ανθρώπινου λάθους μεγαλώνει [19] .

Παράλληλα, η παρακολούθηση της κατάστασης του δικτύου γίνεται αποσπασματικά. Κάθε συσκευή κρατά τα δικά της στατιστικά, πολλές φορές με διαφορετικό τρόπο παρουσίασης, και δεν υπάρχει μια ενιαία, καθαρή εικόνα για το πού ακριβώς υπάρχει φόρτος, ποιο σημείο είναι κοντά σε κορεσμό ή ποιο τμήμα του δικτύου παραμένει σχεδόν άδειο. Αυτό δυσκολεύει την εφαρμογή πιο έξυπνων πρακτικών, όπως η ανακατεύθυνση της κίνησης από φορτωμένες διαδρομές σε πιο άδειες ή η έγκαιρη αναγνώριση ενός σημείου που προκαλεί καθυστερήσεις πριν εμφανιστεί ως πραγματικό πρόβλημα για τους χρήστες. Σε πολλές περιπτώσεις, η εικόνα του δικτύου βασίζεται σε

συγκεντρωτικές αναφορές που παράγονται με καθυστέρηση και δεν αποτυπώνουν τη στιγμή που ενδιαφέρει [20].

Η κατάσταση είναι ακόμη πιο απαιτητική όταν στο ίδιο δίκτυο συνυπάρχουν υπηρεσίες με πολύ διαφορετικές ανάγκες. Ροές ήχου και βίντεο θέλουν σταθερή και μικρή καθυστέρηση, εφαρμογές μεταφοράς αρχείων αντέχουν μεγαλύτερες διακυμάνσεις, ενώ εφαρμογές ελέγχου ή βιομηχανικές εφαρμογές μπορεί να έχουν αυστηρούς περιορισμούς αξιοπιστίας. Τα παραδοσιακά δίκτυα, που συχνά λειτουργούν με λογική καλύτερης δυνατής προσπάθειας και με περιορισμένα μέσα για λεπτή ρύθμιση της προτεραιότητας, δυσκολεύονται να εξασφαλίσουν εγγυήσεις ποιότητας για κάθε κατηγορία κίνησης. Ο διαχειριστής προσπαθεί να συνδυάσει απλά εργαλεία, όπως βασικούς μηχανισμούς ποιότητας υπηρεσίας και χωρισμό σε εικονικά τοπικά δίκτυα, όμως αυτά αρκούν μόνο μέχρι ένα σημείο και δεν προσφέρουν την ευελιξία που χρειάζεται ένα σύγχρονο περιβάλλον [20].

Σημαντικό ζήτημα είναι και η ένταξη νέων τεχνικών, όπως η αυτοματοποίηση με σενάρια και η χρήση αλγορίθμων ανάλυσης δεδομένων για καλύτερη αξιοποίηση των πόρων. Στα κλασικά δίκτυα, η πληροφορία για την τοπολογία, την κίνηση και την κατάσταση κάθε συσκευής είναι διασκορπισμένη και συχνά δύσκολα προσβάσιμη από ένα κεντρικό εργαλείο. Αυτό δυσκολεύει την ανάπτυξη εφαρμογών που θα μπορούσαν να συλλέγουν σε πραγματικό χρόνο μετρήσεις, να εντοπίζουν πρότυπα συμπεριφοράς και να προτείνουν εγκαίρως διορθωτικές κινήσεις. Έτσι, πολλές δυνατότητες που προσφέρουν σήμερα η ανάλυση μεγάλου όγκου δεδομένων και η τεχνητή νοημοσύνη μένουν ανεκμετάλλευτες, όχι γιατί λείπουν οι ίδιοι οι αλγόριθμοι, αλλά γιατί λείπει η εύκολη πρόσβαση στα κατάλληλα δεδομένα [19].

Τα παραδοσιακά δίκτυα δυσκολεύονται να εξυπηρετήσουν πολλούς διαφορετικούς τύπους χρηστών πάνω στην ίδια υποδομή, με τρόπο πραγματικά ευέλικτο. Η κλασική λύση είναι ο λογικός χωρισμός με εικονικά τοπικά δίκτυα και κανόνες πρόσβασης, όμως αυτό δεν επαρκεί όταν χρειάζεται να δημιουργηθούν γρήγορα νέα «κομμάτια» δικτύου με διαφορετικές απαιτήσεις σε πόρους, σε ποιότητα υπηρεσίας και σε όρια ασφάλειας. Η τροποποίηση τέτοιων δομών απαιτεί πάλι χειροκίνητες παρεμβάσεις σε πολλές συσκευές και δεν μπορεί να γίνει με την ταχύτητα που απαιτούν σύγχρονες υπηρεσίες, όπως εφαρμογές νέων γενιών κινητών δικτύων ή υπηρεσίες σε υποδομές νέφους και άκρου δικτύου [21]. Οι αδυναμίες αυτές εξηγούν γιατί εμφανίστηκαν νέες προσεγγίσεις που μεταφέρουν τον έλεγχο πιο κεντρικά και δίνουν τη δυνατότητα πιο εύκολης προσαρμογής του δικτύου στις ανάγκες των εφαρμογών, οι οποίες αναλύονται σε επόμενα κεφάλαια.

2.2 Αρχές Software-Defined Networking: διαχωρισμός control/data plane και βασικά πρωτόκολλα

Τα παραδοσιακά IP (Internet Protocol) δίκτυα έχουν εξελιχθεί σε βαθμό που η πολυπλοκότητά τους πλέον λειτουργεί ως τροχοπέδη. Ο λόγος είναι ότι η λογική ελέγχου και η λογική προώθησης είναι στενά δεμένες σε κάθε συσκευή: ο κάθε δρομολογητής και κάθε μεταγωγέα πρέπει να διαμορφωθεί ανεξάρτητα, χρησιμοποιώντας συχνά διαφορετικό τρόπο πρόσβασης, δικές του εντολές και ιδιόκτητες διεπαφές. Αυτό όχι μόνο αυξάνει τον χρόνο και την προσπάθεια που απαιτείται για διαχείριση, αλλά δυσκολεύει και οποιαδήποτε απόπειρα αυτοματοποίησης ή μεγάλης κλίμακας ενοποίησης. Επιπλέον, η ανάγκη εξειδικευμένης γνώσης για κάθε μοντέλο συσκευής και

η έλλειψη διαφάνειας λόγω κλειστών αρχιτεκτονικών περιορίζει την ευελιξία. Το αποτέλεσμα είναι ένα δίκτυο που δεν μπορεί να προσαρμοστεί εύκολα σε νέες απαιτήσεις, ενώ η εισαγωγή καινοτομιών απαιτεί υπερβολική προσπάθεια [9].

Μέσα από αυτή την πραγματικότητα αναδύθηκε η ανάγκη για μια πιο δυναμική και προγραμματιζόμενη προσέγγιση – και κάπως έτσι γεννήθηκε η δικτύωση οριζόμενη από λογισμικό (SDN). Η βασική ιδέα πίσω από το SDN είναι ο σαφής διαχωρισμός ανάμεσα στο επίπεδο ελέγχου (control plane) και το επίπεδο προώθησης (data plane). Με απλά λόγια, η «νοημοσύνη» του δικτύου μεταφέρεται από τις μεμονωμένες συσκευές σε έναν κεντρικό ελεγκτή, ενώ οι συσκευές προώθησης περιορίζονται να εκτελούν πιστά τους κανόνες που τους δίνει ο ελεγκτής. Αυτός ο διαχωρισμός επιτρέπει κεντρικό έλεγχο, πλήρη ορατότητα της τοπολογίας και συνεπή εφαρμογή πολιτικών [9],[58].

Ο ελεγκτής SDN είναι το βασικό κέντρο λήψης αποφάσεων. Μέσω τυποποιημένων διεπαφών επικοινωνεί με τους μεταγωγείς και εγκαθιστά κανόνες ροής, διαχειρίζεται πολιτικές, ορίζει διαδρομές και προσαρμόζει τη συμπεριφορά του δικτύου ανάλογα με τις ανάγκες. Ο παράγοντας που κάνει αυτό το μοντέλο τόσο δυνατό είναι ότι η λογική ελέγχου μπορεί πλέον να προγραμματιστεί και να αυτοματοποιηθεί. Αντί να απαιτείται χειροκίνητη αλλαγή σε κάθε συσκευή, οι ενημερώσεις γίνονται κεντρικά και εφαρμόζονται άμεσα σε όλο το δίκτυο. Αυτό βελτιώνει την αποδοτικότητα και μειώνει τα λάθη που προκύπτουν από ανθρώπινη παρέμβαση. Ταυτόχρονα, επιτρέπει την προσαρμογή του δικτύου σε πραγματικό χρόνο, ανάλογα με την κίνηση, τις απειλές ή τις απαιτήσεις των εφαρμογών [9],[58].

Στο επίπεδο προώθησης βρίσκονται οι συσκευές προώθησης – μεταγωγείς και δρομολογητές – οι οποίοι εκτελούν μόνο τις ενέργειες που τους έχουν δοθεί. Ο τρόπος λειτουργίας αυτών των συσκευών στο SDN βασίζεται στους πίνακες ροής. Κάθε πακέτο που φτάνει στον μεταγωγέα ελέγχεται απέναντι στους κανόνες ροής. Αν υπάρχει αντιστοιχία, εκτελείται η ενέργεια (π.χ. προώθηση, τροποποίηση κεφαλίδας, απόρριψη). Αν δεν υπάρχει, γίνεται packet-in προς τον ελεγκτή, ο οποίος αποφασίζει πώς πρέπει να αντιμετωπιστεί η ροή και δημιουργεί ένα νέο κανόνα ώστε τα επόμενα πακέτα να μη χρειαστούν ξανά αποστολή στον ελεγκτή. Αυτό το μοντέλο μειώνει δραστικά την πολυπλοκότητα στα άκρα του δικτύου και κάνει το δίκτυο συνολικά πιο ευέλικτο [8],[9].

Το επίπεδο ελέγχου, δηλαδή ο ελεγκτής ή οι ελεγκτές, έχει πλήρη εικόνα της τοπολογίας και των καταστάσεων του δικτύου. Μπορεί να επιβάλλει πολιτικές, να κατανέμει εύρος ζώνης, να εφαρμόζει κανόνες ασφαλείας και να επιλέγει αποτελεσματικές διαδρομές. Τα συστήματα που διαθέτει – όπως μηχανισμοί ανακάλυψης τοπολογίας, υπολογισμού διαδρομών και μηχανισμοί ροής – προσφέρουν ολοκληρωμένη διαχείριση. Σε αντίθεση με τα κλασικά διανεμημένα πρωτόκολλα δρομολόγησης, ο ελεγκτής έχει πλήρη και συγκεντρωτική εικόνα του δικτύου, κάτι που τον καθιστά πιο ικανό να λαμβάνει αποφάσεις που μεγιστοποιούν την απόδοση [9].

Στο επίπεδο εφαρμογών βρίσκονται υπηρεσίες όπως τείχη προστασίας (firewalls), IDS (Intrusion Detection System), εξισορροπητές φορτίου (load balancers) και εργαλεία διαχείρισης δικτυακής κίνησης (traffic engineering). Αυτές οι εφαρμογές αξιοποιούν northbound διεπαφές[4]

[4] Διεπαφές μέσω των οποίων οι *εφαρμογές* επικοινωνούν προς τα πάνω με τον SDN controller, ζητώντας του να εκτελέσει συγκεκριμένες λειτουργίες στο δίκτυο. Ονομάζονται “northbound” επειδή, στα αρχιτεκτονικά

(συνήθως REST- Representational State Transfer- APIs[5]), οι οποίες ζητούν από τον ελεγκτή συγκεκριμένη συμπεριφορά. Οι προγραμματιστές μπορούν να ορίζουν υψηλού επιπέδου πολιτικές χωρίς να χρειάζεται να γράψουν χαμηλού επιπέδου κανόνες για κάθε συσκευή. Αυτό επιτρέπει ταχύτερη ανάπτυξη νέων υπηρεσιών και πιο αποτελεσματική χρήση των πόρων του δικτύου, καταργώντας την ακαμψία των παραδοσιακών αρχιτεκτονικών [9],[58].

Για την επικοινωνία μεταξύ του επιπέδου ελέγχου και του επιπέδου προώθησης χρησιμοποιείται κυρίως το πρωτόκολλο OpenFlow. Πρόκειται για το πιο διαδεδομένο southbound πρωτόκολλο, το οποίο ορίζει πώς ένας ελεγκτής και ένας μεταγωγέας (switch) ανταλλάσσουν μηνύματα, στατιστικά και κανόνες ροής. Το OpenFlow τυποποιεί τη δομή των πινάκων ροών (flow tables), τους τύπους μηνυμάτων, τους μετρητές και το τρόπο επιβολής κανόνων. Έτσι, διασφαλίζει ότι συσκευές διαφορετικών κατασκευαστών μπορούν να συνεργαστούν με κοινό τρόπο, χωρίς να απαιτούνται ιδιόκτητα interfaces. Είναι επίσης ιδανικό για πειραματισμό, καθώς επιτρέπει λεπτομερή χειρισμό των κεφαλίδων πακέτων και υποστηρίζει ευρύ φάσμα από στοιχεία αντιστοίχισης [8],[9].

Πέρα από το OpenFlow υπάρχουν και άλλες διεπαφές προς το επίπεδο προώθησης (southbound[6] interfaces), όπως NETCONF (Network Configuration Protocol) ή ιδιόκτητα API κατασκευαστών. Όμως το OpenFlow παραμένει θεμέλιο του SDN, επειδή προσφέρει ενιαίο abstraction για τη συμπεριφορά προώθησης και επιτρέπει ευρεία προσαρμογή. Γι' αυτό και προβλέπεται να συνεχίσει να χρησιμοποιείται τόσο σε ερευνητικά όσο και σε παραγωγικά περιβάλλοντα [8]. Σε μεγάλες ή γεωγραφικά κατανεμημένες υποδομές συχνά χρησιμοποιούνται πολλαπλοί ελεγκτές. Μεταξύ τους ανταλλάσσουν πληροφορίες σχετικά με την τοπολογία, την κατάσταση των ροών και αλλαγές που συμβαίνουν στο δίκτυο. Αυτό επιτρέπει επεκτασιμότητα και υψηλή διαθεσιμότητα, καθώς η ευθύνη δεν συγκεντρώνεται σε έναν μόνο κόμβο [9].

Οι διεπαφές μεταξύ ελεγκτών (east-west[7]) διασφαλίζουν ότι οι ελεγκτές λειτουργούν ως ενιαίο σύστημα, μειώνοντας σημεία συμφόρησης και αποτρέποντας μεμονωμένα σημεία αστοχίας [9].

Παρά τα πλεονεκτήματα, το SDN δεν είναι απαλλαγμένο από προκλήσεις. Μία από τις κυριότερες είναι η τοποθέτηση των ελεγκτών στο δίκτυο. Η απόσταση ανάμεσα σε έναν ελεγκτή και τους μεταγωγείς του επηρεάζει άμεσα την καθυστέρηση και συνεπώς την απόδοση του συστήματος. Αν ο ελεγκτής βρίσκεται πολύ μακριά, οι καθυστερήσεις σε packet-in events μπορεί να επηρεάσουν κρίσιμες υπηρεσίες. Γι' αυτό η βέλτιστη τοποθέτηση ελεγκτών αποτελεί ενεργό πεδίο έρευνας, χρησιμοποιώντας μαθηματικά μοντέλα και διάφορους αλγόριθμους (π.χ. της θεωρίας γραφών, clustering, greedy, θεωρία παιγνίων [9].

Άλλο κρίσιμο θέμα είναι η επεκτασιμότητα. Πιο συγκεκριμένα, όταν το δίκτυο μεγαλώνει και αυξάνεται ο αριθμός ροών, ένας μόνο ελεγκτής μπορεί να δυσκολευτεί να εξυπηρετήσει όλα τα

διαγράμματα των SDN, οι εφαρμογές τοποθετούνται πάνω από τον controller, άρα η επικοινωνία πάει προς τα πάνω.

[5] Διεπαφές προγραμματισμού εφαρμογών που βασίζονται στην αρχιτεκτονική REST (Representational State Transfer) και επιτρέπουν σε διαφορετικά συστήματα να επικοινωνούν μέσω του πρωτοκόλλου HTTP.

[6] Διεπαφές μέσω των οποίων ο SDN controller επικοινωνεί προς τα κάτω με τις συσκευές δικτύου, δηλαδή με switches, routers ή virtual network functions.

[7] Πρωτόκολλα και APIs που επιτρέπουν σε controllers να μιλούν μεταξύ τους, να ανταλλάσσουν πληροφορίες και να λειτουργούν συντονισμένα σε ένα κατανεμημένο SDN.

αιτήματα εγκαίρως. Η λύση είναι κατανεμημένοι ελεγκτές, αλλά αυτό δημιουργεί άλλου τύπου πολυπλοκότητα: την ανάγκη για συνεπή κατάσταση δικτύου μεταξύ τους [9].

Η ασφάλεια αποτελεί επίσης κρίσιμο ζήτημα. Ο ελεγκτής είναι στρατηγικό σημείο: αν παραβιαστεί, μπορεί να επηρεαστεί ολόκληρο το δίκτυο. Γι' αυτό απαιτούνται μηχανισμοί αυθεντικοποίησης, ισχυρή κρυπτογράφηση, προστασία του καναλιού ελέγχου και μηχανισμοί πλεονασμού ώστε το δίκτυο να παραμένει λειτουργικό ακόμη και σε περίπτωση αστοχίας ενός ελεγκτή παρά τις δυσκολίες, το SDN συνεχίζει να κερδίζει έδαφος [9] .Ο λόγος είναι ξεκάθαρος: προσφέρει ευελιξία, κεντρικό έλεγχο, αυτοματοποίηση, γρήγορη προσαρμογή σε αλλαγές και δυνατότητα εισαγωγής νέων υπηρεσιών χωρίς αναβαθμίσεις υλικού. Στο σύγχρονο περιβάλλον νέφους (cloud), εικονικοποίησης (virtualization) και δυναμικής διαχείρισης πόρων, το SDN αποτελεί ιδανική βάση για υλοποίηση σύγχρονων δικτυακών υποδομών.

2.3 Έννοια και αρχιτεκτονική του Network Slicing σε δίκτυα 5G, Cloud και IoT

Τα παραδοσιακά μοντέλα δικτύωσης δεν είναι σε θέση να αντιμετωπίσουν αποτελεσματικά την σημαντική αύξηση της αρχιτεκτονικής πολυπλοκότητας και της διαφοροποίησης των απαιτήσεων των υπηρεσιών που προκαλεί η συνεχής ανάπτυξη των σύγχρονων τηλεπικοινωνιακών δικτύων. Ένα μοντέλο υπηρεσιών βέλτιστης προσπάθειας, στο οποίο όλη η κίνηση χρησιμοποιεί τους ίδιους υποκείμενους πόρους με μικρές διαφορές, χρησιμοποιείται συνήθως στο σχεδιασμό των παλαιών δικτυακών συστημάτων. Αυτές οι μέθοδοι δεν είναι πλέον κατάλληλες σε περιβάλλοντα όπου οι εφαρμογές απαιτούν δραστικά διαφορετικές ανάγκες όσον αφορά το εύρος ζώνης, την καθυστέρηση, την αξιοπιστία και την πυκνότητα των συσκευών, παρόλο που μπορεί να είναι επαρκείς για συγκριτικά ομοιογενείς υπηρεσίες. Αυτά τα ζητήματα έχουν γίνει πιο επείγοντα με την έλευση των δικτύων πέμπτης γενιάς (5G), των υποδομών υπολογιστικού νέφους και των μαζικών εφαρμογών του Διαδικτύου των Πραγμάτων (IoT - Internet of Things), καθιστώντας αναγκαία την ανάπτυξη πιο προσαρμόσιμων και προσανατολισμένων στις υπηρεσίες αρχιτεκτονικών δικτύων [10],[11].

Από αυτή την άποψη, η διαμέριση δικτύου έχει παρουσιαστεί ως μια κρίσιμη τεχνολογία που επιτρέπει τη συνύπαρξη πολλών λογικών δικτύων σε μια κοινή φυσική υποδομή. Η τεχνολογία η οποία έχει ως δυνατότητα την διαίρεση ενός φυσικού δικτύου σε πολλαπλά απομονωμένα, end-to-end λογικά δίκτυα —που συχνά αναφέρονται ως «διαμέριση (slice)»— καθένα από τα οποία είναι προσαρμοσμένο ώστε να ικανοποιεί συγκεκριμένες ανάγκες υπηρεσιών, είναι γνωστή ως διαμέριση δικτύου. [10] Παρόλο που μοιράζονται την ίδια υποκείμενη υποδομή, κάθε διαμέριση λειτουργεί ως ξεχωριστή εικονική δικτυακή παρουσία με τα δικά της χαρακτηριστικά απόδοσης, πολιτικές και διαδικασίες διαχείρισης. Η διαμέριση δικτύου, προσφέρει βαθύτερα επίπεδα προσαρμογής και διαχωρισμού σε όλο το δίκτυο ραδιοπρόσβασης (RAN - Radio Access Network)[8], το δίκτυο

[8] Το RAN αποτελεί ουσιαστικά το ασύρματο τμήμα του τηλεπικοινωνιακού δικτύου που συνδέει τις τελικές συσκευές με το υπόλοιπο σύστημα. Περιλαμβάνει τους σταθμούς βάσης, όπως τους eNodeB στο 4G και τους gNodeB στο 5G, καθώς και τον απαραίτητο εξοπλισμό κεραιών και ραδιοσυχνοτήτων. Το δίκτυο ραδιοπρόσβασης λειτουργεί ως το πρώτο σημείο πρόσβασης μιας συσκευής στο δίκτυο και καθορίζει τον

μεταφοράς και το κεντρικό δίκτυο, σε αντίθεση με τις συμβατικές μεθόδους όπως τα εικονικά τοπικά δίκτυα (VLAN)[9] ή οι βασικές διαδικασίες ποιότητας υπηρεσιών (QoS)[10]. Αυτό εξαλείφει την ανάγκη δημιουργίας ξεχωριστών φυσικών δικτύων για κάθε περίπτωση χρήσης, επιτρέποντας στους φορείς εκμετάλλευσης να παρέχουν διαφοροποιημένες υπηρεσίες με εγγυημένα χαρακτηριστικά απόδοσης [10],[11].

Η ποικιλομορφία των σύγχρονων δικτυακών υπηρεσιών αποτελεί σημαντική κινητήρια δύναμη για την υιοθέτηση της διαμέρισης δικτυου. Οι υπηρεσίες Enhanced Mobile Broadband (eMBB), Ultra-Reliable Low-Latency Communications (URLLC) και massive Machine-Type Communications (mMTC) συνιστούν τις τρεις βασικές κατηγορίες υπηρεσιών που υποστηρίζονται από τα δίκτυα πέμπτης γενιάς (5G). Κάθε μία από αυτές τις κατηγορίες επιβάλλει διαφορετικές, και συχνά ασυμβίβαστες, απαιτήσεις στο δίκτυο. Ενδεικτικά, οι υπηρεσίες URLLC απαιτούν εξαιρετικά χαμηλή καθυστέρηση και υψηλή αξιοπιστία, οι υπηρεσίες mMTC εστιάζουν στην επεκτασιμότητα και στη δυνατότητα διασύνδεσης μεγάλου αριθμού συσκευών χαμηλής ισχύος, ενώ οι υπηρεσίες eMBB απαιτούν υψηλούς ρυθμούς μετάδοσης δεδομένων και αποδοτική αξιοποίηση του διαθέσιμου φάσματος. Μέσω της αντιστοίχισης κάθε κατηγορίας υπηρεσιών σε μια εξειδικευμένη και βελτιστοποιημένη διαμέριση, η διαμέριση δικτύου καθιστά δυνατή την ταυτόχρονη παροχή αυτών των διαφορετικών τύπων υπηρεσιών [11].

Η εικονικοποίηση και η υλοποίηση μέσω λογισμικού αποτελούν θεμελιώδη στοιχεία της αρχιτεκτονικής της διαμέρισης δικτύου (network slicing). Η φυσική υποδομή, η οποία περιλαμβάνει τον εξοπλισμό ραδιοπρόσβασης, τις γραμμές μεταφοράς, τα βασικά στοιχεία του δικτύου και τους πόρους των κέντρων δεδομένων — όπως υπολογιστική ισχύ και αποθήκευση — συνιστά τη βάση πάνω στην οποία υλοποιούνται οι ανώτερες λειτουργίες. Χάρη στις τεχνολογίες εικονικοποίησης λειτουργιών δικτύου (NFV)[11], οι δικτυακές λειτουργίες μπορούν να υλοποιηθούν ως λογισμικά στοιχεία που εκτελούνται σε εικονικές μηχανές ή κοντέινερ, επιτρέποντας τον διαχωρισμό τους από το ιδιόκτητο υλικό [10]. Αυτή η αφαίρεση των φυσικών πόρων καθιστά εφικτή την ευέλικτη δημιουργία διαμερίσεων και τη δυναμική κατανομή των απαιτούμενων πόρων.

Κάθε διαμέριση δικτύου αποτελείται από μια συλλογή εικονικοποιημένων ή εγγενών στο νέφος υπηρεσιών δικτύου που συνδέονται για να δημιουργήσουν ένα λογικό δίκτυο από άκρο σε άκρο. Ανάλογα με τις απαιτήσεις υπηρεσιών του τμήματος, αυτές οι λειτουργίες μπορεί να περιλαμβάνουν διαχείριση κινητικότητας, επεξεργασία επιπέδου χρήστη, δρομολόγηση, μέτρα ασφαλείας και στοιχεία διαχείρισης κυκλοφορίας. Το επίπεδο απομόνωσης μεταξύ των τμημάτων μπορεί να ποικίλλει, από πλήρως αποκλειστικούς πόρους έως επιλεκτική κοινή χρήση ορισμένων

τρόπο με τον οποίο η ασύρματη κίνηση μεταδίδεται και δρομολογείται προς τα επόμενα επίπεδα της αρχιτεκτονικής.

[9] Τα VLAN επιτρέπουν τον λογικό διαχωρισμό της κυκλοφορίας μέσα στο ίδιο φυσικό δίκτυο, προσφέροντας βασική απομόνωση, χωρίς όμως να υποστηρίζουν από μόνα τους πλήρη network slicing από άκρο σε άκρο.

[10] Το QoS αφορά μηχανισμούς προτεραιοποίησης της κυκλοφορίας, συμβάλλοντας στην κάλυψη απαιτήσεων απόδοσης των υπηρεσιών, λειτουργώντας συμπληρωματικά στο network slicing.

[11] Το Network Function Virtualization αποτελεί μια αρχιτεκτονική προσέγγιση που είναι θεμελιώδης για το network slicing, καθώς επιτρέπει, μεταξύ άλλων, την υλοποίηση δικτυακών λειτουργιών ως εικονικοποιημένες οντότητες λογισμικού που εκτελούνται πάνω σε γενικού σκοπού υπολογιστική υποδομή, διαχωρίζοντας τις λειτουργίες του δικτύου από το ιδιόκτητο φυσικό υλικό.

λειτουργιών για αύξηση της αποδοτικότητας. Η επιδιωκόμενη ισορροπία μεταξύ απομόνωσης, απόδοσης και αξιοποίησης πόρων καθορίζει την απόφαση σχεδιασμού [10],[12],[23],[53].

Το πλαίσιο διαχείρισης και συντονισμού, το οποίο είναι υπεύθυνο για ολόκληρο τον κύκλο ζωής της διαμέρισης, αποτελεί βασικό συστατικό της αρχιτεκτονικής της διαμέρισης δικτύου. Σε αυτό περιλαμβάνονται η δημιουργία, η τροποποίηση, η κλιμάκωση, η παρακολούθηση και ο τερματισμός της διαμέρισης. Οι συμφωνίες επιπέδου υπηρεσιών (SLA)[12] και οι υψηλού επιπέδου ανάγκες υπηρεσιών μεταφράζονται σε συγκεκριμένες διαμορφώσεις δικτύου από οργανισμούς διαχείρισης και συντονισμού, οι οποίοι παρακολουθούν επίσης τακτικά την απόδοση της διαμέρισης για να εγγυηθούν την τήρηση των προκαθορισμένων στόχων [10],[11] . Σε αυτό το επίπεδο, η αυτοματοποίηση είναι ζωτικής σημασίας, καθώς η ανθρώπινη διαμόρφωση θα ήταν ανέφικτη σε εξαιρετικά δυναμικά περιβάλλοντα όπου η ζήτηση κυκλοφορίας κυμαίνεται συχνά.

Ο αρχιτεκτονικός σχεδιασμός των δικτύων 5G συνδέεται στενά με την υλοποίηση της διαμέρισης δικτύου. Η αρχιτεκτονική του 5G δικτύου, η οποία είναι βασισμένη σε υπηρεσίες και εγγενής στο νέφος, διευκολύνει την υλοποίηση διαμέρισης από άκρο σε άκρο και την ευέλικτη ανάπτυξη λειτουργιών δικτύου. Επιπλέον, οι μηχανισμοί κατανομής πόρων στο δίκτυο ραδιοπρόσβασης επιτρέπουν τη διαφοροποίηση μεταξύ των διαμερίσεων βάσει προτεραιοτήτων προγραμματισμού, περιορισμών καθυστέρησης και απαιτήσεων αξιοπιστίας. Χάρη σε αυτήν την ενσωμάτωση από άκρο σε άκρο, οι διαμερίσεις μπορούν να διατηρούν σταθερά χαρακτηριστικά απόδοσης σε όλα τα τμήματα του δικτύου, από τον εξοπλισμό των χρηστών έως το κεντρικό δίκτυο και τις υπηρεσίες νέφους [10],[13].

Επειδή η διαμέριση δικτύου βασίζεται σε μεγάλο βαθμό σε εικονικοποιημένους υπολογιστικούς και αποθηκευτικούς πόρους, η υπολογιστική νέφους (cloud computing) είναι απαραίτητο για την υλοποίησή του. Ενώ οι πόροι edge computing επιτρέπουν την παροχή υπηρεσιών που είναι ευαίσθητες στην καθυστέρηση, φέρνοντας την υπολογιστική ισχύ πιο κοντά στους τελικούς χρήστες, οι κεντρικές υποδομές νέφους προσφέρουν επεκτασιμότητα και ευελιξία για την ανάπτυξη διαμέρισης. Για εφαρμογές όπως αυτόνομα συστήματα, βιομηχανικός αυτοματισμός και υπηρεσίες IoT σε πραγματικό χρόνο, όπου πρέπει να πληρούνται αυστηρά κριτήρια καθυστέρησης και αξιοπιστίας, ο συνδυασμός διαμέρισης δικτύου και edge computing είναι ιδιαίτερα κατάλληλος [10],[48].

Στο πλαίσιο των εφαρμογών IoT, η σημασία της διαμέρισης δικτύου γίνεται πιο σαφής. Τα οικοσυστήματα IoT χαρακτηρίζονται από εξαιρετική ετερογένεια, καθώς περιλαμβάνουν συσκευές με πολύ διαφορετικά πρότυπα επικοινωνίας, ενεργειακούς περιορισμούς και απαιτήσεις απόδοσης. Η κίνηση IoT μπορεί να χωριστεί σε εξειδικευμένα τμήματα που είναι προσαρμοσμένα για συγκεκριμένες κατηγορίες συσκευών ή εφαρμογές μέσω της διαμέρισης δικτύου. Ενώ ένα διαφορετικό τμήμα μπορεί να ρυθμιστεί για να χειρίζεται κρίσιμες υπηρεσίες IoT με αυστηρές εγγυήσεις αξιοπιστίας και καθυστέρησης, ένα τμήμα που έχει βελτιστοποιηθεί για mMTC, για παράδειγμα, μπορεί να υποστηρίξει εκατομμύρια αισθητήρες χαμηλού ρυθμού δεδομένων με ελάχιστο επιπλέον κόστος σηματοδότησης [13]. Σε σύγκριση με τις παραδοσιακές τοπολογίες

[12] Το Service Level Agreement αποτελεί μια τυπική συμφωνία που καθορίζει τις ποιοτικές και ποσοτικές παραμέτρους απόδοσης που οφείλει να τηρεί το δίκτυο για μια συγκεκριμένη υπηρεσία ή network slice, λειτουργώντας ως σημείο αναφοράς για τη διαχείριση πόρων και την αξιολόγηση της παρεχόμενης ποιότητας υπηρεσίας.

δικτύου, αυτή η μέθοδος αυξάνει σημαντικά την επεκτασιμότητα και την αποδοτικότητα των πόρων.

Παρά τα οφέλη του, η διαμέριση δικτύου παρουσιάζει μια σειρά από δυσκολίες που βρίσκονται υπό διερεύνηση. Η αποτελεσματική κατανομή των πόρων σε διάφορες διαμερίσεις εξακολουθεί να αποτελεί πρόκληση, ειδικά όταν υπάρχουν αυστηρές απαιτήσεις SLA και δυναμική κίνηση[13]. Απαιτούνται προηγμένα συστήματα παρακολούθησης και ελέγχου για να διασφαλιστεί η ισχυρή απομόνωση μεταξύ των διαμερίσεων κατά την κοινή χρήση των υποκείμενων πόρων. Ένα άλλο σημαντικό ζήτημα είναι η ασφάλεια, καθώς τα ελαττώματα στα κοινόχρηστα μέρη ή στα συστήματα διαχείρισης ενδέχεται να επηρεάσουν ταυτόχρονα πολλά τμήματα. Κατά συνέπεια, η αξιόπιστη εφαρμογή του network slicing απαιτεί ισχυρά μέτρα ασφάλειας και ασφαλή πλαίσια συντονισμού [11],[12].

Συμπερασματικά, η διαμέριση δικτύου σηματοδοτεί μια σημαντική αρχιτεκτονική αλλαγή στον τρόπο σχεδιασμού των σύγχρονων δικτύων επικοινωνιών. Ανταποκρίνεται στην αυξανόμενη ποικιλία αναγκών που δημιουργούνται από τις εφαρμογές 5G, της υπολογιστικής νέφους και του Διαδικτύου των Πραγμάτων, διευκολύνοντας την κατασκευή προσαρμόσιμων, απομονωμένων και ειδικών για κάθε υπηρεσία λογικών δικτύων πάνω σε μια κοινόχρηστη υποδομή. Η διαμέριση δικτύου, το οποίο υποστηρίζεται από NFV, τεχνολογίες cloud-native και εξελιγμένα πλαίσια ενορχήστρωσης, επιτρέπει στους χειριστές να παρέχουν εξατομικευμένες υπηρεσίες με αξιόπιστη απόδοση και οικονομική χρήση των πόρων [10],[11]. Παρόλο που εξακολουθούν να υπάρχουν πολλά τεχνικά εμπόδια που πρέπει να ξεπεραστούν, οι τρέχουσες πρωτοβουλίες έρευνας και τυποποίησης υποδηλώνουν ότι η διαμέριση δικτύου θα παραμείνει ένα κρίσιμο μέρος των αρχιτεκτονικών δικτύων πέρα από το 5G.

2.4 Μηχανισμοί QoS, ασφάλειας και απομόνωσης μεταξύ slices

Ένα βασικό αρχιτεκτονικό χαρακτηριστικό των σύγχρονων δικτύων 5G και μεταγενέστερων δικτύων κινητών επικοινωνιών είναι η διαμέριση δικτύου (network slicing), η οποία επιτρέπει σε πολλά λογικά δίκτυα, το καθένα από τα οποία είναι προσαρμοσμένο σε διαφορετικές ανάγκες υπηρεσιών, να συνυπάρχουν σε μια κοινή φυσική υποδομή. Αν και η ιδέα της διαμέρισης προσφέρει ευελιξία και βέλτιστη χρήση των πόρων, η πρακτική της εφαρμογή εξαρτάται σε μεγάλο βαθμό από το πόσο καλά εφαρμόζονται οι μέθοδοι ασφάλειας, απομόνωσης και ποιότητας υπηρεσιών (QoS) μεταξύ των διαμερίσεων. Αυτοί οι μηχανισμοί εγγυώνται ότι οι διαμερίσεις με διαφορετικά επίπεδα εμπιστοσύνης και απαιτήσεις απόδοσης μπορούν να λειτουργούν ταυτόχρονα χωρίς να παρεμβαίνουν το ένα στο άλλο, προκαλώντας υποβάθμιση της υπηρεσίας ή θέτοντας σε κίνδυνο την ασφάλεια. Οι αυστηρές εγγυήσεις QoS[14] και η αυστηρή απομόνωση γίνονται ουσιαστικοί στόχοι σχεδιασμού και όχι προαιρετικές προσθήκες, καθώς οι διαμερίσεις μπορούν να επιτρέψουν

[13] Με τον όρο δυναμική κίνηση αναφέρεται η μεταβαλλόμενη κυκλοφορία δεδομένων στο δίκτυο, η οποία μεταβάλλεται με τον χρόνο και καθιστά απαραίτητη τη συνεχή προσαρμογή της κατανομής των διαθέσιμων πόρων, ώστε να διασφαλίζεται η τήρηση των συμφωνημένων επιπέδων υπηρεσίας.

[14] Οι αυστηρές εγγυήσεις QoS αναφέρονται σε μηχανισμούς του δικτύου που εξασφαλίζουν συγκεκριμένα και προκαθορισμένα επίπεδα ποιότητας υπηρεσίας, όπως καθυστέρηση, jitter, απώλειες πακέτων και διαθέσιμο εύρος ζώνης, τα οποία τηρούνται σταθερά ακόμη και σε συνθήκες αυξημένης κυκλοφορίας.

τα πάντα, από εφαρμογές ευρυζωνικής σύνδεσης με βέλτιστη προσπάθεια έως εξαιρετικά αξιόπιστες επικοινωνίες χαμηλής καθυστέρησης [15],[22],[23].

Ο στόχος των μηχανισμών QoS[15] στη διαμέριση δικτύων είναι να μετατρέψουν τις ανάγκες υψηλού επιπέδου υπηρεσιών σε συγκεκριμένες συμπεριφορές σε επίπεδο δικτύου. Αυτές οι απαιτήσεις συνήθως κοινοποιούνται μέσω Συμφωνιών Επιπέδου Υπηρεσιών (SLA). Τα συστήματα QoS με αναγνώριση διαμερίσεων πρέπει να λειτουργούν από άκρο σε άκρο και να διατηρούν τη συνέπεια σε όλο το δίκτυο ραδιοπρόσβασης, το δίκτυο μεταφοράς και το κεντρικό δίκτυο, σε αντίθεση με τις συμβατικές προσεγγίσεις QoS[16] που λειτουργούν σε κατηγορίες ή ροές κυκλοφορίας. Συγκεκριμένοι δείκτες απόδοσης, όπως όρια απώλειας πακέτων, περιορισμοί διακύμανσης, ελάχιστο εγγυημένο εύρος ζώνης και όρια καθυστέρησης, συνδέονται με κάθε τμήμα. Για την επιβολή αυτών των δεικτών χρησιμοποιούνται συντονισμένες τεχνικές κατανομής πόρων, προγραμματισμού κυκλοφορίας και ιεράρχησης προτεραιοτήτων που λειτουργούν σε διάφορα επίπεδα της δικτυακής στοίβας. Οι προγραμματιστές με αναγνώριση διαμερίσεων στο δίκτυο ραδιοπρόσβασης κατανέμουν το φάσμα και τις ευκαιρίες μετάδοσης σύμφωνα με τις προτεραιότητες των διαμερίσεων και τους περιορισμούς καθυστέρησης, προστατεύοντας τις διαμερίσεις που είναι ευαίσθητες στην καθυστέρηση, όπως το URLLC[17], από την συμφόρηση που προκαλείται από την κυκλοφορία eMBB υψηλής απόδοσης [22]. Στα τμήματα μεταφοράς και πυρήνα, εφαρμόζονται μέθοδοι όπως η κράτηση εύρους ζώνης, η διαφορική ουρά αναμονής και η διαμόρφωση της κυκλοφορίας για τη διατήρηση των χαρακτηριστικών απόδοσης που είναι συγκεκριμένα για κάθε διαμέριση.

Η προσαρμοστική διαχείριση QoS είναι απαραίτητη λόγω της δυναμικής φύσης της σύγχρονης δικτυακής κίνησης. Όταν τα πρότυπα κίνησης αλλάζουν γρήγορα, η στατική κατανομή πόρων σε διαμερίσεις μπορεί να οδηγήσει σε σπατάλη ή παραβιάσεις SLA [53]. Τα πλαίσια διαχείρισης διαμερίσεων χρησιμοποιούν βρόχους παρακολούθησης και ανατροφοδότησης για να αντιμετωπίσουν αυτό το πρόβλημα, επιτρέποντας τις μετρήσεις απόδοσης σε πραγματικό χρόνο να επηρεάζουν τις επιλογές ανακατανομής πόρων. Σε αυτή την περίπτωση, ο κεντρικός έλεγχος που καθίσταται δυνατός χάρη στο SDN (Software-Defined Networking) είναι απαραίτητος, καθώς προσφέρει μια ολοκληρωμένη εικόνα της κατάστασης του δικτύου και επιτρέπει τον ακριβή έλεγχο της συμπεριφοράς προώθησης ανά τμήμα. Οι ελεγκτές SDN διατηρούν τις εγγυήσεις QoS σε όλες τις διαμερίσεις χρησιμοποιώντας προγραμματιζόμενες διεπαφές για να τροποποιούν δυναμικά τα χαρακτηριστικά της ουράς, να επιβάλλουν πολιτικές κυκλοφορίας και να αλλάζουν τις διαδρομές δρομολόγησης σε αντίδραση σε παρατηρήσιμες αποκλίσεις απόδοσης [1],[22],[31].

Στα συστήματα δικτύου με διαμέριση δικτύου, οι διαδικασίες ασφαλείας είναι εξίσου σημαντικές, καθώς η υποκείμενη υποδομή μοιράζεται από διάφορους χρήστες ή υπηρεσίες με διαφορετικές απαιτήσεις εμπιστοσύνης. Η εφαρμογή του διαχωρισμού του δικτύου σε διαμερίσεις

[15] Ως μηχανισμοί QoS ορίζονται οι τεχνικές που εφαρμόζονται σε ένα δίκτυο για την ταξινόμηση, καθορισμό προτεραιοτήτων και διαχείριση της κυκλοφορίας, με στόχο τη βελτίωση της απόδοσης και την εξασφάλιση αποδεκτής ποιότητας υπηρεσίας για διαφορετικούς τύπους δεδομένων.

[16] Συμβατικές προσεγγίσεις QoS είναι οι παραδοσιακές μέθοδοι διαχείρισης της κυκλοφορίας στα δίκτυα, οι οποίες βασίζονται σε μηχανισμούς όπως η ταξινόμηση πακέτων, η ιεράρχηση της κίνησης και ο έλεγχος της συμφόρησης, χωρίς δυναμική προσαρμογή στις μεταβαλλόμενες απαιτήσεις των υπηρεσιών.

[17] URLLC (Ultra-Reliable Low-Latency Communications) είναι κατηγορία υπηρεσιών δικτύου που στοχεύει στην παροχή εξαιρετικά χαμηλής καθυστέρησης και πολύ υψηλής αξιοπιστίας, απαραίτητων για εφαρμογές κρίσιμου χρόνου, όπως βιομηχανικός αυτοματισμός και απομακρυσμένος έλεγχος.

αυξάνει την επιφάνεια επίθεσης, καθώς οι ευπάθειες των κοινόχρηστων στοιχείων ή οι λανθασμένες διαμορφώσεις σε επίπεδο συντονισμού ενδέχεται να έχουν αλυσιδωτές επιπτώσεις σε διάφορες διαμερίσεις. Ως αποτέλεσμα, η ασφάλεια στον διαχωρισμό του δικτύου σε διαμερίσεις πρέπει να προσεγγίζεται από όλες τις οπτικές γωνίες, συμπεριλαμβανομένων των επιπέδων διαχείρισης, δεδομένων και ελέγχου. Για να διασφαλιστεί ότι μόνο εξουσιοδοτημένες οντότητες μπορούν να δημιουργούν, να επεξεργάζονται ή να έχουν πρόσβαση σε διαμορφώσεις διαμερίσεων, απαιτούνται ισχυρές διαδικασίες ελέγχου ταυτότητας, εξουσιοδότησης και λογιστικής στα επίπεδα ελέγχου και διαχείρισης. Για την προστασία των αλληλεπιδράσεων μεταξύ συστημάτων συντονισμού, ελεγκτών SDN και δραστηριοτήτων εικονικού δικτύου, είναι ζωτικής σημασίας τα ασφαλή κανάλια επικοινωνίας, τα οποία συνήθως προστατεύονται μέσω κρυπτογράφησης και αμοιβαίου ελέγχου ταυτότητας [15],[23],[25],[46].

Τα μέτρα ασφαλείας στο επίπεδο δεδομένων επικεντρώνονται στη διατήρηση της διαθεσιμότητας, της εμπιστευτικότητας και της ακεραιότητας της κυκλοφορίας εντός κάθε διαμέρισης. Εικονικά τείχη προστασίας, συστήματα ανίχνευσης εισβολών και λειτουργίες φιλτραρίσματος της κυκλοφορίας που υλοποιούνται ως μέρος της ίδιας της διαμέρισης μπορούν να χρησιμοποιηθούν για την εφαρμογή πολιτικών ασφαλείας ειδικών για κάθε διαμέριση. Αντί να παρέχει συνεπή προστασία σε όλο το δίκτυο, αυτή η μέθοδος επιτρέπει την προσαρμογή των μεθόδων ασφαλείας στο μοντέλο απειλών και στην ευαισθησία κάθε υπηρεσίας [23]. Για παράδειγμα, μια διαμέριση που έχει σχεδιαστεί για την καλύτερη δυνατή κυκλοφορία καταναλωτών μπορεί να βασίζεται σε ασθενέστερα χαρακτηριστικά ασφαλείας, αλλά μια διαμέριση που υποστηρίζει ζωτικές υποδομές ή υπηρεσίες υγειονομικής περίθαλψης μπορεί να απαιτεί αυστηρούς ελέγχους πρόσβασης και διεξοδική επιθεώρηση πακέτων. Διευκολύνοντας την έγκαιρη ανίχνευση επιβλαβών δραστηριοτήτων ή παραβιάσεων πολιτικών σε συγκεκριμένες διαμερίσεις, η συνεχής παρακολούθηση και η ανίχνευση ανωμαλιών βελτιώνουν περαιτέρω την ασφάλεια [15],[25].

Τόσο η QoS όσο και οι εγγυήσεις ασφάλειας βασίζονται σε μεθόδους απομόνωσης. Η απομόνωση απόδοσης, η απομόνωση ασφάλειας και η απομόνωση διαχείρισης είναι μόνο μερικές από τις μεθόδους με τις οποίες μπορεί να διερευνηθεί η απομόνωση στη διαμέριση δικτύου. Ακόμη και σε περιόδους υψηλού φορτίου, η απομόνωση απόδοσης εγγυάται ότι η χρήση πόρων από μια διαμέριση δεν επηρεάζει αρνητικά την απόδοση των άλλων [24]. Προκειμένου να μετριαστούν οι επιπτώσεις της υπερβολικής ζήτησης σε μια μεμονωμένη διαμέριση, χρησιμοποιούνται διαδικασίες ρητής κατανομής πόρων, ελέγχου πρόσβασης και ελέγχου της κυκλοφορίας [15]. Οι τεχνολογίες εικονικοποίησης, οι οποίες διαχωρίζουν τους πόρους υπολογισμού, αποθήκευσης και δικτύωσης, επιτρέποντας ταυτόχρονα τον ελεγχόμενο διαμοιρασμό για αύξηση της αποδοτικότητας, χρησιμοποιούνται συχνά για την υλοποίηση λογικού διαχωρισμού [23],[26].

Ο στόχος της απομόνωσης ασφαλείας είναι να σταματήσει η πλευρική κίνηση μεταξύ των διαμερίσεων και η ανεπιθύμητη πρόσβαση. Με την απομόνωση των πλαισίων εκτέλεσης και τον περιορισμό της συνδεσιμότητας μεταξύ των διαμερίσεων σε καλά καθορισμένες διεπαφές, οι τεχνολογίες εικονικοποίησης και χρήσης container[18] συμβάλλουν στην επίτευξη αυτού του στόχου.

[18] Με τον περιορισμό της συνδεσιμότητας των επιμέρους τμημάτων σε σαφώς καθορισμένες διεπαφές (π.χ. APIs), επιδιώκεται η χαλαρή σύζευξη και η αυξημένη αρθρωτότητα του συστήματος. Σε αυτό το πλαίσιο, οι τεχνολογίες εικονικοποίησης και χρήσης containers ενισχύουν την απομόνωση των εξαρτήσεων και του

Ωστόσο, κοινά στοιχεία όπως οι πλατφόρμες ενορχήστρωσης[19], οι ελεγκτές SDN[20] και οι υπερ-εποπτικές μηχανές[21] εξακολουθούν να αποτελούν πιθανά αδύνατα σημεία. Επομένως, προκειμένου να αποφευχθεί η παραβίαση που θα μπορούσε να θέσει σε κίνδυνο τις εγγυήσεις απομόνωσης των διαμερίσεων, αυτά τα στοιχεία πρέπει να ενισχυθούν και να παρακολουθούνται συνεχώς [23]. Σε περιβάλλοντα πολλαπλών χρηστών, όπου οι διαμερίσεις μπορεί να διαχειρίζονται διάφορους διοικητικούς τομείς, η απομόνωση της διαχείρισης εγγυάται περαιτέρω ότι οι δραστηριότητες ελέγχου που πραγματοποιούνται σε μια διαμέριση δεν επηρεάζουν τα άλλα. Για να επιτευχθεί αυτό, χρησιμοποιούνται έλεγχος πρόσβασης βάσει ρόλων, διεπαφές διαχείρισης ειδικές για κάθε διαμέριση και αυστηρός διαχωρισμός των δεδομένων διαμόρφωσης [15],[25],[46].

Για να μπορούν τα συστήματα διαμέρισης δικτύου να εφαρμόζουν αποτελεσματικά μέτρα QoS, ασφάλειας και απομόνωσης, πρέπει να ενσωματωθούν τα SDN και NFV[22] (Network Function Virtualization). Το SDN καθιστά δυνατή την κεντρική, προγραμματιζόμενη έλεγχο των ροών κυκλοφορίας, επιτρέποντας την ομοιόμορφη εφαρμογή πολιτικών σε όλο το δίκτυο και τη δυναμική προσαρμογή σε ανταπόκριση στις μεταβαλλόμενες συνθήκες. Επιτρέποντας την ανάπτυξη λειτουργιών δικτύου, όπως υπηρεσίες ασφάλειας και επιβολή QoS, ως περιπτώσεις λογισμικού που μπορούν να επεκταθούν ή να μετακινηθούν ανάλογα με τις ανάγκες, το NFV ενισχύει αυτές τις δυνατότητες. Όταν συνδυάζονται, αυτές οι τεχνολογίες παρέχουν αυτοματοποιημένη διαχείριση του κύκλου ζωής των τμημάτων, η οποία μειώνει την λειτουργική πολυπλοκότητα και τα ανθρώπινα λάθη από την δημιουργία και διαμόρφωση έως την παρακολούθηση και τον τερματισμό [1],[15],[23],[48].

Δεδομένου ότι ο λογικός διαχωρισμός ενδέχεται να μην είναι αρκετός για να εξασφαλίσει ισχυρή απομόνωση σε περιβάλλοντα υψηλού φορτίου ή εχθρικά, πρόσφατες έρευνες έχουν επικεντρωθεί περισσότερο σε στρατηγικές απομόνωσης σε επίπεδο πόρων. Προκειμένου να αποφευχθούν διαμάχες και διαρροές απόδοσης μεταξύ των διαμερίσεων, είναι ζωτικής σημασίας η ενεργή διαχείριση των πόρων υπολογιστικής ισχύος, μνήμης και δικτύου, σύμφωνα με έρευνα του IEEE (Institute of Electrical and Electronics Engineers) σχετικά με αρχιτεκτονικές διαχωρισμού με γνώμονα την απομόνωση [26]. Αυτές οι μέθοδοι βελτιώνουν την προβλεψιμότητα της απόδοσης και την ασφάλεια, εισάγοντας πλαίσια συντονισμού με γνώμονα την απομόνωση, τα οποία λαμβάνουν υπόψη τις εξαρτήσεις των πόρων και επιβάλλουν όρια σε ολόκληρο τον κύκλο ζωής των διαμερίσεων. Σε περιβάλλοντα υπολογιστικής νέφους και υπολογιστικής περιφέρειας, όπου οι

περιβάλλοντος εκτέλεσης κάθε τμήματος, βελτιώνοντας τη φορητότητα και την επαναληψιμότητα της ανάπτυξης/εκτέλεσης.

[19] Οι πλατφόρμες ενορχήστρωσης είναι εργαλεία λογισμικού που συντονίζουν και αυτοματοποιούν την ανάπτυξη, τη διαχείριση και τη λειτουργία δικτυακών και υπολογιστικών πόρων, εξασφαλίζοντας τη σωστή συνεργασία μεταξύ επιμέρους υπηρεσιών και συστημάτων.

[20] Οι ελεγκτές SDN είναι τα κεντρικά στοιχεία ενός SDN περιβάλλοντος που αναλαμβάνουν τον έλεγχο και τον προγραμματισμό της δικτυακής λειτουργίας, διαχωρίζοντας τη λογική ελέγχου από τη μεταφορά των δεδομένων.

[21] Οι Υπερ-εποπτικές μηχανές είναι συστήματα λογισμικού που παρακολουθούν και συντονίζουν τη λειτουργία πολλαπλών υποδομών ή υπηρεσιών, παρέχοντας κεντρική εποπτεία και έλεγχο σε σύνθετα περιβάλλοντα.

[22] Το NFV είναι προσέγγιση δικτύωσης κατά την οποία βασικές δικτυακές λειτουργίες υλοποιούνται ως λογισμικό σε εικονικά περιβάλλοντα, αντί για εξειδικευμένο υλικό, προσφέροντας μεγαλύτερη ευελιξία και ευκολότερη διαχείριση.

διαμερίσεις μπορεί να εκτείνονται σε κατανεμημένες υποδομές με διαφορετικά χαρακτηριστικά πόρων, αυτές οι προσεγγίσεις είναι ιδιαίτερα σχετικές [23].

Επιπλέον, οι εξελίξεις στην έξυπνη διαχείριση διαμερίσεων χρησιμοποιούν αναλυτικά στοιχεία και μηχανική μάθηση για να ενισχύσουν την απομόνωση και την εφαρμογή πολιτικών QoS. Οι έξυπνοι ελεγκτές μπορούν να τροποποιούν προληπτικά την κατανομή των πόρων και τις διαμορφώσεις ασφαλείας, μειώνοντας την πιθανότητα παραβιάσεων SLA ή επιτυχημένων επιθέσεων, προβλέποντας τις τάσεις της κυκλοφορίας και εντοπίζοντας ασυνήθιστες δραστηριότητες. Αυτές οι μέθοδοι προσφέρουν μια πιθανή οδό για τον έλεγχο του μεγέθους και της δυναμικής των μελλοντικών τμηματοποιημένων δικτύων, παρόλο που προσθέτουν περισσότερη πολυπλοκότητα [14].

Η συνεκτική ενοποίηση των μέτρων QoS, ασφάλειας και απομόνωσης που λειτουργούν με συνέπεια σε όλα τα επίπεδα του δικτύου είναι απαραίτητη για την επιτυχή εφαρμογή της διαμέρισης δικτύου. Ενώ οι μέθοδοι ασφάλειας προστατεύουν τα δεδομένα και την υποδομή σε περιβάλλοντα πολλαπλών χρηστών, οι μηχανισμοί QoS διασφαλίζουν ότι πληρούνται διάφορες απαιτήσεις υπηρεσιών μέσω της δυναμικής και ευαίσθητης στη διαίρεση διαχείρισης πόρων. Ο διαχωρισμός της δομής που απαιτείται για να σταματήσει η επιδείνωση της απόδοσης και η εξάπλωση των τρωτών σημείων ασφάλειας μεταξύ των τμημάτων παρέχεται από τεχνικές απομόνωσης. Τα SDN, NFV και τα πλαίσια συντονισμού με γνώμονα την απομόνωση συνεργάζονται για να παρέχουν ευέλικτες, επεκτάσιμες και ασφαλείς αρχιτεκτονικές δικτύου με τμηματοποίηση, οι οποίες μπορούν να ικανοποιήσουν τις πολλές απαιτήσεις του 5G και των επόμενων γενεών. Η βελτίωση αυτών των διαδικασιών, οι οποίες υποστηρίζουν την αξιοπιστία και την εγκυρότητα των δικτύων επικοινωνίας επόμενης γενιάς, εξακολουθεί να αποτελεί σημαντική πρόκληση για την έρευνα και την τυποποίηση, καθώς εξελίσσεται η τεχνολογία διαμέρισης δικτύου [1],[15],[22],[23],[26].

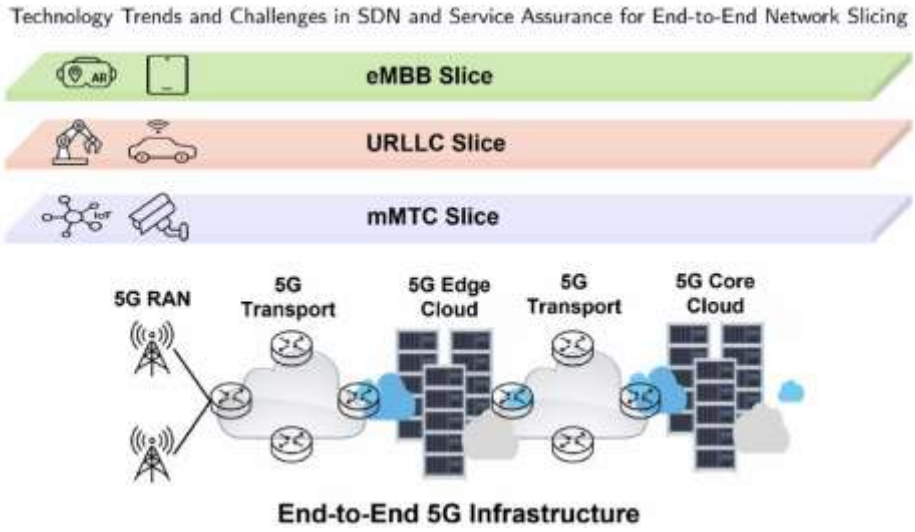
2.5 Εφαρμογές SDN/Network Slicing σε σύγχρονα δίκτυα

Καθώς οι επικοινωνίες 5G έχουν εισέλθει σε ένα στάδιο μαζικής ανάπτυξης, οι πάροχοι υπηρεσιών δημιουργούν νέες υπηρεσίες με χρήση τεχνολογιών αυτού του είδους. Ένας από τους βασικούς στόχους της τεχνολογίας 5G είναι η παροχή εγγυήσεων ποιότητας υπηρεσιών (QoS) για τους πελάτες και τις αντίστοιχες συμφωνίες επιπέδου υπηρεσιών (SLA - Service Level Agreement)[23] που αντικατοπτρίζουν τις εγγυήσεις QoS [5]. Η διαμέριση δικτύου αποτελεί βασική τεχνολογία του 5G, πληροί τις απαιτήσεις SLA και δημιουργεί νέες πηγές εσόδων, ενώ θεωρείται βασική τεχνολογία για τα μελλοντικά πρότυπα πέραν του 5G και του 6G [6]. Συγκεκριμένα, η διαμέριση δικτύου επιτρέπει νέες περιπτώσεις χρήσης διαφόρων υπηρεσιών 5G με απαιτήσεις SLA και παρέχει νέες αρχιτεκτονικές δικτύου για τον αυτόνομο έλεγχο του δικτύου 5G [11].

Για να καταστεί σαφές το πως η παραπάνω λογική μεταφράζεται σε μια ενιαία υποδομή που εξυπηρετεί πολλαπλές, ανεξάρτητες υπηρεσίες, είναι χρήσιμη μια συνοπτική σχηματική απεικόνιση. Η Εικόνα που ακολουθεί, παρουσιάζει εννοιολογικά την διαμέριση δικτύου ως σύνολο λογικών διαμερίσεων που συνυπάρχουν πάνω στους ίδιους φυσικούς πόρους, με διαφορετικές

[23] Νομικά δεσμευτική σύμβαση μεταξύ ενός Παρόχου υπηρεσιών, όπως π.χ., μιας εταιρείας πληροφορικής, τηλεπικοινωνιών και ενός πελάτη.

απαιτήσεις και πολιτικές για κάθε διαμέριση (slice). Υπό αυτό το πρίσμα, ο ελεγκτής SDN μπορεί να ιδωθεί ως ο μηχανισμός που συντονίζει την εφαρμογή των κανόνων σε κάθε διαμέριση, διατηρώντας ταυτόχρονα τη συνοχή της λειτουργίας του συνολικού δικτύου [1],[3].



Εικόνα 1: Η ιδέα της διαμέρισης δικτύου. Τεχνολογικές τάσεις και προκλήσεις στο SDN και στη διασφάλιση υπηρεσιών για κατάτμηση δικτύου από άκρο σε άκρο (End-to-End Network Slicing) [3].

Η πρακτική αξία της διαμέρισης δικτύου (network slicing) και του SDN φαίνεται καθαρά όταν περάσουμε από τη θεωρία των εγγυήσεων QoS/SLA σε σενάρια όπου, στο ίδιο φυσικό δίκτυο, συνυπάρχουν υπηρεσίες με διαφορετικές απαιτήσεις και χαρακτηριστικά λειτουργίας. Σε περιβάλλοντα παρόχων, αλλά και σε ιδιωτικά δίκτυα 5G (π.χ. πανεπιστημιουπόλεις, βιομηχανικές εγκαταστάσεις, λιμάνια), η κατάτμηση επιτρέπει να δημιουργηθεί ένας λογικός χώρος λειτουργίας ειδικά για εφαρμογές κρίσιμες ως προς την καθυστέρηση, ενώ ταυτόχρονα μια άλλη διαμέριση εξυπηρετεί βαριά κίνηση δεδομένων, όπως βίντεο υψηλής ανάλυσης ή μεταφορές αρχείων [3],[11],[22].

Με αυτόν τον τρόπο, η συμπεριφορά του δικτύου γίνεται προβλέψιμη για κάθε κατηγορία χρήσης, χωρίς να απαιτείται ξεχωριστή φυσική υποδομή για κάθε υπηρεσία. Παράλληλα, οι πάροχοι μπορούν να αξιοποιούν τις δυνατότητες του δικτύου ως εμπορικά πακέτα υπηρεσιών, προσφέροντας σε επιχειρήσεις διαφορετικά επίπεδα υπηρεσίας με μετρήσιμες δεσμεύσεις, κάτι που μετατρέπει τεχνικές δυνατότητες σε άμεσα αξιοποιήσιμη εμπορική αξία [2],[6].

Στον χώρο της βιομηχανίας, για παράδειγμα, μια διαμέριση μπορεί να εξυπηρετεί ροές ελέγχου και αυτοματισμού που απαιτούν σταθερότητα και πολύ χαμηλή καθυστέρηση, ενώ μια δεύτερη μπορεί εξυπηρετεί αισθητήρες μεγάλης κλίμακας και τηλεμετρία, όπου η προτεραιότητα είναι η μαζικότητα και η ενεργειακή αποδοτικότητα των συσκευών. Αντίστοιχα, στην υγεία ή στη δημόσια ασφάλεια συναντώνται σενάρια όπου απαιτείται υψηλή αξιοπιστία, διαθεσιμότητα και αυστηρός έλεγχος πρόσβασης, ώστε η κρίσιμη επικοινωνία να μην επηρεάζεται από την υπόλοιπη κίνηση δεδομένων στο ίδιο δίκτυο. Σε τέτοιες περιπτώσεις, η διαμέριση δεν λειτουργεί μόνο ως μέσο διαχείρισης επιδόσεων, αλλά και ως πρακτική μορφή οργανωτικής απομόνωσης: ξεχωριστές πολιτικές, ξεχωριστή παρακολούθηση και σαφέστερα όρια ευθύνης ανά υπηρεσία ή ανά πελάτη.

Έτσι μειώνεται η πιθανότητα μια βλάβη ή μια κακή ρύθμιση να διαχυθεί σε όλο το δίκτυο και να επηρεάσει ετερογενείς υπηρεσίες [2],[11],[13],[23].

Ο ρόλος του SDN καθίσταται ιδιαίτερα κρίσιμος όταν οι διαμερίσεις δεν παραμένουν σταθερές, αλλά απαιτείται να προσαρμόζονται δυναμικά στις μεταβολές της ζήτησης. Η κίνηση σε ένα δίκτυο παρουσιάζει έντονες διακυμάνσεις στον χρόνο και στον χώρο, ενώ μπορεί να επηρεάζεται και από απρόβλεπτα γεγονότα που προκαλούν αιχμές φορτίου. Με την ύπαρξη κεντρικού επιπέδου ελέγχου, οι πολιτικές δρομολόγησης και κατανομής πόρων μπορούν να ενημερώνονται άμεσα, ώστε κάθε διαμέριση να λαμβάνει τους απαραίτητους πόρους όταν απαιτείται και να τους αποδεσμεύει όταν η πίεση μειώνεται [1],[5],[6].

Επιπλέον, το SDN διευκολύνει την ενοποιημένη εποπτεία της υποδομής, καθώς συγκεντρώνει μετρήσεις λειτουργίας, δείκτες απόδοσης και κανόνες ασφάλειας σε ένα συνεκτικό πλαίσιο διαχείρισης, αντί για μεμονωμένες ρυθμίσεις σε μεμονωμένες συσκευές. Με αυτόν τον τρόπο υποστηρίζεται μια διαδικασία συνεχούς παρακολούθησης και προσαρμογής, όπου τα δεδομένα λειτουργίας αξιοποιούνται αφενός για λήψη αποφάσεων, και αφετέρου για άμεση εφαρμογή διορθωτικών ενεργειών, με στόχο την τήρηση των απαιτήσεων ποιότητας υπηρεσίας (QoS) και των συμφωνιών επιπέδου υπηρεσίας [2],[6].

Στο σημείο αυτό υπογραμμίζεται το γεγονός ότι στις σύγχρονες υλοποιήσεις οι διαμερίσεις συχνά δεν περιορίζονται σε ένα μόνο τμήμα του δικτύου. Μπορεί να καλύπτουν ταυτόχρονα το ασύρματο τμήμα πρόσβασης, το μεταφορικό δίκτυο και τον πυρήνα, καθώς και υποδομές cloud/edge όπου εκτελούνται λειτουργίες και εφαρμογές. Αυτό σημαίνει ότι για να διαθέτει μια διαμέριση ουσιαστική επιχειρησιακή αξία πρέπει να υπάρχει συνέπεια από άκρο σε άκρο. Οι ίδιες απαιτήσεις, όπως χαμηλή καθυστέρηση, επαρκές διαθέσιμο εύρος και σαφής απομόνωση, χρειάζεται να μεταφράζονται σε ρυθμίσεις που εφαρμόζονται με τον ίδιο τρόπο σε όλα τα τμήματα της υποδομής [5],[6],[10] .

Μέσα σε αυτό το πλαίσιο, η διαμέριση δικτύου μαζί με τον προγραμματιζόμενο έλεγχο του δικτύου δίνουν έναν πρακτικό μηχανισμό ώστε οι απαιτήσεις των εφαρμογών να γίνονται συγκεκριμένοι κανόνες και λειτουργίες στο δίκτυο. Έτσι ενισχύεται ο έλεγχος, διευκολύνεται η αυτοματοποίηση και διατηρείται καλύτερη αντιστοίχιση με τις πραγματικές συνθήκες λειτουργίας των σύγχρονων υποδομών [1],[6].

2.6 Ενορχήστρωση και διαχείριση κύκλου ζωής διαμερίσεων δικτύου

Η πρακτική υλοποίηση της διαμέρισης δικτύου δεν εξαντλείται στον αρχικό σχεδιασμό της αρχιτεκτονικής ή στην απομόνωση της κίνησης. Καθώς οι υπηρεσίες ενεργοποιούνται και απενεργοποιούνται δυναμικά, ο φορέας εκμετάλλευσης χρειάζεται μηχανισμούς που να μετατρέπουν τις απαιτήσεις υπηρεσίας σε συγκεκριμένες ενέργειες στο δίκτυο, με τρόπο επαναληπτικό και ελεγχόμενο. Αυτό σημαίνει ότι η διαμέριση πρέπει να αντιμετωπίζεται ως οντότητα με κύκλο ζωής: σχεδίαση, δημιουργία, ενεργοποίηση, εποπτεία, κλιμάκωση, βελτιστοποίηση και τελικά τερματισμός, χωρίς να απαιτείται χειροκίνητη παρέμβαση σε πλήθος συσκευών κάθε φορά [1],[10].

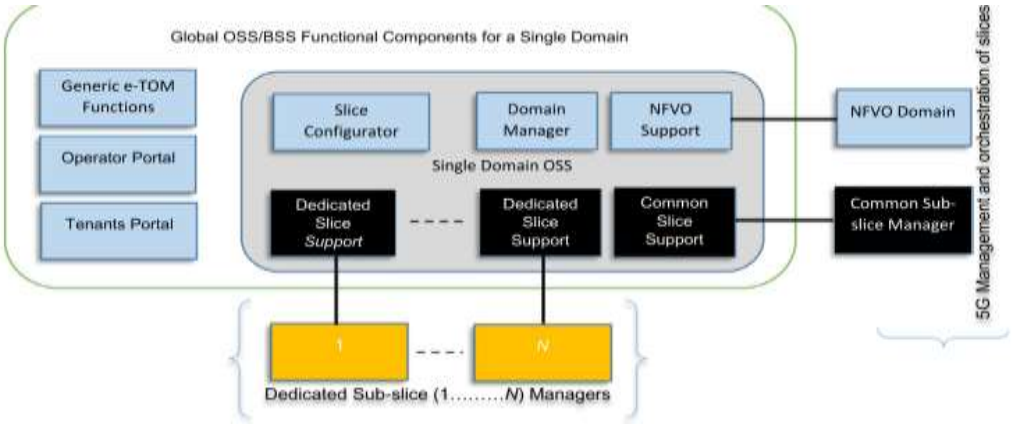
Στο επίπεδο των λειτουργιών, η διαχείριση κύκλου ζωής διαμερίσεων βασίζεται συνήθως σε έναν διαχωρισμό ρόλων ανάμεσα σε επιχειρησιακά συστήματα και τεχνικούς μηχανισμούς ελέγχου. Τα επιχειρησιακά συστήματα του Παρόχου, όπως τα OSS (Operations Support Systems) και BSS (Business Support Systems), συλλέγουν αιτήματα υπηρεσιών, διαχειρίζονται πολιτικές, έγκριση, χρέωση και συμφωνίες επιπέδου υπηρεσίας, και τροφοδοτούν το τεχνικό επίπεδο με παραμέτρους που είναι άμεσα εφαρμόσιμες. Στην πράξη, οι λειτουργίες αυτές ευθυγραμμίζονται με γνωστά πλαίσια επιχειρησιακών διεργασιών, όπως το eTOM, ώστε η τεχνική υλοποίηση να συνδέεται με τυποποιημένους κύκλους εργασιών λειτουργίας δικτύου [1].

Σε ένα σενάριο ενός μόνο διοικητικού τομέα, η ενορχήστρωση υλοποιείται ως αλληλεπίδραση μεταξύ επιμέρους λειτουργικών ενοτήτων. Ένας διαμορφωτής διαμερίσεων αναλαμβάνει να μετατρέψει τις απαιτήσεις υπηρεσίας σε παραμετροποιήσιμα (customizable) πρότυπα, να επιλέξει κατάλληλες επιλογές υλοποίησης και να ενεργοποιήσει την αντίστοιχη αλυσίδα λειτουργιών δικτύου. Παράλληλα, ένας διαχειριστής τομέα συντονίζει τις αλλαγές εντός της υποδομής, λαμβάνοντας υπόψη περιορισμούς πόρων, διαθέσιμη χωρητικότητα και πολιτικές απομόνωσης. Η υποστήριξη ενορχήστρωσης NFV συμπληρώνει το σχήμα, καθώς αναλαμβάνει την εγκατάσταση και κλιμάκωση εικονικοποιημένων λειτουργιών δικτύου πάνω σε γενικούς υπολογιστικούς πόρους [1],[10].

Ένα κρίσιμο πρακτικό σημείο είναι ο τρόπος με τον οποίο διαχειρίζονται οι υπο-διαμερίσεις, δηλαδή τα τμήματα που αντιστοιχούν σε επιμέρους περιοχές ή τεχνολογικά στρώματα, όπως πρόσβαση, μεταφορά και πυρήνας. Σε πολλές περιπτώσεις χρησιμοποιούνται ειδικοί διαχειριστές υποδιαμερίσεων για κάθε διαμέριση, ώστε οι πολιτικές και οι μετρήσεις να παραμένουν αυστηρά απομονωμένες. Ταυτόχρονα, είναι συνηθισμένη η ύπαρξη κοινών λειτουργιών υποστήριξης, οι οποίες παρέχουν κοινόχρηστες υπηρεσίες διαχείρισης όπου αυτό δεν μειώνει την απομόνωση, ώστε να βελτιώνεται η αποδοτικότητα και να περιορίζεται το λειτουργικό κόστος [1],[23].

Η παρακάτω Εικόνα συνοψίζει ένα αντιπροσωπευτικό μοντέλο διαχείρισης και ενορχήστρωσης σε έναν μόνο διοικητικό τομέα, όπου τα επιχειρησιακά συστήματα του Παρόχου συνδέονται με λειτουργίες διαμόρφωσης, διαχείρισης τομέων και εγκατάστασης εικονικοποιημένων λειτουργιών. Η Εικόνα αναδεικνύει ότι η λογική της διαμέρισης συνδέεται ταυτόχρονα με δύο κατευθύνσεις: από τη μία με τα επιχειρησιακά κανάλια αλληλεπίδρασης, όπως τις πύλες διαχειριστή και μισθωτών, και από την άλλη με τις τεχνικές μονάδες που επιβάλλουν πολιτικές και δεσμεύουν πόρους. Με αυτόν τον τρόπο, ένα αίτημα υπηρεσίας μπορεί να μετατραπεί σε συγκεκριμένη δέσμευση υπολογιστικής ισχύος, εύρους ζώνης και κανόνων προώθησης, ενώ

παράλληλα ενεργοποιούνται οι αντίστοιχοι μηχανισμοί παρακολούθησης ώστε να είναι μετρήσιμη η συμμόρφωση με τους στόχους απόδοσης και απομόνωσης [1] .



Εικόνα 2: Υψηλού επιπέδου σχήμα διαχείρισης και ενορχήστρωσης διαμερίσεων σε ένα διοικητικό τομέα [1].

Στην καθημερινή λειτουργία, η διαχείριση κύκλου ζωής χρειάζεται κλειστό βρόχο ελέγχου. Οι μετρήσεις απόδοσης, καθυστέρησης, απωλειών, χρήσης πόρων και συμβάντων ασφάλειας συλλέγονται συνεχώς και αντιστοιχίζονται σε κάθε διαμέριση. Όταν ανιχνεύεται απόκλιση από τους στόχους, ενεργοποιούνται ενέργειες κλιμάκωσης ή ανακατανομής, όπως μετακίνηση εικονικοποιημένων λειτουργιών, αλλαγές στην προτεραιοποίηση της κίνησης, ή διαφορετική δρομολόγηση ροών μέσω του ελεγκτή SDN. Το σημαντικό είναι ότι οι ενέργειες αυτές πρέπει να είναι συνεπείς με τις πολιτικές απομόνωσης, ώστε μια επιθετική κλιμάκωση σε μια διαμέριση να μην προκαλεί υποβάθμιση σε άλλη [1],[6],[23]. Στον Πίνακα που ακολουθεί συνοψίζονται οι βασικές λειτουργικές ενότητες του παραπάνω μοντέλου και ο ρόλος τους στη διαχείριση διαμερίσεων.

Πίνακας 1: Αντιστοίχιση λειτουργικών ενοτήτων σε ρόλους διαχείρισης και ενορχήστρωσης διαμερίσεων [1]

Λειτουργική ενότητα	**Ρόλος στη διαχείριση διαμερίσεων**	**Ενδεικτικές ενέργειες**
Πύλη διαχειριστή και πύλη μισθωτών	Σημείο εισόδου αιτημάτων και πολιτικών	Υποβολή αιτήματος υπηρεσίας, έγκριση, συσχέτιση με SLA
Διαμορφωτής διαμερίσεων	Μεταφράζει απαιτήσεις σε πρότυπα και παραμέτρους υλοποίησης	Επιλογή προτύπου, παραμετροποίηση, ενεργοποίηση αλυσίδας λειτουργιών
Διαχειριστής τομέα	Συντονίζει την εφαρμογή πολιτικών εντός του τομέα	Κατανομή πόρων, επιβολή απομόνωσης, ενεργοποίηση κανόνων
Υποστήριξη ενορχήστρωσης NFV	Διαχειρίζεται την εγκατάσταση και κλιμάκωση εικονικοποιημένων λειτουργιών	Δημιουργία, μετακίνηση και κλιμάκωση λειτουργιών, παρακολούθηση υπολογιστικών πόρων
Ειδικοί διαχειριστές υπο-διαμερίσεων	Τοπική διαχείριση υπο-διαμερίσεων με αυστηρή απομόνωση	Παρακολούθηση κατά στρώμα, τοπικές προσαρμογές χωρίς επίδραση σε άλλα τμήματα
Κοινός διαχειριστής υπο-διαμερίσεων και κοινή υποστήριξη	Κοινόχρηστες λειτουργίες όπου δεν θίγεται η απομόνωση	Κοινά εργαλεία εποπτείας, επαναχρησιμοποίηση μηχανισμών ελέγχου

Η παραπάνω προσέγγιση διαχείρισης και ενορχήστρωσης εξηγεί γιατί οι προσομοιώσεις των επόμενων κεφαλαίων δεν περιορίζονται στη συνδεσιμότητα, αλλά εξετάζουν τη συμπεριφορά του δικτύου όταν εφαρμόζονται πολιτικές ανά διαμέριση, όταν μεταβάλλεται ο φόρτος και όταν απαιτείται προσαρμογή πόρων με στόχο τη διατήρηση της ποιότητας υπηρεσίας και της απομόνωσης.

2.7 Εργαλεία υλοποίησης που απαιτούνται για τα πειράματα

Η θεωρία του SDN, του OpenFlow, των VLAN, των ACL και των μηχανισμών QoS έχει ήδη αναπτυχθεί στις προηγούμενες ενότητες. Για τον λόγο αυτό, εδώ καταγράφεται μόνο ο ρόλος των εργαλείων που είναι απαραίτητος για την κατανόηση των πειραμάτων. Το Cisco Packet Tracer χρησιμοποιείται για λειτουργική επαλήθευση λογικού διαχωρισμού με VLAN, πολιτικών πρόσβασης με ACL και διαφοροποιημένης μεταχείρισης με QoS [16],[17]. Δεν υλοποιεί εγγενές 5G διαμέρισης δικτύου από άκρο σε άκρο, επομένως το αντίστοιχο πείραμα αντιμετωπίζεται ως ελεγχόμενη προσέγγιση της λογικής του slicing με συμβατικούς μηχανισμούς δικτύωσης [28]–[30].

Για το πείραμα SDN χρησιμοποιείται το Mininet για τη δημιουργία εικονικών υπολογιστών-ξενιστών (hosts) και ζεύξεων και το Open vSwitch ως προγραμματιζόμενο επίπεδο προώθησης. Ο OpenDaylight αναλαμβάνει τον κεντρικό έλεγχο και επικοινωνεί με τους OVS μεταγωγείς μέσω OpenFlow, ενώ η RESTCONF[24](REST-based Network Configuration Protocol) χρησιμοποιείται για την εγκατάσταση και επιθεώρηση κανόνων. Οι παραπάνω λειτουργίες αρκούν για το ζητούμενο πείραμα: σύγκριση της ίδιας τοπολογίας πριν και μετά την εγκατάσταση πολιτικής προώθησης. Η γενική αρχιτεκτονική επιπέδου ελέγχου και επιπέδου προώθησης δεν επαναλαμβάνεται, καθώς έχει ήδη παρουσιαστεί στην ενότητα 2.2 [32].

Το GNS3 παραμένει διαθέσιμο για σενάρια όπου απαιτείται συμπεριφορά λογισμικού δρομολογητών και πιο σύνθετη παραμετροποίηση. Στο Κεφάλαιο 3, όμως, επιλέγονται μόνο τα εργαλεία που συνδέονται άμεσα με τα πειράματα που τελικά αξιολογούνται, ώστε η παρουσίαση να παραμένει εφαρμοσμένη και να μη μετατρέπεται σε δεύτερη θεωρητική περιγραφή των ίδιων τεχνολογιών [18],[27].

2.8 Δυναμική διαχείριση πόρων και αυτοματοποίηση με Python

Η δυναμική διαχείριση πόρων βασίζεται σε έναν κλειστό βρόχο παρακολούθησης και απόφασης: συλλέγονται μετρικές, ελέγχονται έναντι ορίων ή στόχων SLA και, όταν απαιτείται, ενεργοποιείται αλλαγή στην κατανομή πόρων. Η Python είναι κατάλληλη για αυτή τη λογική επειδή μπορεί να συνδέσει πηγές μετρήσεων και προγραμματιζόμενα API με απλούς κανόνες ελέγχου. Στο πείραμα της εργασίας χρησιμοποιούνται μετρικές καθυστέρησης και χρήσης CPU (Central Processing Unit), Prometheus ως πηγή μετρήσεων και μια ενδεικτική ενέργεια κλιμάκωσης υπηρεσίας σε περιβάλλον Kubernetes.

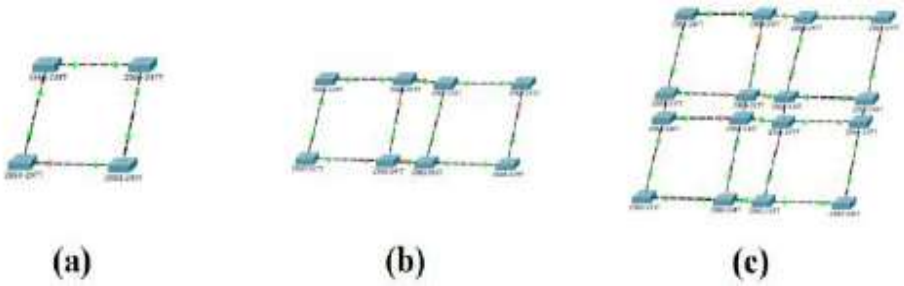
[24] RESTful Configuration Protocol: Πρωτόκολλο διαχείρισης και διαμόρφωσης δικτυακών συσκευών, το οποίο χρησιμοποιεί το HTTP και επιτρέπει την πρόσβαση και τροποποίηση δεδομένων μέσω RESTful API.

Οι τεχνικές μηχανικής μάθησης μπορούν να επεκτείνουν αυτό το μοντέλο, προβλέποντας τη μελλοντική ζήτηση ή υποστηρίζοντας πιο σύνθετες αποφάσεις κατανομής πόρων [33]–[35]. Ωστόσο, στο εφαρμοσμένο μέρος της παρούσας εργασίας δεν παρουσιάζεται εκπαιδευμένο μοντέλο ML ούτε αποδίδονται σε αυτό μετρημένα κέρδη. Η πρακτική αξιολόγηση περιορίζεται συνειδητά σε έναν ντετερμινιστικό μηχανισμό Python βασισμένο σε SLA, ώστε κάθε απόφαση να είναι ελέγξιμη και να μπορεί να συσχετιστεί άμεσα με τις τιμές εισόδου.

2.9 Αρχές πειραματικής αξιολόγησης, baseline και αναπαραγωγιμότητας

Η συγκριτική αξιολόγηση οργανώνεται γύρω από ένα κοινό πρότυπο: πρώτα ορίζεται μία κατάσταση αναφοράς (baseline) στην οποία απουσιάζει ο μηχανισμός που εξετάζεται και στη συνέχεια εφαρμόζεται η αντίστοιχη παρέμβαση στην ίδια, κατά το δυνατόν, τοπολογία και στις ίδιες αρχικές συνθήκες. Έτσι, η διαφορά στη λειτουργική συμπεριφορά μπορεί να αποδοθεί στην εφαρμογή της διαμέρισης δικτύου, του SDN ή της προσαρμοστικής πολιτικής και όχι σε αλλαγή της φυσικής υποδομής. Η λογική κατάσταση αναφοράς–παρέμβαση–επαλήθευση αποτελεί το μεθοδολογικό πλαίσιο των πειραμάτων του Κεφαλαίου 3 [27].

Οι μετρικές επιλέγονται ανάλογα με το τι μπορεί να τεκμηριωθεί από κάθε εργαλείο. Στο Packet Tracer χρησιμοποιούνται κυρίως λειτουργικά τεκμήρια, όπως η ύπαρξη λογικών ορίων, η εφαρμογή ACL και η ενεργοποίηση πολιτικής QoS. Στο Mininet/OVS μπορούν επιπλέον να ελεγχθούν η συνδεσιμότητα, οι εγκατεστημένοι κανόνες OpenFlow και οι μετρητές τους. Για τον μηχανισμό Python αξιολογείται η ορθότητα της απόφασης κλιμάκωσης σε ελεγχόμενες τιμές εισόδου. Δεν παρουσιάζονται αριθμητικές βελτιώσεις για μετρικές που δεν έχουν πραγματικά μετρηθεί.



Εικόνα 3: Οι διαφορετικές τοπολογίες που χρησιμοποιούνται στο προτεινόμενο σενάριο: (a) τοπολογία βασικού στοιχείου, (b) τοπολογία δύο βασικών στοιχείων, (c) τοπολογία τεσσάρων βασικών στοιχείων [27].

Η ελεγχόμενη μεταβολή της πολυπλοκότητας μιας τοπολογίας, όπως απεικονίζεται στην Εικόνα 3, είναι χρήσιμη όταν εξετάζονται όρια κλιμάκωσης ή κατανάλωσης πόρων. Στην παρούσα εργασία η αρχή αυτή χρησιμοποιείται ως μεθοδολογική αναφορά και όχι ως ανεξάρτητο αποτέλεσμα. Για αναπαραγωγιμότητα πρέπει να καταγράφονται οι εκδόσεις λογισμικού, οι παράμετροι τοπολογίας, οι κανόνες πολιτικής, οι τιμές εισόδου και τα τεκμήρια κάθε εκτέλεσης. Η συστηματική καταγραφή επιτρέπει να συνδεθεί κάθε αποτέλεσμα με τη διαμόρφωση που το παρήγαγε και περιορίζει την πιθανότητα λανθασμένης ερμηνείας [55]-[57].

3 *Πειραματική εφαρμογή και συγκριτική αξιολόγηση SDN και Network Slicing*

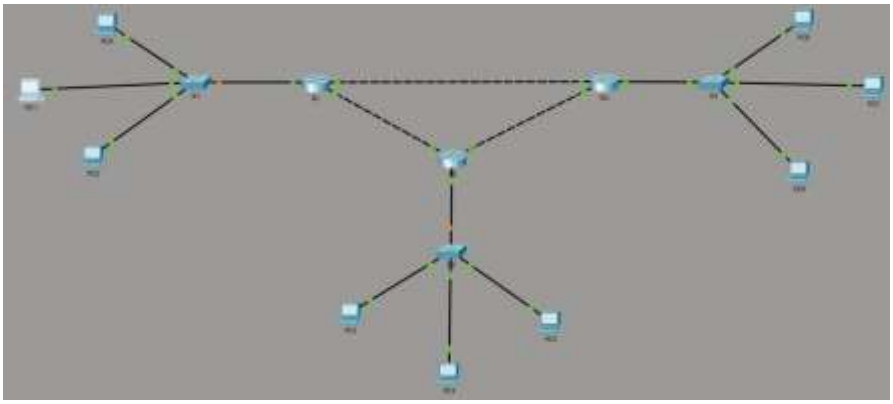
3.1 Πειραματικός σχεδιασμός: baseline, εφαρμογή και άμεση αξιολόγηση

Στο Κεφάλαιο 3 δεν επαναλαμβάνεται το θεωρητικό υπόβαθρο του Κεφαλαίου 2. Κάθε εφαρμογή οργανώνεται ως ελεγχόμενη σύγκριση: (α) ορίζεται μία ελαττωματική ή ανεπαρκής κατάσταση αναφοράς, (β) εφαρμόζεται ο εξεταζόμενος μηχανισμός στην ίδια λογική υποδομή και (γ) καταγράφεται αμέσως το λειτουργικό αποτέλεσμα. Με αυτόν τον τρόπο, η υλοποίηση και η αξιολόγηση παρουσιάζονται μαζί και γίνεται σαφές ποιο συγκεκριμένο πρόβλημα επιλύει κάθε τεχνική.

Τα τρία εφαρμοσμένα σενάρια είναι: λογική διαμέριση με VLAN/ACL/QoS στο Cisco Packet Tracer, προγραμματιζόμενη προώθηση με Mininet/OVS και OpenDaylight, και προσαρμοστική κατανομή πόρων με Python. Για κάθε σενάριο αναφέρονται μόνο τα στοιχεία του εργαλείου που χρειάζονται για την εκτέλεση και την ερμηνεία του πειράματος. Οι περιορισμοί κάθε αποτελέσματος δηλώνονται ρητά, ώστε λειτουργικές επαληθεύσεις να μη συγχέονται με μετρήσεις που δεν πραγματοποιήθηκαν.

3.2 Υλοποίηση Network Slicing με χρήση VLANs, ACLs, QoS και routing σε Cisco Packet Tracer

Η ίδια φυσική τοπολογία της Εικόνας 4 εκτελείται σε δύο καταστάσεις. Στην B0 υπάρχει βασική δρομολόγηση, αλλά δεν υπάρχει λογικός διαχωρισμός υπηρεσιών, πολιτική απομόνωσης ή προτεραιοποίηση. Στην S1 εφαρμόζονται VLAN 110 για eMBB, VLAN 210 για URLLC και VLAN 11 για διαχείριση, μαζί με ACL και QoS. Επειδή η φυσική συνδεσμολογία δεν αλλάζει, το αποτέλεσμα μπορεί να αποδοθεί στους μηχανισμούς διαμέρισης και όχι σε διαφορετική υποδομή [28]-[30] .



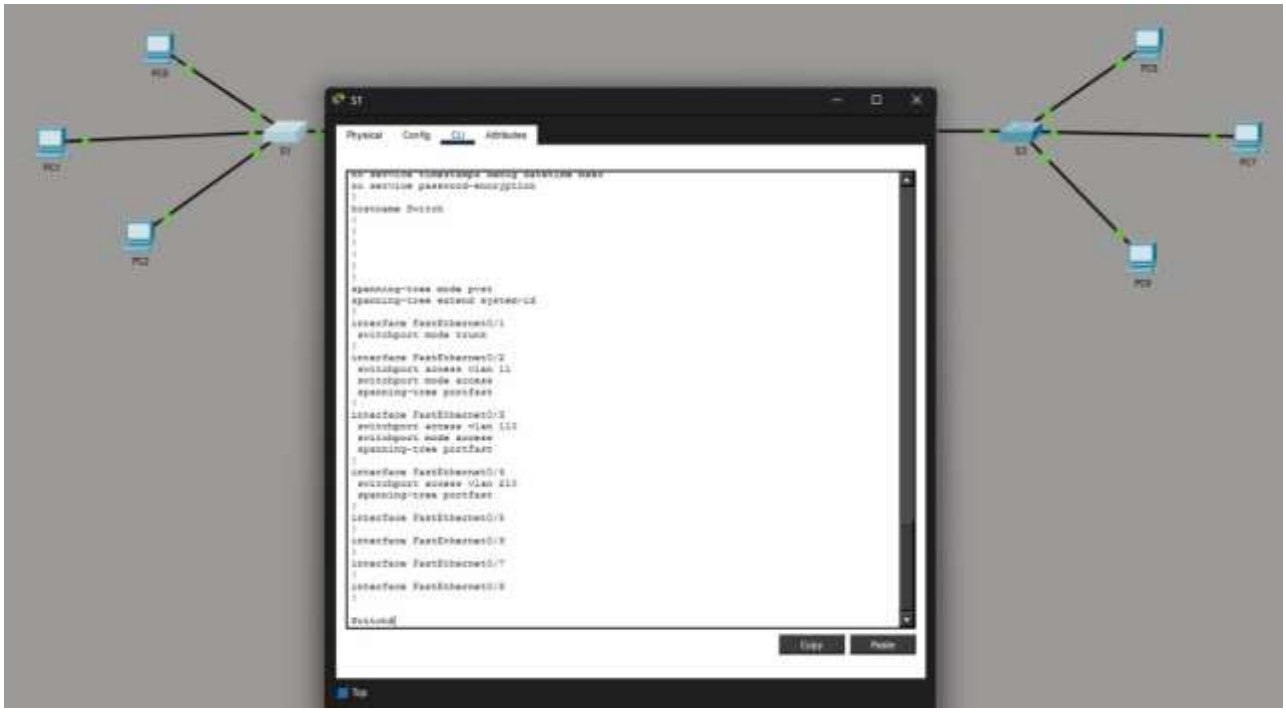
Εικόνα 4: Κοινή φυσική τοπολογία για τις καταστάσεις B0 και S1.

3.2.1 Ελαττωματικό πρότυπο αναφοράς χωρίς Network Slicing

Ως κατάσταση αναφοράς B0 χρησιμοποιείται η ίδια τοπολογία με ενεργή βασική δρομολόγηση, αλλά χωρίς τους μηχανισμούς που χρησιμοποιούνται στη συνέχεια για την προσέγγιση της διαμέρισης δικτύου. Συγκεκριμένα, δεν γίνεται διαχωρισμός των υπηρεσιών σε VLAN 110 (eMBB), VLAN 210 (URLLC) και VLAN 11 (διαχείριση), δεν εφαρμόζεται η ACL Deny_Subnet για έλεγχο της επικοινωνίας μεταξύ των λογικών τμημάτων και δεν χρησιμοποιούνται οι Servers_Priority, CRITICAL_TRAFFIC και SLICING_QOS_POLICY για ταξινόμηση και προτεραιοποίηση της κρίσιμης κίνησης. Επομένως, η τοπολογία μπορεί να διαθέτει κανονική IP συνδεσιμότητα, αλλά δεν διαθέτει μηχανισμό που να μεταφράζει τις διαφορετικές απαιτήσεις των υπηρεσιών σε ξεχωριστή δικτυακή μεταχείριση [28]-[30] .

Το πρότυπο B0 θεωρείται ελαττωματικό όχι επειδή το δίκτυο παύει να επικοινωνεί, αλλά επειδή αποτυγχάνει στις απαιτήσεις απομόνωσης και ποιότητας υπηρεσίας. Εφόσον υπάρχει διαδρομή μεταξύ των υποδικτύων, η κίνηση από το 192.168.110.0/24 προς το 192.168.210.0/24 δεν απορρίπτεται από κάποια πολιτική πρόσβασης. Παράλληλα, χωρίς class-map και policy-map η κρίσιμη κίνηση δεν διαθέτει ιδιαίτερη προτεραιότητα και ανταγωνίζεται την κίνηση υψηλού όγκου για τους ίδιους πόρους. Σε συνθήκες συμφόρησης, επομένως, δεν υπάρχει μηχανισμός που να προστατεύει μια υπηρεσία ευαίσθητη στην καθυστέρηση από μια ταυτόχρονη ροή best effort. Αυτό είναι το συγκεκριμένο πρόβλημα που καλείται να αντιμετωπίσει η διαμόρφωση διαμέρισης δικτύου [29]-[30] .

3.2.2 Διορθωτική διαμόρφωση με λογική Network Slicing



Εικόνα 5: Διαμόρφωση switch με trunk port και access ports στα VLAN 11, 110 και 210.

Η Εικόνα 5 τεκμηριώνει την παρέμβαση S1 στο επίπεδο μεταγωγής: οι τελικές συσκευές δεν αντιμετωπίζονται πλέον ως μία ενιαία κατηγορία, αλλά αντιστοιχίζονται σε ξεχωριστά VLAN. Ο έλεγχος με show vlan brief στην Εικόνα 6 επιβεβαιώνει ότι η επιθυμητή αντιστοίχιση θυρών έχει

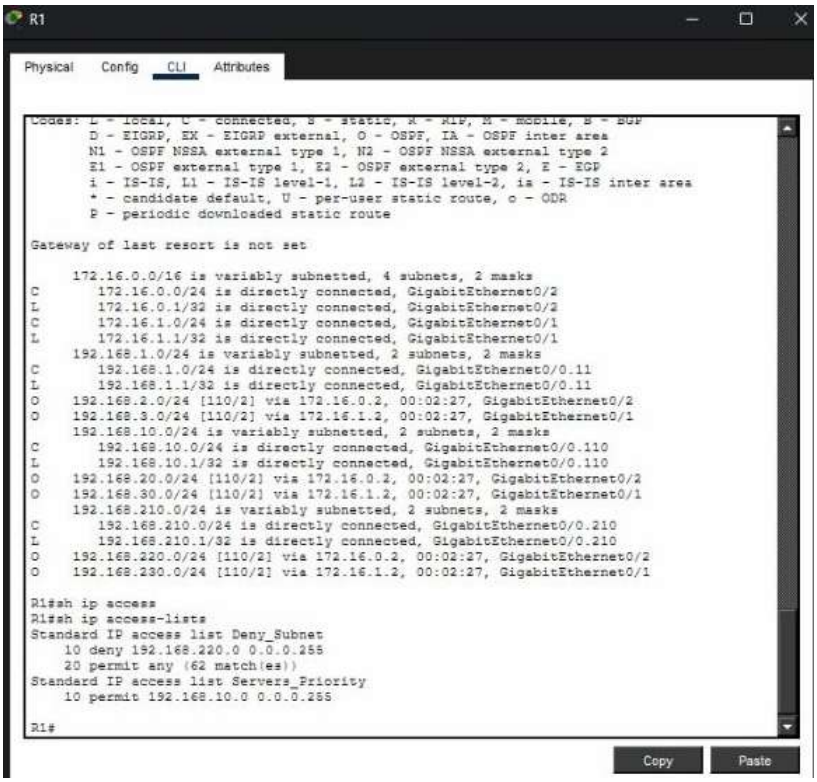
εφαρμοστεί. Πρόκειται για άμεσο λειτουργικό αποτέλεσμα της διαμόρφωσης και όχι για θεωρητική περιγραφή των VLAN [28] .

Εικόνα 6: Έλεγχος VLANs με show vlan brief και αντιστοίχιση θυρών στις τρεις λογικές κατηγορίες.

Εικόνα 7: Εφαρμογή της ACL Deny_Subnet στις διεπαφές και ρυθμίσεις δρομολόγησης OSPF (Open Shortest Path First).

Εικόνα 8: Ορισμός ACL για απομόνωση υποδικτύου και αναγνώριση της κρίσιμης κίνησης.

Οι Εικόνες 7–9 δείχνουν το δεύτερο αποτέλεσμα της S1: η επικοινωνία μεταξύ κατηγοριών υπηρεσίας παύει να εξαρτάται μόνο από την ύπαρξη διαδρομής και ελέγχεται από ρητές πολιτικές. Η Deny_Subnet απορρίπτει τη ροή από το υποδίκτυο eMBB προς το URLLC, ενώ η Servers_Priority αναγνωρίζει την κίνηση που πρέπει να αντιμετωπιστεί ως κρίσιμη. Έτσι, η απομόνωση και η ταξινόμηση μπορούν να επαληθευτούν από τη διαμόρφωση του router [29] .



Εικόνα 9: Προβολή των ACL Deny_Subnet και Servers_Priority μαζί με τον πίνακα δρομολόγησης.

Εικόνα 10: Διαμόρφωση QoS με class-map και policy-map για την προτεραιοποίηση της κρίσιμης κίνησης.

Στην Εικόνα 10 η αναγνωρισμένη κρίσιμη κίνηση συνδέεται με τη class-map CRITICAL_TRAFFIC και την SLICING_QOS_POLICY. Η εντολή priority percent 30 παρέχει συγκεκριμένο μηχανισμό προτεραιότητας που απουσιάζει από την B0. Συνεπώς, το πείραμα δεν ισχυρίζεται μη μετρημένη αριθμητική μείωση καθυστέρησης· αποδεικνύει ότι η S1 διαθέτει ρητό μηχανισμό προστασίας της κρίσιμης ροής σε συνθήκες ανταγωνισμού για πόρους [29],[30].

3.2.3 Συγκριτική επαλήθευση: χωρίς και με Network Slicing

Για να είναι σαφές τι επιτυγχάνεται από τη διαμόρφωση, η κατάσταση B0 συγκρίνεται με την κατάσταση S1, δηλαδή με την ίδια φυσική τοπολογία μετά την εφαρμογή των VLANs, ACLs και QoS που παρουσιάζονται στις Εικόνες 5–10. Η σύγκριση γίνεται σε επίπεδο λειτουργικής συμπεριφοράς και επιβολής πολιτικών. Με αυτόν τον τρόπο αποφεύγεται το ασαφές συμπέρασμα ότι το δίκτυο απλώς «λειτουργεί καλύτερα» και αποτυπώνεται ποια συγκεκριμένη απαίτηση δεν ικανοποιείται χωρίς slicing και ποιος μηχανισμός τη διορθώνει.

Πίνακας 2: Σύγκριση του ελαττωματικού προτύπου B0 χωρίς Network Slicing με τη διαμόρφωση S1 με VLANs, ACLs και QoS.

Κριτήριο / δοκιμή	**B0 – χωρίς Network Slicing**	**S1 – με Network Slicing**	**Τι επιτυγχάνεται**
Λογικός διαχωρισμός υπηρεσιών	Δεν υπάρχουν διακριτές κατηγορίες υπηρεσίας σε VLAN 110/210/11. Η κίνηση αντιμετωπίζεται ενιαία.	VLAN 110 για eMBB, VLAN 210 για URLLC και VLAN 11 για διαχείριση, με αντιστοίχιση access/trunk θυρών.	Δημιουργούνται σαφή λογικά όρια πάνω στην ίδια φυσική υποδομή.

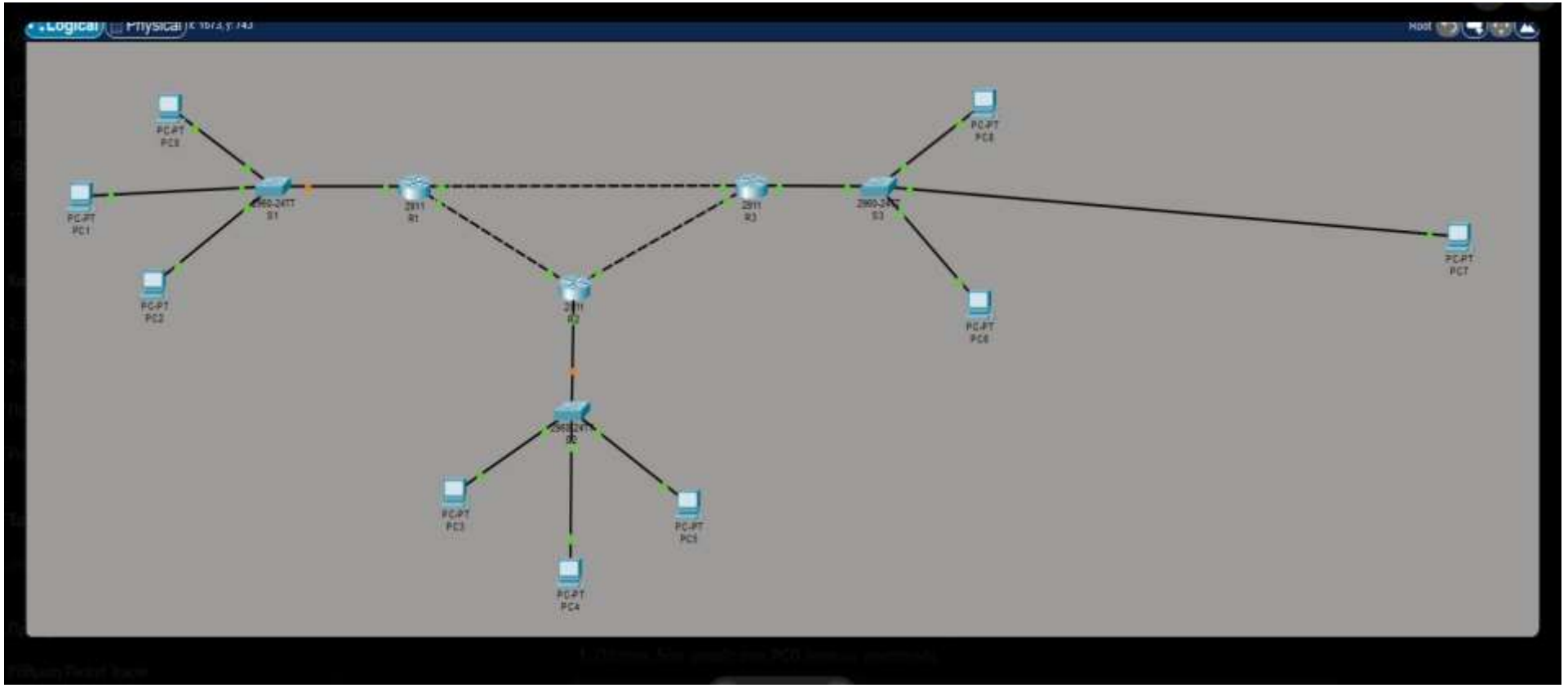
Έλεγχος επικοινωνίας eMBB → URLLC	Με ενεργή δρομολόγηση και χωρίς ACL, δεν υπάρχει πολιτική που να απορρίπτει τη ροή 192.168.110.0/24 → 192.168.210.0/24.	Η ACL Deny_Subnet εφαρμόζει ρητό deny για τη συγκεκριμένη κατεύθυνση κίνησης.	Η απομόνωση παύει να είναι υπόθεση της τοπολογίας και γίνεται ελεγχόμενη πολιτική.
Αναγνώριση κρίσιμης κίνησης	Δεν υπάρχει ειδική κλάση υπηρεσίας· τα πακέτα ακολουθούν την προεπιλεγμένη μεταχείριση.	Η ACL Servers_Priority και η class-map CRITICAL_TRAFFIC αναγνωρίζουν τις ροές που πρέπει να προστατευθούν.	Οι διαφορετικές απαιτήσεις υπηρεσίας μετατρέπονται σε συγκεκριμένη ταξινόμηση κίνησης.
Προτεραιότητα σε συνθήκες συμφόρησης	Δεν υπάρχει ρητή προτεραιότητα ή δέσμευση πόρων για την κρίσιμη υπηρεσία.	Η SLICING_QOS_POLICY αποδίδει στην κλάση CRITICAL_TRAFFIC προτεραιότητα 30% μέσω της ρύθμισης priority percent 30.	Η κρίσιμη κίνηση αποκτά μηχανισμό προστασίας απέναντι στον ανταγωνισμό από best-effort ροές.
Δυνατότητα επαλήθευσης	Οι έλεγχοι δείχνουν μόνο βασική συνδεσιμότητα και δρομολόγηση, χωρίς διαφοροποίηση ανά υπηρεσία.	Οι show vlan brief, show access-lists και οι ρυθμίσεις class-map/policy-map τεκμηριώνουν τον διαχωρισμό και την επιβολή πολιτικής.	Η βελτίωση είναι αναπαραγώγιμη και συνδέεται με συγκεκριμένες ρυθμίσεις, όχι με γενική ποιοτική εκτίμηση.

Η σύγκριση είναι σκόπιμα λειτουργική. Δεν παρουσιάζεται τεχνητή αριθμητική βελτίωση καθυστέρησης ή απωλειών που δεν έχει μετρηθεί στο Packet Tracer. Το B0 αποτυγχάνει να επιβάλει απομόνωση και διαφοροποιημένη μεταχείριση, ενώ το S1 τις υλοποιεί με ρητούς και ελέγξιμους κανόνες. Άρα, το αποτέλεσμα της εφαρμογής είναι σαφές: πάνω στην ίδια φυσική τοπολογία δημιουργούνται λογικά όρια υπηρεσιών, ελεγχόμενη πρόσβαση και προτεραιότητα κρίσιμης κίνησης. Οι περιορισμοί του Packet Tracer ως προς το εγγενές 5G slicing έχουν ήδη διευκρινιστεί στο Κεφάλαιο 2.

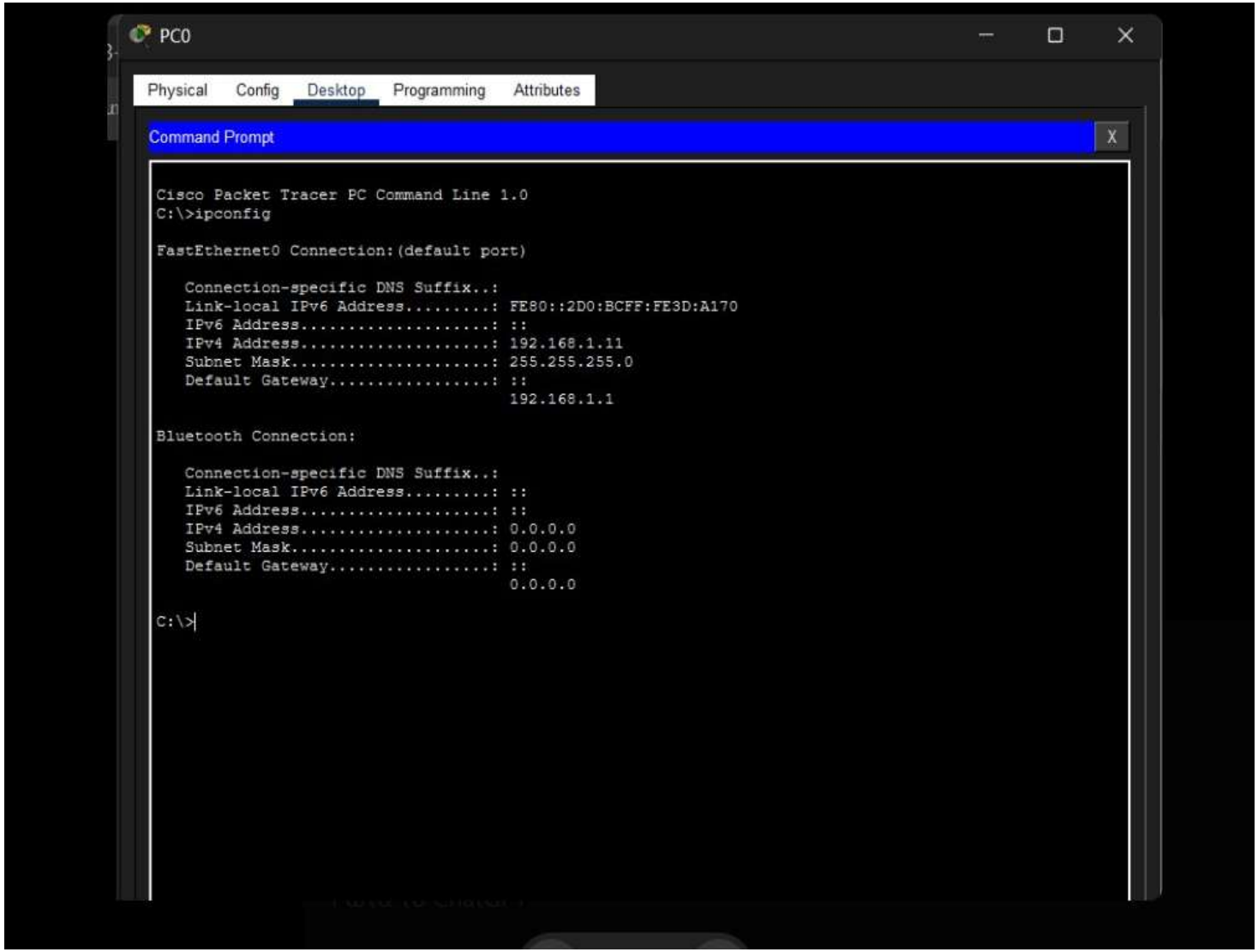
Συμπερασματικά, το ελαττωματικό πρότυπο B0 έχει συνδεσιμότητα αλλά δεν μπορεί να διαφοροποιήσει υπηρεσίες. Η S1 προσθέτει ακριβώς τους μηχανισμούς που λείπουν: VLAN για λογικά όρια, ACL για ελεγχόμενη απομόνωση και QoS για προτεραιοποίηση της κρίσιμης κίνησης. Η αξιολόγηση αυτή απαντά άμεσα στο ερώτημα τι επιτυγχάνει η εφαρμογή της λογικής διαμέρισης δικτύου στην εξεταζόμενη τοπολογία.

3.2.4 Στιγμιότυπα εκτέλεσης Packet Tracer και Mininet

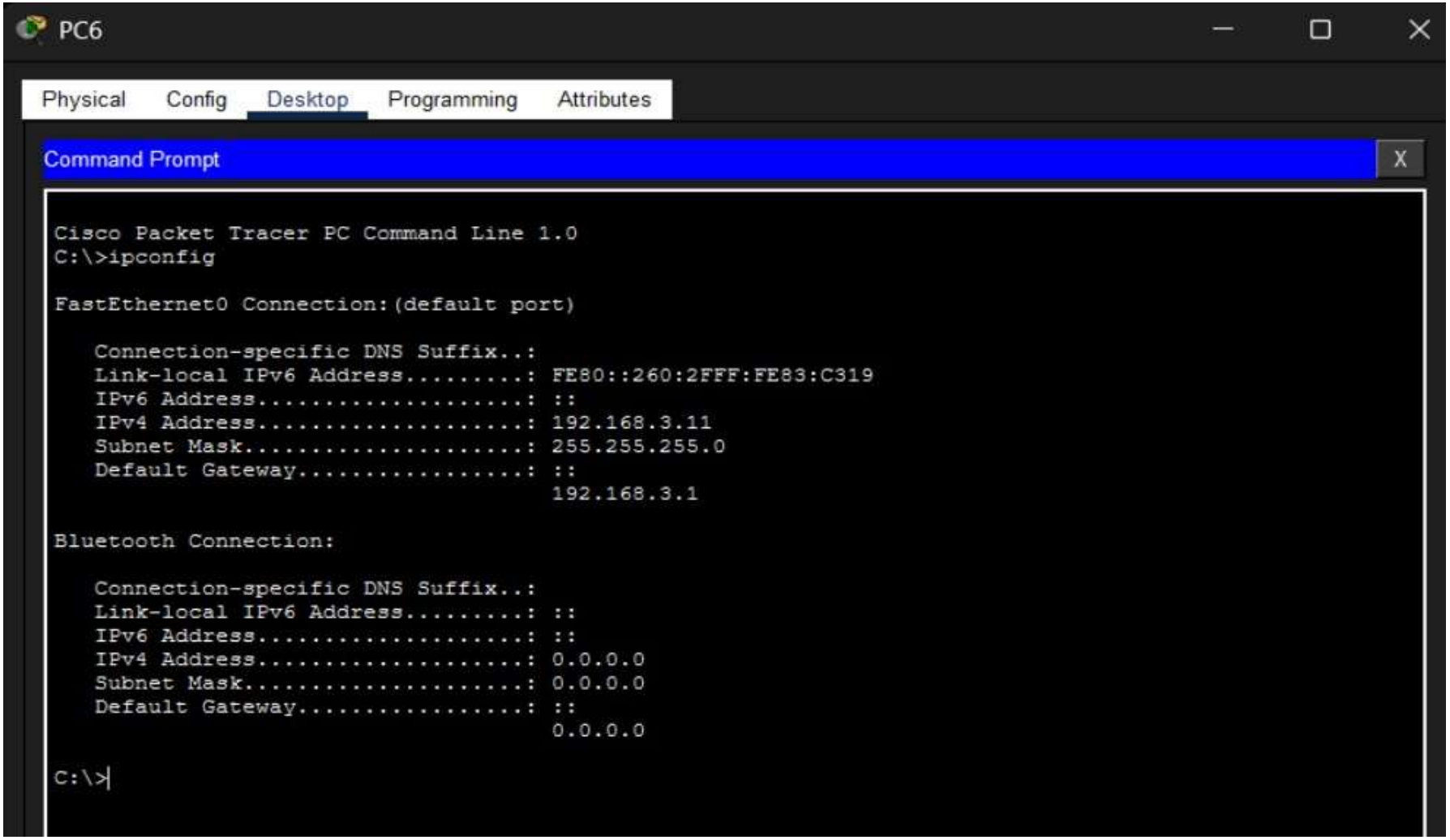
Στο παρόν υποκεφάλαιο παρουσιάζονται στιγμιότυπα από την εκτέλεση Packet Tracer και Mininet



Εικόνα 11: Παρουσιάζεται η τοπολογία που υλοποιήθηκε στο Cisco Packet Tracer, αποτελούμενη από τρία routers (R1, R2, R3), τρία switches (S1, S2, S3) και εννέα PCs (PC0–PC8), τα οποία κατανέμονται στα αντίστοιχα τμήματα του δικτύου.



Εικόνα 12: Παρουσιάζεται η IP configuration του PC0 μέσω της εντολής ipconfig, με διεύθυνση IPv4 192.168.1.11, μάσκα υποδικτύου 255.255.255.0 και προεπιλεγμένη πύλη 192.168.1.1.



Εικόνα 13: Παρουσιάζεται η IP configuration του PC6 μέσω της εντολής ipconfig, με διεύθυνση IPv4 192.168.3.11, μάσκα υποδικτύου 255.255.255.0 και προεπιλεγμένη πύλη 192.168.3.1.

```
C:\>ping 192.168.3.11

Pinging 192.168.3.11 with 32 bytes of data:

Reply from 192.168.3.11: bytes=32 time<1ms TTL=128
Reply from 192.168.3.11: bytes=32 time=7ms TTL=128
Reply from 192.168.3.11: bytes=32 time=3ms TTL=128
Reply from 192.168.3.11: bytes=32 time=3ms TTL=128

Ping statistics for 192.168.3.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 7ms, Average = 3ms

C:\>
```

Εικόνα 14: Αποτυπώνεται η επιτυχής εκτέλεση της εντολής ping προς τη διεύθυνση 192.168.3.11, επιβεβαιώνοντας τη δυνατότητα επικοινωνίας μεταξύ απομακρυσμένων hosts.

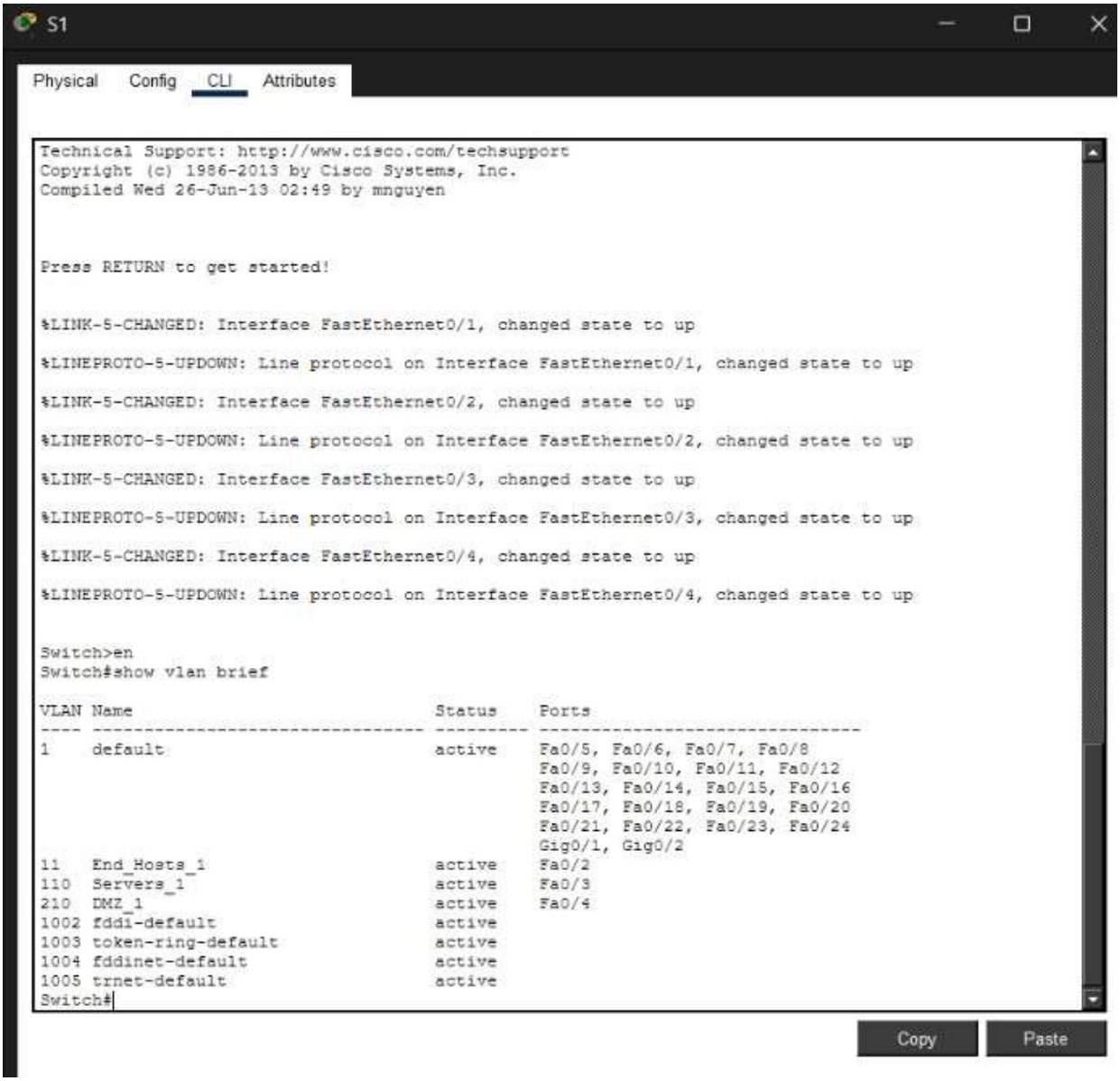
```
R1>en
R1#show access lists
R1#
R1#show access-lists
Standard IP access list Deny_Subnet
    10 deny 192.168.220.0 0.0.0.255
    20 permit any (96 match(es))
Standard IP access list Servers_Priority
    10 permit 192.168.10.0 0.0.0.255

R1#
```

Copy Paste

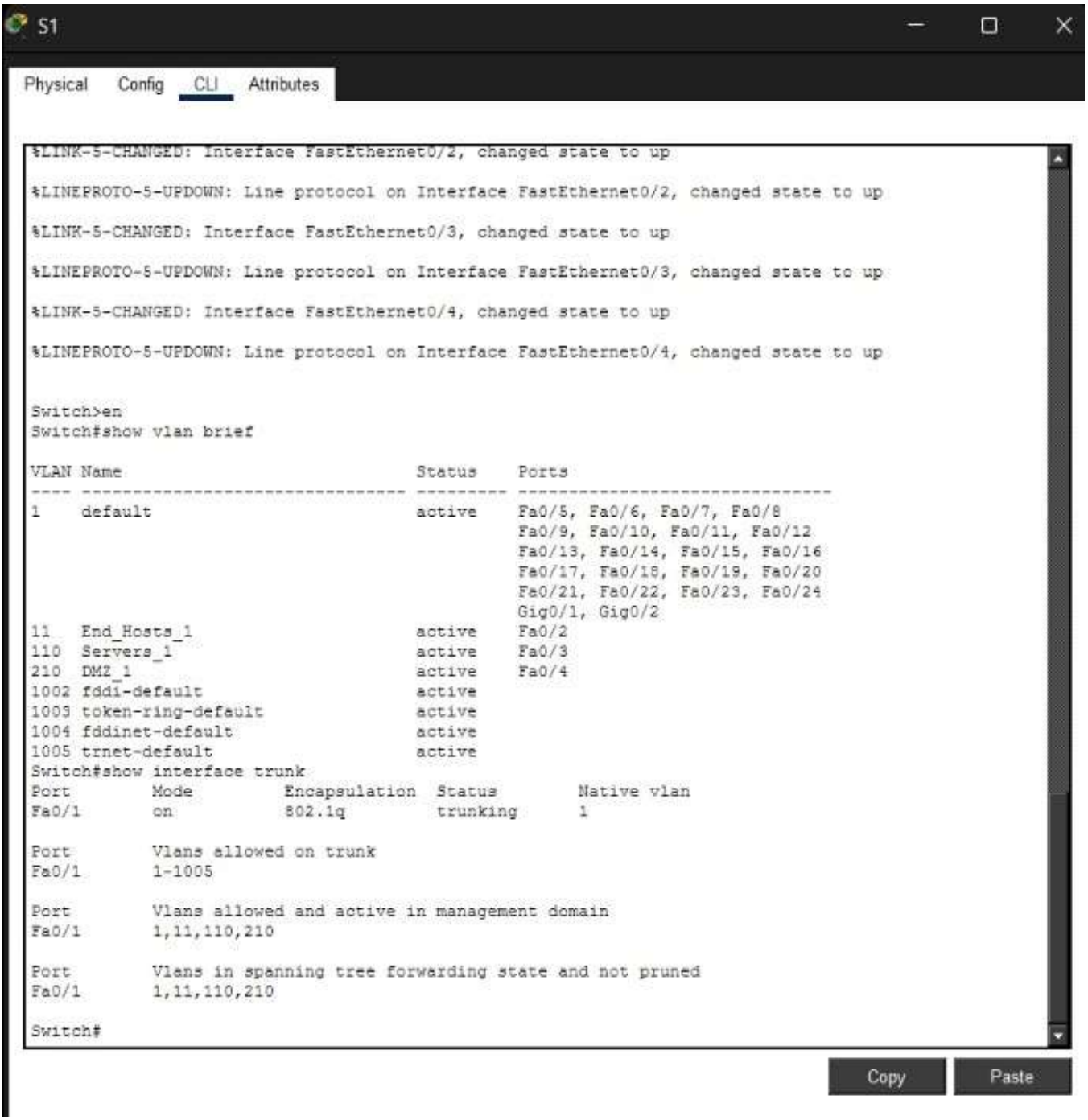
Εικόνα 15: Παρουσιάζεται η ACL Deny_Subnet στον router R1, η οποία περιλαμβάνει κανόνα απόρριψης για το υποδίκτυο 192.168.220.0/24 και κανόνα αποδοχής για την υπόλοιπη κίνηση.

```
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.11
 encapsulation dot1Q 11
 ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet0/0.110
 encapsulation dot1Q 110
 ip address 192.168.10.1 255.255.255.0
!
interface GigabitEthernet0/0.210
 encapsulation dot1Q 210
 ip address 192.168.210.1 255.255.255.0
!
interface GigabitEthernet0/1
 ip address 172.16.1.1 255.255.255.0
 ip access-group Deny_Subnet in
 duplex auto
 speed auto
!
interface GigabitEthernet0/2
 ip address 172.16.0.1 255.255.255.0
 ip access-group Deny_Subnet in
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
router ospf 1
 router-id 1.1.1.1
 log-adjacency-changes
 passive-interface GigabitEthernet0/0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.210.0 0.0.0.255 area 0
 network 172.16.0.0 0.0.0.255 area 0
 network 172.16.1.0 0.0.0.255 area 0
 network 192.168.1.0 0.0.0.255 area 0
!
ip classless
```

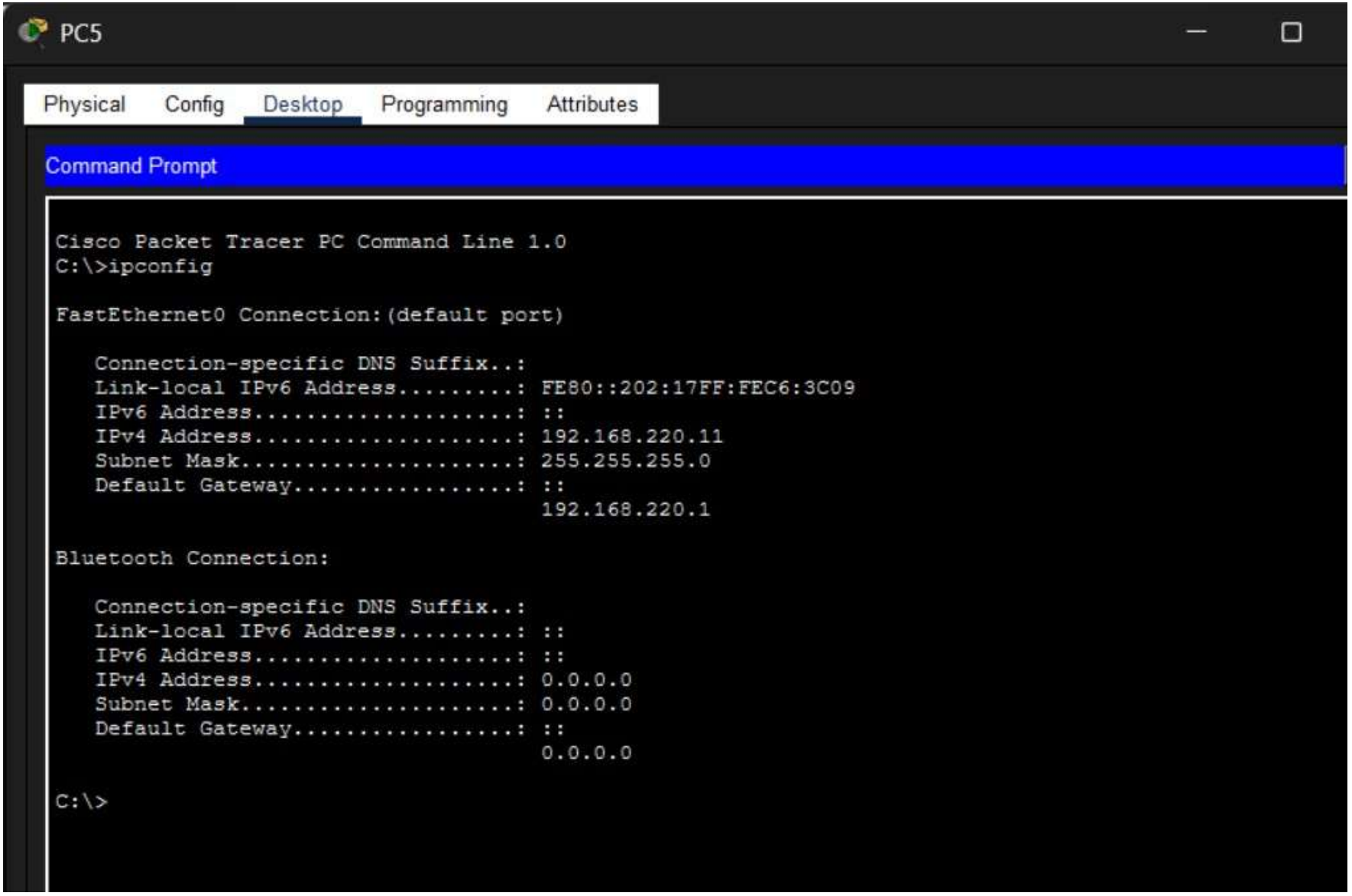
Εικόνα 16: Παρουσιάζεται τμήμα της διαμόρφωσης του router R1, με τις αντίστοιχες δικτυακές διεπαφές και τις ρυθμίσεις του πρωτοκόλλου OSPF.



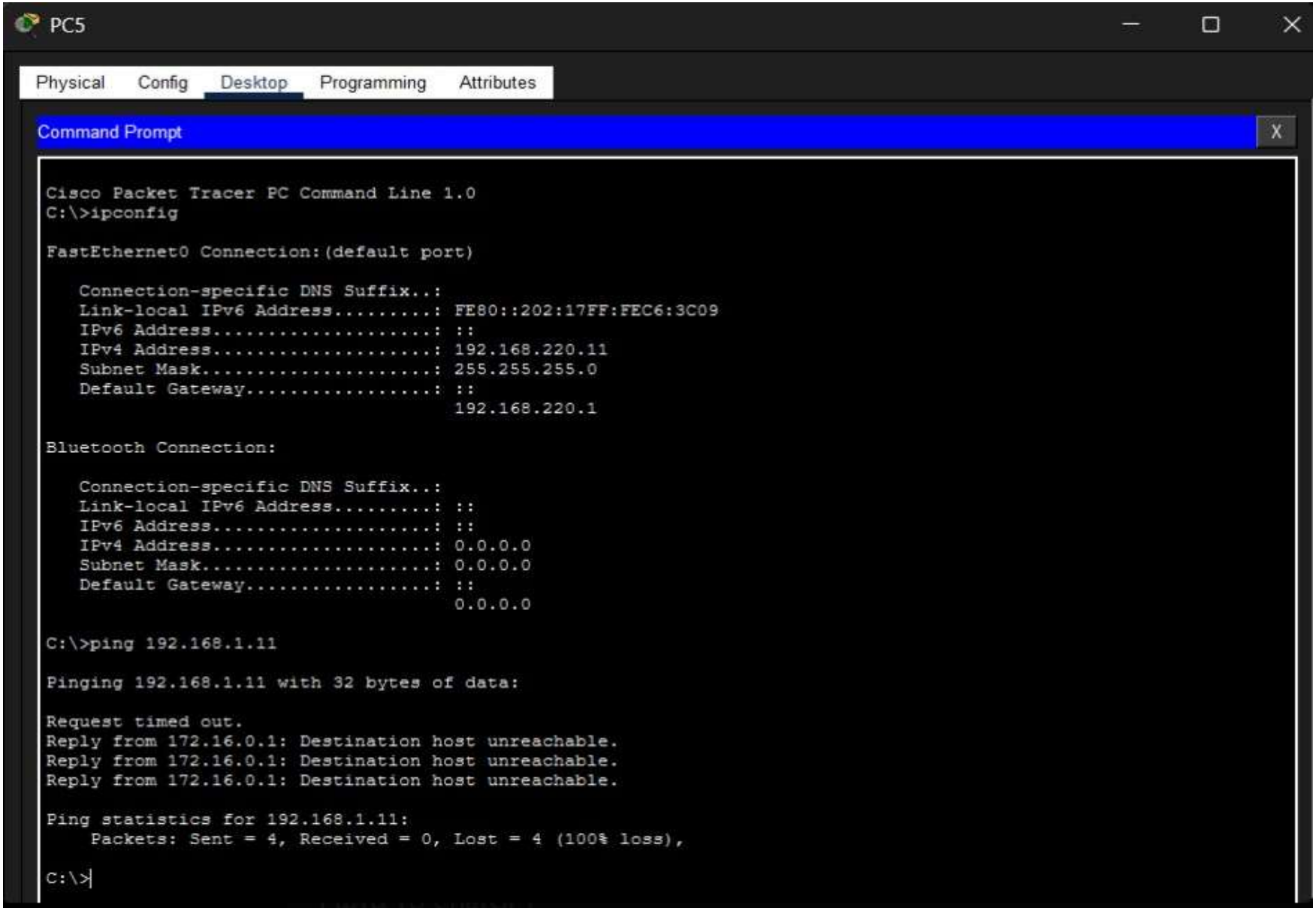
Εικόνα 17: Παρουσιάζεται η διαμόρφωση των VLANs στο switch S1 μέσω της εντολής show vlan brief, με την εμφάνιση των ενεργών VLANs και των αντίστοιχων access ports.



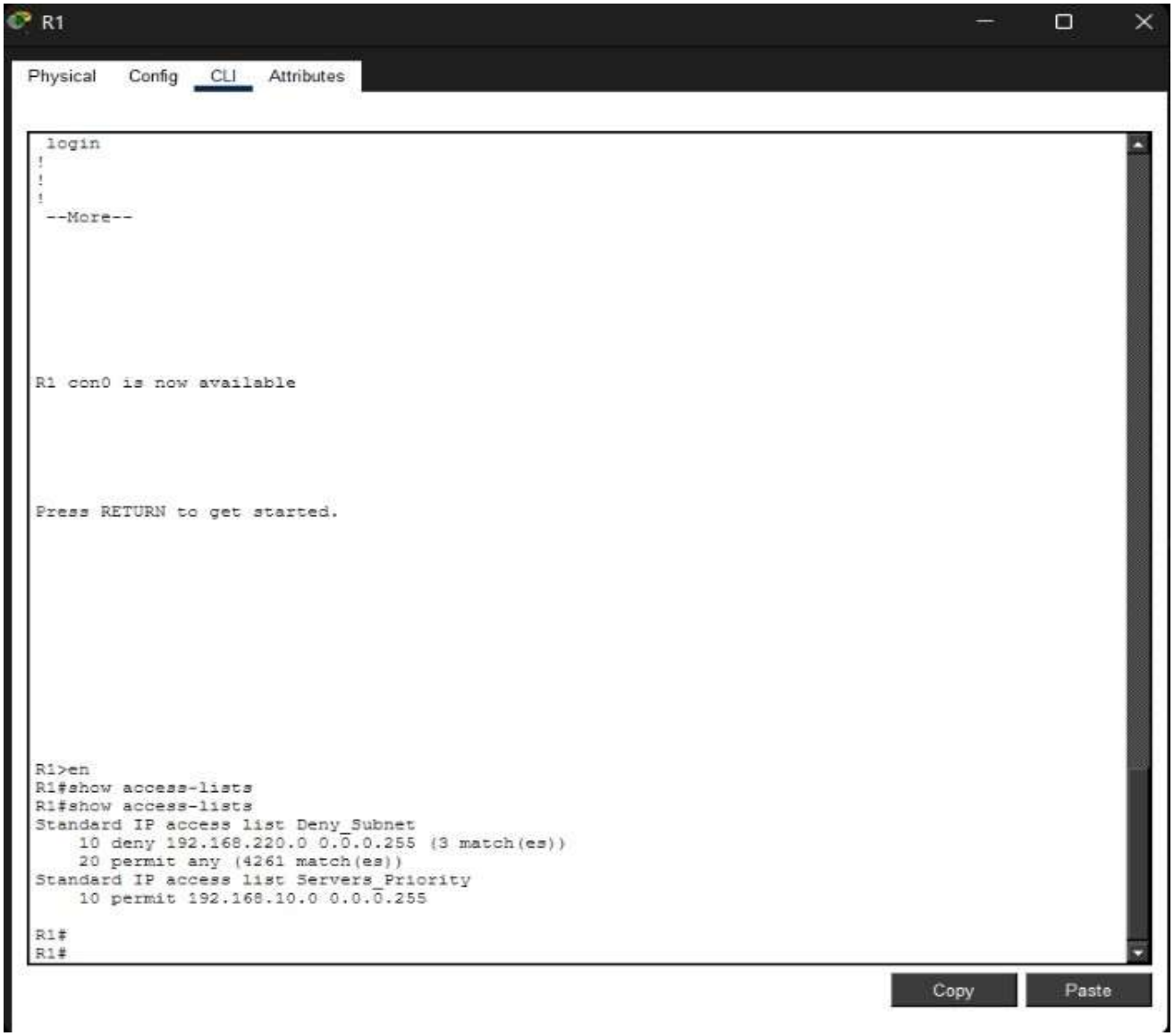
Εικόνα 18: Παρουσιάζεται η trunk σύνδεση στο switch S1 μέσω της εντολής show interfaces trunk, με την εμφάνιση της κατάστασης της σύνδεσης και των αντίστοιχων VLANs.



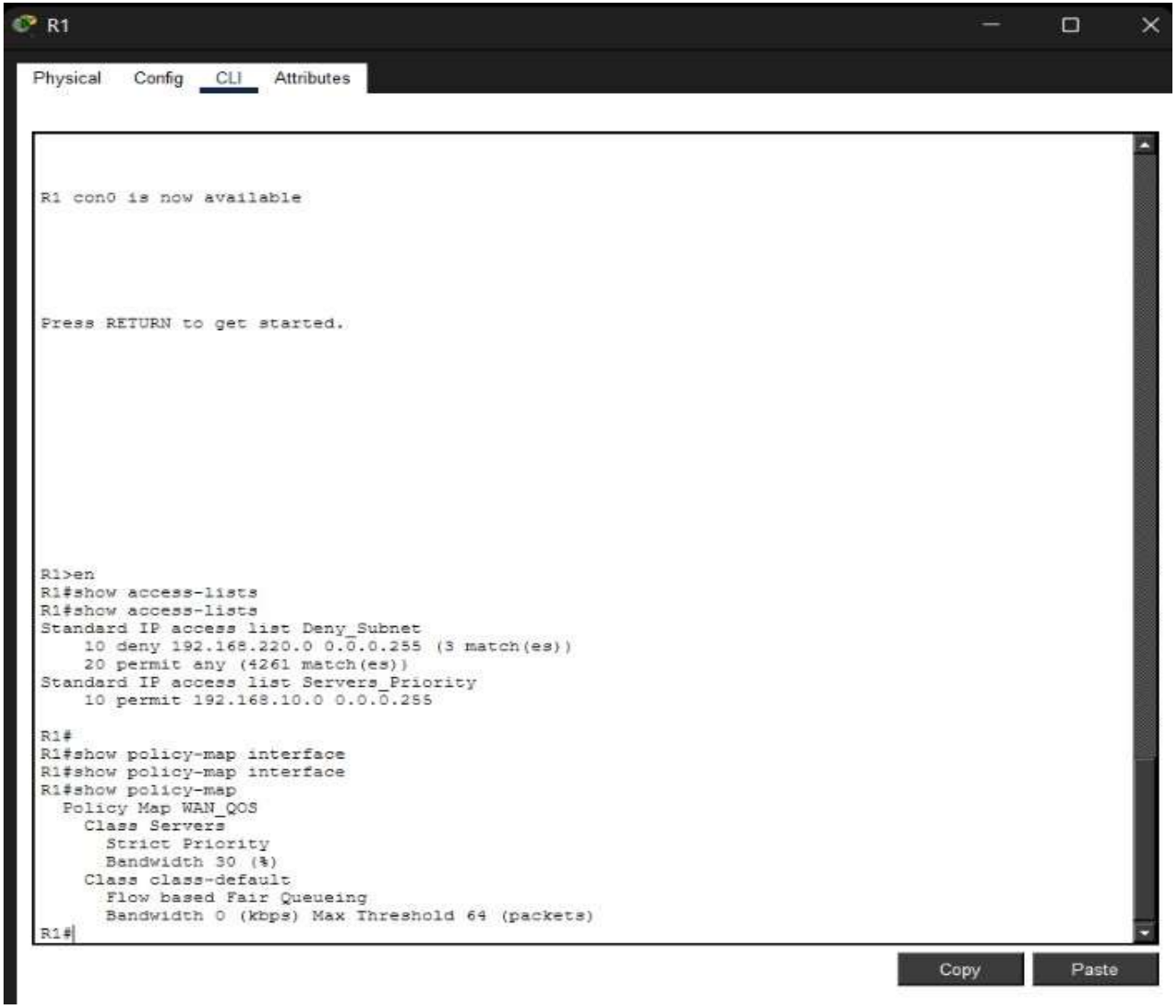
Εικόνα 19: Εμφανίζεται η IP configuration του PC5, με διεύθυνση 192.168.220.11/24 και προεπιλεγμένη πύλη 192.168.220.1, πριν από τη δοκιμή επικοινωνίας.



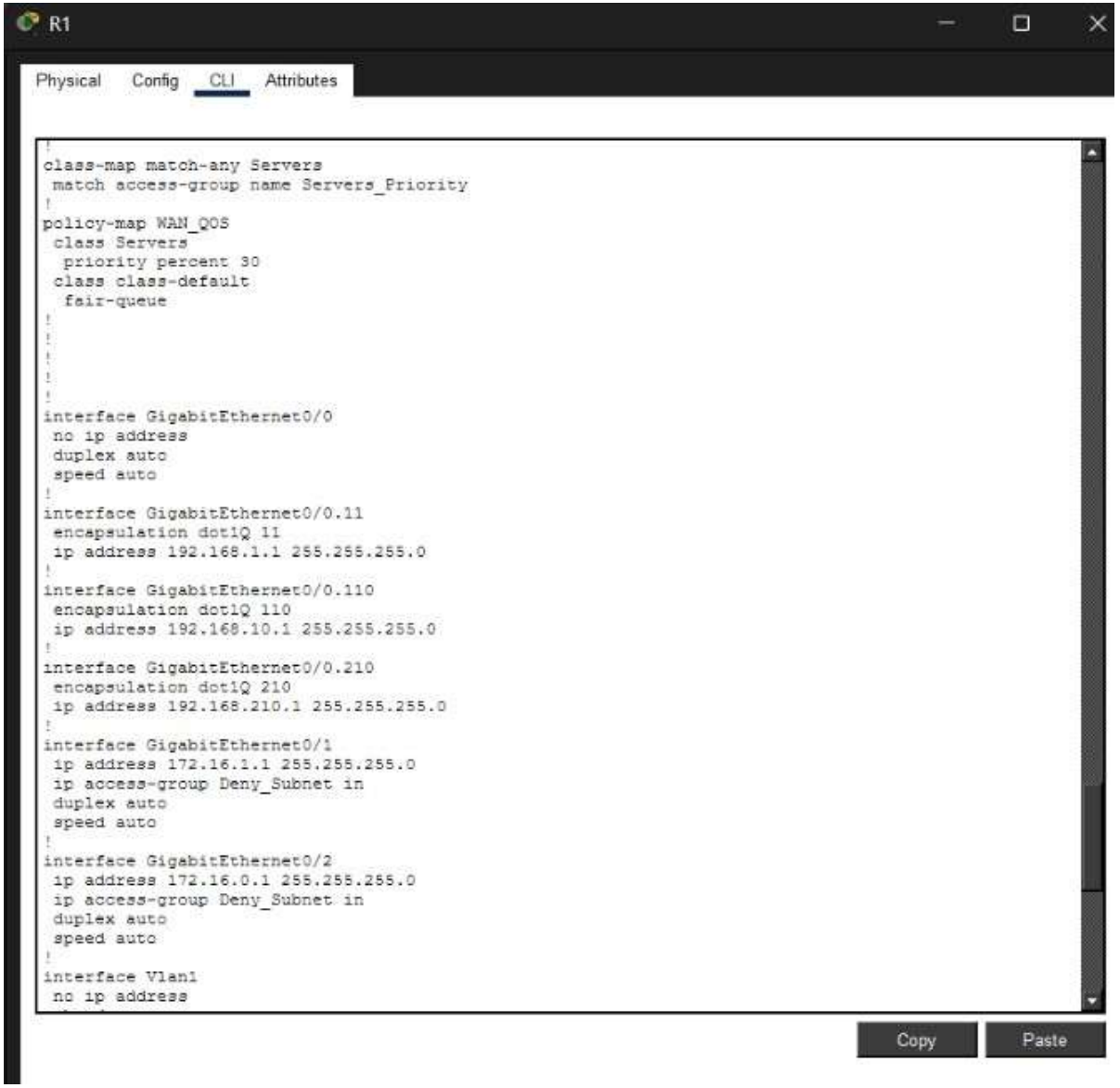
Εικόνα 20: Παρουσιάζεται η αποτυχημένη προσπάθεια επικοινωνίας από το PC5 προς το PC0 μέσω της εντολής ping, με απώλεια πακέτων 100%, ως αποτέλεσμα της εφαρμοσμένης πολιτικής πρόσβασης



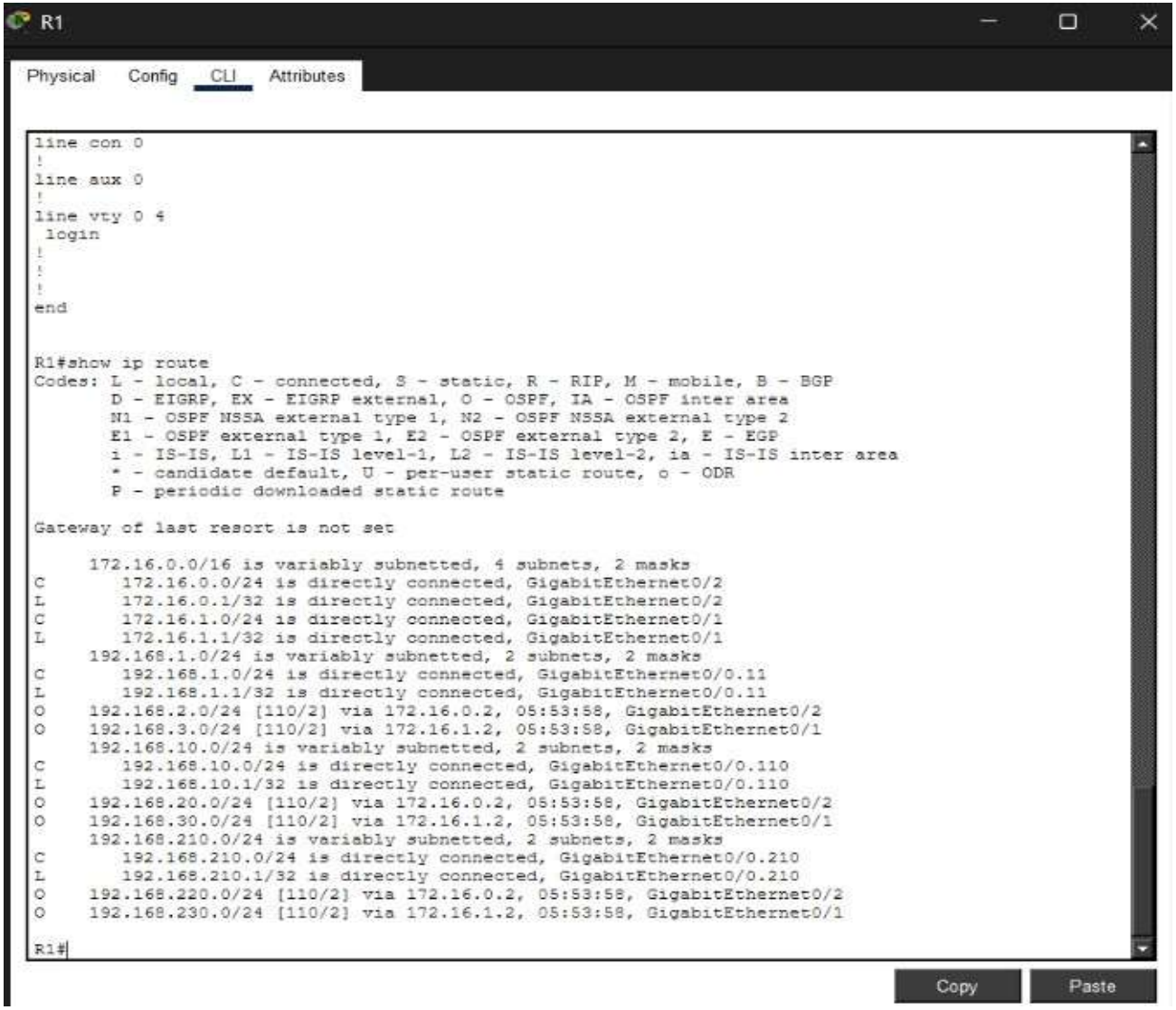
Εικόνα 21: Εμφανίζονται οι μετρητές της ACL Deny_Subnet στον router R1, καταγράφοντας τις αντιστοιχίσεις του κανόνα απόρριψης για το υποδίκτυο 192.168.220.0/24



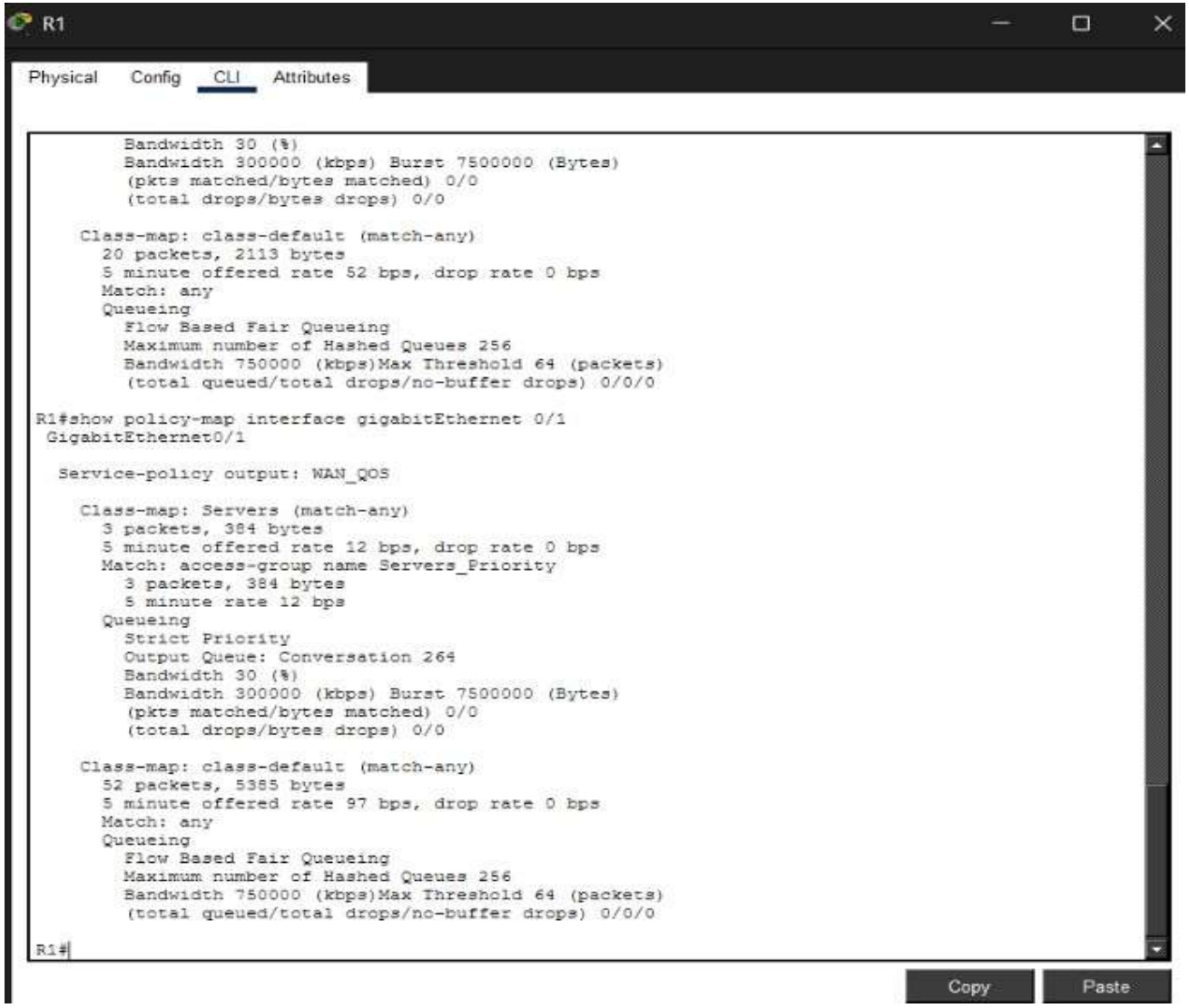
Εικόνα 22: Παρουσιάζεται η πολιτική WAN_QOS στον router R1 μέσω της εντολής show policy-map interface, με την εμφάνιση των κλάσεων κίνησης και των αντίστοιχων ρυθμίσεων προτεραιότητας.



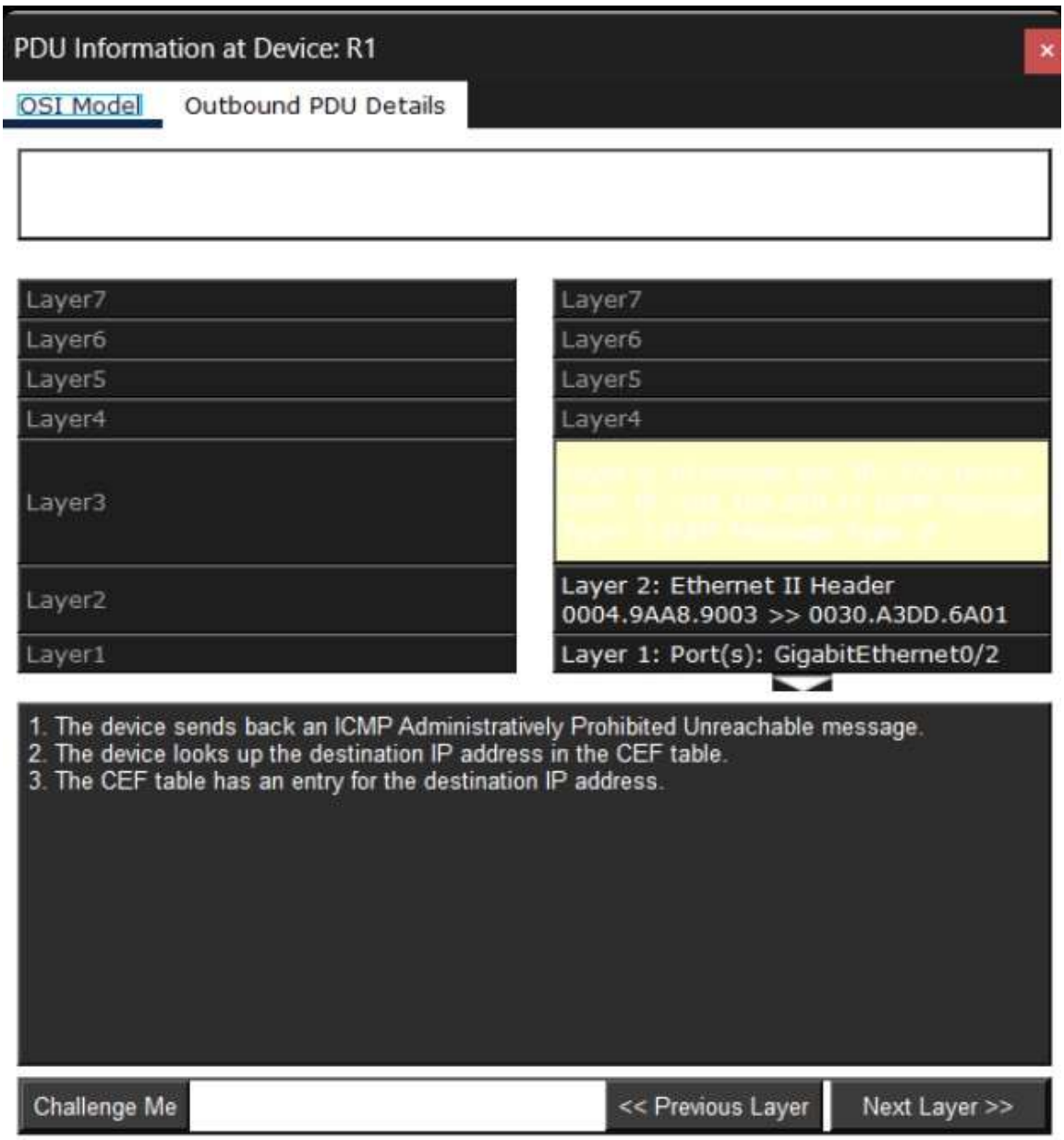
Εικόνα 23: Παρουσιάζεται τμήμα της διαμόρφωσης του router R1, στο οποίο εμφανίζεται η πολιτική WAN_QOS με προτεραιότητα 30% για την κλάση Servers, καθώς και οι ρυθμίσεις των δικτυακών interfaces.



Εικόνα 24: Παρουσιάζεται ο πίνακας δρομολόγησης του router R1 μέσω της εντολής show ip route, όπου εμφανίζονται τα απευθείας συνδεδεμένα δίκτυα και οι διαδρομές που έχουν αποκτηθεί μέσω OSPF



Εικόνα 25: Μέσω της εντολής show policy-map interface gigabitEthernet 0/1 επιβεβαιώνεται η εφαρμογή της WAN_QOS στο εξερχόμενο interface του R1, με καταγραφή πακέτων στις κλάσεις Servers και class-default



Εικόνα 26: Παρουσιάζεται η απόρριψη του ICMP (Internet Control Message Protocol) πακέτου στον router R1, με την εμφάνιση του μηνύματος Administratively Prohibited Unreachable (Type 3, Code 13), επιβεβαιώνοντας τη λειτουργία της ACL.

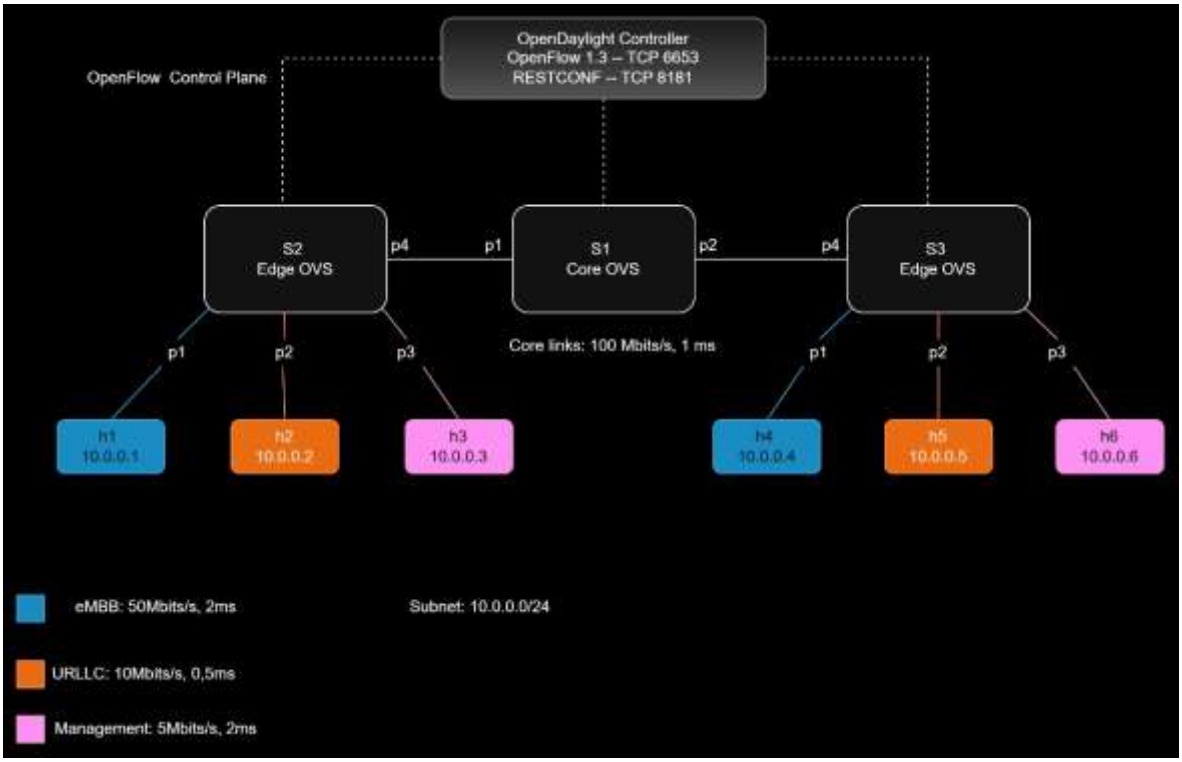
3.3 *Προγραμματιζόμενη προώθηση με Mininet/OVS και OpenDaylight: χωρίς και με ενεργή πολιτική SDN*

Το πείραμα της ενότητας εξετάζει αν ένας ελεγκτής SDN μπορεί να επιβάλει με κανόνες OpenFlow την ίδια λογική απομόνωσης που υλοποιήθηκε στο Packet Tracer με VLAN και ACL. Το Mininet δημιουργεί τους υπολογιστές-ξενιστές και τις ζεύξεις, οι μεταγωγείς Open vSwitch εκτελούν την προώθηση και ο OpenDaylight δέχεται την πολιτική μέσω RESTCONF και την εγκαθιστά στους μεταγωγείς. Για την εγκατάσταση του OpenDaylight και τη σύνδεσή του με το Mininet ακολουθήθηκε η διαδικασία που περιγράφεται στο [32], ενώ η τοπολογία, η πολιτική και ο τρόπος επαλήθευσης σχεδιάστηκαν για την παρούσα εργασία.

Το πείραμα διαφοροποιείται από το [32] σε τέσσερα σημεία. Πρώτον, αντί για τις γενικές τοπολογίες δέντρου και spine–leaf που εξετάζονται στο [32], χρησιμοποιείται τοπολογία με τρεις διαμερίσεις, eMBB, URLLC και διαχείρισης, που αντιστοιχούν στα VLAN 110, 210 και 11 του Packet Tracer. Δεύτερον, στο [32] οι κανόνες ροής στοχεύουν στην πλήρη συνδεσιμότητα όλων των υπολογιστών, με πλημμύρα πακέτων ή απλή προώθηση μεταξύ θυρών, ενώ εδώ η πολιτική επιτρέπει την επικοινωνία μόνο εντός κάθε διαμέρισης και απορρίπτει ρητά την κίνηση μεταξύ διαμερίσεων. Η επιτυχία του πειράματος κρίνεται επομένως από την απομόνωση και όχι μόνο από τη συνδεσιμότητα. Τρίτον, οι κανόνες δεν συντάσσονται ένας προς έναν σε αρχεία ούτε αποστέλλονται χειροκίνητα με curl, όπως στο [32], αλλά παράγονται από πρόγραμμα Python με βάση τον ορισμό των διαμερίσεων και αποστέλλονται στο RESTCONF του OpenDaylight· το ίδιο πρόγραμμα αφαιρεί την πολιτική και επαναφέρει το δίκτυο στην κατάσταση αναφοράς. Τέταρτον, οι ζεύξεις πρόσβασης κάθε διαμέρισης έχουν διαφορετικό εύρος ζώνης και καθυστέρηση, ενώ η αξιολόγηση στηρίζεται στον πίνακα επικοινωνίας του pingall και στους μετρητές τόσο των επιτρεπτικών κανόνων όσο και του κανόνα απόρριψης.

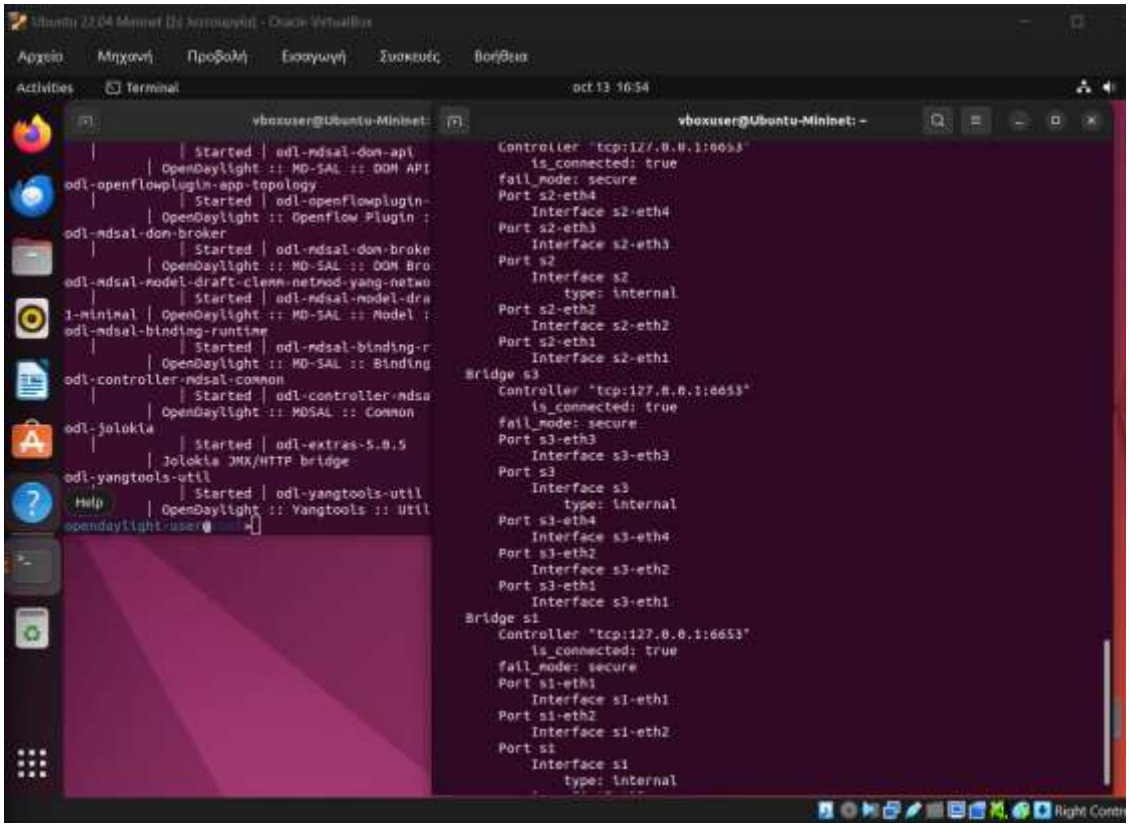
3.3.1 Ελαττωματικό πρότυπο αναφοράς: συνδεδεμένος controller χωρίς κανόνες προώθησης

Η τοπολογία της Εικόνας 27 αποτελείται από τον κεντρικό μεταγωγέα s1 και τους ακραίους μεταγωγείς s2 και s3. Σε κάθε ακραίο μεταγωγέα συνδέεται ένας υπολογιστής ανά διαμέριση: οι h1 και h4 ανήκουν στην eMBB, οι h2 και h5 στην URLLC και οι h3 και h6 στη διαμέριση διαχείρισης. Όλοι οι υπολογιστές βρίσκονται στο υποδίκτυο 10.0.0.0/24, ώστε ο διαχωρισμός να μην προκύπτει από τη διευθυνσιοδότηση, αλλά αποκλειστικά από την πολιτική του ελεγκτή. Οι ζεύξεις πρόσβασης ορίζονται στα 50 Mbit/s για την eMBB, στα 10 Mbit/s με καθυστέρηση 0,5 ms για την URLLC και στα 5 Mbit/s για τη διαχείριση, ενώ οι ζεύξεις κορμού στα 100 Mbit/s. Οι πίνακες ARP των υπολογιστών συμπληρώνονται στατικά, ώστε κάθε αποτυχία επικοινωνίας να οφείλεται στους κανόνες ροής και όχι στην επίλυση διευθύνσεων. Ο κώδικας της τοπολογίας και της πολιτικής παρατίθεται στο Παράρτημα Ι.4.

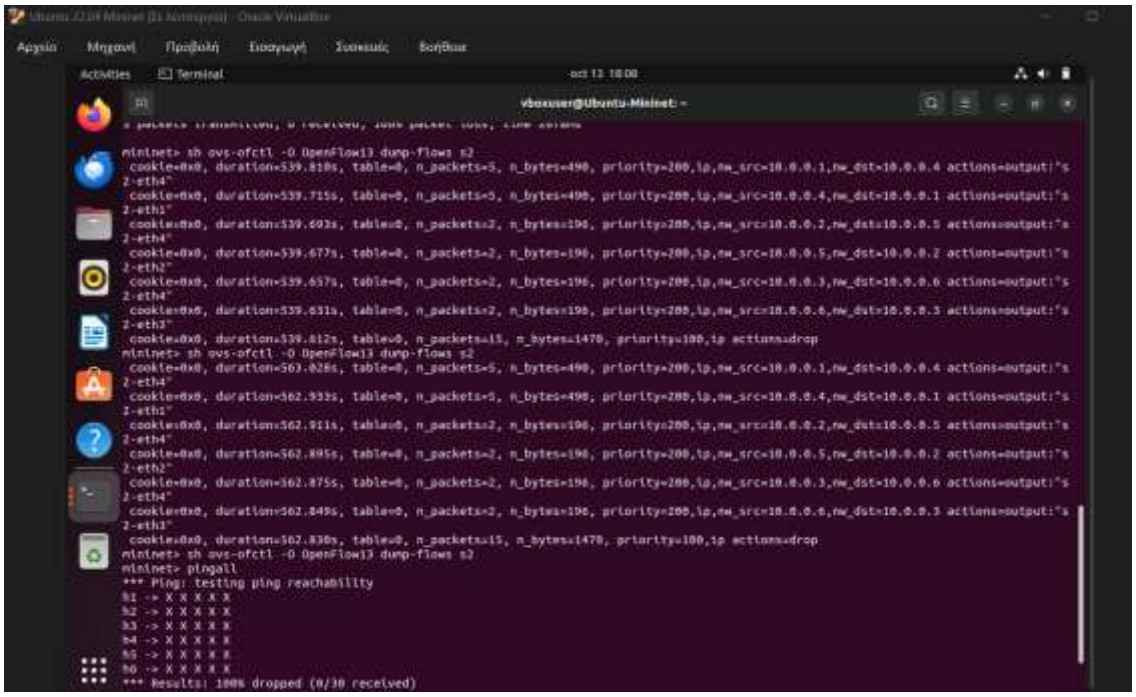


Εικόνα 27: Τοπολογία του πειράματος με τρεις διαμερίσεις πάνω στην ίδια υποδομή Open vSwitch (ίδια επεξεργασία, μεθοδολογική αναφορά από την [32]).

Στην κατάσταση αναφοράς M0 οι τρεις μεταγωγείς συνδέονται στον OpenDaylight με OpenFlow 1.3 στη θύρα 6653 και λειτουργούν σε ασφαλή κατάσταση αστοχίας, δηλαδή δεν μετατρέπονται σε αυτόνομους μεταγωγείς μάθησης όταν δεν υπάρχουν κανόνες. Η Εικόνα 28 δείχνει ότι το κανάλι ελέγχου είναι ενεργό και στους τρεις μεταγωγείς. Επειδή στον ελεγκτή δεν έχει εγκατασταθεί εφαρμογή προώθησης, ο πίνακας ροών του s2 δεν περιέχει κανόνα για την κίνηση IPv4 και το pingall αποτυγχάνει και στις 30 δοκιμές (Εικόνα 29). Η αποτυχία απομονώνει το πρόβλημα που εξετάζεται: η σύνδεση με τον ελεγκτή δεν αρκεί όταν δεν υπάρχει πολιτική προώθησης.



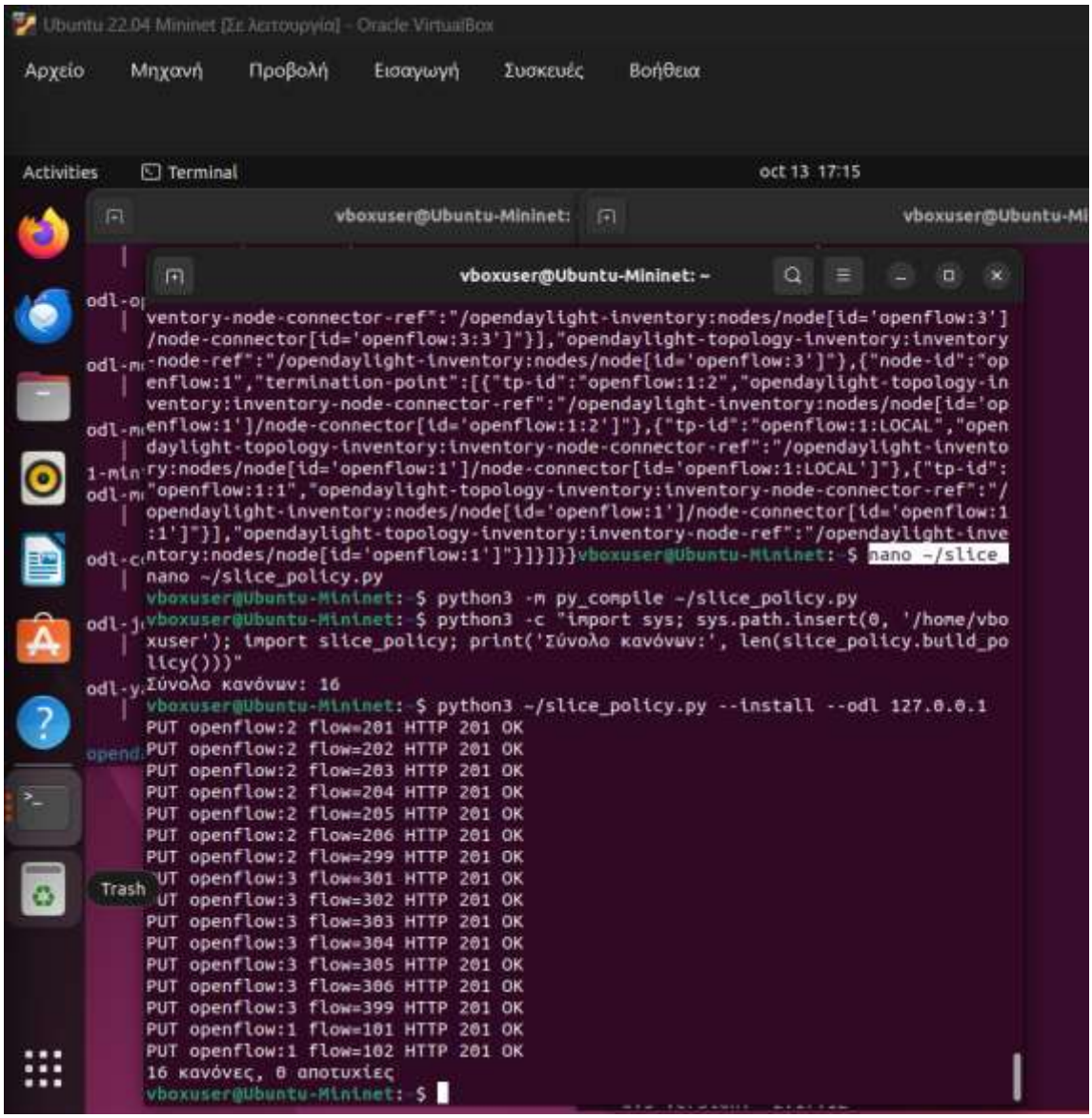
Εικόνα 28: Σύνδεση των μεταγωγέων s1–s3 με τον OpenDaylight στην κατάσταση M0 (is_connected: true).



Εικόνα 29: Κατάσταση M0: πίνακας ροών του s2 χωρίς κανόνα IPv4 και αποτυχία του pingall (100% απώλεια).

3.3.2 Διορθωτική παρέμβαση: εγκατάσταση κανόνων OpenFlow από τον controller

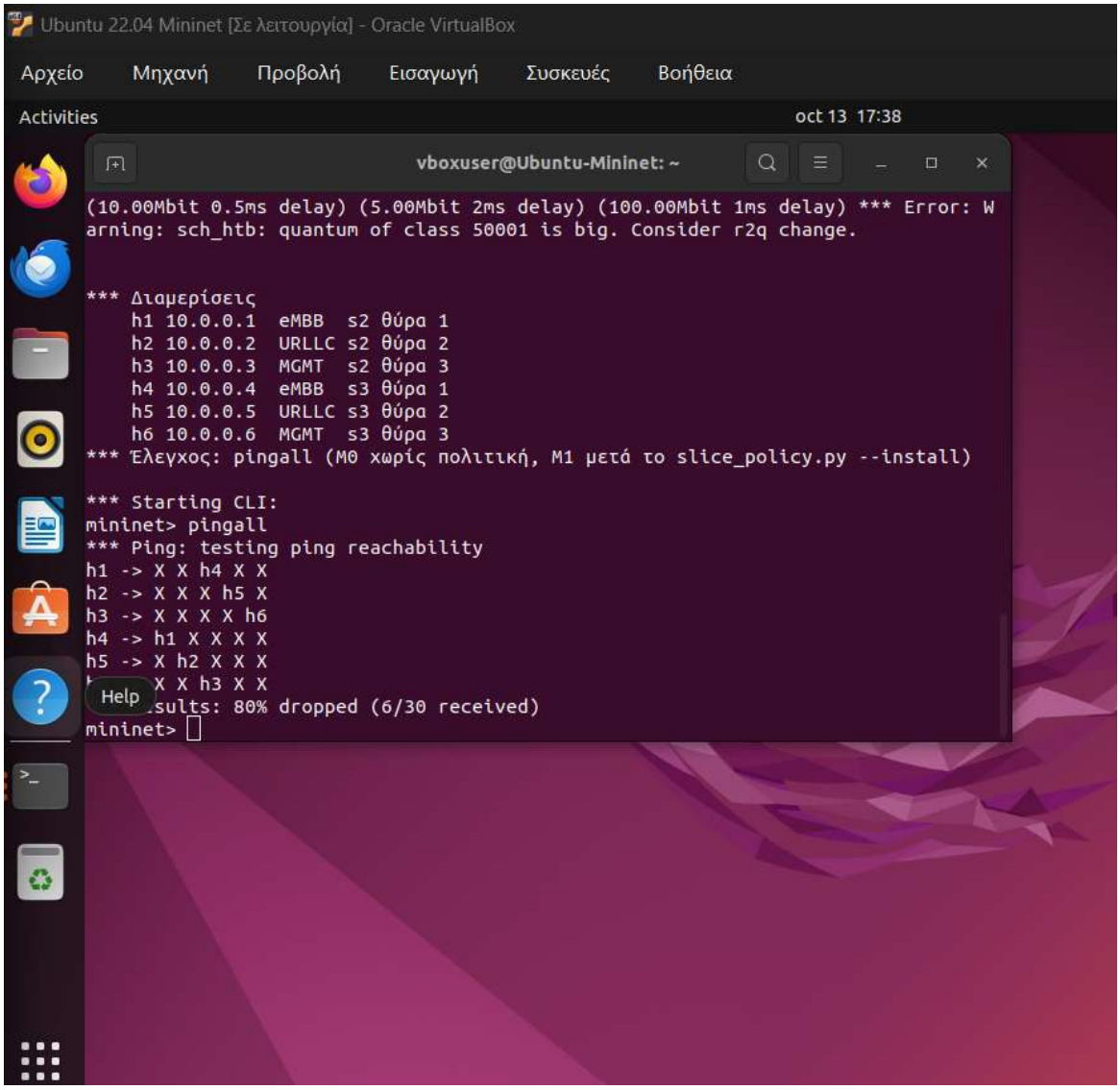
Στην κατάσταση M1 η πολιτική παράγεται από το πρόγραμμα slice_policy.py, το οποίο δημιουργεί δεκαέξι κανόνες από τον ορισμό των διαμερίσεων. Σε κάθε ακραίο μεταγωγέα εγκαθίστανται έξι κανόνες προτεραιότητας 200, που προωθούν την κίνηση IPv4 μόνο όταν η πηγή και ο προορισμός ανήκουν στην ίδια διαμέριση, και ένας κανόνας προτεραιότητας 100, που απορρίπτει κάθε άλλη κίνηση IPv4. Ο κεντρικός μεταγωγέας δέχεται δύο κανόνες διέλευσης, επειδή η πολιτική επιβάλλεται στα άκρα του δικτύου. Οι κανόνες αποστέλλονται με αιτήσεις PUT στο RESTCONF του OpenDaylight, ο οποίος τους εγκαθιστά στους μεταγωγείς (Εικόνα 30).



Εικόνα 30: Εγκατάσταση των 16 κανόνων της πολιτικής M1 μέσω RESTCONF από το πρόγραμμα slice_policy.py.

Μετά την εγκατάσταση, το ίδιο pingall δεν δίνει πλήρη συνδεσιμότητα, αλλά τον αναμενόμενο πίνακα επικοινωνίας: κάθε υπολογιστής φτάνει μόνο τον ομόλογό του στην ίδια διαμέριση, οπότε επιτυγχάνουν 6 από τις 30 δοκιμές και η απώλεια είναι 80% (Εικόνα 31). Το ποσοστό αυτό δεν

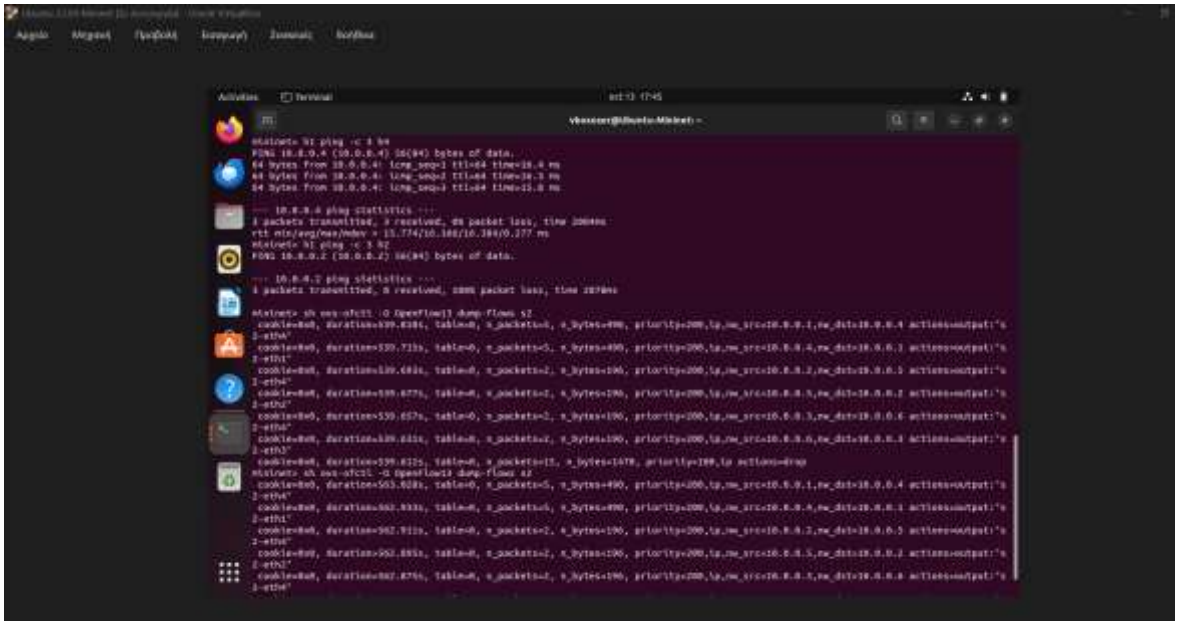
αποτελεί αστοχία, αλλά την ποσοτική έκφραση της απομόνωσης, αφού οι 24 αποτυχημένες δοκιμές αντιστοιχούν ακριβώς στα ζεύγη υπολογιστών διαφορετικών διαμερίσεων.



Εικόνα 31: Κατάσταση M1: πίνακας επικοινωνίας του pingall με επιτυχία μόνο εντός των διαμερίσεων (6/30).

3.3.3 Λειτουργική επαλήθευση και αξιολόγηση

Η επαλήθευση στηρίζεται στους μετρητές του πίνακα ροών του s2, όπως εμφανίζονται με την εντολή ovs-ofctl -O OpenFlow13 dump-flows s2. Μετά από ping του h1 προς τον h4, που ανήκουν στην eMBB, αυξάνονται οι μετρητές των κανόνων h1→h4 και h4→h1. Μετά από ping του h1 προς τον h2, που ανήκει στην URLLC, αυξάνεται μόνο ο μετρητής του κανόνα απόρριψης (Εικόνα 32). Έτσι επιβεβαιώνεται όχι μόνο ότι οι κανόνες υπάρχουν, αλλά και ότι κάθε πακέτο ταξινομείται από τον κανόνα που προβλέπει η πολιτική.



Εικόνα 32: Μετρητές του πίνακα ροών του s2 στην κατάσταση M1 μετά από κίνηση εντός και μεταξύ διαμερίσεων.

Η σύγκριση M0–M1 αναδεικνύει και έναν περιορισμό. Η κεντρικοποίηση του ελέγχου δεν εγγυάται από μόνη της σωστή λειτουργία, αφού το αποτέλεσμα εξαρτάται από την ορθότητα των κανόνων: αν ο κανόνας απόρριψης είχε μεγαλύτερη προτεραιότητα από τους επιτρεπτικούς, θα απέκοπτε και την κίνηση εντός των διαμερίσεων. Γι' αυτό η αξιολόγηση συνδυάζει τον πίνακα επικοινωνίας με την άμεση επιθεώρηση των μετρητών. Επιπλέον, το πείραμα επαληθεύει την απομόνωση και όχι την απόδοση· οι παράμετροι των ζεύξεων πρόσβασης ορίζουν το περιβάλλον κάθε διαμέρισης, χωρίς να παρουσιάζονται μετρήσεις ρυθμού μετάδοσης.

Συμπερασματικά, στο M0 ο ελεγκτής είναι συνδεδεμένος αλλά καμία κίνηση δεν προωθείται, ενώ στο M1 η ίδια τοπολογία αποκτά επικοινωνία εντός των διαμερίσεων και ελεγχόμενη απόρριψη μεταξύ τους. Η συμβολή του SDN τεκμηριώνεται έτσι από μια συγκεκριμένη και μετρήσιμη αλλαγή συμπεριφοράς, που αντιστοιχεί λειτουργικά στην ACL Deny_Subnet του Packet Tracer, με τη διαφορά ότι εδώ η πολιτική ορίζεται μία φορά κεντρικά και εγκαθίσταται αυτόματα σε όλους τους μεταγωγείς.

3.4 Δυναμική διαχείριση πόρων με Python: στατική έναντι προσαρμοστικής πολιτικής

3.4.1 Ελαττωματικό πρότυπο αναφοράς: σταθερή κατανομή πόρων

Ως κατάσταση αναφοράς P0 θεωρείται μία υπηρεσία με σταθερό αριθμό αντιγράφων. Σε αυτή την κατάσταση η κατανομή δεν αλλάζει όταν η καθυστέρηση ξεπεράσει το όριο SLA και επίσης δεν μειώνεται όταν το φορτίο είναι χαμηλό. Η υπηρεσία μπορεί να παραμένει λειτουργική, αλλά η πολιτική δεν αντιδρά στην κατάσταση του συστήματος: είτε διατηρεί ανεπαρκείς πόρους σε περίοδο πίεσης είτε κρατά περισσότερους πόρους από όσους χρειάζονται σε χαμηλό φορτίο.

3.4.2 Διορθωτική παρέμβαση: βρόχος ελέγχου με βάση SLA και χρήση CPU

Στην κατάσταση P1 εφαρμόζεται ο παρακάτω βρόχος Python. Το όριο της 95ης εκατοστιαίας τιμής καθυστέρησης τίθεται στα 200 ms. Αν το p95 υπερβεί το όριο, η πολιτική αυξάνει τα αντίγραφα (replicas) κατά δύο, μέχρι το μέγιστο των 20. Αν η καθυστέρηση πέσει κάτω από το 60% του ορίου και η χρήση CPU είναι μικρότερη από 30%, μειώνει τα αντίγραφα κατά ένα, μέχρι το ελάχιστο του ενός. Σε κάθε άλλη περίπτωση διατηρεί την τρέχουσα κατανομή. Η λογική είναι ντετερμινιστική και επομένως μπορεί να ελεγχθεί με συγκεκριμένα διανύσματα εισόδου.

```
import time
import requests

PROM_URL = "http://prometheus-server.monitoring.svc:9090"
SLA_P95_MS = 200.0
MIN_REPLICAS, MAX_REPLICAS = 1, 20

def prom_query(query: str) -> float:
    r = requests.get(f"{PROM_URL}/api/v1/query", params={"query": query}, timeout=5)
    r.raise_for_status()
    result = r.json()["data"]["result"]
    return float(result[0]["value"][1]) if result else 0.0

def decide_replicas(current: int, p95_ms: float, util: float) -> int:
    if p95_ms > SLA_P95_MS:
        return min(current + 2, MAX_REPLICAS)
    if p95_ms < 0.6 * SLA_P95_MS and util < 30.0:
        return max(current - 1, MIN_REPLICAS)
    return current

def scale_k8s(deployment: str, namespace: str, replicas: int) -> None:
    # Ενδεικτικό σημείο κλήσης του Kubernetes API.
    print(f"[ACTION] scale {namespace}/{deployment} -> {replicas} replicas")

if __name__ == "__main__":
    deployment, namespace = "inference-service", "ml-inference"
    current_replicas = 4
    while True:
        p95_latency = prom_query(
            "histogram_quantile(0.95,
sum(rate(http_request_duration_seconds_bucket[2m])) by (le))"
        ) * 1000
        cpu_util = prom_query(
            "avg(rate(container_cpu_usage_seconds_total[2m])) * 100"
        )
        target = decide_replicas(current_replicas, p95_latency, cpu_util)
        if target != current_replicas:
            scale_k8s(deployment, namespace, target)
            current_replicas = target
        time.sleep(30)
```

Κώδικας 3.4: Μηχανισμός προσαρμοστικής κλιμάκωσης με Python, με είσοδο p95 καθυστέρηση και χρήση CPU και έξοδο τον επιθυμητό αριθμό replicas.

3.4.3 Λειτουργική επαλήθευση και αξιολόγηση της πολιτικής

Για να αξιολογηθεί η λογική χωρίς να παρουσιαστούν ως πραγματικές μετρήσεις τιμές που δεν προέρχονται από παραγωγικό cluster, χρησιμοποιούνται ελεγχόμενα διανύσματα δοκιμής της συνάρτησης decide_replicas. Οι τιμές του Πίνακα 3 είναι είσοδοι unit test της πολιτικής και όχι μετρήσεις δικτύου. Το P0 θα διατηρούσε τον ίδιο αριθμό αντιγράφων σε όλες τις περιπτώσεις, ενώ το P1 αντιδρά όταν ικανοποιούνται οι ρητές συνθήκες του κώδικα.

Πίνακας 3: Ελεγχόμενη λειτουργική επαλήθευση της στατικής P0 και της προσαρμοστικής P1 πολιτικής.

Τρέχοντα replicas	p95 καθυστέρηση (ms)	CPU (%)	P0 – στατική πολιτική	P1 – απόφαση	Ερμηνεία
4	150	55	4	4	Καμία συνθήκη αλλαγής
4	230	80	4	6	Παραβίαση SLA → αύξηση κατά 2
6	100	25	6	5	Χαμηλή καθυστέρηση και CPU → μείωση κατά 1
5	130	40	5	5	Ενδιάμεση κατάσταση → διατήρηση

Τα αποτελέσματα επιβεβαιώνουν την αναμενόμενη λειτουργία: σε παραβίαση SLA η P1 αυξάνει άμεσα τη διαθέσιμη υπολογιστική ικανότητα, σε σαφώς χαμηλό φορτίο μειώνει συντηρητικά τους πόρους και στις ενδιάμεσες καταστάσεις αποφεύγει άσκοπες μεταβολές. Το αποτέλεσμα αποδεικνύει ότι η εφαρμογή μετατρέπει τις μετρήσεις σε ελεγχόμενη απόφαση πόρων. Δεν αποδεικνύει από μόνο του βελτίωση πραγματικής καθυστέρησης, επειδή η συνάρτηση scale_k8s παραμένει ενδεικτική και δεν εκτελεί πραγματικό Kubernetes API στο συγκεκριμένο πείραμα.

3.5 Συνολική συγκριτική αξιολόγηση των εφαρμογών του Κεφαλαίου 3

Τα τρία πειράματα έχουν κοινή λογική: η κατάσταση αναφοράς δεν είναι απαραίτητα μη λειτουργική ως προς τη βασική συνδεσιμότητα ή εκτέλεση, αλλά αποτυγχάνει στη συγκεκριμένη απαίτηση που εξετάζεται. Η παρέμβαση προσθέτει έναν σαφώς ορισμένο μηχανισμό και η αξιολόγηση ελέγχει αν εμφανίζεται η αναμενόμενη λειτουργική αλλαγή. Ο Πίνακας 4 συνοψίζει τα αποτελέσματα και, εξίσου σημαντικά, τα όρια της τεκμηρίωσης.

Πίνακας 4: Συνοπτική σύγκριση baseline, παρέμβασης, αποτελέσματος και περιορισμών των τριών εφαρμογών.

Εφαρμογή	Baseline / πρόβλημα	Παρέμβαση	Άμεσο αποτέλεσμα	Όριο αξιολόγησης
Packet Tracer – Network Slicing	Βασική δρομολόγηση χωρίς διαχωρισμό, ACL και QoS	VLAN 110/210/11, Deny_Subnet, Servers_Priority, SLICING_QOS_POLICY	Λογικά όρια, ελεγχόμενη απομόνωση και ρητή προτεραιότητα κρίσιμης κίνησης	Λειτουργική προσέγγιση· όχι εγγενές 5G slicing ούτε μη μετρημένη αριθμητική βελτίωση
Mininet/OVS – OpenDaylight	Controller συνδεδεμένος, αλλά χωρίς χρήσιμους κανόνες ροής· pingall αποτυγχάνει	Πολιτική διαμερίσεων με OpenFlow κανόνες που παράγονται σε Python και εγκαθίστανται μέσω RESTCONF	Επικοινωνία μόνο εντός διαμέρισης (6/30 στο pingall), ρητή απόρριψη μεταξύ διαμερίσεων και αύξηση των μετρητών	Εξομοιωμένο περιβάλλον· η εγκυρότητα εξαρτάται από την ορθότητα της πολιτικής

Python – διαχείριση πόρων	Σταθερός αριθμός replicas ανεξάρτητα από SLA/φορτίο	Ντετερμινιστικός βρόχος p95 latency + CPU	Scale-up σε παραβίαση SLA, scale-down σε χαμηλό φορτίο, διατήρηση αλλιώς	Unit-test της λογικής· η ενέργεια Kubernetes είναι ενδεικτική και όχι πραγματική εκτέλεση cluster

Η παράλληλη αξιολόγηση δείχνει ότι το ουσιαστικό κριτήριο επιτυχίας δεν είναι η απλή ύπαρξη ενός εργαλείου ή μιας τεχνολογίας, αλλά η παρατηρήσιμη αλλαγή που επιφέρει. Στη διαμέριση δικτύου η αλλαγή είναι η επιβολή διαφορετικής πολιτικής ανά υπηρεσία, στο SDN η εγκατάσταση επαληθεύσιμων ροών που αποκαθιστούν την προώθηση και στην αυτοματοποίηση η μετατροπή των μετρικών σε συγκεκριμένη απόφαση κλιμάκωσης. Με αυτή τη δομή το Κεφάλαιο 3 παρουσιάζει εφαρμογή και αξιολόγηση ταυτόχρονα, ενώ το επόμενο κεφάλαιο συνθέτει τα ευρήματα σε ευρύτερο επίπεδο.

4 *Μελλοντικά σενάρια εφαρμογής αρχιτεκτονικών SDN και Network Slicing*

4.1 Πλαίσιο σχεδιασμού και παραδοχές των μελλοντικών σεναρίων

Το παρόν κεφάλαιο μεταφέρει τα αποτελέσματα του Κεφαλαίου 3 σε μελλοντικά περιβάλλοντα λειτουργίας. Δεν παρουσιάζει τις ακόλουθες περιπτώσεις ως ήδη υλοποιημένες ή ως πηγή μετρημένων επιδόσεων. Πρόκειται για τεκμηριωμένα σενάρια διερεύνησης, τα οποία δείχνουν πώς οι αρχιτεκτονικές διαμέρισης δικτύου, SDN και αυτοματοποιημένης διαχείρισης πόρων θα μπορούσαν να εξελιχθούν σε δίκτυα 5G Advanced, 6G και Edge Computing. Κάθε σενάριο ορίζει το επιχειρησιακό πλαίσιο, το γεγονός που προκαλεί την προσαρμογή, την αναμενόμενη απόκριση της αρχιτεκτονικής, τις μετρικές αξιολόγησης και τους βασικούς περιορισμούς.

Η αφετηρία παραμένει η πειραματική λογική κατάσταση αναφοράς–παρέμβαση–επαλήθευση. Η διαμόρφωση VLAN, ACL και QoS του Packet Tracer χρησιμοποιείται ως απλουστευμένο υπόδειγμα λογικού διαχωρισμού και διαφοροποίησης υπηρεσιών. Η εγκατάσταση κανόνων OpenFlow μέσω OpenDaylight αποτυπώνει τον ρόλο του κεντρικού ελέγχου στην προώθηση. Τέλος, ο ντετερμινιστικός μηχανισμός Python αποτελεί το αρχικό επίπεδο ενός κλειστού βρόχου, ο οποίος στο μέλλον μπορεί να εμπλουτιστεί με πρόβλεψη ζήτησης και ελεγχόμενη χρήση μηχανικής μάθησης. Η μετάβαση από τα πειράματα στα σενάρια είναι επομένως κλιμακωτή και δεν εξισώνει τις προσομοιώσεις της εργασίας με πλήρη παραγωγική υλοποίηση 5G ή 6G.

Για όλα τα σενάρια θεωρείται ότι η κοινή φυσική υποδομή διαθέτει μηχανισμούς τηλεμετρίας, αναγνωριστικά ανά διαμέριση, προγραμματιζόμενες διεπαφές και δυνατότητα εφαρμογής πολιτικών σε πρόσβαση, μεταφορά, πυρήνα και άκρο. Η αξιολόγηση πρέπει να γίνεται ανά υπηρεσία και όχι μόνο με συνολικούς μέσους όρους. Ενδεικτικά, καταγράφονται καθυστέρηση και διακύμανσή της, απώλεια πακέτων, ρυθμός μετάδοσης, επιτυχία εγκατάστασης υπηρεσίας, χρόνος εφαρμογής πολιτικής, χρόνος αποκατάστασης, κατανάλωση υπολογιστικών πόρων και αριθμός παραβιάσεων SLA. Όπου υπάρχουν κρίσιμες ουρές κατανομής, είναι απαραίτητα και υψηλά εκατοστημόρια, όπως το 95ο και το 99ο, ώστε να μην αποκρύπτονται σπάνια αλλά σοβαρά συμβάντα [36].

Τα μελλοντικά σενάρια θα πρέπει να σχεδιαστούν λαμβάνοντας υπόψη τον ευρύτερο προσανατολισμό των δικτύων IMT-2030[25]. Τα μελλοντικά συστήματα κινητής τηλεφωνίας αναμένεται να παρέχουν ένα ευρύτερο φάσμα υπηρεσιών και προδιαγραφών. Η εξέλιξη αυτή θα επεκτείνει παράλληλα τις δυνατότητες του IMT-2020, σύμφωνα με το πλαίσιο της ITU-R

[25] IMT-2030 (International Mobile Telecommunications-2030): το πλαίσιο της ITU (International Telecommunication Union) που αναφέρεται στη μελλοντική ανάπτυξη των κινητών επικοινωνιών για το 2030 και μετά.

(International Telecommunication Union- Radiocommunication Sector). Αξίζει να σημειωθεί ότι οι βελτιώσεις στη χωρητικότητα του δικτύου και στους ρυθμούς μεταφοράς δεδομένων δεν αποτελούν τις μόνες πτυχές αυτής της ανάπτυξης, αφού θα προστεθούν πρόσθετοι σχεδιαστικοί στόχοι που θα επικεντρώνονται στη διάχυτη νοημοσύνη, τη βιωσιμότητα, την ασφάλεια, την ανθεκτικότητα και τη διαλειτουργικότητα. Με βάση τα παραπάνω, τα σενάρια που εξετάζονται στο παρόν κεφάλαιο πρέπει να εξεταστούν στο πλαίσιο ενός μελλοντικού δικτυακού περιβάλλοντος που χαρακτηρίζεται από τη σταδιακή ενσωμάτωση δυνατοτήτων επικοινωνίας, υπολογισμού και τεχνητής νοημοσύνης [59].

Βασική παραδοχή αποτελεί το γεγονός ότι οι υποδομές του μέλλοντος θα πρέπει να είναι αρκετά ευέλικτες, ώστε να μπορούν να εξυπηρετούν υπηρεσίες με ριζικά διαφορετικές λειτουργικές ανάγκες. Παράλληλα, πέρα από την εισαγωγή σεναρίων που σχετίζονται με τη διάχυτη συνδεσιμότητα, την τεχνητή νοημοσύνη και την ολοκληρωμένη ανίχνευση, το IMT-2030 αναμένεται να διευρύνει τις υπάρχουσες κατηγορίες υπηρεσιών eMBB, URLLC και mMTC προς την κατεύθυνση της καθηλωτικής επικοινωνίας (Immersive Communication), της υπερ-αξιόπιστης επικοινωνίας χαμηλής καθυστέρησης (Hyper Reliable and Low-Latency Communication) και της μαζικής επικοινωνίας (Massive Communication). Επειδή αυτές οι υπηρεσίες ενδέχεται να έχουν πολύ διαφορετικές απαιτήσεις όσον αφορά την καθυστέρηση, την αξιοπιστία, την πυκνότητα σύνδεσης, τη διακίνηση δεδομένων και το υπολογιστικό φορτίο, δεν μπορούν να αντιμετωπιστούν με μια τυποποιημένη πολιτική κατανομής πόρων [59]. Οι παραπάνω συνθήκες ενισχύουν την ανάγκη για προσαρμοστικότητα και σχεδίαση βάσει αυτόνομων δομικών στοιχείων, επιτρέποντας με αυτόν τον τρόπο την τροποποίηση της λειτουργικότητας του δικτύου καθώς αλλάζουν οι συνθήκες και οι απαιτήσεις της ανάπτυξης.

Η εφαρμογή της διαμέρισης δικτύου στα προτεινόμενα σενάρια συνάδει απόλυτα με αυτή την κατεύθυνση. Το RAN slicing ορίζεται ως μια τεχνική που επιτρέπει τη λειτουργία πολλών ξεχωριστών λογικών δικτύων σε μια κοινή φυσική υποδομή, με κάθε διαμέριση να διαμορφώνεται σύμφωνα με τις ανάγκες συγκεκριμένων χρηστών, υπηρεσιών ή εφαρμογών. Επιπλέον, προβλέπεται ότι η παροχή QoS στο μέλλον θα είναι πιο δυναμική, προσανατολισμένη στις υπηρεσίες και ικανή να διασφαλίζει μια συνεπή εμπειρία χρήστη. Αυτά τα χαρακτηριστικά ενισχύουν την υπόθεση του παρόντος κεφαλαίου, σύμφωνα με την οποία οι πόροι και οι πολιτικές μπορούν να τροποποιούνται δυναμικά, αντί να παραμένουν σταθεροί καθ’ όλη τη διάρκεια της λειτουργίας του δικτύου.

Αναμένεται ότι η αυτοματοποίηση θα διαδραματίσει έναν ολοένα και πιο σημαντικό ρόλο. Στο πλαίσιο του IMT-2030 λαμβάνεται υπόψη η ενσωμάτωση των δυνατοτήτων που παρέχουν η τεχνητή νοημοσύνη (AI) και η μηχανική μάθηση (ML) στα συστήματα επικοινωνίας. Αξίζει να σημειωθεί ότι σε αυτές συμπεριλαμβάνονται η κατανεμημένη επεξεργασία, η εξαγωγή συμπερασμάτων και άλλες υπολογιστικές εργασίες που σχετίζονται με το δίκτυο. Έτσι, τα μελλοντικά δίκτυα ενδέχεται να περιλαμβάνουν δυνατότητες αυτοδιαχείρισης και, πιο συγκεκριμένα, να μπορούν να αυτοπαρακολουθούνται, να αυτοβελτιστοποιούνται και, σε κάποιο βαθμό, να αυτοεπιδιορθώνονται. Παράλληλα, όταν οι εφαρμογές απαιτούν αποκρίσεις σε πραγματικό χρόνο, τα φορτία εργασίας θα μπορούν να τοποθετούνται πιο κοντά στις πηγές των δεδομένων, μέσω της επέκτασης των υπολογιστικών πόρων προς την άκρη του δικτύου. Η συγκεκριμένη εξέλιξη προσφέρει ένα ευρύτερο τεχνολογικό πλαίσιο για το ντετερμινιστικό σύστημα διαχείρισης πόρων βασισμένο στη Python που εξετάστηκε στο Κεφάλαιο 3. Ο μηχανισμός

αυτός μπορεί να θεωρηθεί ως μια απλούστερη βάση για την ανάπτυξη πιο σύνθετων μηχανισμών ελέγχου κλειστού βρόχου [59].

Τέλος, οι συμβατικές μετρικές απόδοσης του δικτύου δεν θα πρέπει να αποτελούν το μοναδικό κριτήριο για την αξιολόγηση των μελλοντικών σεναρίων. Εκτός από την καθυστέρηση, την αξιοπιστία, την κάλυψη και τη χωρητικότητα, στο IMT-2030 λαμβάνονται υπόψη και άλλες σημαντικές δυνατότητες. Σε αυτές περιλαμβάνονται η ασφάλεια και η ανθεκτικότητα, η βιωσιμότητα και η διαλειτουργικότητα. Για τον λόγο αυτό, σε μελλοντικές επεκτάσεις του πειραματικού πλαισίου, η αξιολόγηση σε επίπεδο υπηρεσιών θα μπορούσε να εξετάζει παράλληλα την αποδοτική χρήση των πόρων, τη συμπεριφορά του δικτύου κατά την αποκατάσταση και τη συνέπεια στην εφαρμογή των πολιτικών. Με αυτόν τον τρόπο, οι ελεγχόμενες υλοποιήσεις του Κεφαλαίου 3 μπορούν να αποτελέσουν τη βάση για τη μελέτη πιο σύνθετων περιβαλλόντων IMT-2030. Παράλληλα, διατηρείται η σύνδεση των μελλοντικών σεναρίων με την πειραματική μεθοδολογία που ακολουθήθηκε στην παρούσα εργασία [59].

4.2 Μελλοντικό σενάριο 1: Δυναμική διαμέριση δικτύου για έξυπνο νοσοκομείο

Στο πρώτο σενάριο, ένα έξυπνο νοσοκομείο της επόμενης δεκαετίας εξυπηρετεί ταυτόχρονα Τηλεχειρουργική και απομακρυσμένη υποστήριξη, συνεχή μετάδοση ιατρικής απεικόνισης υψηλής ανάλυσης, φορετούς αισθητήρες ασθενών, αυτόνομα οχήματα εσωτερικής μεταφοράς και κοινή πρόσβαση επισκεπτών. Η ίδια φυσική υποδομή υποστηρίζει διακριτές λογικές διαμερίσεις: μία URLLC για εντολές και ανάδραση πραγματικού χρόνου, μία eMBB για απεικονιστικά δεδομένα και βίντεο, μία mMTC για μεγάλο πλήθος αισθητήρων, μία διαμέριση διοίκησης και μία best effort για μη κρίσιμες χρήσεις. Η αρχιτεκτονική επεκτείνει τη λογική των VLAN 110, 210 και 11 του Κεφαλαίου 3 σε διαμέριση από άκρο σε άκρο, η οποία δεν περιορίζεται στο τοπικό δίκτυο αλλά καλύπτει πρόσβαση, μεταφορά, πυρήνα και edge εφαρμογές [37].

Το γεγονός ενεργοποίησης είναι ένα έκτακτο χειρουργικό περιστατικό που συμπίπτει με απότομη αύξηση τηλεμετρίας και μεταφοράς ιατρικών εικόνων. Ο ενορχηστρωτής αναγνωρίζει το προφίλ της κρίσιμης υπηρεσίας, δεσμεύει προσωρινά πρόσθετο εύρος ζώνης, τοποθετεί τις λειτουργίες επεξεργασίας σε κοντινό edge κόμβο και εφαρμόζει αυστηρότερη προτεραιοποίηση. Παράλληλα, η πολιτική απομόνωσης περιορίζει κάθε μη αναγκαία επικοινωνία προς τη διαμέριση URLLC. Η λογική αυτή αντιστοιχεί λειτουργικά στην ACL και στην πολιτική QoS της S1, αλλά υλοποιείται δυναμικά και σε περισσότερους διοικητικούς και τεχνολογικούς τομείς.

Η κρίσιμη απαίτηση του σεναρίου είναι η προστασία της ιατρικής υπηρεσίας χωρίς ανεξέλεγκτη υποβάθμιση των υπολοίπων διαμερίσεων. Για τον λόγο αυτό, η αξιολόγηση θα συγκρίνει στατική κατανομή με δυναμική ενορχήστρωση υπό ταυτόσημο φορτίο [53]. Θα μετρηθούν η καθυστέρηση άκρου σε άκρο και το 99ο εκατοστημόριό της για την URLLC, η απώλεια πακέτων, ο ρυθμός μετάδοσης της eMBB, η επιτυχία εξυπηρέτησης των αισθητήρων, ο χρόνος ενεργοποίησης πρόσθετων πόρων και οι επιπτώσεις στη best effort κίνηση. Επίσης θα ελεγχθεί αν η απομόνωση διατηρείται όταν ένας αισθητήρας ή μια εφαρμογή επισκεπτών εμφανίσει κακόβουλη ή εσφαλμένη συμπεριφορά [47].

Το αναμενόμενο όφελος είναι η δυνατότητα προσωρινής ενίσχυσης της κρίσιμης υπηρεσίας χωρίς κατασκευή αποκλειστικού φυσικού δικτύου. Η βασική αβεβαιότητα αφορά τη συνέπεια της διαμέρισης μεταξύ ασύρματης πρόσβασης, πυρήνα, edge και εσωτερικού δικτύου του νοσοκομείου. Απαιτούνται έλεγχος αλλαγών, ισχυρή ταυτοποίηση, καταγραφή ενεργειών και ασφαλής επαναφορά πολιτικής, επειδή μια λανθασμένη απόφαση ενορχήστρωσης μπορεί να επεκταθεί ταχύτατα σε ολόκληρη την κοινόχρηστη υποδομή.

Σε ένα μελλοντικό «έξυπνο» νοσοκομείο πρέπει επίσης να λαμβάνεται υπόψη η συνύπαρξη διαφορετικών ιατρικών υπηρεσιών και τεχνολογιών επικοινωνίας. Ένα νοσοκομειακό δίκτυο δεν βασίζεται αποκλειστικά στη συνδεσιμότητα 5G. Ιατρικός εξοπλισμός, συστήματα παρακολούθησης και άλλες συσκευές μπορούν παράλληλα να χρησιμοποιούν Wi-Fi, Bluetooth, NB-IoT ή καλωδιακές συνδέσεις. Η ξεχωριστή λειτουργία αυτών των δικτύων αυξάνει την πολυπλοκότητα της συνολικής υποδομής. Παράλληλα, τα ιατρικά δεδομένα μπορεί να παραμένουν κατανεμημένα σε διαφορετικές πλατφόρμες. Για τον λόγο αυτό, η ενοποιημένη διαχείριση του δικτύου αποκτά ιδιαίτερη σημασία, κυρίως όταν πολλές συσκευές και εφαρμογές λειτουργούν ταυτόχρονα [60].

Σε ένα τέτοιο περιβάλλον, σημαντική είναι και η αξιοποίηση του edge computing. Μέρος της επεξεργασίας μπορεί να πραγματοποιείται κοντά στο νοσοκομειακό δίκτυο και στις εφαρμογές που παράγουν τα δεδομένα, χωρίς να απαιτείται η μεταφορά όλης της ιατρικής κίνησης σε μια απομακρυσμένη υποδομή νέφους . Με αυτόν τον τρόπο μειώνεται η κίνηση που μεταφέρεται μέσω του δικτύου οπισθόζευξης (backhaul), ενώ μπορεί να περιοριστεί και η καθυστέρηση σε εφαρμογές που απαιτούν γρήγορη απόκριση. Έτσι, ένα δίκτυο για υπηρεσίες υγειονομικής περίθαλψης μπορεί να συνδυάζει τη διαμέριση δικτύου με μια αποκλειστική User Plane Function (UPF) και το Multi-access Edge Computing (MEC). Με αυτόν τον συνδυασμό, μπορούν να υποστηρίζονται διαφορετικές απαιτήσεις ως προς την καθυστέρηση, τον ρυθμό μετάδοσης δεδομένων και τη συνδεσιμότητα κάθε ιατρικής υπηρεσίας. Επιπλέον, μέσω κοινών διεπαφών μπορούν να παρέχονται δυνατότητες όπως το QoS και τη διαμέριση δικτύου, διευκολύνοντας τη διαχείριση των διαφορετικών ιατρικών εφαρμογών [60].

Η δυνατότητα αυτή είναι ιδιαίτερα χρήσιμη όταν ο φόρτος του νοσοκομειακού δικτύου μεταβάλλεται. Υπό κανονικές συνθήκες, οι διαθέσιμοι πόροι κατανέμονται μεταξύ της ιατρικής απεικόνισης, της παρακολούθησης ασθενών, των διοικητικών εφαρμογών και άλλων μη κρίσιμων υπηρεσιών. Η κατανομή αυτή μπορεί να αλλάξει γρήγορα σε περίπτωση έκτακτης ανάγκης. Σε μια τέτοια περίπτωση, περισσότεροι πόροι μπορούν να διατεθούν στο τμήμα που μεταφέρει κρίσιμη ιατρική κίνηση, ενώ οι υπηρεσίες χαμηλότερης προτεραιότητας συνεχίζουν να λειτουργούν με περιορισμένους πόρους. Αυτή η προσέγγιση υποστηρίζεται και από τα αποτελέσματα των Tang et al. Στις δοκιμές τους, η χρήση εξειδικευμένων πόρων επικοινωνίας επέτρεψε στην ιατρική κίνηση να διατηρήσει πιο σταθερή απόδοση καθώς αυξανόταν ο αριθμός των χρηστών. Αντίθετα, σε συνθήκες αυξημένου φόρτου, η κίνηση που χρησιμοποιούσε κοινόχρηστους πόρους παρουσίασε μείωση του ρυθμού μετάδοσης δεδομένων και αύξηση της καθυστέρησης από άκρο σε άκρο [60].

Ωστόσο, η κατανομή πόρων δεν αρκεί σε ένα νοσοκομειακό περιβάλλον. Μέσω του νοσοκομειακού δικτύου μεταφέρονται ευαίσθητες ιατρικές πληροφορίες, επομένως η πρόσβαση στις υπηρεσίες και τις λειτουργίες του πρέπει να ελέγχεται. Η αρχιτεκτονική υγειονομικής περίθαλψης που προτείνεται στη μελέτη περιλαμβάνει μηχανισμούς ελέγχου πρόσβασης στους

δικτυακούς και υπολογιστικούς πόρους, καθώς και διαδικασίες εξουσιοδότησης χρηστών και υπηρεσιών. Οι μηχανισμοί αυτοί είναι απαραίτητοι για τον διαχωρισμό από άκρο σε άκρο, καθώς η απομόνωση των υπηρεσιών πρέπει να διατηρείται ακόμη και όταν οι διαθέσιμοι πόροι μεταβάλλονται δυναμικά. Η τοπική διαχείριση των πόρων στα άκρα του δικτύου μπορεί επίσης να προσφέρει στο νοσοκομείο μεγαλύτερο έλεγχο των ιατρικών εφαρμογών, των χρηστών και των δεδομένων, χωρίς να μεταφέρονται όλες οι λειτουργίες διαχείρισης εκτός της νοσοκομειακής υποδομής [60].

Στο πλαίσιο αυτό, η δυναμική διαμέριση δικτύου σε ένα μελλοντικό έξυπνο νοσοκομείο δεν περιορίζεται μόνο στην κράτηση εύρους ζώνης. Η αξιοποίησή της συνδέεται με τον συντονισμό της δικτυακής συνδεσιμότητας, του edge computing, της προτεραιότητας των υπηρεσιών και του ελέγχου πρόσβασης, ανάλογα με τις εκάστοτε ανάγκες του νοσοκομείου. Με αυτόν τον τρόπο μπορεί να περιοριστεί η ανάγκη για ξεχωριστή φυσική υποδομή για κάθε υπηρεσία. Η ίδια υποδομή μπορεί να εξυπηρετεί υπηρεσίες με διαφορετικές απαιτήσεις και, όταν είναι απαραίτητο, να διαθέτει προσωρινά περισσότερους πόρους σε κρίσιμες ιατρικές εφαρμογές [60].

4.3 Μελλοντικό σενάριο 2: Προγραμματιζόμενος έλεγχος για συνεργατική αυτόνομη κινητικότητα

Στο δεύτερο σενάριο, μια μελλοντική αστική περιοχή υποστηρίζει αυτόνομα οχήματα, σηματοδότες, οδικούς αισθητήρες και edge κόμβους σε ένα κοινό δίκτυο. Η αρχιτεκτονική SDN χρησιμοποιεί πολλαπλούς συνεργαζόμενους ελεγκτές: ένας τοπικός ελεγκτής διαχειρίζεται τις ροές χαμηλής καθυστέρησης στην περιοχή, ενώ ένας ανώτερος ελεγκτής συντονίζει πολιτικές μεταξύ περιοχών. Οι μεταγωγείς του επιπέδου προώθησης εκτελούν κανόνες προώθησης ανά κατηγορία υπηρεσίας, όπως ακριβώς οι OVS μεταγωγείς του πειράματος M1, αλλά σε μεγαλύτερη κλίμακα και με απαίτηση συνέχειας κατά την κίνηση των οχημάτων.

Η προσαρμογή ενεργοποιείται από δύο ταυτόχρονα γεγονότα: τη διακοπή της ζεύξης που συνδέει την περιοχή με τον πυρήνα του δικτύου και την απότομη συγκέντρωση οχημάτων ύστερα από οδικό συμβάν. Οι μετρήσεις που συλλέγονται από το δίκτυο δείχνουν στον ελεγκτή αύξηση της καθυστέρησης και των απωλειών πακέτων στην περιοχή που επηρεάζεται. Με βάση τις ενδείξεις αυτές, ο ελεγκτής υπολογίζει εναλλακτικές διαδρομές, εγκαθιστά εκ των προτέρων κανόνες προώθησης για τα μηνύματα που αφορούν την ασφάλεια των οχημάτων και μεταφέρει τις ροές ψυχαγωγίας σε διαδρομές χαμηλότερης προτεραιότητας. Αν ένας τοπικός ελεγκτής τεθεί εκτός λειτουργίας, τον έλεγχο της περιοχής αναλαμβάνει εφεδρικός ελεγκτής, ενώ οι κανόνες που έχουν ήδη εγκατασταθεί στους μεταγωγείς κρατούν προσωρινά σε λειτουργία τη βασική προώθηση.

Η αξιολόγηση του σεναρίου θα συγκρίνει τρεις πολιτικές: αποκλειστικά αντιδραστική εγκατάσταση ροών, προληπτική εγκατάσταση για τις κρίσιμες κατηγορίες και υβριδική πολιτική. Οι βασικές μετρικές είναι ο χρόνος από το πρώτο πακέτο έως την εγκατάσταση κανόνα, ο αριθμός μηνυμάτων Packet In και Flow Mod, η επιβάρυνση του ελεγκτή, ο χρόνος αναδρομολόγησης, η διαθεσιμότητα υπηρεσίας και η καθυστέρηση κατά τη μετάβαση μεταξύ περιοχών. Με αυτή τη σύγκριση ελέγχεται αν η κεντρική ορατότητα βελτιώνει πραγματικά την απόκριση ή αν η σηματοδοσία και η απόσταση από τον ελεγκτή δημιουργούν νέο σημείο συμφόρησης.

Η λειτουργική σύνδεση με το Κεφάλαιο 3 είναι άμεση: το M0 απέδειξε ότι η απλή σύνδεση του ελεγκτή δεν αρκεί, ενώ το M1 απέδειξε ότι οι εγκατεστημένοι κανόνες καθιστούν το επίπεδο προώθησης λειτουργικό. Το μελλοντικό πείραμα προσθέτει κινητικότητα, μεταβολή φορτίου, βλάβη και κατανεμημένο έλεγχο. Δεν θεωρεί δεδομένο ότι το SDN μειώνει πάντοτε την καθυστέρηση· εξετάζει υπό ποιες συνθήκες η τοποθέτηση ελεγκτών, η προληπτική πολιτική και η εφεδρεία διατηρούν την υπηρεσία χωρίς υπερβολικό κόστος ελέγχου.

Στο πλαίσιο αυτό, σημαντικό ρόλο στην αυτόνομη κινητικότητα έχει και η δυνατότητα επεξεργασίας των δεδομένων κοντά στα οχήματα. Η χρήση μόνο απομακρυσμένων υποδομών νέφους μπορεί να αυξήσει την καθυστέρηση, ειδικά όταν πρόκειται για ένα οδικό περιβάλλον που μεταβάλλεται συνεχώς. Τα δεδομένα χρειάζεται να διασχίσουν το δίκτυο, να υποβληθούν σε επεξεργασία και η αντίστοιχη απόφαση να επιστρέψει στο όχημα. Η αρχιτεκτονική Software-Defined Vehicular Edge Computing (SD-VEC) προσεγγίζει διαφορετικά αυτή τη διαδικασία, αξιοποιώντας δυνατότητες edge computing σε κόμβους-άγκυρες κοντά στα σημεία πρόσβασης. Ένα μέρος της επεξεργασίας πραγματοποιείται έτσι τοπικά και δεν χρειάζεται να εξαρτάται κάθε λειτουργία από το απομακρυσμένο νλεφος. Η μικρότερη καθυστέρηση που προκύπτει είναι σημαντική κυρίως για υπηρεσίες που σχετίζονται με την ασφάλεια. Σε ένα δίκτυο οχημάτων, άλλωστε, τόσο ο αριθμός όσο και η θέση των συνδεδεμένων οχημάτων μπορούν να αλλάζουν συνεχώς [61].

Η συγκεκριμένη αρχιτεκτονική δεν βασίζεται αποκλειστικά σε έναν κεντρικό ελεγκτή. Αντίθετα, μπορούν να χρησιμοποιηθούν πολλαπλοί ελεγκτές SDN, οι οποίοι λειτουργούν σε κατανεμημένους κόμβους-άγκυρες. Η θέση τους δεν επιλέγεται ανεξάρτητα από τις συνθήκες του δικτύου, καθώς πρέπει να λαμβάνονται υπόψη η κινητικότητα των οχημάτων και οι υπολογιστικές δυνατότητες των κόμβων. Με βάση αυτά τα στοιχεία καθορίζονται ο αριθμός των ελεγκτών, οι θέσεις τους και οι περιοχές ελέγχου που αναλαμβάνουν. Η κινητικότητα, όμως, δημιουργεί μια επιπλέον δυσκολία. Καθώς τα οχήματα μετακινούνται, μεταβάλλεται και η κυκλοφορία των δεδομένων ελέγχου, ιδιαίτερα σε περιοχές με αυξημένη κίνηση. Για τον λόγο αυτό, μια στατική κατανομή των ελεγκτών δεν είναι πάντα κατάλληλη. Η δρομολόγηση των ροών ελέγχου μπορεί να προσαρμόζεται δυναμικά στην κίνηση των οχημάτων, ώστε να περιορίζεται η μέση καθυστέρηση της επικοινωνίας ελέγχου [61].

Η ύπαρξη πολλών ελεγκτών σημαίνει ότι χρειάζεται και συντονισμός μεταξύ τους. Οι ελεγκτές πρέπει να έχουν πληροφορίες τόσο για την κατάσταση του δικτύου όσο και για τους διαθέσιμους υπολογιστικούς πόρους. Στην αρχιτεκτονική SD-VEC αυτό επιτυγχάνεται μέσω του συγχρονισμού τους, ώστε οι πληροφορίες που χρησιμοποιούνται για τον έλεγχο του δικτύου να παραμένουν κοινές μεταξύ των διαφορετικών κόμβων. Παράλληλα, οι αποφάσεις μπορούν να λαμβάνονται τοπικά από κάθε ελεγκτή, περιορίζοντας τον χρόνο απόκρισης του επιπέδου ελέγχου. Ο συγχρονισμός αυτός έχει ιδιαίτερη σημασία σε ένα δίκτυο με οχήματα, όπου οι συνθήκες μεταβάλλονται συνεχώς και ο έλεγχος πρέπει να προσαρμόζεται ανάλογα [61].

Η ίδια αρχιτεκτονική υποστηρίζει και την προληπτική διαχείριση της κινητικότητας. Σε αυτή την περίπτωση, πληροφορίες από προηγούμενες συνδέσεις ενός οχήματος μπορούν να αξιοποιηθούν στην άκρη του δικτύου, ώστε να προβλεφθούν τα σημεία πρόσβασης με τα οποία είναι πιθανό να συνδεθεί στη συνέχεια. Το δίκτυο μπορεί έτσι να προετοιμάζεται για την επόμενη σύνδεση, αντί να περιμένει πρώτα τη μετακίνηση του οχήματος για να προσαρμοστεί. Οι

προβλέψεις αυτές μπορούν να χρησιμοποιηθούν για την προληπτική σύνδεση και την κατανομή των διαθέσιμων πόρων, περιορίζοντας την εξάρτηση από καθαρά αντιδραστικές λειτουργίες. Ένα ακόμη στοιχείο που εξετάζει η μελέτη είναι η χρήση προηγούμενων μοτίβων σύνδεσης με τα σημεία πρόσβασης. Μέσα από αυτά μπορεί να γίνει πρόβλεψη της επόμενης σύνδεσης, χωρίς να απαιτείται συνεχής χρήση δεδομένων GPS (Global Positioning System). Με τον τρόπο αυτό, ο προληπτικός έλεγχος SDN στο συγκεκριμένο σενάριο αυτόνομης κινητικότητας μπορεί να λαμβάνει υπόψη την αναμενόμενη κίνηση των οχημάτων κατά τη λήψη των αποφάσεων του δικτύου [61].

4.4 Μελλοντικό σενάριο 3: Προγνωστική διαχείριση πόρων σε βιομηχανικό Edge

Στο τρίτο σενάριο, μια βιομηχανική εγκατάσταση χρησιμοποιεί εκατοντάδες αισθητήρες mMTC, ρομποτικούς βραχίονες με απαιτήσεις URLLC, εφαρμογές επαυξημένης πραγματικότητας για τεχνικούς και συστήματα οπτικού ελέγχου υψηλού ρυθμού δεδομένων. Οι υπηρεσίες εκτελούνται σε ομάδα edge κόμβων και μετακινούνται ή κλιμακώνονται ανάλογα με το πρόγραμμα παραγωγής. Ο μηχανισμός Python του Κεφαλαίου 3 εξελίσσεται από αντιδραστικό κανόνα δύο ορίων σε ελεγχόμενο σύστημα πρόβλεψης, το οποίο εκτιμά τη ζήτηση των επόμενων χρονικών παραθύρων και εισηγείται κλιμάκωση αντιγράφων, ανακατανομή εύρους ζώνης ή μετακίνηση λειτουργίας [47].

Το γεγονός ενεργοποίησης είναι προγραμματισμένη αλλαγή γραμμής παραγωγής, η οποία συνήθως δημιουργεί σύντομη αλλά έντονη αύξηση εικόνων, τηλεμετρίας και μηνυμάτων ελέγχου. Η στατική πολιτική P0 διατηρεί τους ίδιους πόρους και κινδυνεύει να παραβιάσει SLA. Η αντιδραστική P1 κλιμακώνει αφού καταγραφεί η υπέρβαση. Η μελλοντική P2 χρησιμοποιεί ιστορικές μετρήσεις και τρέχουσα τηλεμετρία για να ενεργοποιήσει πόρους πριν από την αιχμή. Κάθε απόφαση περνά από όρια ασφαλείας: μέγιστο ρυθμό μεταβολής, ελάχιστο χρόνο παραμονής σε μια κατάσταση, διαθέσιμο προϋπολογισμό και δυνατότητα άμεσης επιστροφής στην τελευταία σταθερή πολιτική.

Η αξιολόγηση θα χρησιμοποιήσει κοινά ίχνη κίνησης και επαναλαμβανόμενες εκτελέσεις για τις P0, P1 και P2. Θα μετρηθούν το ποσοστό και η διάρκεια παραβιάσεων SLA, η ακρίβεια πρόβλεψης, ο χρόνος απόφασης, η αξιοποίηση CPU και μνήμης, το ενεργειακό κόστος, ο αριθμός περιττών κλιμακώσεων και οι ταλαντώσεις μεταξύ αύξησης και μείωσης πόρων. Για μοντέλο ενισχυτικής μάθησης θα προστεθούν ο χρόνος σύγκλισης, η σταθερότητα της πολιτικής και η συμπεριφορά σε μοτίβα που δεν εμφανίστηκαν κατά την εκπαίδευση [42]–[45].

Το σενάριο δεν θεωρεί δεδομένο ότι η μηχανική μάθηση υπερέχει ενός σαφούς κανόνα. Η πολιτική P2 θα κριθεί χρήσιμη μόνο εφόσον μειώνει τις παραβιάσεις των συμφωνιών επιπέδου υπηρεσίας, χωρίς να καταναλώνει δυσανάλογους πόρους και χωρίς να παράγει ασταθείς αποφάσεις. Σε μια κρίσιμη βιομηχανική εγκατάσταση ισχύουν επιπλέον τέσσερις απαιτήσεις: ο διαχειριστής πρέπει να μπορεί να κατανοήσει γιατί λήφθηκε κάθε απόφαση, το σύστημα πρέπει να αναγνωρίζει πότε τα δεδομένα λειτουργίας διαφέρουν από εκείνα με τα οποία εκπαιδεύτηκε το μοντέλο, οι κρίσιμες ενέργειες πρέπει να περνούν από ανθρώπινη έγκριση και πρέπει να προβλέπεται ασφαλής επιστροφή στη ντετερμινιστική πολιτική όταν η πρόβλεψη κρίνεται αναξιόπιστη. Οι απαιτήσεις

αυτές δεν αποτελούν πρόσθετες λειτουργίες, αλλά μέρος του ίδιου του σχεδιασμού της αρχιτεκτονικής.

Η προληπτική αυτόματη κλιμάκωση αποτελεί μια διαφορετική προσέγγιση για την προγνωστική διαχείριση πόρων σε ένα βιομηχανικό περιβάλλον edge. Οι αντιδραστικοί μηχανισμοί τροποποιούν τους διαθέσιμους πόρους αφού πρώτα εντοπιστεί κάποια μεταβολή στο φορτίο εργασίας. Αυτό μπορεί να δημιουργήσει καθυστέρηση, καθώς η εκκίνηση ή η διακοπή λειτουργίας των containers δεν πραγματοποιείται άμεσα. Το πρόβλημα γίνεται πιο σημαντικό όταν η ζήτηση αυξάνεται σε σύντομο χρονικό διάστημα. Αντίθετα, η προληπτική αυτόματη κλιμάκωση ακολουθεί διαφορετική λογική. Προσπαθεί να προβλέψει τη μελλοντική ζήτηση και να προετοιμάσει εκ των προτέρων τους απαραίτητους πόρους, αντί να περιμένει πρώτα την αύξηση του φορτίου εργασίας [62].

Το Proactive Pod Autoscaler (PPA), το οποίο έχει σχεδιαστεί για εφαρμογές edge computing που βασίζονται στο Kubernetes, αποτελεί ένα χαρακτηριστικό παράδειγμα αυτής της στρατηγικής, αφού ένα από τα βασικά χαρακτηριστικά του αποτελεί το γεγονός ότι οι αποφάσεις του προτεινόμενου μηχανισμού δεν βασίζονται μόνο στη χρήση της CPU. Αξίζει να σημειωθεί ότι ο τρέχων φόρτος εργασίας μπορεί επίσης να περιγραφεί με διάφορους τρόπους. Κάποιοι από αυτούς είναι η συλλογή δεδομένων σχετικά με τη μνήμη RAM (Random Access Memory), τις εισόδους-εξόδους δικτύου και δεδομένα ειδικά για κάθε εφαρμογή. Αυτό το κάνει ιδιαίτερα σημαντικό σε ένα βιομηχανικό περιβάλλον edge, όπου οι απαιτήσεις σε πόρους ενδέχεται να διαφέρουν σημαντικά ανάλογα με τις υπηρεσίες. Για παράδειγμα, το πρότυπο φόρτου εργασίας μιας υπηρεσίας που επεξεργάζεται μικρά μηνύματα τηλεμετρίας από βιομηχανικούς αισθητήρες μπορεί να διαφέρει από αυτό μιας εφαρμογής οπτικής επιθεώρησης. Εξαιτίας αυτού, η εξάρτηση από έναν μόνο δείκτη δεν θα παρέχει πάντα επαρκή δεδομένα για την επιλογή μιας αποτελεσματικής κλιμάκωσης [62].

Η λειτουργία του PPA βασίζεται σε τρία κύρια στοιχεία και χρησιμοποιεί δύο ξεχωριστούς βρόχους. Κατά τη διάρκεια του βρόχου ελέγχου, οι μετρήσεις λαμβάνονται από το σύστημα παρακολούθησης Prometheus Adapter και στη συνέχεια περνούν στον Formulator για την απαραίτητη επεξεργασία. Έπειτα, ο Evaluator χρησιμοποιεί το μοντέλο πρόβλεψης και υπολογίζει τον επιθυμητό αριθμό αντιγράφων. Το αντίστοιχο αίτημα κλιμάκωσης αποστέλλεται τελικά στο επίπεδο ελέγχου του Kubernetes. Παράλληλα υπάρχει ένας δεύτερος βρόχος, στον οποίο το μοντέλο μπορεί να ενημερώνεται με πιο πρόσφατα δεδομένα λειτουργίας. Έτσι, δεν είναι απαραίτητο να παραμένει σταθερό όταν τα μοτίβα του φόρτου εργασίας μεταβάλλονται. Είναι δυνατή και η χρήση διαφορετικών τεχνικών ενημέρωσης. Η επανεκπαίδευση με νέες μετρήσεις μπορεί να είναι καταλληλότερη σε ορισμένες περιπτώσεις, ενώ σε άλλες η διατήρηση του προηγούμενου μοντέλου μπορεί να είναι επαρκής [62].

Ωστόσο, η πρόβλεψη από μόνη της δεν αρκεί. Η διαδικασία κλιμάκωσης πρέπει επίσης να λαμβάνει υπόψη τους περιορισμένους πόρους στους edge κόμβους. Το προτεινόμενο PPA αποτρέπει τις αποφάσεις κλιμάκωσης από το να υπερβαίνουν αυτούς τους φυσικούς περιορισμούς, υπολογίζοντας παράλληλα τον μέγιστο αριθμό αντιγράφων που μπορεί να υποστηρίξει η υποδομή. Υπάρχει επίσης ένας εναλλακτικός τρόπος λειτουργίας. Το εργαλείο αυτόματης κλιμάκωσης έχει τη δυνατότητα να χρησιμοποιήσει τις τρέχουσες μετρήσεις για να λάβει την απόφασή του, εάν το μελλοντικό φορτίο εργασίας δεν μπορεί να προβλεφθεί. Η βεβαιότητα της πρόβλεψης μπορεί επίσης να ληφθεί υπόψη κατά τη χρήση ενός Bayesian μοντέλου. Μόνο όταν αυτή ξεπερνά ένα

προκαθορισμένο όριο χρησιμοποιείται η προγνωστική λειτουργία. Διαφορετικά, η απόφαση βασίζεται στις τρέχουσες μετρήσεις [62].

Ένα άλλο στοιχείο που επηρεάζει αυτή τη διαδικασία είναι η επιλογή του μοντέλου πρόβλεψης. Η CPU, η μνήμη RAM, οι είσοδοι-έξοδοι δικτύου και ο ρυθμός αιτημάτων HTTP (Hypertext Transfer Protocol) χρησιμοποιήθηκαν ως μετρήσεις εισόδου για τη σύγκριση των μοντέλων ARMA (Autoregressive Moving Average) και LSTM (Long Short-Term Memory) στο πλαίσιο της πειραματικής έρευνας. Αξίζει να σημειωθεί ότι το μοντέλο LSTM παρήγαγε μικρότερο σφάλμα πρόβλεψης για την υπό εξέταση εφαρμογή που απαιτεί εντατική χρήση της CPU, σε σύγκριση με το μοντέλο ARMA. Επίσης, στην τελική αξιολόγηση συγκρίθηκαν το προληπτικό PPA και το αντιδραστικό Horizontal Pod Autoscaler (HPA) του Kubernetes, με αποτέλεσμα οι εργασίες edge να παρουσιάζουν μικρότερη τυπική απόκλιση, ενώ ο μέσος χρόνος απόκρισης μειώθηκε από 0,592 δευτερόλεπτα με το HPA σε 0,508 δευτερόλεπτα με το PPA. Τέλος, παρόμοια αποτελέσματα παρατηρήθηκαν και στις εργασίες υπολογιστικού νέφους του πειράματος [62].

4.5 Μελλοντικό σενάριο 4 Ενοποιημένη αρχιτεκτονική 6G και Edge για αντιμετώπιση καταστροφών

Το τέταρτο σενάριο συνδυάζει τις τρεις αρχιτεκτονικές σε ένα μελλοντικό δίκτυο αντιμετώπισης φυσικής καταστροφής. Μετά από σεισμό, τμήματα της επίγειας υποδομής τίθενται εκτός λειτουργίας και η συνδεσιμότητα αποκαθίσταται προσωρινά μέσω κινητών σταθμών βάσης, μη επανδρωμένων αεροσκαφών και δορυφορικών ζεύξεων. Δημιουργούνται μία κρίσιμη διαμέριση για ομάδες διάσωσης και τηλεϊατρική, μία διαμέριση για αισθητήρες και εντοπισμό, μία eMBB για εικόνα από drones και μία περιορισμένη δημόσια υπηρεσία επικοινωνίας [51]. Η χωρητικότητα, η καθυστέρηση και η διαθεσιμότητα μεταβάλλονται συνεχώς καθώς οι προσωρινοί κόμβοι κινούνται ή εξαντλούν την ενέργειά τους.

Ο ενορχηστρωτής ενεργοποιεί και τερματίζει διαμερίσεις ανά περιοχή, ο ελεγκτής SDN επιλέγει διαδρομές μεταξύ επίγειων, εναέριων και δορυφορικών τμημάτων, ενώ ο μηχανισμός πρόβλεψης εκτιμά πού θα αυξηθεί η ζήτηση με βάση τη θέση των συνεργείων και την κατάσταση των ζεύξεων. Πριν εφαρμοστεί μια μεγάλης κλίμακας αλλαγή, ένα ψηφιακό δίδυμο εξετάζει αν η νέα κατανομή δημιουργεί ανεπιθύμητη παρεμβολή μεταξύ διαμερίσεων ή υπερφορτώνει το επίπεδο ελέγχου [50]. Οι ενέργειες υψηλού κινδύνου απαιτούν επιβεβαίωση ή εφαρμόζονται αρχικά σε περιορισμένο τμήμα της υποδομής [51], [52].

Το βασικό πείραμα θα εισάγει διαδοχικά απώλεια ζεύξης, αποτυχία edge κόμβου, υπερφόρτωση της eMBB και απώλεια ενός ελεγκτή. Θα ελεγχθούν ο χρόνος ανίχνευσης, ο χρόνος αποκατάστασης, η διαθεσιμότητα ανά διαμέριση, η διατήρηση της απομόνωσης, η καθυστέρηση της κρίσιμης υπηρεσίας, η κατανάλωση ενέργειας και η επιβάρυνση σηματοδοσίας [50],[51],[52]. Ιδιαίτερη σημασία έχει η μέτρηση της υποβάθμισης στις διαμερίσεις που δεν προκάλεσαν το συμβάν, επειδή αυτή δείχνει αν η κοινόχρηστη υποδομή διατηρεί πραγματική απομόνωση υπό πίεση [53],[54].

Η αρχιτεκτονική θα αξιολογηθεί με δύο στρατηγικές ανθεκτικότητας. Η προληπτική στρατηγική διατηρεί εφεδρικές διαδρομές, πλεονάζοντες ελεγκτές και δεσμευμένο απόθεμα πόρων. Η αντιδραστική στρατηγική χρησιμοποιεί λιγότερους πόρους σε κανονική λειτουργία, αλλά

δημιουργεί νέες διαδρομές μετά την ανίχνευση της βλάβης. Η σύγκριση αναδεικνύει το πραγματικό αντάλλαγμα μεταξύ ταχύτητας αποκατάστασης, ενεργειακού κόστους και αποδοτικής χρήσης πόρων, χωρίς να προδικάζει ότι μία στρατηγική είναι κατάλληλη για όλες τις υπηρεσίες [52].

Εκτός από αυτές τις στρατηγικές ανθεκτικότητας, το μη επίγειο τμήμα του δικτύου μπορεί να διαδραματίσει ευρύτερο ρόλο στη διατήρηση της συνδεσιμότητας όταν η επίγεια υποδομή επηρεάζεται από μια φυσική καταστροφή. Τα μη επίγεια δίκτυα (NTN - Non-Terrestrial Network) έχουν τη δυνατότητα επέκτασης της συνδεσιμότητας μέσω δορυφόρων και εναέριων πλατφορμών. Αξιοσημείωτο είναι το γεγονός ότι κάτι τέτοιο μπορεί να επιτευχθεί ακόμη και όταν η συμβατική υποδομή δεν είναι διαθέσιμη ή δεν μπορεί να προσφέρει επαρκή κάλυψη. Αυτό είναι ιδιαίτερα σημαντικό μετά από μια φυσική καταστροφή, καθώς η κατάσταση του επίγειου δικτύου μπορεί να διαφέρει σημαντικά από περιοχή σε περιοχή. Ορισμένοι σταθμοί βάσης μπορεί να παραμένουν σε λειτουργία, ενώ άλλοι μπορεί να έχουν αποσυνδεθεί, να έχουν υπερφορτωθεί ή ακόμα και να έχουν καταστραφεί. Για τον λόγο αυτό, είναι απαραίτητο το σύστημα επικοινωνιών να μπορεί να αξιοποιεί τόσο επίγεια όσο και μη επίγεια τμήματα, αντί να εξαρτάται μόνο από ένα από τα δύο. Η ανάπτυξη του 6G αναμένεται να ενισχύσει αυτή την ενοποίηση, οδηγώντας σε έναν περισσότερο ενοποιημένο σχεδιασμό επίγειων και μη επίγειων δικτύων [63].

Ωστόσο, παρατηρείται ότι η διαχείριση του δικτύου γίνεται πιο δύσκολη ως αποτέλεσμα αυτής της ενσωμάτωσης. Αφού τα UAV (Unmanned Aerial Vehicle) και άλλοι εναέριοι κόμβοι ενδέχεται να αλλάζουν θέση κατά τη διάρκεια μιας επιχείρησης έκτακτης ανάγκης, η κατάσταση γίνεται ακόμη πιο σύνθετη στην περίπτωση των δορυφόρων σε χαμηλή τροχιά γύρω από τη Γη (LEO - Low Earth Orbit), οι οποίοι κινούνται συνεχώς και καλύπτουν μια συγκεκριμένη περιοχή μόνο προσωρινά. Η κίνηση αυτή έχει ως αποτέλεσμα η τοπολογία του δικτύου και οι διαθέσιμες συνδέσεις να μεταβάλλονται συνεχώς. Κάτι τέτοιο οδηγεί στη συνεχή εναλλαγή των χρηστών μεταξύ επίγειας και μη επίγειας κάλυψης, καθιστώντας έτσι τις επιλογές μεταγωγής (handover) κρίσιμες για τη διατήρηση της σύνδεσης. Παρόλα αυτά, η κίνηση των δορυφόρων μπορεί να προβλεφθεί σε κάποιο βαθμό. Με αυτόν τον τρόπο, είναι δυνατός ο προσδιορισμός πιθανών στόχων μεταγωγής και της μελλοντικής κάλυψης πριν από την απώλεια της τρέχουσας σύνδεσης. Αυτή η δυνατότητα θα μπορούσε να εξασφαλίσει πιο σταθερή επικοινωνία για τις κινητές ομάδες διάσωσης, τα μη επανδρωμένα αεροσκάφη (UAV) και άλλες υπηρεσίες που δραστηριοποιούνται σε περιοχές που έχουν υποστεί ζημιές ή έχουν μερική κάλυψη κατά τη διάρκεια μιας καταστροφής [63].

Ταυτόχρονα, οι διαθέσιμοι πόροι επεξεργασίας, αποθήκευσης και επικοινωνίας μπορούν να θεωρηθούν ως μια κοινόχρηστη δεξαμενή εικονικών πόρων. Το SDN προσφέρει, ωστόσο, τη δυνατότητα προγραμματιζόμενης διαχείρισης αυτών των πόρων. Επιπροσθέτως, παρέχει τη δυνατότητα τροποποίησης της δρομολόγησης της κυκλοφορίας με βάση τις συνθήκες του δικτύου, τη χρήση του εύρους ζώνης και τη διαθεσιμότητα των συνδέσεων. Επειδή οι λειτουργίες του δικτύου δεν εξαρτώνται πλέον από εξειδικευμένο υλικό, το NFV προσφέρει ένα επιπλέον επίπεδο ελευθερίας. Με αυτόν τον τρόπο, ανάλογα με τους πόρους που είναι διαθέσιμοι σε κάθε συγκεκριμένη χρονική στιγμή, οι εικονικές λειτουργίες δικτύου μπορούν να αναπτυχθούν σε διαφορετικούς κόμβους, όπως δορυφόρους, μη επανδρωμένα αεροσκάφη (UAV) ή επίγειους σταθμούς. Τέλος, αυτή η δυνατότητα αποκτά ιδιαίτερη σημασία όταν ένας προσωρινός κόμβος χάνει τη συνδεσιμότητά του ή όταν η διαθέσιμη ενέργεια και η υπολογιστική ισχύς του μειώνονται κατά τη διάρκεια μιας κατάστασης έκτακτης ανάγκης [63].

Στη συνέχεια, μέσω της διαμέρισης δικτύου, αυτή η κοινή υποδομή μπορεί να αξιοποιηθεί για υπηρεσίες με διαφορετικές απαιτήσεις, διατηρώντας παράλληλα ξεχωριστές ρυθμίσεις για καθεμία από αυτές. Για παράδειγμα, μια υπηρεσία χαμηλής καθυστέρησης μπορεί να επωφεληθεί από λειτουργίες που βρίσκονται πιο κοντά στους χρήστες, όπως σε έναν εναέριο ή σε έναν κοντινό επίγειο κόμβο, σε αντίθεση με μια υπηρεσία η οποία απαιτεί τη μεταφορά μεγαλύτερου όγκου δεδομένων, είναι πιθανό να χρειάζονται κόμβοι που διαθέτουν μεγαλύτερη επικοινωνιακή και υπολογιστική χωρητικότητα. Παρόμοια λογική μπορεί να εφαρμοστεί και σε υπηρεσίες που βασίζονται σε μεγάλο αριθμό αισθητήρων, όπου μέρος της επεξεργασίας μπορεί να κατανέμεται σε κατάλληλους edge ή μη επίγειους κόμβους. Επομένως, η κατανομή των διαθέσιμων πόρων δεν είναι απαραίτητο να παραμένει σταθερή καθ' όλη τη διάρκεια μιας κατάστασης έκτακτης ανάγκης. Αντίθετα, μπορεί να προσαρμόζεται ανάλογα με την κατάσταση του δικτύου και τις απαιτήσεις που παρουσιάζει κάθε υπηρεσία [63].

Ωστόσο, αυτή η προσαρμοστικότητα δημιουργεί μια ακόμη πρόκληση. Η κίνηση των δορυφόρων, οι αλλαγές στη θέση των εναέριων κόμβων ή οι δυσλειτουργίες στην υπόλοιπη επίγεια υποδομή μπορούν να επηρεάσουν τις διαθέσιμες διαδρομές. Επομένως, μια διαδρομή που είναι κατάλληλη σε μια συγκεκριμένη χρονική στιγμή μπορεί λίγο αργότερα να μην είναι πλέον διαθέσιμη. Για τον λόγο αυτό, η δρομολόγηση δεν μπορεί να αντιμετωπίζεται ως μια ξεχωριστή διαδικασία. Αντίθετα, η διαχείριση ενός μελλοντικού δικτύου έκτακτης ανάγκης 6G είναι αναγκαίο να λαμβάνει συνολικά υπόψη τους διαθέσιμους πόρους επικοινωνίας, υπολογιστικής ισχύος και αποθήκευσης. Εν κατακλείδι, το SDN, το NFV και η διαμέριση δικτύου μπορούν να προσφέρουν από κοινού ένα πλαίσιο που επιτρέπει την αναδιάταξη των υπηρεσιών καθώς μεταβάλλονται οι συνθήκες του δικτύου, ενώ, υπάρχει η δυνατότητα τα επίγεια και μη επίγεια στοιχεία της υποδομής να συνεχίσουν να λειτουργούν ως μέρη του ίδιου συστήματος επικοινωνίας [63].

4.6 Συγκριτικό πρωτόκολλο αξιολόγησης των σεναρίων

Τα τέσσερα σενάρια των προηγούμενων υποκεφαλαίων διατυπώνουν υποθέσεις και όχι αποτελέσματα. Για να αποκτήσουν ερευνητική αξία πρέπει να διατυπωθούν με τρόπο που να επιτρέπει τον έλεγχό τους, δηλαδή να ορίζεται εκ των προτέρων τι θα μετρηθεί, με ποια κατάσταση θα συγκριθεί και υπό ποιες συνθήκες θα θεωρηθεί ότι ο εξεταζόμενος μηχανισμός δεν προσέφερε τίποτε. Το παρόν υποκεφάλαιο ορίζει αυτό το κοινό πρωτόκολλο. Η βασική λογική παραμένει εκείνη του Κεφαλαίου 3, δηλαδή κατάσταση αναφοράς, παρέμβαση και τεκμήριο, επεκτείνεται όμως σε περιβάλλοντα με κινητικότητα, βλάβες, μεταβαλλόμενη ζήτηση και πολλές διαμερίσεις που λειτουργούν ταυτόχρονα, όπου η απλή επίδειξη λειτουργίας δεν αρκεί ως απόδειξη.

Για κάθε σενάριο ορίζονται τουλάχιστον δύο καταστάσεις. Η κατάσταση αναφοράς A0 υλοποιεί στατική ή ανεπαρκή πολιτική, χωρίς να είναι κατ' ανάγκη μη λειτουργική. Η κατάσταση A1 προσθέτει τον εξεταζόμενο μηχανισμό, δηλαδή τη δυναμική ενορχήστρωση διαμερίσεων, την προληπτική εγκατάσταση κανόνων, τον προσαρμοστικό βρόχο πόρων ή τη στρατηγική ανθεκτικότητας, ανάλογα με το σενάριο. Όπου εξετάζεται πρόβλεψη ή μάθηση προστίθεται τρίτη κατάσταση A2, ώστε να διαχωρίζεται η αντιδραστική από την προγνωστική συμπεριφορά. Ισχύει ένας απαράβατος κανόνας: μεταξύ δύο συγκρινόμενων καταστάσεων μεταβάλλεται ένας μόνο

παράγοντας. Αν χρειαστεί να αλλάξει και η τοπολογία ή το προφίλ κίνησης, η σύγκριση παύει να είναι ελεγχόμενη και το αποτέλεσμα δεν μπορεί να αποδοθεί στον μηχανισμό.

Ανάμεσα στις καταστάσεις παραμένουν αμετάβλητα η φυσική και λογική τοπολογία, τα ίχνη κίνησης και το χρονικό τους προφίλ, η διάρκεια εκτέλεσης, η στιγμή και η σειρά εισαγωγής των βλαβών, οι αρχικές τιμές των γεννητριών τυχαίων αριθμών, τα ανώτατα όρια πόρων και οι εκδόσεις του λογισμικού. Ορίζεται επίσης μια αρχική περίοδος σταθεροποίησης, τα δεδομένα της οποίας δεν λαμβάνονται υπόψη, και κοινό χρονικό παράθυρο μέτρησης για όλες τις εκτελέσεις. Υπάρχουν ωστόσο παράγοντες που δεν μπορούν να κρατηθούν σταθεροί, όπως η κίνηση των οχημάτων ή η μεταβαλλόμενη ορατότητα των δορυφόρων. Οι παράγοντες αυτοί καταγράφονται χωριστά και αναφέρονται μαζί με το αποτέλεσμα, ώστε να μην αποδίδεται στον εξεταζόμενο μηχανισμό μια μεταβολή που στην πραγματικότητα προήλθε από το περιβάλλον. Ο Πίνακας 5 συνοψίζει σε ποια αρχιτεκτονική και σε ποιους δείκτες εστιάζει κάθε σενάριο.

Πίνακας 5: Αντιστοίχιση μελλοντικών σεναρίων, αρχιτεκτονικών και βασικών δεικτών αξιολόγησης.

Σενάριο	Κύρια αρχιτεκτονική	Γεγονός ενεργοποίησης	Βασικοί δείκτες
Έξυπνο νοσοκομείο	Network Slicing και QoS	Έκτακτο περιστατικό και αιχμή τηλεμετρίας	Καθυστέρηση P99, απώλεια, χρόνος ενεργοποίησης, απομόνωση
Αυτόνομη κινητικότητα	Κατανεμημένο SDN	Βλάβη ζεύξης και συγκέντρωση οχημάτων	Χρόνος εγκατάστασης ροής, σηματοδοσία, χρόνος αναδρομολόγησης
Βιομηχανικό Edge	Python και ελεγχόμενη ML	Προβλέψιμη μεταβολή παραγωγικού φορτίου	Παραβιάσεις SLA, ακρίβεια πρόβλεψης, πόροι, ταλαντώσεις
Αντιμετώπιση καταστροφής	SDN, slicing, Edge και ψηφιακό δίδυμο	Πολλαπλές βλάβες και μεταβαλλόμενη κάλυψη	Χρόνος αποκατάστασης, διαθεσιμότητα, απομόνωση, ενέργεια

Η αξιολόγηση δεν στηρίζεται σε έναν συγκεντρωτικό δείκτη απόδοσης αλλά σε πέντε διακριτές οικογένειες δεικτών, καθεμία από τις οποίες απαντά σε διαφορετικό ερώτημα. Οι δείκτες υπηρεσίας μετρώνται πάντοτε ανά διαμέριση και όχι ως μέσος όρος του δικτύου, επειδή ένας ικανοποιητικός συνολικός μέσος όρος μπορεί να συγκαλύπτει πλήρη αποτυχία μιας κρίσιμης υπηρεσίας, ενώ για τις υπηρεσίες με αυστηρές απαιτήσεις αναφέρονται υποχρεωτικά υψηλά εκατοστημόρια [36]. Οι δείκτες του επιπέδου ελέγχου αποτυπώνουν το κόστος της κεντρικοποίησης, οι δείκτες απομόνωσης ελέγχονται πάντοτε στις διαμερίσεις που δεν προκάλεσαν το συμβάν, οι δείκτες κόστους αναφέρονται χωριστά και ποτέ συγχωνευμένοι με τους δείκτες επίδοσης, ενώ για τις προγνωστικές πολιτικές προστίθεται ξεχωριστή οικογένεια που αφορά την ποιότητα και τη σταθερότητα της ίδιας της πρόβλεψης [38],[39].

Πίνακας 6: Οικογένειες δεικτών του κοινού πρωτοκόλλου αξιολόγησης και το ερώτημα στο οποίο απαντά κάθε μία.

Οικογένεια δεικτών	Ενδεικτικοί δείκτες	Ερώτημα που απαντά	Πηγή τεκμηρίου
Υπηρεσία ανά διαμέριση	Καθυστέρηση (διάμεσος, P95, P99), διακύμανση, απώλεια, ρυθμός μετάδοσης, παραβιάσεις SLA	Τηρείται η δηλωμένη απαίτηση κάθε υπηρεσίας χωριστά;	Μετρήσεις ανά διαμέριση [36], [39]
Επίπεδο ελέγχου	Χρόνος εγκατάστασης κανόνα, μηνύματα Packet In και Flow Mod, φόρτος ελεγκτή, χρόνος αναδρομολόγησης και επαναφοράς πολιτικής	Κοστίζει ο κεντρικός έλεγχος περισσότερο από όσα προσφέρει;	Καταγραφές ελεγκτή, πίνακες ροών [53], [59]
Απομόνωση	Υποβάθμιση των διαμερίσεων που δεν προκάλεσαν το συμβάν, διαρροή κίνησης, διατήρηση ορίων στην ανακατανομή	Αντέχει η απομόνωση υπό πίεση και όχι μόνο σε κανονική λειτουργία;	Σενάριο εσφαλμένης διαμέρισης [23], [26], [47]
Κόστος και βιωσιμότητα	CPU και μνήμη στους κόμβους άκρου, ενέργεια, σηματοδοσία, δεσμευμένοι αχρησιμοποίητοι πόροι, πλήθος κλιμακώσεων	Με τι τίμημα επιτυγχάνεται το αποτέλεσμα;	Τηλεμετρία υποδομής [45], [54]
Προγνωστικές πολιτικές	Σφάλμα πρόβλεψης, χρόνος σύγκλισης, ταλαντώσεις, ενεργοποιήσεις ασφαλούς επαναφοράς, μοτίβα εκτός εκπαίδευσης	Υπερέχει πράγματι το μοντέλο έναντι ρητού κανόνα;	Επαναλήψεις με κοινά ίχνη [40], [41], [50]

Κάθε κατάσταση εκτελείται επαναλαμβανόμενα με τους ίδιους σπόρους τυχαιότητας, ώστε οι συγκρίσεις A0 προς A1 να γίνονται κατά ζεύγη και όχι μεταξύ ανεξάρτητων δειγμάτων. Αναφέρονται η κατανομή των τιμών, η διάμεσος, τα υψηλά εκατοστημόρια και ένα μέτρο διασποράς, ενώ ο μέσος όρος από μόνος του δεν θεωρείται επαρκής περιγραφή. Πριν από κάθε σύγκριση υπολογίζεται η διακύμανση μεταξύ επαναλήψεων της ίδιας κατάστασης και ορίζεται ως κατώφλι θορύβου: διαφορά μικρότερη από αυτή δεν αναφέρεται ως βελτίωση. Για πολιτικές που βασίζονται σε μάθηση προστίθενται ο διαχωρισμός δεδομένων εκπαίδευσης και αξιολόγησης, ο έλεγχος σε μοτίβα που δεν εμφανίστηκαν κατά την εκπαίδευση και η αναφορά του σφάλματος μαζί με τη μεταβλητότητά του [39]-[41].

Η αποδοχή μιας παρέμβασης δεν στηρίζεται στη βελτίωση ενός μόνο δείκτη αλλά σε έναν σύνθετο κανόνα. Η κατάσταση A1 γίνεται αποδεκτή έναντι της A0 μόνο όταν ισχύουν ταυτόχρονα τέσσερις συνθήκες: καμία κρίσιμη υπηρεσία δεν πέφτει κάτω από το ελάχιστο όριο που έχει δηλωθεί γι' αυτήν, ο δείκτης που επιδιώκεται να βελτιωθεί παρουσιάζει διαφορά μεγαλύτερη από τη φυσιολογική διακύμανση μεταξύ των επαναλήψεων, η κατανάλωση πόρων, ενέργειας και μηνυμάτων ελέγχου παραμένει μέσα στα όρια που είχαν τεθεί εκ των προτέρων, και οι διαμερίσεις που δεν προκάλεσαν το συμβάν δεν υποβαθμίζονται περισσότερο από όσο έχει συμφωνηθεί. Αν έστω και μία συνθήκη δεν ικανοποιείται, το αποτέλεσμα καταγράφεται ως αντιστάθμισμα και όχι ως βελτίωση [54]. Ο κανόνας αυτός αποτρέπει το συνηθέστερο σφάλμα αξιολόγησης, δηλαδή την

παρουσίαση μιας μείωσης της καθυστέρησης που στην πραγματικότητα επιτεύχθηκε με δέσμευση περισσότερων πόρων από όσους χρειάζονται, με αύξηση των μηνυμάτων ελέγχου ή με υποβάθμιση μιας άλλης διαμέρισης.

Κάθε αποτέλεσμα συνοδεύεται από τον χαρακτηρισμό του είδους τεκμηρίου στο οποίο στηρίζεται, με την ίδια διάκριση που τηρήθηκε στο Κεφάλαιο 3 ανάμεσα σε λειτουργική επαλήθευση, ελεγχόμενη δοκιμή λογικής και ποσοτική μέτρηση. Καταγράφονται ρητά οι απειλές εγκυρότητας: η εσωτερική εγκυρότητα απειλείται από μη ελεγχόμενες μεταβολές φόρτου ή εκδόσεων λογισμικού, η εγκυρότητα της μέτρησης από το γεγονός ότι οι χρονισμοί ενός εξομοιωμένου περιβάλλοντος δεν αντιστοιχούν σε πραγματικό ασύρματο και φυσικό επίπεδο, και η εξωτερική εγκυρότητα από τη μικρή κλίμακα των τοπολογιών και τη συνθετική φύση των ιχνών κίνησης [27]. Τα συμπεράσματα περιορίζονται στο συγκεκριμένο περιβάλλον και στο επίπεδο ωριμότητας της δοκιμής, χωρίς αυτόματη γενίκευση σε παραγωγικά δίκτυα [49].

Για κάθε εκτέλεση αποθηκεύονται οι εκδόσεις ελεγκτή, Open vSwitch, Mininet, Kubernetes και βιβλιοθηκών Python, τα αρχεία διαμόρφωσης και πολιτικής, οι τοπολογίες, τα ίχνη κίνησης, οι σπόροι τυχαιότητας και τα ακατέργαστα δεδομένα των μετρήσεων. Για τις πολιτικές που βασίζονται σε μάθηση αποθηκεύονται επιπλέον το μοντέλο, οι υπερπαράμετροι, τα δεδομένα εκπαίδευσης και οι συνθήκες υπό τις οποίες ενεργοποιήθηκε ο μηχανισμός ασφαλούς επαναφοράς [56],[57]. Η καταγραφή γίνεται με ενιαίο υπόδειγμα ανά εκτέλεση, σύμφωνα με τον Πίνακα ΠΙ.2 του Παραρτήματος, ώστε ένας τρίτος ερευνητής να μπορεί να αναπαραγάγει τη σύγκριση και να διακρίνει αν μια διαφορά οφείλεται στην αρχιτεκτονική ή σε τυχαία μεταβολή του περιβάλλοντος εκτέλεσης .

Με το πρωτόκολλο αυτό τα τέσσερα σενάρια παύουν να είναι αφηγήσεις δυνατοτήτων και γίνονται ελέγξιμες υποθέσεις με προκαθορισμένο κριτήριο απόρριψης. Η βασική διαφορά από την αξιολόγηση του Κεφαλαίου 3 είναι ότι εκεί αρκούσε η επίδειξη μιας λειτουργικής αλλαγής στην ίδια τοπολογία, ενώ εδώ απαιτούνται ταυτόχρονη τήρηση απαιτήσεων ανά υπηρεσία, διατήρηση της απομόνωσης υπό πίεση και ρητή λογιστική του κόστους. Το επόμενο υποκεφάλαιο εξετάζει τις προϋποθέσεις υπό τις οποίες το πρωτόκολλο αυτό μπορεί να εφαρμοστεί σταδιακά, ξεκινώντας από τα υπάρχοντα εργαλεία της εργασίας.

4.7 Προϋποθέσεις υλοποίησης και ερευνητικός οδικός χάρτης

Η σταδιακή υλοποίηση των σεναρίων μπορεί να ξεκινήσει από τα υφιστάμενα εργαλεία της εργασίας. Σε πρώτο στάδιο, το Mininet και το Open vSwitch μπορούν να αναπαραστήσουν πολλαπλές κατηγορίες κίνησης, ελεγχόμενη συμφόρηση και απώλεια ζεύξης. Ο OpenDaylight μπορεί να εφαρμόσει προληπτικές και αντιδραστικές πολιτικές, ενώ η Python μπορεί να συλλέγει μετρήσεις, να αποφασίζει και να καταγράφει κάθε αλλαγή. Στο στάδιο αυτό ο στόχος είναι η έγκυρη σύγκριση πολιτικών και όχι η πιστή αναπαράσταση ολόκληρου δικτύου κινητών επικοινωνιών.

Σε δεύτερο στάδιο, οι υπηρεσίες μπορούν να μεταφερθούν σε περιβάλλον Kubernetes και να συνδεθούν με πραγματική τηλεμετρία, ώστε η λογική P1 να εκτελεί κλιμάκωση και όχι μόνο unit tests. Η υποδομή θα πρέπει να περιλαμβάνει πολλαπλούς edge κόμβους, ελεγχόμενη κινητικότητα

και μηχανισμούς εισαγωγής βλαβών. Παράλληλα, η απομόνωση θα εξεταστεί σε επίπεδο υπολογιστικών πόρων, δικτύου και δικαιωμάτων διαχείρισης, καθώς η κοινή χρήση πλατφόρμας δημιουργεί κινδύνους που δεν εμφανίζονται σε απλή προσομοίωση VLAN.

Στο τρίτο στάδιο εισάγεται μοντέλο πρόβλεψης ή μηχανισμός ενισχυτικής μάθησης. Η δοκιμή γίνεται πρώτα πάνω στο ψηφιακό δίδυμο του δικτύου και έπειτα σε μικρό, περιορισμένο τμήμα της πραγματικής υποδομής [49]. Το μοντέλο αποκτά δικαίωμα να αλλάζει ρυθμίσεις μόνο εφόσον έχει δώσει καλύτερα αποτελέσματα από τον σαφή κανόνα, σε κριτήρια που έχουν οριστεί από πριν, και εφόσον οι αποφάσεις του παραμένουν μέσα στα επιτρεπτά όρια λειτουργίας. Με τη διάταξη αυτή μια λανθασμένη πρόβλεψη δεν μπορεί να προκαλέσει εκτεταμένη αλλαγή στο δίκτυο, ενώ παράλληλα μπορούν να μελετηθούν συστηματικά δίκτυα που προσαρμόζονται και αποκαθιστούν μόνα τους τη λειτουργία τους [51],[52].

Τα σενάρια δείχνουν ότι η αξία των SDN και της διαμέρισης δικτύου δεν περιορίζεται στον λογικό διαχωρισμό των υπηρεσιών ούτε στην κεντρική εγκατάσταση κανόνων. Προκύπτει από τον συνδυασμό τεσσάρων στοιχείων: της διαμέρισης, της προγραμματιζόμενης προώθησης, της συνεχούς συλλογής μετρήσεων και της αυτοματοποίησης που λειτουργεί μέσα σε καθορισμένα όρια. Η κύρια ερευνητική πρόκληση είναι να αποδειχθεί ότι ο συνδυασμός αυτός εξακολουθεί να τηρεί τις συμφωνίες επιπέδου υπηρεσίας και να διατηρεί την απομόνωση όταν μεταβάλλονται το φορτίο, η τοπολογία και οι διαθέσιμοι πόροι. Με αυτή την έννοια, το Κεφάλαιο 4 ορίζει τη συνέχεια της εργασίας: από την επαλήθευση της λειτουργίας κάθε μηχανισμού χωριστά, προς πειράματα που επαναλαμβάνονται με τις ίδιες συνθήκες και αξιολογούνται με πολλαπλά κριτήρια, σε περιβάλλοντα 5G Advanced, 6G και Edge.

Κρίσιμο στάδιο του ερευνητικού αυτού σχεδίου είναι η ομαλή μετάβαση από τον ελεγχόμενο πειραματισμό σε ένα πιο ρεαλιστικό δικτυακό περιβάλλον. Αν μια μέθοδος περάσει απευθείας από την προσομοίωση σε υποδομή που βρίσκεται σε λειτουργία, υπεισέρχονται παράγοντες που δύσκολα προσδιορίζονται και η αξιολόγηση χάνει την αξιοπιστία της. Για τον λόγο αυτό, κάθε νέα μέθοδος δοκιμάζεται πρώτα σε περιβάλλοντα όπου τα πρότυπα κυκλοφορίας, η διαθεσιμότητα των πόρων και τα περιστατικά βλάβης μπορούν να αναπαραχθούν με τις ίδιες συνθήκες όσες φορές χρειαστεί. Η μεταφορά της σε μεγαλύτερο περιβάλλον δοκιμών γίνεται μόνο αφού η συμπεριφορά της έχει καταγραφεί επαρκώς. Με τη σταδιακή αυτή προσέγγιση είναι επίσης ευκολότερο να διαπιστωθεί αν μια βελτίωση οφείλεται στην ίδια την προτεινόμενη πολιτική ή σε αλλαγές της υποδομής πάνω στην οποία εκτελέστηκε η δοκιμή [64].

Για τον λόγο αυτό, θα μπορούσε να προσφερθεί ένα ενδιάμεσο περιβάλλον μέσω ενός «Ψηφιακού Δίδυμου Δικτύου» (NDT - Network Digital Twin). Μια ψηφιακή αναπαράσταση μπορεί να αναπαράγει τα σχετικά στοιχεία της τοπολογίας ενός λειτουργικού δικτύου, τις συνθήκες κυκλοφορίας, τη διαμόρφωση δρομολόγησης και τους διαθέσιμους πόρους, αντί να πραγματοποιούνται άμεσα πειράματα στο δίκτυο. Στη συνέχεια, μπορούν να δοκιμαστούν διάφορες διαμορφώσεις χωρίς να επηρεάζονται οι χρήστες ή οι υπηρεσίες που βρίσκονται σε λειτουργία, γεγονός που το καθιστά ιδιαίτερα χρήσιμο όταν οι δοκιμές περιλαμβάνουν καταστάσεις όπως ακραία συμφόρηση, αστοχίες συνδέσεων ή ακατάλληλες ρυθμίσεις, οι οποίες θα ήταν απαράδεκτες σε ένα περιβάλλον παραγωγής. Αξίζει να σημειωθεί ότι, αυτές οι συνθήκες μπορούν να επιτευχθούν χωρίς να παρεμβαίνουν στις κανονικές λειτουργίες του δικτύου, χρησιμοποιώντας, όχι μόνο ελεγχόμενα δοκιμαστικά περιβάλλοντα αλλά και περιβάλλοντα προσομοίωσης [50],[64].

Επίσης, οι δοκιμές αστοχίας δεν θα αποτελούσαν τη μόνη λειτουργία του ψηφιακού δίδυμου, αφού θα μπορούσε να παρέχει τη σύγκριση διαφορετικών επιλογών δρομολόγησης ή κατανομής πόρων πριν από την εφαρμογή τους στην πραγματική υποδομή. Ενώ δείκτες όπως η καθυστέρηση και η αξιοποίηση της σύνδεσης μπορούν να αναλυθούν ως έξοδοι άλλα δεδομένα σχετικά με την κατάσταση του δικτύου, όπως η κίνηση, η τοπολογία και οι πολιτικές δρομολόγησης, μπορούν να παρέχονται ως εισόδους. Αυτό μειώνει την ανάγκη για προσαρμογές με τη μέθοδο δοκιμής και σφάλματος που γίνονται απευθείας στο λειτουργικό δίκτυο κατά τη διαδικασία λήψης αποφάσεων. Οι τεχνικές παρακολούθησης και συντονισμού που προτάθηκαν στις προηγούμενες φάσεις του οδικού χάρτη θα μπορούσαν στη συνέχεια να συνδεθούν με την ίδια στρατηγική [64].

Μια άλλη σημαντική προϋπόθεση αποτελεί η ποιότητα των δεδομένων που χρησιμοποιούνται από τα συστήματα πρόβλεψης. Η κανονική λειτουργία δεν πρέπει να είναι το μόνο στοιχείο που περιγράφουν τα δεδομένα εκπαίδευσης. Εάν το τελικό μοντέλο πρόκειται να λειτουργήσει υπό μεταβαλλόμενες συνθήκες δικτύου, απαιτείται επίσης να ληφθούν υπόψη τα επίπεδα συμφόρησης, τα διάφορα προφίλ κίνησης, οι διακοπές σύνδεσης και άλλες ακραίες καταστάσεις. Ωστόσο, όταν αλλάζει η τοπολογία, η κατανομή της κίνησης ή η διαθέσιμη χωρητικότητα, ένα μοντέλο που εκπαιδεύτηκε σε ένα πειραματικό περιβάλλον μπορεί να συμπεριφερθεί διαφορετικά. Επομένως, αντί να θεωρείται δεδομένη, η γενίκευση πρέπει να εξετάζεται άμεσα. Καθώς οι δοκιμές μετατοπίζονται από σχετικά μικρές τοπολογίες Mininet προς μεγαλύτερες και πιο ποικιλόμορφες υποδομές ακραίων σημείων, αυτό καθίσταται ακόμη πιο κρίσιμο [64].

Τέλος βλέπουμε ότι, η τελική μετάβαση στην αυτοματοποιημένη λειτουργία θα πρέπει να συνεχίσει να είναι σταδιακή. Αρχικά, ένα προγνωστικό μοντέλο ή ένας μηχανισμός ενισχυτικής μάθησης θα μπορούσε να υποβάλλει προτάσεις χωρίς να έχει τη δυνατότητα να τροποποιήσει το δίκτυο, ενώ οι επιλογές του θα μπορούν στη συνέχεια να αξιολογηθούν χρησιμοποιώντας τα ίδια πρότυπα SLA και αξιοποίησης πόρων με την τρέχουσα ντετερμινιστική πολιτική. Επιπλέον, θα μπορούσαν να επιτραπούν περιορισμένες ενέργειες εντός προκαθορισμένων λειτουργικών ορίων, μόλις η συμπεριφορά του μοντέλου κριθεί επαρκώς σταθερή. Επειδή η αβεβαιότητα στις προβλέψεις που βασίζονται στη μηχανική μάθηση (ML) εξακολουθεί να αποτελεί σημαντικό πρόβλημα για την εφαρμογή σε πραγματικές υποδομές επικοινωνιών, αυτοί οι περιορισμοί είναι ιδιαίτερα σημαντικοί. Τα ασφαλή εύρη λειτουργίας ενός μοντέλου μπορούν να προσδιοριστούν με τη βοήθεια ελεγχόμενων δοκιμών.

Συμπεραίνουμε ότι, η προσομοίωση, τα ψηφιακά δίδυμα, τα περιβάλλοντα δοκιμών και οι πραγματικές υποδομές δεν αντιμετωπίζονται ως ξεχωριστά ερευνητικά θέματα στον προτεινόμενο οδικό χάρτη, καθώς αποτελούν διαδοχικά στάδια επικύρωσης. Κάθε επίπεδο αυξάνει τον ρεαλισμό, αλλά προσθέτει επίσης νέες πηγές αβεβαιότητας οι οποίες που πρέπει να ποσοτικοποιηθούν και να καταγραφούν [64]. Επομένως, η επίτευξη ενός υψηλότερου επιπέδου αυτοματοποίησης δεν αποτελεί τον μοναδικό μακροπρόθεσμο στόχο. Καθώς οι μέθοδοι SDN και διαμέρισης δικτύου μεταφέρονται σε ολοένα και πιο σύνθετα περιβάλλοντα 5G-Advanced, 6G και Edge, δημιουργώντας έτσι σαν στόχο την δημιουργία μιας προσεγγιστικής διαχείρισης που θα διατηρεί τις αυτοματοποιημένες αποφάσεις ποσοτικοποιήσιμες, επαναλήψιμες και σωστά διαχειριζόμενες.

Συμπεράσματα εργασίας

Το κεντρικό ερώτημα της εργασίας ήταν αν ο συνδυασμός Network Slicing και SDN βελτιώνει τη διαχείριση πόρων, την ποιότητα υπηρεσίας και την ευελιξία. Η απάντηση που στηρίζουν τα τεκμήρια του Κεφαλαίου 3 είναι καταφατική με συγκεκριμένο νόημα: η συμβολή των δύο τεχνολογιών δεν είναι κάποια αυτόματη βελτίωση επιδόσεων, αλλά η μετατροπή σιωπηρών παραδοχών σε ρητές, επαληθεύσιμες και αναστρέψιμες πολιτικές. Στο B0 η απομόνωση ήταν συνέπεια της τοπολογίας και στο S1 έγινε ελέγξιμος κανόνας, στο M0 η προώθηση ήταν σιωπηρή προσδοκία και στο M1 εγγραφή ροής με μετρητές, στο P0 η κατανομή πόρων ήταν σταθερή παραδοχή και στο P1 συνάρτηση απόφασης με ελέγξιμες εισόδους.

Το κριτήριο επιτυχίας δεν μπορεί επομένως να είναι αν το δίκτυο λειτουργεί. Για κάθε υπηρεσία χρειάζονται τρία πράγματα: μια απαίτηση δηλωμένη ρητά, ένας μηχανισμός που την επιβάλλει και ένα τεκμήριο ότι η επιβολή γίνεται στην πράξη. Στο ίδιο οδηγεί και η διαπίστωση ότι καμία τεχνική από μόνη της δεν συνιστά διαμέριση. Τα VLAN δημιούργησαν όρια μεταξύ των υπηρεσιών, χωρίς να ορίζουν ποια επικοινωνία επιτρέπεται. Οι λίστες ελέγχου πρόσβασης όρισαν τι επιτρέπεται, χωρίς να δίνουν διαφορετική μεταχείριση στην κρίσιμη κίνηση. Η προτεραιότητα στην ουρά έδωσε αυτή τη μεταχείριση, αλλά μόνο μέσα στα όρια που είχαν θέσει οι δύο προηγούμενοι μηχανισμοί. Η διαμέριση προέκυψε μόνο από τον συνδυασμό τους. Η σύγκριση M0 και M1 δείχνει με τη σειρά της ότι η συγκέντρωση του ελέγχου σε ένα σημείο δεν εξαλείφει το σφάλμα, αλλά το μεταφέρει από τη συσκευή στην πολιτική· το κέρδος του SDN είναι ότι η πολιτική μπορεί πλέον να διαβαστεί, να ελεγχθεί και να διορθωθεί.

Ως προς την αυτοματοποίηση, το δύσκολο μέρος δεν είναι η απόφαση αλλά η διατύπωσή της ώστε να ελέγχεται πριν αποκτήσει εξουσία να μεταβάλλει το σύστημα· τα όρια και τα κατώφλια της πολιτικής αποτρέπουν την ταλάντωση, και άρα μια πολιτική πόρων πρέπει να σχεδιάζεται ντετερμινιστική και ελέγξιμη πριν γίνει προσαρμοστική. Τα εργαλεία, εξάλλου, διαφέρουν κυρίως στο είδος του τεκμηρίου: το Packet Tracer παρήγαγε τεκμήριο διαμόρφωσης, το Mininet με τον OpenDaylight τεκμήριο συμπεριφοράς και η Python τεκμήριο λογικής, ενώ κανένα δεν παρήγαγε τεκμήριο επίδοσης. Η αντιστοίχιση ισχυρισμού και τεκμηρίου αποδείχθηκε πιο καθοριστική για την αξιοπιστία της αξιολόγησης από την πιστότητα του περιβάλλοντος.

Από τα παραπάνω προκύπτουν και τα όρια της εργασίας. Δεν αποδείχθηκε ότι η καθυστέρηση ή οι απώλειες μειώνονται, γιατί τέτοιες μετρήσεις δεν έγιναν. Η απομόνωση ελέγχθηκε μόνο για μία κατεύθυνση κίνησης και σε κανονικές συνθήκες, οι κανόνες ροής μόνο ως προς το αν αποκαθιστούν την επικοινωνία, και η κλιμάκωση των πόρων μόνο ως λογική, όχι σε πραγματικό σύστημα. Όσα υποστηρίζει η βιβλιογραφία για ποσοτική βελτίωση ούτε επιβεβαιώνονται ούτε αναιρούνται εδώ· η εργασία δείχνει μόνο με ποιον τρόπο θα μπορούσε να προκύψει. Εκεί βρίσκεται και η μεθοδολογική συμβολή: όταν η κατάσταση αναφοράς αποτυγχάνει σκόπιμα σε ένα μόνο σημείο, φαίνεται καθαρά τι προσθέτει η παρέμβαση· γι' αυτό η αποτυχία του ελέγχου στο M0 ήταν το πιο χρήσιμο αποτέλεσμα των πειραμάτων.

Για τον σχεδιαστή προκύπτει συγκεκριμένη σειρά: πρώτα η απαίτηση ανά υπηρεσία, έπειτα ο μηχανισμός και τέλος το τεκμήριο επιβολής· και επειδή ο κεντρικός έλεγχος διαδίδει εξίσου γρήγορα μια ορθή και μια λανθασμένη πολιτική, ο έλεγχος εκδόσεων, η καταγραφή ενεργειών και η ασφαλής επαναφορά ανήκουν στην αρχιτεκτονική. Ανοιχτά παραμένουν η αντοχή της

απομόνωσης υπό κακόβουλη συμπεριφορά διαμέρισης, το κόστος του κεντρικού ελέγχου σε μεγαλύτερη κλίμακα και η υπεροχή μιας προγνωστικής πολιτικής έναντι ενός ρητού κανόνα, ερωτήματα που το Κεφάλαιο 4 μετατρέπει σε σενάρια με κοινό πρωτόκολλο. Τελικό συμπέρασμα: η αξία των SDN και Network Slicing δεν βρίσκεται στο ότι κάνουν το δίκτυο ταχύτερο, αλλά στο ότι το καθιστούν δηλώσιμο, επαληθεύσιμο και αναστρέψιμο, ιδιότητες που επιτρέπουν να τεθεί σε επόμενο στάδιο, με μετρήσεις, το ερώτημα της επίδοσης.

Βιβλιογραφία

[1] Barakabitze, Alcardo Alex, Arslan Ahmad, Rashid Mijumbi, and Andrew Hines. "5G Network Slicing Using SDN and NFV: A Survey of Taxonomy, Architectures and Future Challenges." *Computer Networks* 167 (2020): 106984. https://www.sciencedirect.com/science/article/pii/S1389128619304773?via%3Dihub

[2] Qureshi, Hassaan N., Manzoor Manalastas, Alcardo Alex Barakabitze, Ali Imran, Sajjad A. Al-Ahmadi, and Muhammad Ali. "Service Level Agreements for 5G and Beyond: Overview, Challenges and Enablers of 5G-Healthcare Systems." *IEEE Access* 9 (2021): 1044–1061. https://ieeexplore.ieee.org/document/9305243

[3] Foukas, Xenofon, Georgios Patounas, Ahmed Elmokashfi, and Mahesh K. Marina. "Network Slicing in 5G: Survey and Challenges." *IEEE Communications Magazine* 55, no. 5 (2017): 94–100. https://ieeexplore.ieee.org/document/7926923

[4] Kreutz, Diego, Fernando M. V. Ramos, Paulo Esteves Verissimo, Christian Esteve Rothenberg, Siamak Azodolmolky, and Steve Uhlig. "Software-Defined Networking: A Comprehensive Survey." *Proceedings of the IEEE* 103, no. 1 (2015): 14–76. https://ieeexplore.ieee.org/document/6994333

[5] Ebrahimi, Sina, Faouzi Bouali, and Olivier C. L. Haas. "Resource Management From Single-Domain 5G to End-to-End 6G Network Slicing: A Survey." *IEEE Communications Surveys & Tutorials* 26, no. 4 (2024): 2836–2866. https://ieeexplore.ieee.org/document/10504277

[6] Park, Kibeom, Sangmo Sung, Hokeun Kim, and Jae-il Jung. "Technology Trends and Challenges in SDN and Service Assurance for End-to-End Network Slicing." *Computer Networks* 234 (2023): 109908. https://www.sciencedirect.com/science/article/pii/S1389128623003535?via%3Dihub

[7] Goyal, Pankaj, Rao Mikkilineni, and Murthy Ganti. "FCAPS in the Business Services Fabric Model." *2009 18th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises* (2009): 45–51. https://ieeexplore.ieee.org/document/5159212

[8] Jimson, Edwin R., Katsuhiro Nisar, and Mohammad Hijazi. "Bandwidth Management Using Software Defined Network and Comparison of the Throughput Performance with Traditional Network." *2017 International Conference on Information and Communication Technology Convergence (IConDA)* (2017): 71–76. https://ieeexplore.ieee.org/document/8270402

[9] Mousa, Mohammad, Ayman M. Bahaa-Eldin, and Mohamed Sobh. "Software Defined Networking Concepts and Challenges." *2016 11th International Conference on Computer Engineering & Systems (ICCES)* (2016): 79–90. https://ieeexplore.ieee.org/document/7821979

[10] Debbabi, Fadoua, Rihab Jmal, and Lamia Chaari Fourati. "5G Network Slicing: Fundamental Concepts, Architectures, Algorithmics, Projects Practices, and Open Issues." *Concurrency and Computation:*

Practice and Experience 33, no. 20 (2021): e6352. https://onlinelibrary.wiley.com/doi/10.1002/cpe.6352

[11] Khan, Latif U., Ibrar Yaqoob, Nguyen H. Tran, Zhu Han, and Choong Seon Hong. "Network Slicing: Recent Advances, Taxonomy, Requirements, and Open Research Challenges." *IEEE Access* 8 (2020): 36009–36028. https://ieeexplore.ieee.org/document/9003208/

[12] De Alwis, Chamitha, Pawani Porambage, Kapal Dev, Thippa Reddy Gadekallu, and Madhusanka Liyanage. "A Survey on Network Slicing Security: Attacks, Challenges, Solutions and Research Directions." *IEEE Communications Surveys & Tutorials* 26, no. 1 (2024): 534–570. https://ieeexplore.ieee.org/document/10242032

[13] Wijethilaka, Shalitha, and Madhusanka Liyanage. "Survey on Network Slicing for Internet of Things Realization in 5G Networks." *IEEE Communications Surveys & Tutorials* 23, no. 2 (2021): 957–994. https://ieeexplore.ieee.org/document/9382385

[14] Phyu, Hnin Pann, Diala Naboulsi, and Razvan Stanica. "Machine Learning in Network Slicing—A Survey." *IEEE Access* 11 (2023): 39123–39153. https://ieeexplore.ieee.org/document/10103689

[15] Olimid, Ruxandra F., and Gianfranco Nencioni. "5G Network Slicing: A Security Overview." *IEEE Access* 8 (2020): 99999–100009. https://ieeexplore.ieee.org/document/9099823

[16] Asadi, Somayeh, John Allison, Manpreet Khurana, and Mehrbakhsh Nilashi. "Simulation-Based Learning for Computer and Networking Teaching: A Systematic Literature Review and Bibliometric Analysis." *Education and Information Technologies* 29, no. 12 (2024): 15655–15690. https://link.springer.com/article/10.1007/s10639-024-12476-7

[17] Mwansa, Gift, M. R. Ngandu, and Z. S. Dasi. "Enhancing Practical Skills in Computer Networking: Evaluating the Unique Impact of Simulation Tools, Particularly Cisco Packet Tracer, in Resource-Constrained Higher Education Settings." *Education Sciences* 14, no. 10 (2024): 1099. https://www.mdpi.com/2227-7102/14/10/1099

[18] Han, M. P., S. Y. Htet, and L. Wuttisittikulkij. "Hybrid GNS3 and Mininet-WiFi Emulator for SDN Backbone Network Supporting Wireless IoT Traffic." *Proceedings of the 37th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC)* (2022): 768–771. https://ieeexplore.ieee.org/document/9895019

[19] Chaudhary, Rishabh, Gagangeet Singh Aujla, Neeraj Kumar, and P. K. Chouhan. "A Comprehensive Survey on Software Defined Networking for Smart Communities." *International Journal of Communication Systems* 38, no. 1 (2025): e5296. https://onlinelibrary.wiley.com/doi/10.1002/dac.5296

[20] Al Jameel, Mohammed. *Multimedia Traffic Management over Software-Defined Networking*. PhD thesis, University of Northampton, 2024. https://nectar.northampton.ac.uk/id/eprint/20861

[21] Minardi, Mario. *Traffic Engineering Algorithms for Software Defined Satellite-Terrestrial Networks*. PhD thesis, University of Luxembourg, 2023. https://orbilu.uni.lu/handle/10993/57763

[22] Wang, Qi, José M. Alcaraz-Calero, Ruben Ricart-Sanchez, Maria Barros Weiss, Anastasius Gavras, Navid Nikaein, Xenofon Vasilakos, et al. “Enable Advanced QoS-Aware Network Slicing in 5G Networks for Slice-Based Media Use Cases.” *IEEE Transactions on Broadcasting* 65, no. 2 (2019): 444–453. https://ieeexplore.ieee.org/document/8667001/

[23] Wong, Stan, Bin Han, and Hans D. Schotten. “5G Network Slice Isolation.” *Network* 2, no. 1 (2022): 153–167. https://www.mdpi.com/2673-8732/2/1/11

[24] Geesu, Lilian, and Raman Sabri. *The Impact of Slice Isolation on Fault Recovery and Reliability in 5G Networks*. Bachelor’s thesis, KTH Royal Institute of Technology, 2025. https://www.diva-portal.org/smash/get/diva2:2001288/FULLTEXT01.pdf

[25] Gao, Shujuan, Ruyan Lin, Yulong Fu, Hui Li, and Jin Cao. “Security Threats, Requirements and Recommendations on Creating 5G Network Slicing System: A Survey.” *Electronics* 13, no. 10 (2024): 1860. https://www.mdpi.com/2079-9292/13/10/1860

[26] Bolourian, Mehdi, Noura Limam, Mohammad Ali Salahuddin, and Raouf Boutaba. “5Guard: Isolation-Aware End-to-End Slicing of 5G Networks.” *IEEE Transactions on Mobile Computing* 25, no. 4 (2026): 4979–4996. https://ieeexplore.ieee.org/document/11223090

[27] Bakni, Michel, Yudith Cardinale, and Luis Manuel Moreno. “Experiences on Evaluating Network Simulators: A Methodological Approach.” *Journal of Communications* 14, no. 10 (2019): 866–875. https://www.jocm.us/show-231-1433-1.html

[28] Cisco Systems. VLAN Configuration Guide, Cisco IOS XE 17.17.x (Catalyst 9400 Switches). Cisco. https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9400/software/release/17-17/configuration_guide/vlan/b_1717_vlan_9400_cg/configuring_vlans.html

[29] Cisco Systems. *Security Configuration Guide: Access Control Lists, Cisco NCS 4200 Series.* Cisco. https://www.cisco.com/c/en/us/td/docs/routers/ncs4200/configuration/guide/security/17-1-1/b-sec-data-acl-17-1-1-ncs4200.pdf

[30] Cisco Systems. *Quality of Service Configuration Guide, Cisco IOS XE 17.18.x (Catalyst 9300 Switches).* Cisco. https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst9300/software/release/17-18/configuration_guide/qos/b_1718_qos_9300_cg.html

[31] Shu, Zhaogang, and Tarik Taleb. “A Novel QoS Framework for Network Slicing in 5G and Beyond Networks Based on SDN and NFV.” *IEEE Network* 34, no. 3 (2020): 256–263. https://ieeexplore.ieee.org/document/9076109

[32] Arjona Villicaña, Pedro David. *Testing Software Defined Networks with OpenDaylight and Mininet*. Facultad de Ingeniería, Universidad Autónoma de San Luis Potosí, 2025. https://repositorioinstitucional.uaslp.mx/xmlui/handle/i/8772

[33] Chiang, Min-Chi, and Jerry Chou. “DynamoML: Dynamic Resource Management Operators for Machine Learning Workloads.” *Proceedings of the 11th International Conference on Cloud Computing and Services Science (CLOSER 2021)* (2021): 122–132. https://www.scitepress.org/PublishedPapers/2021/104834

[34] Chiang, Min-Chi, Lu-Wen Zhang, Yu-Min Chou, and Jerry Chou. “Dynamic Resource Management for Machine Learning Pipeline Workloads.” *SN Computer Science* 4, no. 5 (2023): 665. https://link.springer.com/article/10.1007/s42979-023-02101-8

[35] Goswami, Amit. *Dynamic Load Balancing and Resource Management Using Machine Learning*. Master's thesis, National College of Ireland, 2023. https://norma.ncirl.ie/6470/

[36] European Telecommunications Standards Institute (ETSI). *ETSI TS 128 554 V16.18.0 (2025-07): 5G; Management and Orchestration; 5G End to End Key Performance Indicators (KPI) (3GPP TS 28.554 Version 16.18.0 Release 16)*. ETSI, 2025. https://www.etsi.org/deliver/etsi_ts/128500_128599/128554/16.18.00_60/ts_128554v161800p.pdf

[37] European Telecommunications Standards Institute (ETSI). *ETSI TS 123 501 V18.8.0 (2025-01): 5G; System Architecture for the 5G System (5GS) (3GPP TS 23.501 Version 18.8.0 Release 18)*. ETSI, 2025. https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/18.08.00_60/ts_123501v180800p.pdf

[38] European Telecommunications Standards Institute (ETSI). *ETSI TS 128 552 V17.17.0 (2025-04): 5G; Management and Orchestration; 5G Performance Measurements (3GPP TS 28.552 Version 17.17.0 Release 17)*. ETSI, 2025. https://www.etsi.org/deliver/etsi_ts/128500_128599/128552/17.17.00_60/ts_128552v171700p.pdf

[39] Rainio, Oona, Jarmo Teuho, and Riku Klén. "Evaluation Metrics and Statistical Tests for Machine Learning." *Scientific Reports* 14 (2024): 6086. https://www.nature.com/articles/s41598-024-56706-x

[40] Chief Digital and Artificial Intelligence Office (CDAO). *Test and Evaluation of Artificial Intelligence Models: What to Consider in a Test & Evaluation Strategy*. U.S. Department of Defense, 2024. https://www.ai.mil/Portals/137/Documents/Resources%20Page/CDAO_TE_Framework_-_Model_TES_2024-04-compressed.pdf

[41] Comet. *Standardizing the ML Experimentation Process: Why You Need a Standard Approach to Achieve Reproducibility in ML and How to Get There*. Comet. https://go.comet.ml/rs/912-JJP-445/images/eBook-Comet-Standardizing_ML_Experimentation_Process.pdf

[42] Mao, Hongzi, Mohammad Alizadeh, Ishai Menache, and Srikanth Kandula. "Resource Management with Deep Reinforcement Learning." *Proceedings of the 15th ACM Workshop on Hot Topics in Networks (HotNets '16)* (2016): 50–56. https://dl.acm.org/doi/10.1145/3005745.3005750

[43] Batista, Bruno Guazzelli, Julio Cezar Estrella, Carlos Henrique Gomes Ferreira, Dionisio Machado Leite Filho, Luis Hideo Vasconcelos Nakamura, Stephan Reiff-Marganiec, Marcos José Santana, and Regina Helena Carlucci Santana. "Performance Evaluation of Resource Management in Cloud Computing Environments." *PLOS ONE* 10, no. 11 (2015): e0141914. https://pmc.ncbi.nlm.nih.gov/articles/PMC4640522

[44] Moreno-Vozmediano, Rafael, Eduardo Huedo, Rubén S. Montero, and Ignacio M. Llorente. "AI-Driven Resource Allocation and Auto-Scaling of VNFs in Edge-5G-IoT Ecosystems." *Electronics* 14, no. 9 (2025): 1808. https://www.mdpi.com/2079-9292/14/9/1808

[45] Moritz, Philipp, Robert Nishihara, Stephanie Wang, Alexey Tumanov, Richard Liaw, Eric Liang, Melih Elibol, Zongheng Yang, William Paul, Michael I. Jordan, and Ion Stoica. "Ray: A Distributed Framework for Emerging AI Applications." *13th USENIX Symposium on Operating Systems Design and Implementation (OSDI '18)* (2018): 561–577. https://www.usenix.org/conference/osdi18/presentation/moritz

[46] European Union Agency for Cybersecurity (ENISA). *NFV Security in 5G: Challenges and Best Practices*. ENISA, 2022. https://www.enisa.europa.eu/publications/nfv-security-in-5g-challenges-and-best-practices

[47] Donatti, Adnei Willian, Sand L. Corrêa, Joberto S. B. Martins, Antonio J. G. Abelém, Cristiano Bonato Both, Flávio de Oliveira Silva, José A. Suruagy, Rafael Pasquini, Rodrigo Moreira, Kleber V. Cardoso, and Tereza C. Carvalho. "Survey on Machine Learning-Enabled Network Slicing: Covering the Entire Life Cycle." *IEEE Transactions on Network and Service Management* 21, no. 1 (2024): 994–1011. https://ieeexplore.ieee.org/document/10158410/

[48] Shah, Syed Danial Ali, Mark A. Gregory, and Shuo Li. "Cloud-Native Network Slicing Using Software Defined Networking Based Multi-Access Edge Computing: A Survey." *IEEE Access* 9 (2021): 10903–10924. https://ieeexplore.ieee.org/document/9317860

[49] Lavin, Alexander, Ciarán M. Gilligan-Lee, Alessya Visnjic, Siddha Ganju, Dava Newman, Sujoy Ganguly, Danny Lange, et al. "Technology Readiness Levels for Machine Learning Systems." *Nature Communications* 13 (2022): 6039. https://www.nature.com/articles/s41467-022-33128-9

[50] Bikkasani, Dileesh Chandra. "Network Resiliency and Fault Tolerance through Digital Twins and Data Science." *American Journal of Data, Information and Knowledge Management* 6, no. 1 (2025): 1–14. https://ajpojournals.org/journals/index.php/ajdikm/article/view/2682

[51] Osman, Mutaz Salah Mohamed. "Resilient AI-Driven Network Slicing for Disaster-Aware 6G Infrastructures." *Acta Scientific Computer Sciences* 7, no. 6 (2025): 11–20. https://actascientific.com/ASCS/pdf/ASCS-07-0582.pdf

[52] Vittal, Shwetha, Sourav Sarkar, and A. Antony Franklin. "Revamping the Resilience and High Availability of 5G Core for 6G Ready Network Slices." *IEEE Transactions on Network and Service Management* 21, no. 2 (2024): 2287–2302. https://ieeexplore.ieee.org/document/10376225

[53] Sasan, Zeinab, and Siavash Khorsandi. "Balancing Resource Utilization and Slice Dissatisfaction through Dynamic Soft Slicing for 6G Wireless Networks." *Scientific Reports* 15 (2025): 22987. https://www.nature.com/articles/s41598-025-06521-9

[54] Esmat, Haitham H., Beatriz Lorenzo, and Weisong Shi. "Toward Resilient Network Slicing for Satellite-Terrestrial Edge Computing IoT." *IEEE Internet of Things Journal* 10, no. 16 (2023): 14621–14645. https://ieeexplore.ieee.org/document/10129129

[55] Dalle, Olivier, and Cyrine Mrabet. "An Instrumentation Framework for Component-Based Simulations Based on the Separation of Concerns Paradigm." *Proceedings of the 6th EUROSIM Congress on Modelling and Simulation (EUROSIM 2007)*, Ljubljana, Slovenia, 2007: 10 pp. https://www-sop.inria.fr/mascotte/Publications/Year/2007.complete.html

[56] Stubbe, Henning, Sebastian Gallenmüller, and Georg Carle. "The Pos Experiment Controller: Reproducible & Portable Network Experiments." *2024 19th Wireless On-Demand Network Systems and Services Conference (WONS)* (2024): 85–92. https://ieeexplore.ieee.org/document/10449532

[57] Handigol, Nikhil, Brandon Heller, Vimalkumar Jeyakumar, Bob Lantz, and Nick McKeown. "Reproducible Network Experiments Using Container-Based Emulation." *Proceedings of the 8th International Conference on Emerging Networking Experiments and Technologies (CoNEXT '12)* (2012):

253–264.
https://dl.acm.org/doi/10.1145/2413176.2413206
[58] Open Networking Foundation (ONF). *SDN Architecture*. Issue 1.1, ONF TR-521. Open Networking Foundation, 2016. https://opennetworking.org/wp-content/uploads/2014/10/TR-521_SDN_Architecture_issue_1.1.pdf
[59] International Telecommunication Union (ITU). *Framework and Overall Objectives of the Future Development of IMT for 2030 and Beyond*. Recommendation ITU-R M.2160-0, 2023. https://www.itu.int/rec/R-REC-M.2160-0-202311-I
[60] Tang, Xiaoyong, Lijun Zhao, Jing Chong, Zhengpeng You, Lei Zhu, Haiying Ren, Yuxiang Shang, et al. "5G-Based Smart Healthcare System Designing and Field Trial in Hospitals." *IET Communications* 16, no. 1 (2022): 1–13. https://ietresearch.onlinelibrary.wiley.com/doi/10.1049/cmu2.12300
[61] Lin, Shih-Chun, Kwang-Cheng Chen, and Ali Karimoddini. "SD-VEC: Software-Defined Vehicular Edge Computing with Ultra-Low Latency." *IEEE Communications Magazine* 59, no. 12 (2022): 66–72. https://arxiv.org/abs/2103.14225
[62] Ju, Li, Prashant Singh, and Salman Toor. "Proactive Autoscaling for Edge Computing Systems with Kubernetes." *2021 IEEE/ACM 14th International Conference on Utility and Cloud Computing (UCC '21) Companion* (2021). DOI: 10.1145/3492323.3495588. https://arxiv.org/abs/2112.10127
[63] Wang, Feng, Shengyu Zhang, Huiting Yang, and Tony Q. S. Quek. "Non-Terrestrial Networking for 6G: Evolution, Opportunities, and Future Directions." *Engineering* 54 (2025): 56–68. https://www.sciencedirect.com/science/article/pii/S2095809925002917
[64] Almasan, Paul, Miquel Ferriol-Galmés, Jordi Paillisse, José Suárez-Varela, Diego Perino, Diego López, Antonio Agustin Pastor Perales, Paul Harvey, Laurent Ciavaglia, Leon Wong, et al. "Network Digital Twin: Context, Enabling Technologies, and Opportunities." *IEEE Communications Magazine* 60, no. 11 (2022): 22–27. DOI: 10.1109/MCOM.001.2200012. https://ieeexplore.ieee.org/document/9795043

Παράρτημα Ι: Συμπληρωματικό υλικό προσομοιώσεων και ενδεικτικές ρυθμίσεις

Το παρόν παράρτημα συγκεντρώνει συμπληρωματικό υλικό που υποστηρίζει την πρακτική πλευρά της διπλωματικής εργασίας. Δεν επαναλαμβάνει τη θεωρητική ανάλυση των προηγούμενων κεφαλαίων, αλλά παρουσιάζει με πιο συγκεντρωμένο τρόπο ενδεικτικές ρυθμίσεις, βοηθητικό κώδικα και πίνακες τεκμηρίωσης που χρησιμοποιούνται για την αναπαραγωγή των σεναρίων προσομοίωσης. Το υλικό συνδέεται κυρίως με τις ενότητες που αφορούν την υλοποίηση Network Slicing με VLANs, ACLs, QoS και routing, καθώς και με τις SDN τοπολογίες σε GNS3/Mininet και τη δυναμική διαχείριση πόρων με Python.

Ι.1 Συνοπτική αντιστοίχιση διαμερίσεων, μηχανισμών και μετρικών αξιολόγησης

Στα σενάρια της εργασίας οι διαμερίσεις δικτύου αντιμετωπίζονται ως λογικά απομονωμένα περιβάλλοντα πάνω στην ίδια φυσική υποδομή. Κάθε διαμέριση εξυπηρετεί διαφορετικό είδος υπηρεσίας και επομένως αξιολογείται με διαφορετική έμφαση στις μετρικές απόδοσης. Ο ακόλουθος πίνακας λειτουργεί ως συμπληρωματικός οδηγός για τον τρόπο με τον οποίο αντιστοιχίζονται οι απαιτήσεις των υπηρεσιών με τους μηχανισμούς υλοποίησης.

Πίνακας ΠΙ.1: Συμπληρωματική αντιστοίχιση διαμερίσεων και μηχανισμών αξιολόγησης

Διαμέριση / χρήση	**Κύρια απαίτηση**	**Ενδεικτικός μηχανισμός**	**Μετρικές ελέγχου**
eMBB / υψηλή χωρητικότητα	Μεγάλο εύρος ζώνης και σταθερή διεκπεραιωτική ικανότητα	VLAN, QoS class, προτεραιοποίηση σε policy-map	Throughput, αξιοποίηση συνδέσεων, απώλεια πακέτων
URLLC / χαμηλή καθυστέρηση	Μικρή καθυστέρηση και αυξημένη αξιοπιστία	ACLs, traffic classification, SDN κανόνες ροής	Latency, jitter, packet loss, χρόνος εγκατάστασης κανόνων
mMTC / IoT κίνηση	Μεγάλος αριθμός συσκευών με μικρές ροές δεδομένων	Λογική απομόνωση, βασικό routing, έλεγχος συμφόρησης	Πλήθος ενεργών ροών, σταθερότητα, συμπεριφορά σε αιχμές
Διαχείριση και έλεγχος	Ασφαλής παραμετροποίηση και εποπτεία του δικτύου	Ξεχωριστό management VLAN, περιοριστικές ACLs	Διαθεσιμότητα ελέγχου, χρόνος απόκρισης, απομόνωση πρόσβασης

Ι.2 Ενδεικτική διαμόρφωση VLANs, trunk και access θυρών σε Cisco Packet Tracer

Το παρακάτω απόσπασμα δείχνει μια ενδεικτική λογική διαμόρφωσης μεταγωγέα για τρεις διακριτές κατηγορίες κίνησης. Οι αριθμοί των VLANs ακολουθούν το πνεύμα των σεναρίων της

εργασίας, όπου διαφορετικά τμήματα της υποδομής αντιστοιχίζονται σε διαφορετικές υπηρεσίες ή πολιτικές απομόνωσης. Η εντολή trunk επιτρέπει τη μεταφορά περισσότερων από ένα VLANs μεταξύ μεταγωγέων ή μεταξύ μεταγωγέα και δρομολογητή, ενώ οι access θύρες αντιστοιχίζουν τελικές συσκευές σε συγκεκριμένη διαμέριση.

```
enable
configure terminal
!
vlan 11
 name MANAGEMENT_SLICE
vlan 110
 name EMBB_SLICE
vlan 210
 name URLLC_SLICE
!
interface fastEthernet0/1
 description Trunk προς δρομολογητή ή κεντρικό switch
 switchport mode trunk
 switchport trunk allowed vlan 11,110,210
!
interface range fastEthernet0/2-5
 description Τελικές συσκευές eMBB
 switchport mode access
 switchport access vlan 110
 spanning-tree portfast
!
interface range fastEthernet0/6-8
 description Τελικές συσκευές URLLC
 switchport mode access
 switchport access vlan 210
 spanning-tree portfast
end
write memory
```

I.3 Ενδεικτική διαμόρφωση ACL και QoS για απομόνωση και προτεραιοποίηση

Η χρήση ACLs και QoS αποτελεί πρακτικό τρόπο για να προσεγγιστεί η λογική του Network Slicing σε περιβάλλοντα παραδοσιακής δικτύωσης. Η ACL μπορεί να περιορίσει την επικοινωνία ανάμεσα σε διαμερίσεις, ενώ η πολιτική QoS μπορεί να αναγνωρίσει κρίσιμη κίνηση και να της δώσει προτεραιότητα. Με τον τρόπο αυτό επιτυγχάνεται καλύτερη απομόνωση, περιορισμός ανεπιθύμητης πρόσβασης και πιο ελεγχόμενη συμπεριφορά σε συνθήκες αυξημένου φόρτου.

```
configure terminal
!
ip access-list extended Deny_Subnet
 deny ip 192.168.110.0 0.0.0.255 192.168.210.0 0.0.0.255
 permit ip any any
!
ip access-list extended Servers_Priority
 permit tcp any host 192.168.210.10 eq 443
 permit udp any host 192.168.210.20 range 5000 6000
!
class-map match-any CRITICAL_TRAFFIC
 match access-group name Servers_Priority
!
policy-map SLICING_QOS_POLICY
 class CRITICAL_TRAFFIC
```

```
  priority percent 30
 class class-default
  fair-queue
!
interface gigabitEthernet0/0
 description Σύνδεση προς το δίκτυο κορμού
 ip access-group Deny_Subnet in
 service-policy output SLICING_QOS_POLICY
end
```

I.4 Σενάριο Mininet και πολιτική διαμερίσεων του πειράματος της ενότητας 3.3

Παρατίθενται τα δύο προγράμματα του πειράματος της ενότητας 3.3. Το slicing_topo.py δημιουργεί την τοπολογία της Εικόνας 27 και συνδέει τους μεταγωγείς με τον OpenDaylight. Από το slice_policy.py παρατίθεται το τμήμα που παράγει τους κανόνες της πολιτικής M1 και τους αποστέλλει στο RESTCONF· οι επιλογές --remove και --show του ίδιου προγράμματος αφαιρούν και εμφανίζουν την πολιτική.

```
# ---- slicing_topo.py ----
"""
Τοπολογία τριών διαμερίσεων (eMBB, URLLC, MGMT) για το πείραμα M0/M1 της ενότητας
3.3.

    h1 (eMBB)  10.0.0.1 --1-+                    +-1-- h4 (eMBB)  10.0.0.4
    h2 (URLLC) 10.0.0.2 --2-+ s2 -4---1- s1 -2---4- s3 +-2-- h5 (URLLC) 10.0.0.5
    h3 (MGMT)  10.0.0.3 --3-+                    +-3-- h6 (MGMT)  10.0.0.6

Οι αριθμοί στις ζεύξεις είναι οι θύρες OpenFlow των μεταγωγέων.
Όλοι οι υπολογιστές ανήκουν στο 10.0.0.0/24, ώστε η απομόνωση να προκύπτει
μόνο από την πολιτική του ελεγκτή και όχι από τη διευθυνσιοδότηση.

Εκτέλεση (με τον OpenDaylight ήδη ενεργό):
    sudo python3 slicing_topo.py --controller-ip 127.0.0.1
"""
import argparse

from mininet.cli import CLI
from mininet.link import TCLink
from mininet.log import info, setLogLevel
from mininet.net import Mininet
from mininet.node import OVSSwitch, RemoteController

# Παράμετροι ζεύξεων πρόσβασης ανά διαμέριση
ACCESS_LINK = {
    "eMBB": dict(bw=50, delay="2ms"),
    "URLLC": dict(bw=10, delay="0.5ms"),
    "MGMT": dict(bw=5, delay="2ms"),
}
CORE_LINK = dict(bw=100, delay="1ms")

# υπολογιστής: (διαμέριση, μεταγωγέας, θύρα μεταγωγέα, διεύθυνση IP)
HOSTS = {
    "h1": ("eMBB", "s2", 1, "10.0.0.1"),
    "h2": ("URLLC", "s2", 2, "10.0.0.2"),
    "h3": ("MGMT", "s2", 3, "10.0.0.3"),
    "h4": ("eMBB", "s3", 1, "10.0.0.4"),
    "h5": ("URLLC", "s3", 2, "10.0.0.5"),
    "h6": ("MGMT", "s3", 3, "10.0.0.6"),
}
UPLINK_PORT = 4               # θύρα των s2 και s3 προς τον s1
CORE_PORT = {"s2": 1, "s3": 2}  # θύρα του s1 προς κάθε ακραίο μεταγωγέα
```

```
def build_network(controller_ip, controller_port):
    net = Mininet(controller=None, switch=OVSSwitch, link=TCLink,
                  autoSetMacs=True, build=False)
    net.addController("c0", controller=RemoteController,
                      ip=controller_ip, port=controller_port)

    # failMode="secure": χωρίς κανόνες ο μεταγωγέας δεν προωθεί τίποτα
    # (δεν γίνεται αυτόνομος μεταγωγέας μάθησης), άρα το M0 είναι καθαρό.
    for name, dpid in (("s1", 1), ("s2", 2), ("s3", 3)):
        net.addSwitch(name, dpid="%016x" % dpid,
                      protocols="OpenFlow13", failMode="secure")

    for host, (slice_name, switch, port, ip) in HOSTS.items():
        net.addHost(host, ip=ip + "/24")
        net.addLink(host, switch, port2=port, **ACCESS_LINK[slice_name])

    for edge, core_port in CORE_PORT.items():
        net.addLink(edge, "s1", port1=UPLINK_PORT, port2=core_port, **CORE_LINK)

    net.build()
    net.start()

    # Στατικές εγγραφές ARP: κάθε αποτυχία ping οφείλεται στους κανόνες ροής
    # και όχι σε αποτυχία επίλυσης διευθύνσεων.
    net.staticArp()
    # Απενεργοποίηση IPv6, ώστε οι μετρητές να περιέχουν μόνο την κίνηση της δοκιμής.
    for h in net.hosts:
        h.cmd("sysctl -qw net.ipv6.conf.all.disable_ipv6=1 "
              "net.ipv6.conf.default.disable_ipv6=1")
    return net


def main():
    parser = argparse.ArgumentParser(description="Τοπολογία διαμερίσεων για το
πείραμα M0/M1")
    parser.add_argument("--controller-ip", default="127.0.0.1")
    parser.add_argument("--controller-port", type=int, default=6653)
    args = parser.parse_args()

    setLogLevel("info")
    net = build_network(args.controller_ip, args.controller_port)
    info("\n*** Διαμερίσεις\n")
    for host, (slice_name, switch, port, ip) in HOSTS.items():
        info("    %s  %-9s %-5s %s θύρα %d\n" % (host, ip, slice_name, switch, port))
    info("*** Έλεγχος: pingall (M0 χωρίς πολιτική, M1 μετά το slice_policy.py --
install)\n\n")
    CLI(net)
    net.stop()


if __name__ == "__main__":
    main()

# ---- slice_policy.py (απόσπασμα) ----
SLICES = {
    "eMBB": ["10.0.0.1", "10.0.0.4"],
    "URLLC": ["10.0.0.2", "10.0.0.5"],
    "MGMT": ["10.0.0.3", "10.0.0.6"],
}
# διεύθυνση IP: (αριθμός μεταγωγέα, θύρα) — ίδια με το slicing_topo.py
HOST_LOCATION = {
    "10.0.0.1": (2, 1), "10.0.0.2": (2, 2), "10.0.0.3": (2, 3),
    "10.0.0.4": (3, 1), "10.0.0.5": (3, 2), "10.0.0.6": (3, 3),
}
UPLINK_PORT = 4
CORE_PORTS = (1, 2)
```

```
PRIO_ALLOW, PRIO_DROP, PRIO_CORE = 200, 100, 200


def build_policy():
    """Επιστρέφει τη λίστα κανόνων ως ουδέτερες δομές (ανεξάρτητες από τον
ελεγκτή)."""
    rules = []
    for sw in (2, 3):
        n = 0
        for slice_name, members in SLICES.items():
            for src in members:
                for dst in members:
                    if src == dst:
                        continue
                    src_sw, _ = HOST_LOCATION[src]
                    dst_sw, dst_port = HOST_LOCATION[dst]
                    if sw not in (src_sw, dst_sw):
                        continue
                    n += 1
                    rules.append(dict(
                        switch=sw, flow_id="%d%02d" % (sw, n), priority=PRIO_ALLOW,
                        name="%s_%s_to_%s" % (slice_name, src, dst),
                        match=dict(ipv4_src=src, ipv4_dst=dst),
                        output=dst_port if dst_sw == sw else UPLINK_PORT))
        rules.append(dict(switch=sw, flow_id="%d99" % sw, priority=PRIO_DROP,
                          name="inter_slice_drop", match=dict(ipv4=True),
output=None))
    a, b = CORE_PORTS
    rules.append(dict(switch=1, flow_id="101", priority=PRIO_CORE,
name="core_transit_1_to_2",
                      match=dict(in_port=a), output=b))
    rules.append(dict(switch=1, flow_id="102", priority=PRIO_CORE,
name="core_transit_2_to_1",
                      match=dict(in_port=b), output=a))
    return rules


# ---------------------------------------------------------------- OpenDaylight
(RESTCONF)
def odl_body(rule):
    match = {}
    if "in_port" in rule["match"]:
        match["in-port"] = "openflow:%d:%d" % (rule["switch"],
rule["match"]["in_port"])
    else:
        match["ethernet-match"] = {"ethernet-type": {"type": 2048}}
        if "ipv4_src" in rule["match"]:
            match["ipv4-source"] = rule["match"]["ipv4_src"] + "/32"
            match["ipv4-destination"] = rule["match"]["ipv4_dst"] + "/32"
    if rule["output"] is None:
        action = {"order": 0, "drop-action": {}}
    else:
        action = {"order": 0, "output-action": {
            "output-node-connector": str(rule["output"]), "max-length": 65535}}
    return {"flow-node-inventory:flow": [{
        "id": rule["flow_id"],
        "table_id": 0,
        "priority": rule["priority"],
        "flow-name": rule["name"],
        "match": match,
        "instructions": {"instruction": [{
            "order": 0, "apply-actions": {"action": [action]}}]},
    }]}


def odl_url(args, rule=None, switch=None):
    sw = rule["switch"] if rule else switch
    if args.api == "rfc8040":   # νεότερες εκδόσεις OpenDaylight (/rests)
```

```
        url = ("http://%s:%d/rests/data/opendaylight-
inventory:nodes/node=openflow:%d"
               "/flow-node-inventory:table=0" % (args.odl, args.port, sw))
        return url + ("/flow=%s" % rule["flow_id"] if rule else "")
    url = ("http://%s:%d/restconf/config/opendaylight-
inventory:nodes/node/openflow:%d/table/0"
           % (args.odl, args.port, sw))
    return url + ("/flow/%s" % rule["flow_id"] if rule else "")


def odl_apply(args, rules, remove=False):
    import requests
    auth = (args.user, args.password)
    headers = {"Content-Type": "application/json", "Accept": "application/json"}
    failed = 0
    for rule in rules:
        url = odl_url(args, rule)
        if remove:
            r = requests.delete(url, auth=auth, headers=headers, timeout=10)
        else:
            r = requests.put(url, auth=auth, headers=headers,
                             data=json.dumps(odl_body(rule)), timeout=10)
        ok = r.status_code in (200, 201, 204) or (remove and r.status_code == 404)
        failed += 0 if ok else 1
        print("%-6s openflow:%d flow=%-4s prio=%-3d %-28s HTTP %d %s" % (
            "DELETE" if remove else "PUT", rule["switch"], rule["flow_id"],
            rule["priority"], rule["name"], r.status_code, "OK" if ok else
r.text[:120]))
    return failed
```

I.5 Ενδεικτικός αλγόριθμος δυναμικής προσαρμογής πόρων με Python

Στο πλαίσιο της δυναμικής διαχείρισης πόρων, ο SDN controller μπορεί να λαμβάνει μετρήσεις από το δίκτυο και να προσαρμόζει τους κανόνες δρομολόγησης ή τις πολιτικές QoS. Το παρακάτω παράδειγμα παρουσιάζει μια απλή λογική απόφασης. Αν η καθυστέρηση ή η απώλεια πακέτων υπερβούν τα όρια που έχουν τεθεί για μία διαμέριση, τότε αυξάνεται η προτεραιότητα της αντίστοιχης κίνησης ή προτείνεται αλλαγή διαδρομής.

```
SLICE_LIMITS = {
    "embb":  {"max_latency_ms": 40, "max_loss": 0.02, "min_bw": 50},
    "urllc": {"max_latency_ms": 10, "max_loss": 0.005, "min_bw": 10},
    "mmtc":  {"max_latency_ms": 80, "max_loss": 0.05, "min_bw": 2}
}

def decide_policy(slice_name, latency_ms, packet_loss, available_bw):
    limits = SLICE_LIMITS[slice_name]

    if latency_ms > limits["max_latency_ms"]:
        return "increase_priority_and_select_lower_delay_path"

    if packet_loss > limits["max_loss"]:
        return "reroute_traffic_and_reduce_congestion"

    if available_bw < limits["min_bw"]:
        return "allocate_additional_bandwidth"

    return "keep_current_policy"

measurements = [
    ("embb", 32, 0.01, 70),
    ("urllc", 14, 0.002, 18),
    ("mmtc", 65, 0.03, 5)
]
```

```
for item in measurements:
    slice_name, latency, loss, bw = item
    action = decide_policy(slice_name, latency, loss, bw)
    print(slice_name, "->", action)
```

Ι.6 Συμπληρωματικός πίνακας ελέγχου επαναληψιμότητας πειραμάτων

Για να είναι αξιοποιήσιμα τα αποτελέσματα μιας προσομοίωσης, είναι σημαντικό να καταγράφεται με ενιαίο τρόπο το περιβάλλον εκτέλεσης, οι παράμετροι και οι μετρικές που συλλέχθηκαν. Ο παρακάτω πίνακας μπορεί να χρησιμοποιηθεί ως υπόδειγμα τεκμηρίωσης για κάθε πείραμα, έτσι ώστε να διατηρείται η ιχνηλασιμότητα των αποτελεσμάτων και να είναι δυνατή η επανάληψη των δοκιμών με τις ίδιες συνθήκες.

Πίνακας ΠΙ.2: Υπόδειγμα καταγραφής πειραματικής εκτέλεσης

Πεδίο καταγραφής	**Ενδεικτική τιμή**	**Σκοπός**
Κωδικός πειράματος	SIM-01, SIM-02 κ.λπ.	Μοναδική αναφορά για το συγκεκριμένο σενάριο
Περιβάλλον	Cisco Packet Tracer / GNS3 / Mininet	Εργαλείο στο οποίο εκτελέστηκε η δοκιμή
Τοπολογία	Αριθμός hosts, switches, routers και links	Περιγραφή της λογικής και φυσικής δομής
Παράμετροι κίνησης	Ρυθμός μετάδοσης, διάρκεια, τύπος εφαρμογής	Στοιχεία παραγωγής φόρτου ανά slice
Μηχανισμοί ελέγχου	ACL, QoS, OpenFlow rules, routing	Πολιτικές που εφαρμόστηκαν κατά τη δοκιμή
Μετρικές	Latency, throughput, packet loss, utilization	Δείκτες που χρησιμοποιήθηκαν για αξιολόγηση
Παρατηρήσεις	Συμφόρηση, βλάβη, αλλαγή διαδρομής	Σύντομη ποιοτική ερμηνεία του αποτελέσματος

Ι.7 Συνοπτική ερμηνεία του συμπληρωματικού υλικού

Το υλικό του παραρτήματος δείχνει ότι η πρακτική υλοποίηση του Network Slicing δεν περιορίζεται σε μία μόνο τεχνική. Σε περιβάλλον παραδοσιακής δικτύωσης, η διαμέριση μπορεί να προσεγγιστεί με VLANs, ACLs, μηχανισμούς QoS και κατάλληλη δρομολόγηση. Σε περιβάλλον SDN, η ίδια λογική επεκτείνεται με κεντρικό έλεγχο, προγραμματιζόμενους κανόνες ροής και δυνατότητα δυναμικής προσαρμογής. Επομένως, τα αποσπάσματα κώδικα και οι πίνακες του

παραρτήματος λειτουργούν ως πρακτική συμπλήρωση της θεωρητικής ανάλυσης και της αξιολόγησης που παρουσιάστηκαν στο κύριο σώμα της εργασίας.