



ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Αξιολόγηση ελεγκτών σε ασύρματα δίκτυα καθοριζόμενα από λογισμικό.»

ΟΝΟΜΑΤΕΠΩΝΥΜΟ : ΘΕΙΟΠΟΥΛΟΥ ΕΛΕΝΗ

A.M. 00153

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ : ΕΛΕΥΘΕΡΙΟΣ ΣΤΕΡΓΙΟΥ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ & ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΑΡΤΑ 2024

Ευχαριστίες

Με την ολοκλήρωση της μεταπτυχιακής διπλωματικής μου εργασίας, θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες στον επιβλέπων καθηγητή μου, Κύριο Ελευθέριο Στεργίου , για την στήριξη του , τη συμπαράσταση του και το μεγάλο ενδιαφέρον που έδειξε από την αρχή μέχρι το τέλος, καθώς χωρίς αυτά δεν θα μπορούσα να ολοκληρώσω την διπλωματική μου εργασία. Επίσης ένα μεγάλο ευχαριστώ και σε όλους όσους με βοήθησαν κατά την διάρκεια των σπουδών μου.

Δήλωση μη λογοκλοπής

Δηλώνω υπεύθυνα και γνωρίζοντας τις κυρώσεις του Ν. 2121/1993 περί Πνευματικής Ιδιοκτησίας, ότι η παρούσα διπλωματική εργασία είναι εξολοκλήρου αποτέλεσμα δικής μου ερευνητικής εργασίας, δεν αποτελεί προϊόν αντιγραφής ούτε προέρχεται από ανάθεση σε τρίτους. Όλες οι πηγές που χρησιμοποιήθηκαν (κάθε είδους, μορφής και προέλευσης) για τη συγγραφή της περιλαμβάνονται στη βιβλιογραφία.

ΘΕΙΟΠΟΥΛΟΥ ΕΛΕΝΗ

Περίληψη

Η παρούσα εργασία εστιάζει στην αξιολόγηση ελεγκτών σε ασύρματα δίκτυα που καθορίζονται από λογισμικό, μια σημαντική πτυχή της σύγχρονης τεχνολογίας δικτύωσης. Με την αυξανόμενη χρήση ασύρματων δικτύων σε διάφορους τομείς, όπως οι επικοινωνίες, οι βιομηχανικές εφαρμογές και οι έξυπνες πόλεις, η ανάγκη για αποδοτικούς ελεγκτές που να διαχειρίζονται αυτά τα δίκτυα είναι πιο επιτακτική από ποτέ.

Οι ελεγκτές που λειτουργούν με λογισμικό αποτελούν κρίσιμο κομμάτι της υποδομής ασύρματων δικτύων Salman et al. (Salman, 2016), καθώς αναλαμβάνουν τον ρόλο της λογικής διαχείρισης και ελέγχου των συνδεδεμένων συσκευών. Η ποιοτική αξιολόγηση των ελεγκτών αποκτά ζωτική σημασία, καθώς επηρεάζει την απόδοση, την αξιοπιστία και την αποτελεσματικότητα του δικτύου. Στόχος της εργασίας είναι η διερεύνηση των διάφορων παραμέτρων αξιολόγησης, όπως ο ρυθμός μετάδοσης, η καθυστέρηση, η απώλεια πακέτων και ο μέσος όρος των αλληλοσυσχετίσεων (jitter), που επηρεάζουν την απόδοση των ελεγκτών σε ασύρματα δίκτυα.

Στην εργασία χρησιμοποιούνται διάφοροι ελεγκτές που λειτουργούν με λογισμικό, όπως ο ONOS, ο Ryu, ο POX και ο OpenDayLight controller. Μέσω πειραματικής διαδικασίας και προσομοιώσεων σε περιβάλλοντα όπως το Mininet, αναλύονται οι επιδόσεις των ελεγκτών υπό διάφορες συνθήκες και φορτία. Τα αποτελέσματα αυτής της αξιολόγησης μπορούν να προσφέρουν πολύτιμες γνώσεις για την επιλογή και τη βελτιστοποίηση ελεγκτών σε ασύρματα δίκτυα, προκειμένου να επιτευχθεί αυξημένη απόδοση, αξιοπιστία και ευελιξία στη διαχείρισή τους.

Μέσα από αυτήν την εργασία, προσδοκάτε να αναδειχθούν πρακτικές κατευθύνσεις για την καλύτερη χρήση και επιλογή ελεγκτών σε ασύρματα δίκτυα, συμβάλλοντας έτσι στη συνεχή εξέλιξη και βελτίωση των ασύρματων δικτύων και των εφαρμογών τους.

Περιεχόμενα

1.Εισαγωγή.....	8
1.1. Αντικείμενο και συνεισφορά.....	8
1.2.Οργάνωση Εργασίας.....	13
2.Σχετικές Εργασίες	13
3.Αξιολόγηση του SDN.....	18
3.1.Εισαγωγή και ορισμοί.....	18
3.1.1.Ασύρματη SDN Δικτύωση	20
3.1.2.Εισαγωγή στην Ασύρματη Δικτύωση SDN	20
3.1.3.Βασικές Αρχές του SDN	20
3.1.4.Προκλήσεις και Επικείμενες Εξελίξεις	21
3.2.Εφαρμογές SDN Δικτύωσης.....	21
3.3. Ασύρματη SDN Δικτύωση έναντι Legacy Networks.....	25
4.Γενική Αρχιτεκτονική SDN	27
4.1.Πρωτόκολλα SDN Δικτύωσης	31
4.1.1. OPENFLOW.....	32
4.1.2.NETCONF.....	34
4.1.3.YANG.....	35
4.1.4.BGP-SDN.....	37
4.1.5.OF-CONFIG.....	38
5.Ο Ρόλος των ελεγκτών Ανοικτού και Κλειστού Λογισμικού.....	39
5.1.Οι πιο διαδεδομένοι Ελεγκτές Ανοικτού κώδικα στον χώρο του SDN	41
5.1.1.Floodlight.....	41
5.1.2.POX.....	43
5.1.3.Ryu.....	45
5.1.4.Beacon.....	47
5.1.5.ONOS.....	48
5.1.6.OpenDaylight.....	49

5.2.Οι πιο διαδεδομένοι Ελεγκτές Κλειστού κώδικα στον χώρο του SDN	51
5.2.1.Cisco Application Policy Infrastructure Controller.....	51
5.2.2.VMware NSX.....	52
5.2.3.Juniper Contrail SDN	54
5.3.Δείκτες απόδοσης Ελεγκτών.....	57
5.3.1.Throughput.....	57
5.3.2.Bandwidth.....	58
5.3.3.Καθυστέρηση (Delay).....	59
5.3.4.Jitter.....	60
5.3.5.Απώλεια πακέτων.....	61
6.Mininet Πακέτο προσομοίωσης	63
6.1.Mininet.....	63
6.1.1.Πλεονεκτήματα Mininet.....	65
6.1.2.Μειονεκτήματα Mininet.....	66
6.2.Mininet WiFi.....	67
6.2.1.Χαρακτηριστικά του Mininet WiFi.....	68
6.2.2.Πλεονεκτήματα του Mininet WiFi.....	69
6.2.3.Μειονεκτήματα του Mininet WiFi.....	70
6.3.Γενικός δείκτης επιδόσεων για την αξιολόγηση του δικτύου SDWN	71
7.Προσομοίωση και αποτελέσματα.....	73
7.1.Μεθοδολογία.....	73
7.2.Μετρικές Πειραμάτων.....	74
7.3.Πειραματικό Πλαίσιο.....	75
7.4.Αποτελέσματα.....	76
7.5.Αποτελέσματα του γενικού συντελεστή απόδοσης (GPI).....	80
8.Συμπεράσματα.....	84
9.Αναφορές.....	86

1. ΕΙΣΑΓΩΓΗ

Η συνεχής εξέλιξη της υπολογιστικής τεχνολογίας δημιουργεί ένα πεδίο συνεχών αναζητήσεων για πιο αποδοτικές δικτυακές υποδομές, ώστε να ανταποκριθούν στις αυξανόμενες απαιτήσεις λειτουργικότητας. Ταχέως αναπτυσσόμενες εφαρμογές με αυξανόμενες λειτουργικές απαιτήσεις και η ανάγκη για αποθήκευση υπερβολικών δεδομένων ενθαρρύνουν τους κατασκευαστές να εξερευνήσουν και να αξιοποιήσουν τις καινοτόμες δυνατότητες της νέας τεχνολογίας δικτύωσης SDN.

Εν μέσω αυτού του συναρπαστικού περιβάλλοντος, οι διάφορες εφαρμογές που λειτουργούν μέσω ιδιωτικών ή δημόσιων υποδομών cloud αντιμετωπίζουν την πρόκληση της πρόσβασης σε πληθώρα βάσεων δεδομένων και διακομιστών, ανεξαρτήτως της γεωγραφικής τοποθεσίας τους. Το αποτέλεσμα είναι η ανάγκη για ευέλικτη διαχείριση της ροής δεδομένων και η απαίτηση για άμεση πρόσβαση σε δίκτυα όποτε αυτά απαιτούνται. Οι υπηρεσίες cloud εξαρτώνται από ταχεία είσοδο σε εφαρμογές και σε δομές IT, καθιστώντας την ασφάλεια και την δυναμική ροή δεδομένων επιτακτικά αναγκαίες.

Όλα αυτά εκτρέπουν το ενδιαφέρον προς τα Δίκτυα Καθοριζόμενα από Λογισμικό (Software Defined Networks - SDN). Το SDN δημιουργεί μια νέα πραγματικότητα στην δικτυακή ανάπτυξη, χαρακτηριζόμενο από την δυνατότητα προγραμματισμού του δικτύου. Αυτή η τεχνολογία, που αποτελεί πυρήνα της προοπτικής επανάστασης στη βιομηχανία των δικτύων, απαιτεί σημαντική έρευνα στη διαχείριση και αξιολόγηση των θεμάτων ασφάλειας, προκειμένου να δημιουργηθούν αξιόπιστες δικτυακές υλοποιήσεις.

1.1. Αντικείμενο και συνεισφορά

Το ταχύτατο ρυθμό με τον οποίο η τεχνολογία εξελίσσεται στον τομέα των ασύρματων δικτύων καθοριζόμενων από λογισμικό (SDN) έχει ανοίξει νέους ορίζοντες για τη διαχείριση και τον έλεγχο των δικτύων. Το SDN αντιπροσωπεύει μια επαναστατική προσέγγιση, επιτρέποντας τη διαχείριση του δικτύου μέσω λογισμικού. Αυτή η πρωτοποριακή δομή δίνει τη δυνατότητα για δυναμικό, ευέλικτο και αποτελεσματικό έλεγχο των ασύρματων δικτύων. Η παρούσα διπλωματική εργασία επικεντρώνεται στην αξιολόγηση των ελεγκτών σε ασύρματα δίκτυα που εφαρμόζουν την τεχνολογία SDN. Εξετάζει πώς οι ελεγκτές αυτοί επηρεάζουν την απόδοση, την ασφάλεια, και τη διαθεσιμότητα των δικτύων. Επιπλέον, εστιάζει στον τρόπο με τον οποίο η αξιολόγηση αυτών των ελεγκτών μπορεί να συνεισφέρει στη

βελτίωση της απόδοσης και της ασφάλειας των ασύρματων δικτύων, ανοίγοντας νέες προοπτικές για τον τομέα των επικοινωνιών.

Από SDN σε SDN Δικτύωση μέσω Ασύρματων Δικτύων: Ένα Αναδρομικό Ταξίδι

Κατά την εξερεύνηση του πανίσχυρου κόσμου του Λογισμικού Ορισμού Δικτύωσης (SDN), ανακαλύπτουμε μια επανάσταση όπου το λογισμικό κατέχει την ηγετική θέση στον έλεγχο και τη διαχείριση των δικτυακών πόρων. Αυτή η ανατροπή μας επιτρέπει να κατανοήσουμε την αληθινή ουσία της δικτύωσης σε μια εποχή που η τεχνολογία εξελίσσεται με εκπληκτικούς ρυθμούς.

- Εστιάζουμε στη συναρπαστική διάσταση της ασύρματης SDN δικτύωσης, που συνδυάζει την ευελιξία της ασύρματης τεχνολογίας με τον ενδιαφέροντα κόσμο του SDN.
- Αναδεικνύουμε τον τρόπο με τον οποίο μπορούμε να εκμεταλλευτούμε αυτήν τη συνάντηση της τεχνολογίας για να σχεδιάσουμε και να διαχειριστούμε αποτελεσματικά τους δικτυακούς πόρους.
- Παρέχουμε νέες δυνατότητες και αποδεικνύουμε την καινοτομία που προσφέρει η ενσωμάτωση των δύο τεχνολογιών.

Αυτό το αναδρομικό ταξίδι αποτελεί μια ευκαιρία να αναλύσουμε τις τρέχουσες τάσεις, τις προκλήσεις και τις προοπτικές της τεχνολογικής εξέλιξης, αφήνοντας τον αναγνώστη να ανακαλύψει τον επαναστατικό κόσμο της SDN δικτύωσης.

Πλεονεκτήματα και Αδυναμίες της Ασύρματης SDN Δικτύωσης:

Σε αυτήν την αναδρομική ανάλυση, εστιάζουμε και αναδεικνύουμε την πνοή της τεχνολογίας, εξερευνώντας τα πλεονεκτήματα που φέρνει η ασύρματη Δικτύωση (SDN) στον κόσμο της επικοινωνίας. Κατά τη διάρκεια αυτής της ανάλυσης, εξετάζουμε επίσης τις πιθανές προκλήσεις και αδυναμίες που μπορεί να παρουσιάσει.

- Τα πλεονεκτήματα της ασύρματης SDN δικτύωσης είναι ενδιαφέροντα και πολυδιάστατα, παρέχοντας ευελιξία, απλότητα και ευκολία εγκατάστασης.
- Επιπλέον, επιτρέπει τη δημιουργία εξυπνότερων δικτύων που ενισχύουν την απόδοση και την ασφάλεια.
- Ωστόσο, δεν πρέπει να παραβλέψουμε τις προκλήσεις, συμπεριλαμβανομένης της αποτελεσματικής διαχείρισης του φόρτου δεδομένων και των πόρων, καθώς και τη διαχείριση της ασφάλειας σε ασύρματες συνδέσεις.

Αυτή η ανάλυση ανοίγει την πόρτα για μια περαιτέρω συζήτηση σχετικά με τις δυνατότητες και τις προκλήσεις της ασύρματης SDN δικτύωσης, προκαλώντας μας να εξερευνήσουμε την επιρροή της στο μέλλον των επικοινωνιών.

Αρχιτεκτονική SDN και Πρωτόκολλα: Η Δομή και η Κινητήρια Δύναμη της SDN

Στο πλαίσιο αυτής της αναλυτικής εξέτασης, εστιάζουμε στην αρχιτεκτονική του SDN και στα κυριότερα πρωτόκολλα που τη διαμορφώνουν. Προσφέρουμε μια λεπτομερή επισκόπηση του τρόπου με τον οποίο αυτά τα πρωτόκολλα διευκολύνουν τον έλεγχο και τη διαχείριση των δικτυακών συσκευών.

- Η αρχιτεκτονική του SDN αποτελεί το θεμέλιο για την εξέλιξη του δικτυακού κόσμου, αναδεικνύοντας τον ρόλο του κεντρικού ελεγκτή και των διακριτικών επιπέδων λογισμικού Cabaj et al. (Cabaj , 2014).
- Εξετάζουμε τα πρωτόκολλα που καθορίζουν τη λειτουργία της SDN, εστιάζοντας στον ρόλο του OpenFlow και άλλων πρωτοκόλλων στη διεπαφή (Interface) μεταξύ του κεντρικού ελεγκτή και των δικτυακών συσκευών.
- Αναδεικνύουμε τον τρόπο με τον οποίο αυτά τα πρωτόκολλα διαμορφώνουν την κίνηση των δεδομένων και την ανταλλαγή πληροφοριών.

Αυτή η ανάλυση παρέχει μια ευκαιρία να εμβαθύνουμε στην πολυπλοκότητα της SDN, καλώντας μας να αναλύσουμε τις προοπτικές που ανοίγονται μέσω αυτής της εξελιγμένης τεχνολογίας..

Ελεγκτές σε SDN Δίκτυα: Ο Στρατηγικός Χειριστής της Εξέλιξης

Στο πλαίσιο αυτής της αναλυτικής εξέτασης, εστιάζουμε στον βασικό ρόλο που διαδραματίζουν οι ελεγκτές σε ένα δίκτυο Λογισμικού Ορισμού Δικτύου (SDN). Οι ελεγκτές αναδεικνύονται ως η κεντρική νοητική μονάδα που διαχειρίζεται, ελέγχει και κατευθύνει τους δικτυακούς πόρους σε ένα περιβάλλον SDN. Μέσα από μια εις βάθος ανάλυση, εξετάζουμε τη λειτουργία των ελεγκτών και την ικανότητά τους να λαμβάνουν αποφάσεις, βασιζόμενοι σε δεδομένα και οδηγίες από εφαρμογές και πολιτική δικτύου. Αναδεικνύουμε τη σημασία της συνεισφοράς των ελεγκτών στη διαμόρφωση της ευελιξίας και της αποτελεσματικότητας του δικτύου, καθώς και τον τρόπο με τον οποίο επιτρέπουν την ενσωμάτωση νέων τεχνολογιών και την ανάπτυξη προηγμένων λειτουργιών.

Αναλυτική Εξέταση του Ρόλου των Ελεγκτών σε Ένα Δίκτυο SDN:

- Οι ελεγκτές αποτελούν τον εγκέφαλο των δικτύων SDN, κρίνονται ως κεντρικός παράγοντας για την ομαλή λειτουργία τους Zhu et al. (Zhu ,2019).

- Αναλύουμε τη λειτουργία των ελεγκτών και την ικανότητά τους να λαμβάνουν αποφάσεις βασιζόμενοι σε ανάλυση δεδομένων και οδηγίες από εφαρμογές και πολιτική δικτύου.
- Αποκαλύπτουμε τη συνεισφορά των ελεγκτών στη διαμόρφωση της ευελιξίας και της αποτελεσματικότητας του δικτύου.
- Αναδεικνύουμε τον τρόπο με τον οποίο οι ελεγκτές επιτρέπουν την ενσωμάτωση νέων τεχνολογιών και την ανάπτυξη προηγμένων λειτουργιών.

Δείκτες Απόδοσης Ελεγκτών και Δικτύων στο Πλαίσιο των SDN

Στην παρούσα ενότητα, εξετάζουμε τους διάφορους δείκτες απόδοσης που μπορούμε να χρησιμοποιήσουμε για την αξιολόγηση της απόδοσης των ελεγκτών σε ένα δίκτυο SDN. Επίσης, αναλύουμε κάποια εργαλεία δικτύου που μπορούν να χρησιμοποιηθούν για τη μέτρηση αυτών των δεικτών, όπως η απόδοση (throughput), το delay, η απώλεια πακέτων και το μέσο jitter Umeh et al. (Umeh, 2015).

- Η αξιολόγηση των ελεγκτών απαιτεί κατανόηση της απόδοσής τους, με βασικούς δείκτες να είναι η απόδοση (throughput) και το delay.
- Η απόδοση (throughput) μετρά τον όγκο των δεδομένων που μπορεί να επεξεργαστεί ένας ελεγκτής σε μια συγκεκριμένη χρονική περίοδο.
- Το delay αναφέρεται στον χρόνο που απαιτείται για τη μεταφορά πακέτων δεδομένων από την αρχή μέχρι τον προορισμό.

Επιπλέον, σημαντικοί δείκτες περιλαμβάνουν την απώλεια πακέτων και το μέσο jitter, που αντιπροσωπεύουν το ποσοστό πακέτων που χάνονται κατά τη μετάδοση και τη μεταβολή στην καθυστέρηση της άφιξης των πακέτων αντίστοιχα. Για τη μέτρηση αυτών των δεικτών, χρησιμοποιούμε εργαλεία δικτύου όπως προηγουμένως αναφέρθηκαν. Η κατανόηση και αξιολόγηση αυτών των δεικτών είναι κρίσιμη για τη βελτιστοποίηση της απόδοσης των ελεγκτών και του συνολικού δικτύου SDN.

Mininet: Πακέτο Προσομοίωσης για Δημιουργία και Έλεγχο Εικονικών Δικτύων

Η ταχεία εξέλιξη των ασύρματων δικτύων οφείλεται στην ανάγκη για αποτελεσματική διαχείριση και έλεγχο. Μια καινοτόμος προσέγγιση που έχει επιφέρει επανάσταση είναι το λογισμικό οριοθετημένο δίκτυο (SDN), το οποίο επιτρέπει τον έλεγχο του δικτύου μέσω λογισμικού. Αυτή η τεχνολογία παρέχει δυνατότητες για δυναμικό, ευέλικτο και αποτελεσματικό έλεγχο των ασύρματων δικτύων. Σε αυτό το πλαίσιο, η παρούσα εργασία εστιάζεται στο Mininet, ένα πακέτο προσομοίωσης για τη δημιουργία και τον έλεγχο εικονικών δικτύων. Θα αναλύσουμε την ανάπτυξη του Mininet και πώς μπορεί να χρησιμοποιηθεί για την προσομοίωση δικτύων SDN.

- Το Mininet αναπτύχθηκε με σκοπό τη δημιουργία εύκολων και γρήγορων εικονικών δικτύων Kaur et al. (Kaur, 2014).
- Επιτρέπει τη δημιουργία δικτύων με εικονικούς κόμβους και συνδέσεις μεταξύ τους.
- Παρέχει στους ερευνητές, φοιτητές και επαγγελματίες τη δυνατότητα δοκιμής και αξιολόγησης εφαρμογών και σεναρίων δικτύωσης.
- Μπορεί να χρησιμοποιηθεί για την προσομοίωση του ρόλου των ελεγκτών σε ένα δίκτυο SDN.
- Επιτρέπει την αξιολόγηση της απόδοσης του δικτύου, τους χρόνους καθυστέρησης και άλλες σημαντικές παραμέτρους.

Mininet WiFi.

Το Mininet-WiFi είναι ένα εργαλείο προσομοίωσης δικτύου που βασίζεται στο Mininet, το οποίο επεκτείνει τις δυνατότητες προσομοίωσης για ασύρματα δίκτυα Fontes et al. (Fontes , 2015) . Με το Mininet-WiFi, μπορούμε να δημιουργήσουμε εικονικά ασύρματα δίκτυα που περιλαμβάνουν στοιχεία όπως ασύρματοι κόμβοι, σημεία πρόσβασης, ελεγκτές SDN και πολλά άλλα. Αυτό το εργαλείο είναι χρήσιμο για την εκτέλεση πειραμάτων και την ανάπτυξη και δοκιμή δικτυακών εφαρμογών σε περιβάλλοντα ασύρματου δικτύου πριν από την πραγματική υλοποίηση. Το Mininet-WiFi παρέχει μια ευέλικτη και αποτελεσματική λύση για τη μελέτη και την ανάπτυξη ασύρματων δικτύων

Ανάλυση Αποτελεσμάτων Προσομοίωσης

- Τα αποτελέσματα προσομοίωσης παρουσιάζονται με διαγράμματα, αναδεικνύοντας την απόδοση του δικτύου και των ελεγκτών.
- Η ανάλυση αυτή παρέχει ένα εργαλείο για την αξιολόγηση και τη βελτιστοποίηση των SDN δικτύων μέσω της προσομοίωσης, σύμφωνα με τη μελέτη Fontes et al. (Fontes , 2015).
- Η παρουσίαση αποσκοπεί στο να αναδείξει την ευχρηστία και την επίκαιρη σημασία της ασύρματης SDN δικτύωσης, φωτίζοντας την πολυπλοκότητα και την ευφυΐα που κρύβει αυτή η εξελιγμένη τεχνολογία.
- Η ασύρματη SDN δικτύωση συνδυάζει την ασύρματη τεχνολογία με τα πλεονεκτήματα του λογισμικού ορισμού δικτύου (SDN), δημιουργώντας ένα περιβάλλον που επιτρέπει την ευέλικτη, αποδοτική και έξυπνη διαχείριση των ασύρματων πόρων.
- Οι προηγμένες δυνατότητες που προσφέρει η ασύρματη SDN δικτύωση επιτρέπουν τη δημιουργία δικτύων που προσαρμόζονται δυναμικά στις ανάγκες και τις απαιτήσεις της σύγχρονης κοινωνίας.
- Αναδεικνύει επίσης την πολυπλοκότητα αυτής της τεχνολογίας, όπου η ευφυΐα των συστημάτων είναι κρίσιμη για την αποτελεσματική λειτουργία και αξιοποίηση των πόρων.

1.2 Οργάνωση της εργασίας

Στο 1^ο κεφάλαιο γίνεται αναφορά στην δικτύωση που είναι καθορισμένη από λογισμικό SDN. Εξηγείται τι είναι τα SDN δίκτυα και η ασύρματη SDN δικτύωση, πού χρησιμοποιούνται καθώς και τα πλεονεκτήματα και τα μειονεκτήματα τους σε σύγκριση με τα παραδοσιακά δίκτυα. Στο 2^ο Κεφάλαιο παρουσιάζουμε τις σχετικές εργασίες από τη διεθνή βιβλιογραφία. Στο 3^ο κεφάλαιο αναλύουμε το Σύστημα Οριοθετημένης Ευελιξίας (SDN) σε τρία κύρια μέρη. Παρουσιάζουμε την έννοια του SDN και της ασύρματης SDN δικτύωσης, εστιάζουμε στις βασικές αρχές και τις προκλήσεις, αναφέρουμε τις εφαρμογές του SDN στη δικτύωση, και τέλος, συγκρίνουμε τα ασύρματα SDN δίκτυα με τα παραδοσιακά (Legacy) δίκτυα. Στο 4^ο κεφάλαιο επικεντρωνόμαστε στη Γενική Αρχιτεκτονική του SDN. Παρουσιάζουμε τα βασικά πρωτόκολλα SDN Δικτύωσης, συμπεριλαμβανομένων του OPENFLOW, του NETCONF, του YANG, του BGP-SDN και του OF-CONFIG. Στο 5^ο κεφάλαιο εξετάζουμε τους πιο διαδεδομένους Ελεγκτές Κλειστού κώδικα στον χώρο του SDN, συμπεριλαμβανομένων του Cisco Application Policy Infrastructure Controller, του VMware NSX και του Juniper Contrail SDN. Στη συνέχεια, αναλύουμε τους δείκτες απόδοσης των ελεγκτών, περιλαμβάνοντας το throughput, το bandwidth, την καθυστέρηση (delay), το jitter και την απώλεια πακέτων. Στο 6^ο κεφάλαιο εξετάζουμε το Mininet, ένα πακέτο προσομοίωσης δικτύων. Αναλύουμε πλεονεκτήματα και μειονεκτήματά του, καθώς και τη δυνατότητα ασύρματης προσομοίωσης με το Mininet WiFi. Στο 7^ο κεφάλαιο αναλύουμε τη μεθοδολογία, τις μετρικές πειραμάτων και το πειραματικό πλαίσιο που χρησιμοποιήθηκε. Επίσης, παρουσιάζουμε τα αποτελέσματα της προσομοίωσης και το γενικό συντελεστή απόδοσης (GPI). Στο 8^ο κεφάλαιο παρουσιάζουμε τα συμπεράσματα της μελέτης και τέλος στο 9^ο κεφάλαιο τις αναφορές.

2. Σχετικές εργασίες

Ο Zhu et al. (Zhu, 2019) παρουσίασε μια πλήρη ανάλυση σχετικά με τους ελεγκτές SDN, εξετάζοντας την γενική αρχιτεκτονική και την πορεία εξέλιξής τους. Ανέλυσε 34 διαφορετικούς ελεγκτές για τις ιδιότητές τους και τις δυνατότητές τους, εστιάζοντας σε διάφορες περιπτώσεις χρήσης και προτεινόμενες λύσεις για τη βελτίωση της απόδοσής τους. Η έρευνα περιλαμβάνει μια ποσοτική ανάλυση χρησιμοποιώντας τρία διαφορετικά εργαλεία σύγκρισης: τα CBench, PktBlaster και OFNet. Παρόλα αυτά, κατέληξε στο συμπέρασμα ότι κανένα από αυτά τα εργαλεία δεν μπορεί να καλύψει όλες τις πτυχές των επιδόσεων ενός ελεγκτή. Με βάση την ποιοτική ανάλυσή του, διαπίστωσε ότι οι ελεγκτές Floodlight, OpenMUL, Beacon, Maestro, OpenDaylight και ONOS εμφανίζουν καλύτερες επιδόσεις σε ορισμένες

περιπτώσεις σε σχέση με τους ελεγκτές NOX, POX και Ryu, αλλά απαιτούν επίσης περισσότερους φυσικούς πόρους για την αποτελεσματική λειτουργία τους. Τέλος, υπογράμμισε την ανάγκη για περισσότερες λεπτομέρειες και πληροφορίες στις εργασίες που προτείνονται στη βιβλιογραφία, καθώς είναι δύσκολο να αξιολογηθούν κατάλληλα χωρίς επαρκείς πληροφορίες για το πειραματικό τους μέρος. Επιπλέον, παρατήρησε ότι ορισμένα χαρακτηριστικά των εργαλείων σύγκρισης, όπως το μήκος πακέτων και το μέγεθος του buffer του vSwitch, επηρεάζουν την απόδοση των ελεγκτών.

Σύμφωνα με τον Zhu et al. (Zhu , 2020), οι μελέτες για τα δίκτυα SDN μπορούν να χωριστούν σε δύο κύριους τύπους: γενικές έρευνες που καλύπτουν ευρέως τον τομέα των δικτύων SDN και εστιάζουν σε διάφορες πτυχές τους, και μελέτες που εστιάζουν στους ελεγκτές SDN και εξετάζουν τη λειτουργία και τα χαρακτηριστικά τους. Υπάρχει ένας μεγάλος αριθμός εργασιών για τους ελεγκτές SDN στη βιβλιογραφία. Ορισμένες από αυτές εξετάζουν θεωρητικά διαφορετικούς ελεγκτές, τις ιδιότητές τους και τις δυνατότητες .

Ο Shalimov et al. (Shalimov, 2013) και συνεργάτες , πραγματοποίησαν σύγκριση της αποτελεσματικότητας πολλών ελεγκτών SDN χρησιμοποιώντας το CBench και ένα πλαίσιο που ανέπτυξαν οι ίδιοι, το HCprobe, για τη δοκιμή των ελεγκτών OpenFlow. Συμπεραίνουν ποιοι ελεγκτές έχουν καλύτερη απόδοση σε διάφορες παραμέτρους όπως απόδοση, επεκτασιμότητα, αξιοπιστία και ασφάλεια. Το HCprobe αναπτύχθηκε για να ξεπεράσει τις περιορισμένες δυνατότητες του CBench στην αξιολόγηση της απόδοσης των ελεγκτών SDN/OpenFlow.

Ο Amin et al. (Amin , 2018) και συνεργάτες , παρουσίασαν μια ολοκληρωμένη ενημερωμένη επισκόπηση της έρευνας και της ανάπτυξης στον τομέα των υβριδικών δικτύων SDN. Οργανώσανε την έρευνα σε πέντε κύριες κατηγορίες, δηλαδή στρατηγικές ανάπτυξης υβριδικών δικτύων SDN, ελεγκτές για υβριδικά δίκτυα SDN, πρωτόκολλα για τη διαχείριση υβριδικών δικτύων SDN, μηχανισμούς μηχανικής κίνησης για υβριδικά δίκτυα SDN, καθώς και μηχανισμούς δοκιμής, επαλήθευσης και ασφάλειας για υβριδικά δίκτυα SDN. Εξετάσανε διεξοδικά τις υπάρχουσες μελέτες υβριδικών δικτύων SDN και καταλήξανε στο ότι , ενώ το SDN υπόσχεται ένα ευρύ φάσμα πλεονεκτημάτων, οι οργανισμοί συχνά διστάζουν να αντικαταστήσουν ολόκληρο το παραδοσιακό τους δίκτυο με ένα δίκτυο SDN για διάφορους λόγους, όπως οι περιορισμοί κόστους. Η σταδιακή ανάπτυξη μερικών συσκευών SDN μεταξύ των παλαιών συσκευών σε ένα παραδοσιακό δίκτυο, δημιουργεί ένα λεγόμενο υβριδικό δίκτυο SDN. Ένα υβριδικό δίκτυο SDN απαιτεί μόνο μέτριες επενδύσεις σε συσκευές SDN και μπορεί να παρέχει λειτουργίες ελέγχου που προσεγγίζουν εκείνες ενός αμιγούς δικτύου SDN. Ουσιαστικά, η προσέγγιση υβριδικού δικτύου SDN εξακολουθεί να χρησιμοποιεί την εγκατεστημένη παραδοσιακή υποδομή δικτύου, ενώ παρέχει έλεγχο και διαχείριση τύπου SDN

Η έρευνα πραγματοποιήθηκε από τον Ahmad et al. (Ahmad , 2022) . Μέσα από μια εκτενή και σφαιρική προσέγγιση, εξερευνήθηκαν οι δυνατότητες και οι προκλήσεις που παρουσιάζει το Software-Defined Networking (SDN), εστιάζοντας ιδιαίτερα στο Interface του. Με ανάλυση των διαφόρων πρωτοκόλλων και προτάσεων που σχετίζονται με το SDN, κατηγοριοποιήθηκαν και αναδείχθηκαν οι λειτουργικές τους ιδιότητες, καθώς και οι εξαρτήσεις τους .Η εξέλιξη του προτύπου OpenFlow, ως κυρίαρχου προτύπου στον τομέα του SDN, αναγνωρίστηκε ως ένα σημαντικό στάδιο στη διαχείριση και τον έλεγχο του δικτύου. Ταυτόχρονα, αναδείχθηκαν και οι περιορισμοί του, καθώς και τα ανοιχτά ζητήματα και οι προκλήσεις που αντιμετωπίζει. Επιπλέον, εξετάστηκαν διάφορες προσεγγίσεις για το βόρειο Interface του SDN, ενώ αναδείχθηκαν και οι προτεινόμενες βελτιώσεις προκειμένου να αντιμετωπιστούν οι προκλήσεις που παρουσιάζονται. Το συμπέρασμα είναι ότι, παρά τις σημαντικές καινοτομίες που εισάγει το SDN, υπάρχει ακόμα ένας μακρύς δρόμος για την πλήρη αξιοποίηση των δυνατοτήτων του και την ευρεία διάδοσή του σε διάφορους τομείς.

Ο Rowshanrad et al. (Rowshanrad, 2016) σύγκρινε τους ελεγκτές Floodlight και OpenDaylight χρησιμοποιώντας το Mininet, έναν εξομοιωτή SDN, με βάση παραμέτρους QoS όπως η καθυστέρηση και οι απώλειες. Τα αποτελέσματα δείχνουν ότι ο Floodlight έχει μεγαλύτερη καθυστέρηση σε σύγκριση με τον OpenDaylight, καθιστώντας τον OpenDaylight πιο γρήγορο στην εύρεση διαδρομών και στη λήψη αποφάσεων για νέο-εισερχόμενες ροές, ειδικά σε περιπτώσεις χαμηλής κυκλοφορίας στο δίκτυο. Αυτές οι έρευνες παρέχουν σημαντική πληροφορία για την επιλογή κατάλληλου ελεγκτή SDN ανάλογα με τις απαιτήσεις του δικτύου, όπως η κίνηση πολυμέσων ή οι ειδικές περιπτώσεις χρήσης όπως τα κέντρα δεδομένων και οι cloud υπηρεσίες.

Η τεχνολογία του Δικτύου Καθορισμένου από Λογισμικό (SDN) έχει αναδειχθεί ως μια πρωτοποριακή προσέγγιση που διαχωρίζει τα επίπεδα ελέγχου και δεδομένων σε ανεξάρτητες συσκευές.Μελέτες όπως αυτή του Kobayashi et al. (Kobayashi , 2019) , και συνεργατών επιβεβαιώνουν τη δυνατότητα υποστήριξης πολλαπλών εικονικών δικτύων μέσω της ανάπτυξης του SDN σε φυσική υποδομή. Επιπλέον, η πρόταση ενός υβριδικού μοντέλου δικτύωσης από τους συγγραφείς του αναδεικνύει τη σημασία του ελεγκτή στη διαχείριση της ροής διαδρομής.

Η έρευνα των Benzekki et al. (Benzekki , 2016) σχετικά με το λογισμικού ορισμού δικτύων (SDN) παρουσιάζει μια συνολική επισκόπηση των προκλήσεων και των λύσεων που αφορούν το SDN, συμπεριλαμβανομένων, της ελαστικότητας, της αξιοπιστίας, της υψηλής διαθεσιμότητας, της ανθεκτικότητας, της ασφάλειας και της απόδοσης. Η έρευνα επισημαίνει ότι, παρά την πρόοδο στην ανάπτυξη του SDN, πολλές προκλήσεις παραμένουν αναπάντητες. Η εργασία επισημαίνει την ανάγκη για περαιτέρω έρευνα σε περιοχές όπως η τυποποίηση των στοιχείων του SDN και η εφαρμογή νέων μηχανισμών ελέγχου για την αντιμετώπιση των προκλήσεων.

Επιπλέον, υπογραμμίζεται η σημασία της ανάπτυξης αξιόπιστων μηχανισμών υψηλής διαθεσιμότητας και απόδοσης για την επίτευξη των απαιτήσεων των παροχών υπηρεσιών και των τελικών χρηστών στο πλαίσιο των τηλεπικοινωνιακών υπηρεσιών.

Η έρευνα που πραγματοποιήθηκε από τον Lantz et al. (Lantz , 2015) εστιάζει στην ανάγκη για ανάπτυξη καταμεμημένων συστημάτων SDN και εφαρμογών. Παρουσιάζεται η χρήση ενός εικονικού πειραματικού περιβάλλοντος βασισμένου στο Mininet, το οποίο επιτρέπει την εύκολη ανάπτυξη ενός εικονικού πειραματικού περιβάλλοντος από ελαφριές διανομές σε έναν μόνο υπολογιστή, ένα ad hoc cluster ή ένα αφιερωμένο πειραματικό περιβάλλον υλικού. Με την ενσωμάτωση ενός ανοικτού κώδικα λειτουργικού συστήματος δικτύου όπως το ONOS, προσφέρεται μια ευέλικτη και κλιμακούμενη πλατφόρμα ανάπτυξης λογισμικού για τα καταμεμημένα συστήματα SDN και τις εφαρμογές τους.

Ο Fontes et al. (Fontes , 2015) και συνεργάτες, πραγματοποίησαν έρευνα η οποία επικεντρώνεται στη χρήση του Λογισμικού Ορισμένων Δικτύων (SDWN) για τον σχεδιασμό και τη λειτουργία ασύρματων δικτύων, προσφέροντας πλεονεκτήματα όπως εξοικονόμηση κόστους και προσαρμοστικότητα υπηρεσιών. Η παρουσίαση περιλαμβάνει τον εξομοιωτή Mininet-WiFi, επιτρέποντας σε χρήστες να αλληλεπιδρούν με εικονικούς σταθμούς WiFi σε ένα ασύρματο δίκτυο mesh ή να συνδεθούν στο διαδίκτυο μέσω ενός εξομοιωμένου υποδομής SDWN. Επιπλέον, παρουσιάζεται ο εξομοιωτής Mininet-WiFi, ο οποίος υποστηρίζει την έρευνα στον τομέα του SDWN, ενσωματώνοντας εικονικούς και φυσικούς κόμβους σε ένα πειραματικό περιβάλλον. Και οι δύο αυτές πρωτοβουλίες προσφέρουν δυνατότητες για εκτέλεση ρεαλιστικών πειραμάτων σε υβριδικά περιβάλλοντα, συμπεριλαμβανομένης της αναπαραγωγής φυσικών μέσων και της προσομοίωσης ασύρματης κίνησης.

Ο συγγραφέας Kumar et al. (Kumar , 2019) και συνεργάτες παρουσιάζουν μια ερευνητική εργασία που εστιάζει στην ανθεκτικότητα και την επεκτασιμότητα του Wi-Fi στο Mininet για μικρά έως μεγάλα δίκτυα SDN. Το κείμενο εξετάζει την εφαρμογή της υποστήριξης Wi-Fi σε δίκτυα SDN και παρουσιάζει τα αποτελέσματα πειραμάτων που εξετάζουν την απόδοση του SDN δικτύου βασισμένου σε Wi-Fi στο Mininet, με δοκιμές απόδοσης σε διάφορα δυναμικά σενάρια. Τα πειράματα αποσκοπούν στην αξιολόγηση της απόδοσης του Wi-Fi σε SDN, χρησιμοποιώντας τα πρωτόκολλα TCP και UDP. Παρατηρήθηκε ότι η απόδοση μειώνεται σταδιακά όταν αυξάνεται ο αριθμός των σταθμών. Έτσι, η υλοποίηση του Wi-Fi σε ένα SDN μας επιτρέπει να κατανοήσουμε πώς λειτουργούν οι συσκευές και ποια μπορεί να είναι τα αποτελέσματα με την αύξηση του αριθμού των συσκευών.

Ο συγγραφέας της έρευνας Ammour et al. (Ammour ,2023) , η οποία αφορούσε την αξιολόγηση της απόδοσης και της ανεκτικότητας σε βλάβες των ελεγκτών δικτύων SDN , έδειξε ότι ο εξομοιωτής *estinet* παρήγαγε σωστά και

επαναληπτικά αποτελέσματα σχετικά με τον μέσο χρόνο απόκρισης (RTT), ενώ χρειάστηκε περισσότερος χρόνος για την ολοκλήρωση της προσομοίωσης όταν το δίκτυο ήταν μεγαλύτερο. Από την άλλη πλευρά, ο εξομοιωτής Mininet εμφάνισε περίεργα αποτελέσματα σε ορισμένες περιπτώσεις και απαιτούσε περισσότερο χρόνο για την εκκίνηση και τη λειτουργία του, ιδίως όταν το μέγεθος του δικτύου αυξανόταν.

Ο Ketii et al. (Ketii , 2015) και οι συνεργάτες του, παρουσιάζουν μια έρευνα που αξιολογεί ένα εργαλείο εξομοίωσης SDN που ονομάζεται Mininet. Διεξήχθησαν δοκιμές για να μελετηθούν οι περιορισμοί του Mininet σχετικά με το περιβάλλον προσομοίωσης και τις δυνατότητες των πόρων. Κατά την αξιολόγηση της του Mininet, δοκιμάστηκε η δημιουργία πολλών τοπολογιών με μεταβλητό αριθμό κόμβων και δύο διαφορετικά σενάρια περιβάλλοντος. Τα αποτελέσματα δείχνουν ότι το περιβάλλον προσομοίωσης έχει σημαντική επίδραση στον απαιτούμενο χρόνο για τη δημιουργία μιας τοπολογίας. Επιπλέον, αναφέρεται ότι τα χαρακτηριστικά και οι προδιαγραφές του περιβάλλοντος προσομοίωσης πρέπει να λαμβάνονται υπόψη πριν από τη χρήση του Mininet, και με προσεκτική επιλογή αυτών των χαρακτηριστικών, το Mininet μπορεί να χρησιμοποιηθεί ως ένα ισχυρό εργαλείο στην εξομοίωση των SDN και των εικονικών δικτύων.

Η έρευνα που πραγματοποιήθηκε από τον Shah S et al (Shah S , 2013),εστίασε στην αρχιτεκτονική αξιολόγηση των ελεγκτών SDN. Σκοπός της ήταν η αναγνώριση των βασικών σημείων αδυναμίας απόδοσης και των καλών αρχιτεκτονικών επιλογών για τον σχεδιασμό ελεγκτών SDN βασισμένων σε OpenFlow. Με αυτόν τον στόχο, αξιολόγησε την απόδοση τεσσάρων κορυφαίων ελεγκτών OpenFlow που είναι ανοιχτού κώδικα: NOX, Beacon, Maestro και Floodlight. Μετά την ανάλυση των αποτελεσμάτων τους, πρότεινε κατευθυντήριες γραμμές αρχιτεκτονικής που μπορούν να χρησιμοποιηθούν για τη βελτίωση των υπάρχοντων ελεγκτών ή τον σχεδιασμό νέων. Τέλος, παρουσίασε έναν ελεγκτή βασισμένο στις προτεινόμενες κατευθυντήριες γραμμές, ο οποίος φαίνεται να παρουσιάζει συνεχείς βελτιώσεις σε θέματα ροής και καθυστέρησης .

Ο Assegie et al. (Assegie , 2019) παρουσίασε μια έρευνα στην οποία διερεύνησε τα εργαλεία μοντελοποίησης που χρησιμοποιούνται για το ασύρματο δίκτυο ορισμένου λογισμικού και με βάση την έρευνα χρησιμοποίησε το mininet-Wi-Fi για τη μοντελοποίηση του ασύρματου δικτύου ορισμένου λογισμικού, το οποίο είναι το καλύτερο και πιο ευρέως χρησιμοποιούμενο εργαλείο εξομοίωσης για το ασύρματο δίκτυο ορισμένου λογισμικού. Αξιολόγησε την απόδοση του εύρους ζώνης της κίνησης TCP για διαφορετικό αριθμό εξομοιωμένων τελικών σταθμών και σημείων πρόσβασης. Εξομοίωσε ένα ασύρματο δίκτυο ορισμένου λογισμικού χρησιμοποιώντας το mininet-Wi-Fi και τον ελεγκτή OpenFlow, μια πλατφόρμα λογισμικού που αναπτύχθηκε από την rython, την οποία χρησιμοποίησε ως ελεγκτή με εξομοιωμένους σταθμούς και δημιούργησε τα μοντέλα των ασύρματων δικτύων

ορισμένου λογισμικού .Ανέλυσε την απόδοση του TCP για την κυκλοφορία του δικτύου με διαφορετικό αριθμό εξομοιωμένων τελικών σταθμών ασύρματου δικτύου καθορισμένου λογισμικού και αποδείχθηκε ότι, η απόδοση υποβαθμίζεται με την αύξηση του αριθμού των τελικών σταθμών και ως λύση για την αύξηση της απόδοσης πρότεινε την παράδοση με βάση την εξισορρόπηση φορτίου για τη μετακίνηση των σταθμών από το υπερφορτωμένο σημείο πρόσβασης σε άλλο σημείο πρόσβασης.

Ο Rajesh et al. (Rajesh , 2021) παρουσίασε την εργασία του στην οποία αναφέρει ότι το διαδίκτυο αντιμετωπίζει καθημερινά πολλά προβλήματα, ένα από αυτά είναι η μείωση του εύρους ζώνης του δικτύου λόγω της κατανεμημένης άρνησης παροχής υπηρεσιών στον κεντρικό διακομιστή, η οποία εξαντλεί τους πόρους του κεντρικού υπολογιστή. Ο ερευνητής έχει εφεύρει πολλούς μηχανισμούς προστασίας, όπως η ανίχνευση, η πρόληψη, η αντίδραση και ο χαρακτηρισμός σε περίπτωση επιθέσεων DDoS, οι οποίοι θα ελέγχουν τον αριθμό των κακόβουλων πακέτων που λαμβάνει το θύμα αλλά δεν παρέχει αποτελεσματική τεχνική ανίχνευσης με υψηλό ποσοστό σε υποδομή δικτύου σε πραγματικό χρόνο. Έτσι, οι σύγχρονες τεχνολογίες προετοιμάζονται σε προσομοιωτές δικτύου Mininet, οι οποίοι δίνουν μεγαλύτερο αντίκτυπο στην προσομοίωση του πραγματικού δικτύου. Η αρχιτεκτονική των δικτύων καθορισμένων από λογισμικό (SDN) και η αρχιτεκτονική OpenFlow χρησιμοποιούνται για να επιδείξουν ένα προγραμματιζόμενο μοντέλο δικτύου και την κεντρική διαχείριση του πραγματικού δικτύου. Σε αυτή την ερευνητική εργασία, παρουσιάζουν το σχεδιασμό του δικτύου καθορισμένου από λογισμικό (SDN) με χρήση προσομοιωτή mininet και θέματα ασφάλειας που σχετίζονται με το δίκτυο καθορισμένου από λογισμικό. Συμπερασματικά ο προσομοιωτής Mininet λειτουργεί ως μια χρήσιμη εναλλακτική λύση για την εκτέλεση προβληματικών περιπτώσεων SDN σε προσομοιωμένο δίκτυο. Οι εικονικές μηχανές παρέχουν έναν ευκολότερο τρόπο για την παροχή διαμόρφωσης και αλλαγής τοπολογίας, αλλά με την πραγματική μηχανή είναι δύσκολο. Λόγω της αποσύνδεσης του επιπέδου δεδομένων από το επίπεδο ελέγχου, το SDN είναι ευάλωτο σε περισσότερες επιθέσεις. Λόγω της ευπάθειας, η απόδοση του SDN θα μπορούσε να επηρεαστεί αυστηρά.

3. Αξιολόγηση του SDN

3.1. Εισαγωγή και ορισμοί

Ο όρος "Software-Defined Networking" (SDN) εισήχθη από τον Nick McKeown του Πανεπιστημίου της Στάνφορντ και τον Martin Casado το 2009, καθώς

παρουσίασαν την ιδέα σε ένα συνέδριο. Αυτή η νέα προσέγγιση στο δίκτυο προτείνει να χωριστεί η λειτουργία ελέγχου (control plane) από την προώθηση (data plane) των πακέτων δεδομένων, επιτρέποντας τη διαχείριση του δικτύου μέσω λογισμικού, με αποτέλεσμα την ευελιξία, την επεκτασιμότητα και τη διαχείριση του δικτύου με πιο εξελιγμένους τρόπους. Η ιδέα πίσω από το SDN εξελίσσεται βέβαια από το 1996 με γνώμονα την επιθυμία να παρέχεται ελεγχόμενη από τον χρήστη διαχείριση της προώθησης σε κόμβους δικτύου. Το Software-Defined Networking (SDN) είναι μια εξελιγμένη τεχνολογική προσέγγιση στον χώρο των δικτύων, σχεδιασμένη για να αλλάξει τον τρόπο λειτουργίας, διαχείρισης και αυτοματισμού των δικτύων υπολογιστών. Στο παραδοσιακό μοντέλο, τονίζεται η έννοια του "συγκεκριμένου σκληρού προγραμματισμού" (fixed-function hardware) στις δικτυακές συσκευές, όπως δρομολογητές και commutators, όπου η λειτουργία και ο έλεγχος προσδιορίζονται από τον εκάστοτε κώδικα που είναι "εγκατεστημένος" στην συσκευή.

Στο SDN, αυτό το μοντέλο αλλάζει ριζικά σύμφωνα με τον Benzekki et al. (Benzekki, 2016). Ο έλεγχος (control plane) αποσπάται από το υλικό και εκτελείται σε έναν κεντρικό ελεγκτή. Ο ελεγκτής αποφασίζει πώς θα ρυθμίσει κάθε συσκευή και τη ροή των δεδομένων (data plane) βάσει των αναγκών του δικτύου και των εφαρμογών. Αυτό επιτρέπει την ευελιξία, την επεκτασιμότητα και την εύκολη προσαρμογή του δικτύου σε νέες απαιτήσεις.

Βασικά χαρακτηριστικά του SDN σύμφωνα με τον Gelberger et al. (Gelberger, 2013), περιλαμβάνουν τον διαχωρισμό των επιπέδων (Layer Separation), την κεντρική διαχείριση (Centralized Management) και τη δυναμική του προγραμματισμού. (Dynamic Programmability). Αυτές οι αρχές του SDN επιτρέπουν την αποτελεσματική και ευέλικτη διαχείριση των δικτύων, προσφέροντας νέες δυνατότητες προγραμματισμού και αυτοματισμού.

Κατά συνέπεια, το SDN επαναπροσδιορίζει τον τρόπο με τον οποίο τα δίκτυα διαχειρίζονται, επιτρέποντας την εύκολη ανάπτυξη και προσαρμογή σε νέες ανάγκες, ενισχύοντας την ασφάλεια, την απόδοση και την ευελιξία των δικτύων όπως αναφέρει ο Karakus et al. (Karakus, 2017). Τα δίκτυα SDN (Software-Defined Networking) αναπαριστούν μια εξελιγμένη προσέγγιση στη σχεδίαση και διαχείριση δικτύων. Σε αυτό το προηγμένο μοντέλο, ο έλεγχος και η διαμόρφωση του δικτύου διαχωρίζονται από τον φυσικό εξοπλισμό, με τον ρόλο αυτό να εκτελείται από ένα κεντρικό λογισμικό, γνωστό ως SDN Controller. Ο SDN Controller λειτουργεί ως διαχειριστική ενότητα, επιτρέποντας την επικοινωνία μέσα στο δίκτυο, την παρακολούθηση της κίνησης, τη δρομολόγηση και την εφαρμογή πολιτικών ασφαλείας. Αυτή η απομακρυσμένη διαχείριση επιτρέπει την ευελιξία, την απλούστευση και την αποτελεσματικότητα της δικτυακής υποδομής, καθώς οι αλλαγές και οι προσαρμογές μπορούν να εφαρμοστούν δυναμικά μέσω του λογισμικού ελέγχου, ανεξάρτητα από τον εξοπλισμό.

3.1.1. ΑΣΥΡΜΑΤΗ SDN ΔΙΚΤΥΩΣΗ

Στον εξαιρετικά δυναμικό και εξελιγμένο κόσμο των τηλεπικοινωνιών και των δικτύων, η τεχνολογία συνεχώς εξελίσσεται προκειμένου να προσφέρει αποτελεσματικές και αξιόπιστες λύσεις για την αυξανόμενη ζήτηση των επικοινωνιακών αναγκών. Στο πλαίσιο αυτό, η Ασύρματη Δικτύωση με τη χρήση της τεχνολογίας Software-Defined Networking (SDN) έχει εμφανιστεί ως μια εξαιρετικά καινοτόμος προσέγγιση με πολλά υποσχόμενες δυνατότητες.

3.1.2.Εισαγωγή στην Ασύρματη Δικτύωση SDN

Η Ασύρματη Δικτύωση SDN αναφέρεται στην εφαρμογή των αρχών και της τεχνολογίας της SDN σε ασύρματα δίκτυα Raju et al. (Raju ,2018) . Σε αυτό το προηγμένο μοντέλο, ο έλεγχος και η διαμόρφωση του δικτύου διαχωρίζονται από τον φυσικό εξοπλισμό, με τον ρόλο αυτό να εκτελείται από ένα κεντρικό λογισμικό, γνωστό ως SDN Controller. Αυτή η απομακρυσμένη διαχείριση επιτρέπει την ευελιξία, την απλούστευση και την αποτελεσματικότητα της δικτυακής υποδομής, καθώς οι αλλαγές και οι προσαρμογές μπορούν να εφαρμοστούν δυναμικά μέσω του λογισμικού ελέγχου, ανεξάρτητα από τον εξοπλισμό.

3.1.3.Βασικές Αρχές του SDN

Στο πλαίσιο της Ασύρματης Δικτύωσης SDN, υπάρχουν τρεις βασικές αρχές που καθορίζουν τη λειτουργία του συστήματος όπως αναφέρει και ο Kreutz et al. (Kreutz , 2014):

- **Διαχωρισμός των Επιπέδων (Layer Separation):** Στο SDN, τα επίπεδα του ελέγχου και του δεδομένων διαχωρίζονται. Ο έλεγχος εκτελείται από τον κεντρικό ελεγκτή (SDN Controller), ενώ οι δικτυακές συσκευές (όπως δρομολογητές και access points) είναι υπεύθυνες για τη μεταφορά των δεδομένων.
- **Κεντρική Διαχείριση (Centralized Management):** Ο SDN Controller αναλαμβάνει τον συνολικό έλεγχο και τη διαχείριση του δικτύου. Αποφασίζει πώς πρέπει να ρυθμιστούν οι συσκευές και η ροή των δεδομένων, βασιζόμενος στις ανάγκες του δικτύου και των εφαρμογών.
- **Δυναμική Προγραμματισιμότητα (Dynamic Programmability):** Οι διαχειριστικές εντολές μπορούν να εκδίδονται δυναμικά από τον SDN Controller, αλλάζοντας τη συμπεριφορά του δικτύου κατά τη διάρκεια της λειτουργίας, προσφέροντας έτσι μεγάλη ευελιξία.

Πλεονεκτήματα της Ασύρματης Δικτύωσης SDN:

- Δυναμική Δρομολόγηση (Dynamic Routing): Η ασύρματη δικτύωση SDN επιτρέπει την αλλαγή της δρομολόγησης σύμφωνα με τις ανάγκες.
- Ασφάλεια: Η κεντρική διαχείριση επιτρέπει καλύτερη ανίχνευση και αντίδραση σε προβλήματα ασφάλειας .
- Ευελιξία και Επεκτασιμότητα: Το δίκτυο μπορεί να επεκταθεί και να προσαρμοστεί εύκολα σε νέες απαιτήσεις.

3.1.4. Προκλήσεις και Επικείμενες Εξελίξεις

Ωστόσο, υπάρχουν και προκλήσεις που πρέπει να αντιμετωπιστούν, όπως η ασφάλεια των δεδομένων και η πολυπλοκότητα της διαχείρισης του κεντρικού ελεγκτή. Μελλοντικά, αναμένεται να επιλυθούν αυτές οι προκλήσεις μέσω της εξέλιξης της τεχνολογίας και της περαιτέρω έρευνας στον τομέα Bannour, et al. (Bannour , 2017) .Συνολικά, η ασύρματη δικτύωση SDN αποτελεί μια εξαιρετικά καινοτόμο προσέγγιση που έχει τη δυνατότητα να αλλάξει ριζικά τον τρόπο που αντιλαμβανόμαστε και χρησιμοποιούμε τα ασύρματα δίκτυα. Με την ευελιξία, την ασφάλεια και την αποτελεσματικότητά της, αναμένεται να αποτελέσει έναν σημαντικό παράγοντα για το μέλλον των επικοινωνιών.

3.2 Εφαρμογές SDN Δικτύωσης

Η ασύρματη SDN δικτύωση χρησιμοποιείται σε πολλούς τομείς και εφαρμογές, συμπεριλαμβανομένων εταιρειών και κέντρων δεδομένων όπως αναφέρει ο Valdivieso Caraguay et al. (Valdivieso Caraguay , 2014).Ορισμένα συγκεκριμένα παραδείγματα χρήσης περιλαμβάνουν:

- **Επιχειρήσεις:** Στον κόσμο των επιχειρήσεων, η ασύρματη SDN δικτύωση μπορεί να χρησιμοποιηθεί για τη δημιουργία αξιόπιστων και ασφαλών ασύρματων δικτύων στα γραφεία, επιτρέποντας την ασφαλή πρόσβαση στο διαδίκτυο και τις εταιρικές εφαρμογές. Στον τομέα των επιχειρήσεων, οι ασύρματες SDN (Software-Defined Networking) δικτυώσεις προσφέρουν αρκετές ευκαιρίες για βελτίωση της απόδοσης, της ασφάλειας και της ευελιξίας. Εδώ είναι μερικά παραδείγματα εφαρμογών:

1.Εταιρικά Δίκτυα και Εσωτερική Επικοινωνία (Corporate Networks and Internal Communication): Με την αποκέντρωση και τον ευέλικτο έλεγχο που προσφέρουν οι ασύρματες SDN δικτυώσεις, οι επιχειρήσεις μπορούν να διαχειρίζονται πιο αποτελεσματικά την εσωτερική τους επικοινωνία. Αυτό μπορεί να συμπεριλαμβάνει τη βελτίωση της ποιότητας των υπηρεσιών (QoS) για τη φωνητική κλήση αλλά και τη βιντεοκλήση , αλλά και τη διαχείριση εφαρμογών εντός του δικτύου.

2.Κέντρα Δεδομένων και Ελεγχόμενη Επεκτασιμότητα (Data Centers and Controlled Scalability): Σε μεγάλα κέντρα δεδομένων, οι ασύρματες SDN δικτυώσεις επιτρέπουν τη δυναμική και αυτόματη επεκτασιμότητα των υποδομών τους. Αυτό σημαίνει ότι οι επιχειρήσεις μπορούν να προσαρμόζουν την χωρητικότητα και τους πόρους τους ανάλογα με τις ανάγκες τους, χωρίς διακοπές στις υπηρεσίες τους.

3.Ασφάλεια Δικτύου και Επικοινωνία (Network Security and Communication): Οι ασύρματες SDN δικτυώσεις επιτρέπουν την αυτόματη ανίχνευση και αντίδραση σε κινδύνους και παραβιάσεις ασφαλείας. Μπορούν επίσης να εφαρμόσουν πολιτικές ασφαλείας σε πραγματικό χρόνο ανάλογα με την κατάσταση του δικτύου.

4.Αυξημένη Παρακολούθηση και Διαχείριση Επιδόσεων (Enhanced Performance Monitoring and Management): Οι επιχειρήσεις μπορούν να χρησιμοποιήσουν ασύρματες SDN δικτυώσεις για την παρακολούθηση και την ανάλυση της απόδοσης των εφαρμογών και των υπηρεσιών τους, προκειμένου να βελτιώσουν την ποιότητα και την αποδοτικότητα τους.

- **Έξυπνες Πόλεις (Smart Cities):** Στο πεδίο των έξυπνων πόλεων, η ασύρματη SDN δικτύωση μπορεί να χρησιμοποιηθεί για τη σύνδεση και τη διαχείριση αισθητήρων Ghosh U et al. (Ghosh U , 2020) , καμερών ασφαλείας και άλλων συσκευών που συνεισφέρουν στην παρακολούθηση και βελτίωση της ποιότητας ζωής των πολιτών. Οι έξυπνες πόλεις (smart cities) είναι πόλεις που χρησιμοποιούν τεχνολογία και δεδομένα για να βελτιώσουν την ποιότητα ζωής των κατοίκων τους, να ενισχύσουν τη βιωσιμότητα και να βελτιώσουν την αποτελεσματικότητα των υπηρεσιών που παρέχουν. Οι ασύρματες SDN δικτυώσεις παίζουν σημαντικό ρόλο στη δημιουργία και ανάπτυξη των έξυπνων πόλεων. Ας δούμε παραδείγματα εφαρμογών SDN σε έξυπνες πόλεις:

1.Κυκλοφοριακή ροή και συγκοινωνίες: Συστήματα ελέγχου κυκλοφορίας που χρησιμοποιούν ασύρματες SDN δικτυώσεις για να παρακολουθούν την κίνηση, να ελέγχουν τα φώτα κυκλοφορίας και να συγχρονίζουν τα συστήματα μεταφοράς με σκοπό την μείωση της κυκλοφοριακής συμφόρησης και την βελτίωση της κυκλοφορίας.

2.Βελτιστοποίηση της κατανάλωσης ενέργειας: Συστήματα διαχείρισης ενέργειας σε κτίρια και δημόσιες υποδομές, όπως δρόμοι και δημόσια φωτιστικά σώματα, μπορούν να ρυθμίζονται δυναμικά μέσω ασύρματων SDN δικτυώσεων για εξοικονόμηση ενέργειας και βελτιστοποίηση της χρήσης των πόρων.

3.Περιβάλλον και βιωσιμότητα: Ασύρματα δίκτυα μπορούν να χρησιμοποιηθούν για την παρακολούθηση της ποιότητας του αέρα, των υδάτων, καθώς και για τη διαχείριση των απορριμμάτων με στόχο την βελτίωση του περιβάλλοντος και την προώθηση της βιωσιμότητας.

4. Διαχείριση κρίσεων και ασφάλεια: Συστήματα παρακολούθησης και διαχείρισης καταστάσεων κινδύνου με χρήση ασύρματων SDN δικτύων για αποτελεσματική αντίδραση κατά καταστροφών, φυσικών καταστροφών ή κρίσεων.

- **Ασύρματες Επικοινωνίες IoT:** Στο πλαίσιο του Διαδικτύου των Πραγμάτων (IoT), η ασύρματη SDN δικτύωση μπορεί να υποστηρίξει τη σύνδεση και τον έλεγχο των πολλών συσκευών IoT που επικοινωνούν ασύρματα Cabral et al. (Cabral , 2019), εξασφαλίζοντας αξιόπιστη ανταλλαγή δεδομένων. Οι ασύρματες επικοινωνίες για το Διαδίκτυο των Πραγμάτων (IoT - Internet of Things) είναι απαραίτητες για την ανταλλαγή δεδομένων ανάμεσα σε διάφορες συσκευές και αισθητήρες που συνδέονται με το Διαδίκτυο. Αυτές οι ασύρματες επικοινωνίες κατέχουν κεντρικό ρόλο στην ανάπτυξη του IoT, προσφέροντας σύνδεση, ευελιξία και δυνατότητα ανταλλαγής δεδομένων μεταξύ των διαφόρων συσκευών Tello-Oquendo , et al. (Tello-Oquendo , 2018). Εδώ είναι μερικά παραδείγματα ασύρματων επικοινωνιών IoT:

1.Wi-Fi: Το Wi-Fi είναι μια από τις πιο διαδεδομένες ασύρματες τεχνολογίες που χρησιμοποιούνται για τη σύνδεση συσκευών IoT σε δίκτυα. Επιτρέπει γρήγορη μεταφορά δεδομένων και είναι κατάλληλη για οικιακή χρήση και για περιβάλλοντα γραφείων.

2.Bluetooth: Η τεχνολογία Bluetooth είναι κοινή για σύντομες αποστάσεις επικοινωνίας μεταξύ συσκευών IoT. Συχνά χρησιμοποιείται για αισθητήρες, έξυπνες συσκευές και ακουστικά.

3.Zigbee: Το Zigbee είναι ένα πρωτόκολλο ασύρματων επικοινωνιών που χρησιμοποιείται συχνά για τον έλεγχο και τη διαχείριση συσκευών IoT σε έξυπνα σπίτια, γραφεία και βιομηχανικά περιβάλλοντα.

4.LoRaWAN (Long Range Wide Area Network): Το LoRaWAN είναι μια τεχνολογία μεγάλου εύρους που χρησιμοποιείται για ασύρματη επικοινωνία σε μεγάλες αποστάσεις. Χρησιμοποιείται συχνά για IoT εφαρμογές που απαιτούν επικοινωνία σε αγροτικές περιοχές ή αστικές κοινότητες.

5.NB-IoT (Narrowband IoT): Το NB-IoT είναι ένα πρωτόκολλο επικοινωνιών κινητής τηλεφωνίας που σχεδιάστηκε ειδικά για τις ανάγκες του IoT. Παρέχει μακρινό εύρος κάλυψης, εξοικονόμηση ενέργειας και σύνδεση σε μεγάλο αριθμό συσκευών.

- **Εκπαιδευτικά Ιδρύματα:** Σε σχολεία και πανεπιστήμια, η ασύρματη SDN δικτύωση μπορεί να υποστηρίξει την ασύρματη πρόσβαση στο διαδίκτυο για φοιτητές και προσωπικό, ενώ επιτρέπει τη διαχείριση και την ασφάλεια του ασύρματου δικτύου Caicedo et al. (Caicedo ,2019). Οι ασύρματες επικοινωνίες και η τεχνολογία SDN (Software-Defined Networking) μπορούν να έχουν

σημαντική επίδραση στα εκπαιδευτικά ιδρύματα, βελτιώνοντας τη διαδικασία διδασκαλίας, τη διαχείριση του δικτύου, και τη γενικότερη απόδοση και ασφάλεια. Εδώ είναι μερικά παραδείγματα πώς αυτές οι τεχνολογίες εφαρμόζονται στα εκπαιδευτικά ιδρύματα:

1.Ενισχυμένη Σύνδεση και Διδασκαλία: Ασύρματα δίκτυα μπορούν να επιτρέψουν στους φοιτητές και τους καθηγητές να συνδέονται σε διάφορες πλατφόρμες και εφαρμογές για αποτελεσματική διδασκαλία, διαλέξεις online , και ανταλλαγή εκπαιδευτικού υλικού.

2.Βελτιωμένη Διαχείριση Δικτύου: Η τεχνολογία SDN επιτρέπει στους διαχειριστές των εκπαιδευτικών δικτύων να διαχειρίζονται και να προσαρμόζουν το δίκτυο με ευελιξία, προσφέροντας βελτιωμένη ασφάλεια, απόδοση και αποτελεσματικότητα.

3.Εξελιγμένες Εφαρμογές e-Learning: Ασύρματες επικοινωνίες σε συνδυασμό με την τεχνολογία SDN μπορούν να υποστηρίξουν εξελιγμένες εκπαιδευτικές πλατφόρμες, παρέχοντας δυνατότητες προσαρμοστικής διδασκαλίας και προσαρμοσμένου περιεχομένου.

4.Ασφάλεια και Προστασία Δεδομένων: Οι ασύρματες τεχνολογίες σε συνδυασμό με το SDN μπορούν να βελτιώσουν την ασφάλεια των δικτύων εκπαιδευτικών ιδρυμάτων, εξασφαλίζοντας την προστασία των δεδομένων των φοιτητών και των υπαλλήλων.

5.Αποθήκευση και Διαμοιρασμός Εκπαιδευτικού Υλικού: Με τη χρήση ασύρματων τεχνολογιών, οι φοιτητές και οι καθηγητές μπορούν να αποθηκεύουν, να διαμοιράζονται και να έχουν πρόσβαση σε εκπαιδευτικό υλικό από οπουδήποτε μέσω διαδικτύου.

Αυτά τα παραδείγματα αναδεικνύουν πώς η ασύρματη επικοινωνία και η τεχνολογία SDN μπορούν να μεταμορφώσουν την εκπαίδευση. Αυτά είναι μερικά παραδείγματα της ευρείας εφαρμογής της ασύρματης SDN δικτύωσης σε διάφορους τομείς και περιβάλλοντα.

3.3. Ασύρματη SDN Δικτύωση έναντι Legacy Networks

Η τεχνολογική πρόοδος των τελευταίων δεκαετιών έχει επηρεάσει σημαντικά τον κόσμο των δικτύων σύμφωνα με τον Mtawa et al. (Mtawa, 2021). Ειδικότερα με την ανάδειξη της ασύρματης SDN (Software-Defined Networking) δικτύωσης ως προηγμένου μοντέλου σε σύγκριση με τα παραδοσιακά "legacy networks". Και τα δύο μοντέλα φέρουν τόσο πλεονεκτήματα όσο και μειονεκτήματα. Στο παρακάτω κείμενο, θα εξετάσουμε εκτενώς αυτά τα πλεονεκτήματα και μειονεκτήματα της ασύρματης SDN δικτύωσης έναντι των legacy networks, με έμφαση στο πώς αυτά μπορούν να διαμορφώσουν τις επιλογές και τις αποφάσεις που λαμβάνονται για τη δομή και τη διαχείριση των δικτύων.

Πλεονεκτήματα της Ασύρματης SDN Δικτύωσης

Η ασύρματη SDN δικτύωση, όπως αναφέρει και ο Dorsch et al. (Dorsch, 2014) προσφέρει σημαντικά πλεονεκτήματα που αξίζει να εξετάσουμε:

- **Ευελιξία και Δυναμικότητα:** Η ασύρματη SDN δικτύωση προσφέρει ευελιξία και δυναμικότητα, καθώς μπορεί να αναδιαμορφωθεί εύκολα. Μπορεί να προσαρμοστεί στις συγκεκριμένες ανάγκες του δικτύου με αλλαγές στις διαδρομές, τους πόρους και τις πολιτικές δικτύου.
- **Κεντρική Διαχείριση:** Ένα από τα κύρια πλεονεκτήματα της ασύρματης SDN δικτύωσης είναι η δυνατότητα κεντρικής διαχείρισης. Αυτό σημαίνει ότι μπορεί να γίνει έλεγχος και διαχείριση του δικτύου από ένα κεντρικό σημείο. Αυτή η δυνατότητα βελτιώνει την αποτελεσματικότητα και την ασφάλεια του δικτύου.
- **Ασφάλεια:** Η ασφάλεια είναι μία από τις βασικές προτεραιότητες σε οποιοδήποτε δίκτυο. Με την ασύρματη SDN δικτύωση, μπορούν να εφαρμοστούν προηγμένες πολιτικές ασφαλείας. Αυτό εξασφαλίζει προστασία από απειλές και επιθέσεις, καθιστώντας το δίκτυο ασφαλέστερο για τα δεδομένα και τις επικοινωνίες.

Μειονεκτήματα της Ασύρματης SDN Δικτύωσης

Η μετάβαση σε ασύρματη SDN δικτύωση μπορεί να συναντήσει ορισμένα μειονεκτήματα, Zhang et al. (Zhang, 2018) τα οποία είναι σημαντικά να ληφθούν υπόψη:

- **Ασυμβατότητα με Υφιστάμενο Εξοπλισμό:** Η ασύρματη SDN δικτύωση μπορεί να απαιτήσει την ανανέωση του υφιστάμενου

εξοπλισμού. Αυτός ο εξοπλισμός μπορεί να μην είναι συμβατός με τις νέες τεχνολογίες που εισάγονται με την υλοποίηση της ασύρματης SDN δικτύωσης.

- **Πολυπλοκότητα:** Η ασύρματη SDN δικτύωση μπορεί να είναι περίπλοκη στην εγκατάσταση και την παραμετροποίηση. Απαιτεί εξειδικευμένες γνώσεις και εμπειρία για να διαχειριστεί κανείς αποτελεσματικά το σύστημα. Αυτή η πολυπλοκότητα μπορεί να αυξήσει τον χρόνο και τους πόρους που απαιτούνται για την εφαρμογή της ασύρματης SDN τεχνολογίας.

Είναι σημαντικό να αντιληφθούμε τα περιορισμένα σημεία της ασύρματης SDN δικτύωσης και να τα αντιμετωπίσουμε με κατάλληλες στρατηγικές για να ελαχιστοποιήσουμε τις πιθανές επιπτώσεις αυτών των περιορισμών.

Πλεονεκτήματα των Legacy Networks

Τα legacy networks έχουν ορισμένα πλεονεκτήματα που τους καθιστούν αξιόλογη επιλογή για συγκεκριμένες περιπτώσεις Tarawneh et al. (Tarawneh, 2014).

- **Ευκολία Εγκατάστασης:** Τα legacy networks είναι συχνά πιο εύκολα στην εγκατάσταση σε σχέση με νεότερες τεχνολογίες. Η τεχνολογία τους έχει εδραιωθεί και έχει καταστεί γνωστή, καθιστώντας την διαδικασία εγκατάστασης σχετικά απλή.
- **Συμβατότητα με Υφιστάμενο Εξοπλισμό:** Ένα σημαντικό πλεονέκτημα των legacy networks είναι η συμβατότητά τους με τον υφιστάμενο εξοπλισμό. Σε πολλές περιπτώσεις, η ενσωμάτωση νέων τεχνολογιών μπορεί να προκαλέσει σημαντικό κόστος. Επομένως, η συμβατότητα με υφιστάμενο εξοπλισμό εξοικονομεί χρόνο και πόρους.

Αυτά τα πλεονεκτήματα κάνουν τα legacy networks ελκυστικά, ιδίως όταν η απλούστευση της εγκατάστασης και η συμβατότητα με τον υφιστάμενο εξοπλισμό αποτελούν κρίσιμους παράγοντες.

Μειονεκτήματα των Legacy Networks

Τα legacy networks, παρόλο που έχουν χρησιμοποιηθεί ευρέως για πολλά χρόνια, έχουν ορισμένα μειονεκτήματα που προκύπτουν από την τεχνολογική τους φύση και αρχιτεκτονική σύμφωνα με τον Krikidis et al. (Krikidis, 2009)

- **Περιορισμένη Ευελιξία:** Legacy networks είναι συχνά σχεδιασμένα για συγκεκριμένες χρήσεις ή λειτουργίες. Αυτό μπορεί να οδηγήσει σε

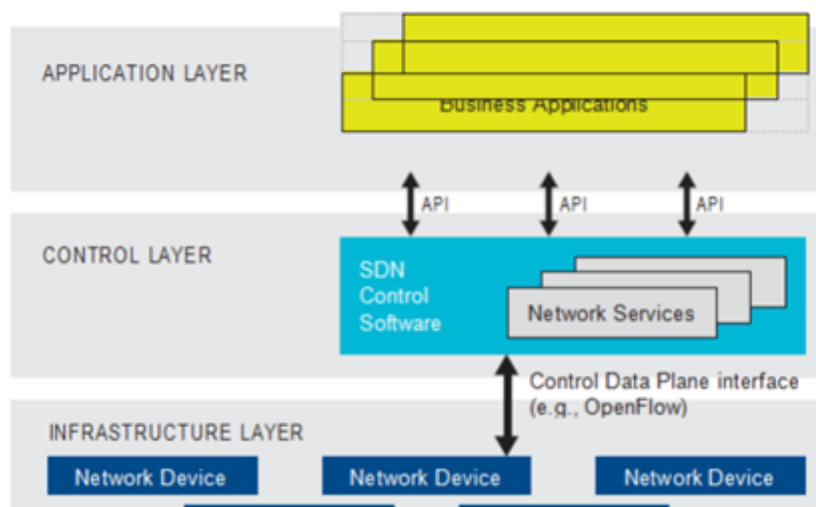
περιορισμένη ευελιξία όταν πρόκειται για αλλαγές, αναβαθμίσεις ή προσθήκη νέων λειτουργιών. Η αναδιαμόρφωση του δικτύου για να προσαρμοστεί σε νέες απαιτήσεις μπορεί να απαιτεί σημαντικό χρόνο και πόρους.

- **Περιορισμένη Κεντρική Διαχείριση:** Τα legacy networks συχνά έχουν αποκεντρωμένη διαχείριση, όπου οι αποφάσεις λήψης γίνονται από διάφορες συσκευές ή υποσυστήματα. Αυτό μπορεί να καθιστά πιο δύσκολη την ολοκληρωμένη και οργανωμένη διαχείριση του δικτύου, καθώς οι διαχειριστικές λειτουργίες είναι αποκεντρωμένες.

Τα παραπάνω μειονεκτήματα μπορούν να δημιουργήσουν δυσκολίες στην προσαρμογή του δικτύου σε αλλαγές και νέες απαιτήσεις, καθώς και στην αποτελεσματική και κεντρική διαχείριση του. Αυτά τα προβλήματα έχουν οδηγήσει στην ανάπτυξη της τεχνολογίας SDN, η οποία προσφέρει ευελιξία και κεντρική διαχείριση, αντιμετωπίζοντας ορισμένες από αυτές τις προκλήσεις.

4. Γενική Αρχιτεκτονική SDN

Η SDN δικτύωση Tao Han et al. (Tao Han, 2018) διαιρείται σε τρία κύρια επίπεδα: το επίπεδο εφαρμογής, το επίπεδο ελέγχου και το επίπεδο δεδομένων. Αυτά τα επίπεδα επικοινωνούν μεταξύ τους μέσω Interfaces που ονομάζονται Northbound και Southbound interfaces. Το Northbound interface διευκολύνει την επικοινωνία μεταξύ του επιπέδου εφαρμογής και του επιπέδου ελέγχου. Αυτή η διεπαφή (Interface) επιτρέπει στις εφαρμογές να αλληλεπιδρούν με τον ελεγκτή SDN, επιτρέποντάς τους να διαχειρίζονται την πολιτική και τις λειτουργίες του δικτύου. Από την άλλη πλευρά, το Southbound interface διευκολύνει την επικοινωνία μεταξύ του επιπέδου ελέγχου και του επιπέδου δεδομένων στην αρχιτεκτονική SDN. Αυτή η διεπαφή (Interface) επιτρέπει στον ελεγκτή να επικοινωνεί με τα φυσικά στοιχεία του



Εικόνα 0-1 Software Defined Network Architecture (Πηγή Tao Han , 2018)

δικτύου, όπως τους δρομολογητές και τους μεταγωγείς , για να υλοποιήσει τις πολιτικές που ορίζονται από το επίπεδο εφαρμογής. Σύμφωνα με το Open Networking Foundation (ONF), τα επίπεδα ελέγχου και δεδομένων σε μια αρχιτεκτονική SDN είναι αποσυνδεδεμένα Thirupathi et al. (Thirupathi , 2019). Στην εικόνα 0-1 απεικονίζεται η αρχιτεκτονική SDN δικτύωσης .

Το **επίπεδο εφαρμογής** στο δίκτυο SDN λειτουργεί ως γέφυρα μεταξύ του δικτύου και των εφαρμογών ή των χρηστών. Αυτό το επίπεδο είναι υπεύθυνο για την παροχή διαφόρων υπηρεσιών και λειτουργιών προς τις εφαρμογές και τους χρήστες. Αυτές οι υπηρεσίες μπορεί να περιλαμβάνουν υπηρεσίες δικτύου, όπως δρομολόγηση και ασφάλεια, καθώς και εφαρμογές δικτύου και διαχείρισης. Επίσης, το επίπεδο εφαρμογής εφαρμόζει πολιτικές δικτύου που έχουν οριστεί από τους διαχειριστές ή τις εφαρμογές, όπως πολιτικές ασφαλείας και περιορισμούς πρόσβασης. Επιπλέον, επικοινωνεί με τις εφαρμογές ή τους χρήστες για να λάβει πληροφορίες σχετικά με τις απαιτήσεις τους και να προσφέρει τις κατάλληλες υπηρεσίες και λειτουργίες. Συνολικά, το επίπεδο εφαρμογής διασφαλίζει τη συνεργασία του δικτύου SDN με το εξωτερικό περιβάλλον, προσφέροντας λύσεις που εξυπηρετούν τις ανάγκες των εφαρμογών και των χρηστών.

- Το **Northbound Interface** Banse et al (Banse, 2015) αποτελεί ένα σημαντικό στοιχείο στο πλαίσιο της αρχιτεκτονικής του Software Defined Networking (SDN). Αναφέρεται στο επίπεδο επικοινωνίας μεταξύ της εφαρμογής και του επιπέδου ελέγχου (control plane) σε ένα δίκτυο SDN. Το Northbound Interface είναι ένας από τους βασικούς πυλώνες του SDN Latif et al. (Latif , 2020) , καθώς παρέχει αφαίρεση προγραμματισμού για τα δίκτυα. Λειτουργεί ως γέφυρα μεταξύ του επιπέδου ελέγχου και του επιπέδου διαχείρισης και παρέχει υψηλού επιπέδου αφαίρεση για την ανάπτυξη εφαρμογών. Η ανάπτυξη εφαρμογών στο επίπεδο διαχείρισης δεν είναι τόσο εύκολη όσο θα έπρεπε να είναι, και ο κύριος λόγος γι' αυτό είναι η έλλειψη τυποποίησης του Northbound Interface. Το Northbound SDN αναφέρεται στη διεπαφή (Interface) μεταξύ των εφαρμογών ή των χρηστών και του ελεγκτή SDN. Αποτελεί το κομμάτι του SDN που επιτρέπει σε μας, τους χρήστες, να επικοινωνούμε με το δίκτυο και να το διαχειριζόμαστε μέσω εντολών και αιτημάτων. Συνήθως, χρησιμοποιούμε πρωτόκολλα όπως το OpenFlow Raju et al. (Raju , 2018) για να επικοινωνήσουμε με τον ελεγκτή SDN και να επιτελέσουμε διάφορες λειτουργίες στο δίκτυο, όπως δρομολόγηση, παρακολούθηση, και ασφάλεια. Το Northbound SDN μας επιτρέπει να προσαρμόζουμε τη συμπεριφορά του δικτύου σύμφωνα με τις ανάγκες μας

και να δημιουργούμε πολιτικές που ανταποκρίνονται στις απαιτήσεις μας. Μέσω αυτού του μηχανισμού, μπορούμε να δημιουργήσουμε πιο ευέλικτα και δυναμικά δίκτυα που μπορούν να προσαρμοστούν στις αλλαγές στις ανάγκες και τις απαιτήσεις των εφαρμογών ή των χρηστών.

Ορισμένα βασικά σημεία και πληροφορίες σχετικά με το Northbound Interface είναι τα εξής:

- **Επικοινωνία μεταξύ Εφαρμογών και Ελέγχου:** Το Northbound Interface επιτρέπει στις εφαρμογές να επικοινωνούν με τον ελεγκτή SDN και να του δίνουν οδηγίες για τον τρόπο διαχείρισης του δικτύου.
- **Πρωτόκολλα και Διεπαφές:** Το Northbound Interface χρησιμοποιεί διάφορα πρωτόκολλα, όπως το RESTful API, για την ανταλλαγή πληροφοριών μεταξύ των εφαρμογών και του ελεγκτή.
- **Προγραμματισμός του Δικτύου:** Το Northbound Interface επιτρέπει στους διαχειριστές να προγραμματίζουν δυναμικά τη συμπεριφορά του δικτύου με βάση τις ανάγκες των εφαρμογών και των υπηρεσιών.
- **Πολυπλοκότητα της Διασύνδεσης:** Η διασύνδεση Northbound είναι πολυδιάστατη και εξαρτάται από τις ανάγκες και τις λειτουργίες των εφαρμογών. Οι εφαρμογές μπορούν να έχουν διάφορες απαιτήσεις σχετικά με τον τρόπο προγραμματισμού και της αλληλεπίδρασης με το δίκτυο.
- **Σημαντικό Εργαλείο Ανάπτυξης:** Οι προγραμματιστές χρησιμοποιούν το Northbound Interface για να αναπτύξουν εφαρμογές που μπορούν να διαχειριστούν δυναμικά το δίκτυο, να προσθέτουν λειτουργίες, και να βελτιστοποιούν την απόδοση.

Το Northbound Interface είναι κρίσιμο για την ανάπτυξη ευέλικτων και δυναμικών δικτύων, όπου ο έλεγχος του δικτύου γίνεται προγραμματιστικά και προσαρμόζεται σύμφωνα με τις ανάγκες των χρηστών και των εφαρμογών.

- Τα **Southbound APIs** (Application Programming Interfaces) αναφέρονται στις διεπαφές προγραμματισμού που επιτρέπουν στον ελεγκτή SDN να επικοινωνεί με τα διάφορα στοιχεία της υποδομής του δικτύου, όπως διακόπτες, δρομολογητές, και άλλες δικτυακές συσκευές. Το Southbound SDN αναφέρεται στο Interface μεταξύ του ελεγκτή SDN και των φυσικών συσκευών του δικτύου, όπως δρομολογητές (routers), μεταγωγείς (switches) και άλλα δικτυακά στοιχεία. Αυτό το στρώμα είναι υπεύθυνο για την επικοινωνία μεταξύ του ελεγκτή SDN και των φυσικών συσκευών προκειμένου να προγραμματιστούν, να διαχειριστούν και να ελεγχθούν απομακρυσμένα. Το Southbound SDN επιτρέπει στον ελεγκτή να εκδίδει

εντολές στις φυσικές συσκευές του δικτύου με σκοπό την εφαρμογή πολιτικών και διαδικασιών δικτύου. Συνήθως, αυτή η επικοινωνία συμβαίνει μέσω πρωτοκόλλων όπως το OpenFlow, το οποίο επιτρέπει στον ελεγκτή να αποστέλλει οδηγίες (flows) στις φυσικές συσκευές για τη διαχείριση της κίνησης των δεδομένων στο δίκτυο σύμφωνα με τον Ventre et al. (Ventre , 2018) . Μέσω του Southbound SDN, οι φυσικές συσκευές γίνονται πιο ευέλικτες και προσαρμόσιμες, επιτρέποντας στο δίκτυο να ανταποκριθεί πιο αποτελεσματικά στις ανάγκες των εφαρμογών και των χρηστών. Επίσης, το Southbound SDN επιτρέπει την εφαρμογή πολιτικών ασφαλείας, διαχείρισης ποιότητας υπηρεσιών και άλλων λειτουργιών δικτύου με πιο αποτελεσματικό τρόπο.

Ορισμένα κυριότερα σημεία και πληροφορίες σχετικά με τα Southbound APIs είναι τα εξής:

- **Επικοινωνία με τις Δικτυακές Συσκευές:** Τα Southbound APIs επιτρέπουν στον ελεγκτή να επικοινωνεί με τους δικτυακούς κόμβους (όπως διακόπτες, δρομολογητές, ολοκληρωμένα συστήματα) για τον έλεγχο τους και τη διαχείριση της κίνησης στο δίκτυο.
- **Πρωτόκολλα Επικοινωνίας:** Τα Southbound APIs χρησιμοποιούν διάφορα πρωτόκολλα για την ανταλλαγή πληροφοριών και εντολών με τις δικτυακές συσκευές. Ένα από τα κοινότερα πρωτόκολλα είναι το OpenFlow.
- **Οδήγηση της Συμπεριφοράς του Δικτύου:** Μέσω των Southbound APIs, ο ελεγκτής δίνει εντολές στις δικτυακές συσκευές για τον τρόπο με τον οποίο θα πρέπει να διαχειρίζονται την κίνηση, τις πορείες των πακέτων, τον έλεγχο της κίνησης κ.λπ.
- **Προγραμματισμός της Δικτυακής Υποδομής:** Τα Southbound APIs επιτρέπουν στους διαχειριστές να προγραμματίζουν δυναμικά τις ροές κίνησης και να προσαρμόζουν τη συμπεριφορά της υποδομής σύμφωνα με τις ανάγκες του δικτύου.
- **Διαχείριση Δικτύου και Ασφάλεια:** Μέσω των Southbound APIs, μπορεί να γίνει διαχείριση της ασφάλειας του δικτύου, έλεγχος προσβάσεων, αλλαγές στις ροές δεδομένων κ.ά.

Τα Southbound APIs είναι ουσιώδη για την ανάπτυξη και τη διαχείριση ενός δικτύου SDN, καθώς επιτρέπουν την επικοινωνία και τον έλεγχο των δικτυακών συσκευών, επιτρέποντας τη δημιουργία ευέλικτων και διαχειρίσιμων δικτύων.

- Το **επίπεδο ελέγχου** στο δίκτυο SDN λειτουργεί ως κεντρικό σημείο διαχείρισης και ελέγχου του δικτύου. Αναλαμβάνει τον συνολικό έλεγχο της ροής των δεδομένων μέσα στο δίκτυο, λαμβάνοντας αποφάσεις βάσει των οδηγιών που λαμβάνει από τις εφαρμογές και τις πολιτικές δικτύου. Ο ελεγκτής SDN αναλύει την κίνηση στο δίκτυο και προβαίνει σε αποφάσεις για

την κατεύθυνση της ροής των δεδομένων, ρυθμίζοντας τους δρομολογητές και τις διακλαδώσεις του δικτύου. Επιπλέον, αναλαμβάνει να αποφύγει τη συμφόρηση του δικτύου και να ανιχνεύει προβλήματα ή απειλές, παρέχοντας έτσι ασφάλεια και αποτελεσματική λειτουργία. Επιπλέον, εφαρμόζει πολιτικές ασφαλείας που έχουν καθοριστεί από τους διαχειριστές του δικτύου, προστατεύοντας το δίκτυο από πιθανές απειλές και επιθέσεις. Ουσιαστικά, το επίπεδο ελέγχου διασφαλίζει την αποτελεσματική διαχείριση και λειτουργία του δικτύου SDN, προσφέροντας ασφάλεια, ευελιξία και δυνατότητα διαχείρισης των ροών κίνησης.

- Το **επίπεδο δεδομένων** στο δίκτυο SDN αντιπροσωπεύει τη φυσική υποδομή του δικτύου, όπως οι δρομολογητές, οι μεταγωγείς και άλλες δικτυακές συσκευές. Αυτό το επίπεδο είναι υπεύθυνο για τη μεταφορά των πακέτων δεδομένων από την πηγή προς τον προορισμό τους μέσα στο δίκτυο. Συγκεκριμένα, οι δικτυακές συσκευές σε αυτό το επίπεδο είναι υπεύθυνες για τη διαχείριση της φυσικής μετάδοσης των δεδομένων, την επικοινωνία μεταξύ των διαφόρων συσκευών και την εφαρμογή των εντολών ελέγχου που λαμβάνουν από το επίπεδο ελέγχου. Επιπλέον, το επίπεδο δεδομένων είναι υπεύθυνο για τη διαχείριση του φυσικού μέσου επικοινωνίας, όπως του ενσύρματου ή ασύρματου δικτύου, καθώς και της μετάδοσης των πακέτων δεδομένων μέσω της δικτυακής υποδομής. Ουσιαστικά, το επίπεδο δεδομένων αποτελεί την "αφετηρία" όπου ξεκινά η μετάδοση των δεδομένων στο δίκτυο και αποτελεί ένα σημαντικό στοιχείο για την ομαλή λειτουργία του συνολικού συστήματος SDN.

4.1. Πρωτόκολλα SDN Δικτύωσης

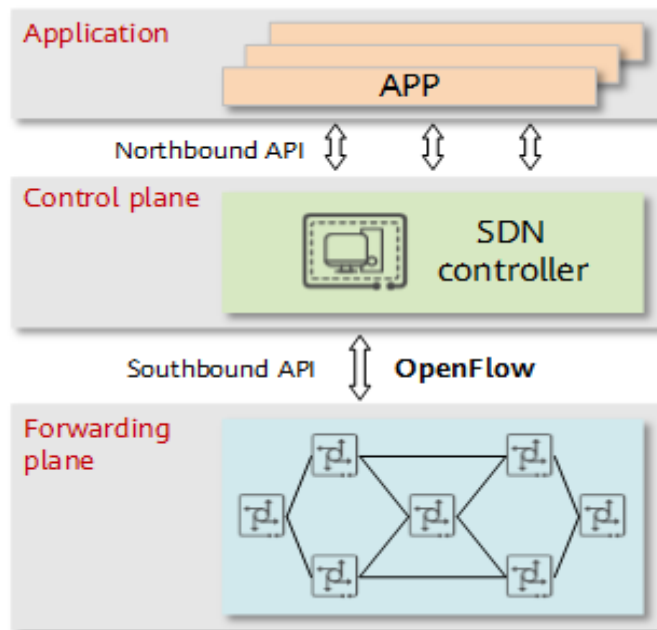
Το πεδίο του λογισμικού ορισμένου δικτύου (Software-Defined Networking - SDN) χρησιμοποιεί διάφορα πρωτόκολλα για την αποδοτική διαχείριση και έλεγχο του δικτύου. Ορισμένα από τα βασικά πρωτόκολλα που χρησιμοποιούνται στο πλαίσιο του SDN περιλαμβάνουν:

- **OpenFlow**: Το OpenFlow είναι το κύριο πρωτόκολλο που χρησιμοποιείται στο SDN. Χρησιμοποιείται για τον έλεγχο του κανονισμού προώθησης των πακέτων σε δρομολογητές και διακόπτες Shalimov et al. (Shalimov ,2013).
- **NETCONF** : (Network Configuration Protocol): Το NETCONF είναι ένα πρωτόκολλο για τη διαχείριση των ρυθμίσεων δικτύου και την διαμόρφωση των συσκευών Enns et al. (Enns , 2006) .
- **YANG** : Το YANG δεν είναι ακριβώς ένα πρωτόκολλο ,αλλά μια γλώσσα μοντελοποίησης δεδομένων για SDN. Χρησιμοποιείται για την περιγραφή των δεδομένων που ανταλλάσσονται μεταξύ του ελεγκτή SDN και των δικτυακών συσκευών, κάνοντας την ανάπτυξη εφαρμογών SDN πιο αποτελεσματική.

- **BGP-SDN** (Border Gateway Protocol - SDN): Αυτό το πρωτόκολλο σχετίζεται με τον έλεγχο της διαδικασίας δρομολόγησης με τη χρήση SDN Kent et al. (Kent ,2000) .
- **OF-CONFIG**: Το OF-CONFIG είναι ένα πρωτόκολλο που χρησιμοποιείται για τη διαμόρφωση και την ενημέρωση των συσκευών OpenFlow Brandt et al. . (Brandt , 2014)

4.1.1 OPENFLOW

Το πρωτόκολλο OpenFlow προήλθε από το Πανεπιστήμιο του Στάνφορντ. Η πρώτη έκδοση του, η 1.0, είδε το φως της δημοσιότητας προς το τέλος του 2009, ενώ η αμέσως επόμενη έκδοση, 1.1, παρουσιάστηκε στις αρχές του 2011. Τον Μάρτιο του 2011, δημιουργήθηκε η Open Networking Foundation (ONF), και τα πνευματικά δικαιώματα του OpenFlow μεταφέρθηκαν σε αυτήν. Η ONF ανέλαβε τον έλεγχο και την εμπορευματοποίηση του OpenFlow. Με αυτόν τον σκοπό, δημοσιεύτηκε η έκδοση OpenFlow v1.3, και το Μάρτιο του 2012, παρουσίασε μια ανοικτή έκδοση λειτουργικότητας σε όλα τα μέλη της ONF. Το OpenFlow Shalimon et al. (Shalimon , 2013) ορίζεται ως ένα πρωτόκολλο επικοινωνίας που παρέχει πρόσβαση στο επίπεδο προώθησης πακέτων δεδομένων σε όλο το δίκτυο η αρχιτεκτονική του οποίου απεικονίζεται στην εικόνα 0-2 . Αποτελεί το μέσο επικοινωνίας μεταξύ ενός διακόπτη ή δρομολογητή και του κεντρικού ελεγκτή του δικτύου. Με την αναγνώριση της αναγκαιότητας σύγχρονων δικτύων για πολλούς φορείς όπως επιχειρήσεις, πανεπιστήμια, ομάδες, και κέντρα διαχείρισης και αποθήκευσης μεγάλου όγκου δεδομένων, η τάση είναι να επιτευχθεί μεγαλύτερη δυναμικότητα μέσω προγραμματιζόμενων εφαρμογών. Ο διαχωρισμός που επιφέρει το OpenFlow μεταξύ του επιπέδου προώθησης πακέτων δεδομένων και του επιπέδου ελέγχου καθιστά το δίκτυο πιο δυναμικό, ευέλικτο και διαχειρίσιμο. Καθιστώντας τον κάθε διακόπτη περισσότερο ελεγχόμενο από τον κεντρικό ελεγκτή, απελευθερώνει τον διακόπτη από τις συγκεκριμένες δομές που του επιβάλλει ο κατασκευαστής και του επιτρέπει να ενσωματωθεί σε διάφορα δίκτυα με διακόπτες διαφορετικών κατασκευαστών , η αρχιτεκτονική του οποίου απεικονίζεται στην εικόνα 0-2.

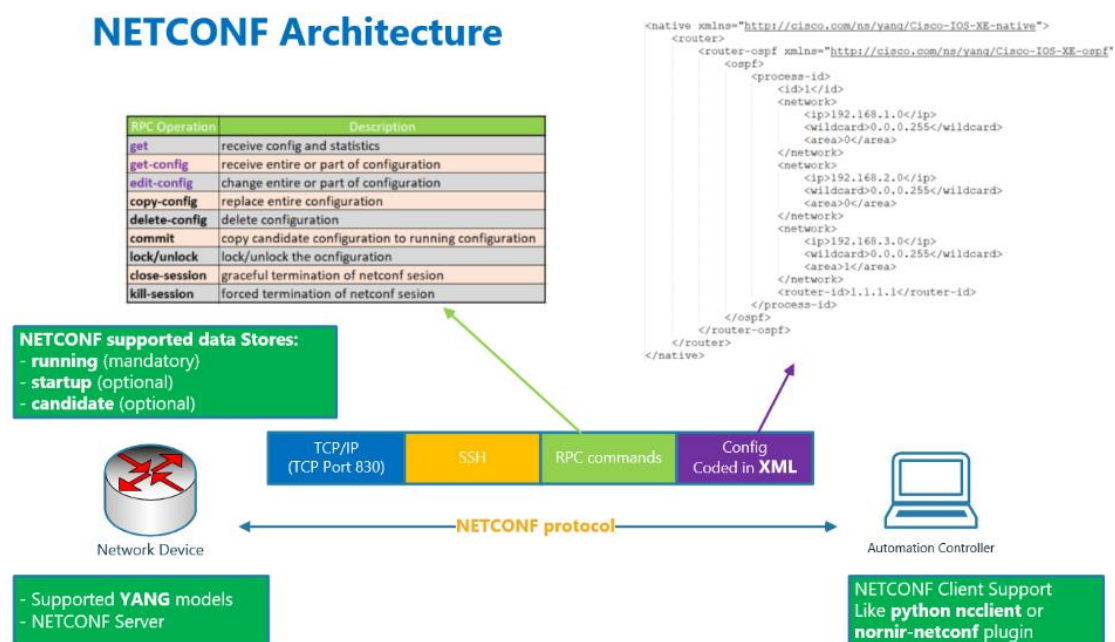


Εικόνα 0-2 Openflow in the SDN Architecture (Πηγή Shalimov, A.2013)

Το πρωτόκολλο OpenFlow επιτρέπει την απομακρυσμένη διαχείριση των πινάκων προώθησης πακέτων σε έναν διακόπτη του επιπέδου 3 Shalimov et al. (Shalimov , 2013) . Αυτό πραγματοποιείται μέσω της προσθήκης, τροποποίησης και άρσης κανόνων και δράσεων που αντιστοιχούν στα πακέτα. Επιτρέπεται, επομένως, στον ελεγκτή να λαμβάνει αποφάσεις δρομολόγησης και να τις μετατρέπει σε κανόνες και δράσεις με ρυθμιζόμενη διάρκεια ζωής. Αυτοί οι κανόνες και δράσεις αναπτύσσονται στον πίνακα ροής του διακόπτη. Τα πακέτα που ταιριάζουν με αυτούς τους κανόνες προωθούνται από τον διακόπτη με την ταχύτητα του φυσικού μέσου ενώ τα αταίριαστα πακέτα προωθούνται αποκλειστικά από τον ελεγκτή. Ο ελεγκτής έχει τη δυνατότητα να τροποποιήσει τους υφιστάμενους κανόνες ενός πίνακα ροής σε έναν ή περισσότερους διακόπτες, ακόμη και να δημιουργήσει νέους, με σκοπό την αποτροπή της διαρθρωτικής ροής της κυκλοφορίας ανάμεσα στον διακόπτη και τον ελεγκτή. Μπορεί ακόμη να αποφασίσει να προωθήσει την ίδια την κυκλοφορία, υπό την προϋπόθεση ότι έχει δώσει εντολή στον διακόπτη να προωθεί ολόκληρα τα πακέτα αντί απλά τις επικεφαλίδες τους.

4.1.2.NETCONF

Το πρωτόκολλο διαμόρφωσης δικτύου (NETCONF) είναι ένα πρωτόκολλο διαχείρισης δικτύου που αναπτύχθηκε και τυποποιήθηκε από την IETF. Αναπτύχθηκε στην ομάδα εργασίας NETCONF και δημοσιεύθηκε τον Δεκέμβριο του 2006 ως RFC 4741 και αργότερα αναθεωρήθηκε τον Ιούνιο του 2011 και δημοσιεύθηκε ως RFC 6241 . Το πρωτόκολλο **NETCONF** (Network Configuration Protocol) Yu et al. (Yu , 2010) αποτελεί ένα σημαντικό στοιχείο των SDN (Software-Defined Networking) δικτύων, επιτρέποντας τη διαχείριση και την διαμόρφωση των δικτύων μέσω λογισμικού. Αν και το NETCONF δεν ανήκει αποκλειστικά στην κατηγορία των SDN, χρησιμοποιείται ευρέως για τη διαμόρφωση και τη διαχείριση των διακοπών στο πλαίσιο της SDN αρχιτεκτονικής. Το πρωτόκολλο NETCONF είναι ένα σημαντικό βήμα προς ένα αυτοματοποιημένο σύστημα διαχείρισης δικτύου , η αρχιτεκτονική του οποίου απεικονίζεται στην εικόνα 0-3. Είναι ένα νέο πρωτόκολλο διαχείρισης που ορίζει λειτουργίες για τη διαχείριση συσκευών δικτύου όπου μπορούν να μεταφορτωθούν δεδομένα διαμόρφωσης ,να ανακτηθούν και να χειριστούν στο σύνολό τους ή εν μέρει. Το NETCONF μπορεί επίσης να χρησιμοποιηθεί για σφάλματα δικτύου .Η αρχιτεκτονική του NETCONF έχει σχεδιαστεί για να διακρίνει μεταξύ των δεδομένων διαμόρφωσης που χρησιμοποιούνται για τον έλεγχο της λειτουργίας μιας συσκευής και των δεδομένων κατάστασης που περιέχουν στατιστικά στοιχεία και κατάσταση της συσκευής. Τα δεδομένα διαμόρφωσης μπορούν να ανακτηθούν με τη λειτουργία <getconfig> και να τροποποιηθούν με τις λειτουργίες <edit-config>, <copy-config> και<delete-config>, ενώ το <get> χρησιμοποιείται για την ανάκτηση των δεδομένων James et al. (James, 2010) .



Εικόνα 0-3 NETCONF Architecture(Πηγή Enns, R. 2006)

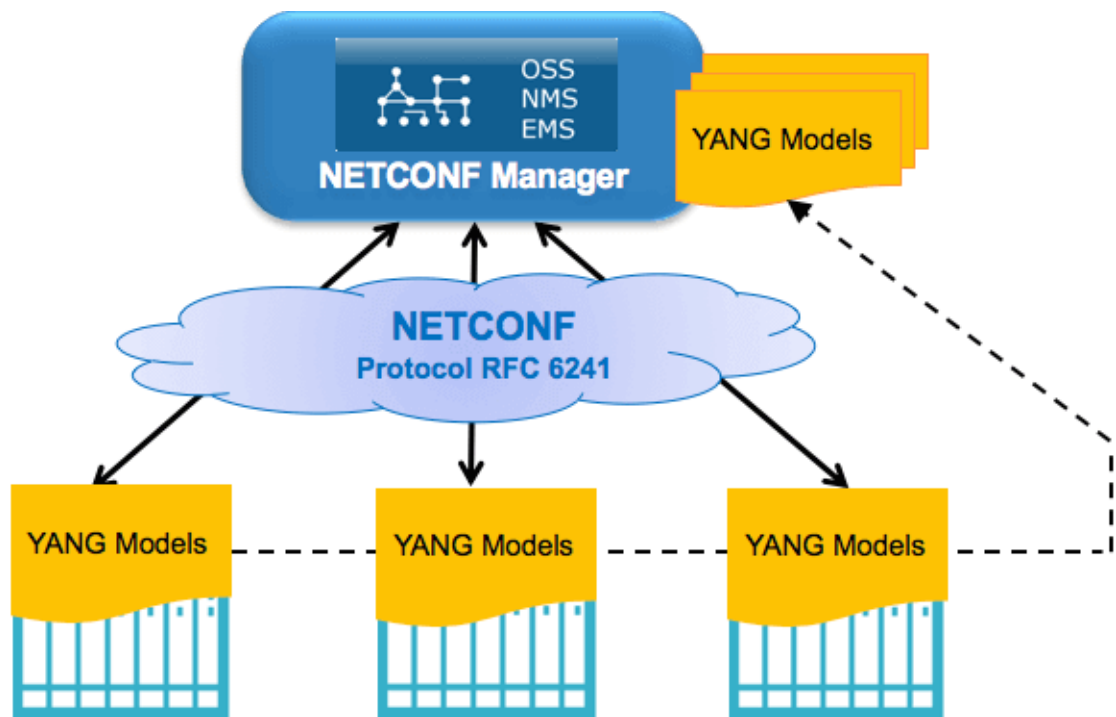
Διαχείριση Ρυθμίσεων Δικτύου: Το NETCONF επιτρέπει την ανάκτηση, την ενημέρωση και την διαμόρφωση των ρυθμίσεων των διακοπών και άλλων δικτυακών συσκευών Enns et al. (Enns, 2006). Ο ελεγκτής μπορεί να επικοινωνεί με τους διακόπτες για να τους διαμορφώσει σύμφωνα με τις απαιτήσεις του δικτύου. Οι διακόπτες δεν χρειάζεται να ρυθμιστούν χειροκίνητα από τους διαχειριστές. Ο κεντρικός ελεγκτής μπορεί να ρυθμίζει δυναμικά τις συσκευές μέσω του NETCONF πρωτοκόλλου.

- **Ατομική Διαχείριση:** Το NETCONF επιτρέπει την ανάκτηση και τη διαμόρφωση επιμέρους ρυθμίσεων και υπηρεσιών, προσφέροντας ακριβή έλεγχο του δικτύου.
- **Ασφάλεια και Αυθεντικοποίηση:** Το πρωτόκολλο παρέχει μηχανισμούς ασφάλειας και αυθεντικοποίησης, εξασφαλίζοντας ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να διαμορφώσουν τις συσκευές.
- **Διαχείριση Σχήματος Δεδομένων:** Το NETCONF επιτρέπει την εύκολη διαχείριση των δεδομένων που αποθηκεύονται στις συσκευές δικτύου. Αυτά τα δεδομένα περιλαμβάνουν τις ρυθμίσεις, τις ροές δεδομένων και άλλες σημαντικές παραμέτρους.

Το πρωτόκολλο NETCONF επιτρέπει στους διαχειριστές να διαχειρίζονται τα δίκτυα με μεγάλη ευελιξία, καθιστώντας το ιδανικό για τη διαχείριση και τη διαμόρφωση των SDN δικτύων.

4.1.3.YANG

Η γλώσσα μοντελοποίησης δεδομένων YANG συντηρείται από την ομάδα εργασίας NETMOD ,της ομάδας εργασίας Internet Engineering Task Force (IETF) και αρχικά δημοσιεύθηκε ως RFC 6020 τον Οκτώβριο του 2010, με μια επικαιροποίηση τον Αύγουστο του 2016 (RFC 7950). Το **YANG** (Yet Another Next Generation) είναι μια γλώσσα μοντελοποίησης δεδομένων που χρησιμοποιείται ευρέως στον τομέα των δικτύων και της τηλεπικοινωνίας για την περιγραφή των δομών δεδομένων που αντιπροσωπεύουν τις ρυθμίσεις, τις υπηρεσίες και την κατάσταση των δικτυακών συσκευών. Το YANG παρέχει έναν τρόπο για τον ορισμό των δεδομένων του δικτύου, Yeung et al. (Yeung ,2020) συμπεριλαμβανομένων των παραμέτρων ρύθμισης, των υπηρεσιών και της κατάστασης του δικτύου. Επίσης, ορίζει τον τρόπο που τα δεδομένα αυτά μπορούν να μεταφερθούν και να διαχειριστούν σε ένα περιβάλλον SDN. Ένα από τα κύρια πλεονεκτήματα του YANG είναι η δυνατότητά του να παρέχει μια τυπική, ομαλή και εύκολα κατανοητή μορφή για την ανταλλαγή δεδομένων μεταξύ του ελεγκτή SDN και των δικτυακών συσκευών. Αυτό καθιστά πιο εύκολο τον προγραμματισμό, τη διαχείριση και την αυτοματοποίηση των δικτύων σε ένα περιβάλλον SDN. Το YANG παρέχει ένα πολύτιμο εργαλείο για την ανάπτυξη και τη διαχείριση ευέλικτων, επεκτάσιμων και αυτοματοποιημένων δικτύων στο πλαίσιο της τεχνολογίας SDN , όπως απεικονίζεται στην εικόνα 0-4 .



Εικόνα 0- 4 Yang (Πηγή Yeung ,2020)

- **Απλότητα και Ευαναγνωσιμότητα:** Ο σχεδιασμός του YANG έχει ως στόχο την απλότητα και την ευαναγνωσιμότητα των μοντέλων δεδομένων, προκειμένου να διευκολυνθεί η κατανόηση από τους ανθρώπους.
- **Ανεξαρτησία από την Πλατφόρμα:** Το YANG επιτρέπει την περιγραφή των δεδομένων χωρίς να εξαρτώνται από τις λεπτομέρειες της πλατφόρμας, παρέχοντας ένα ανεξάρτητο πλαίσιο μοντελοποίησης.
- **Επαναχρησιμοποίηση και Επέκταση:** Το YANG δίνει τη δυνατότητα για την επαναχρησιμοποίηση των ορισμών μοντέλων και την επέκτάσή τους για να ανταποκρίνονται σε νέες απαιτήσεις.
- **Προσαρμοστικότητα σε Εφαρμογές:** Το YANG σχεδιάστηκε για να είναι προσαρμοστικό σε διάφορες εφαρμογές, όπως η διαμόρφωση, ο έλεγχος, η διαχείριση και η παρακολούθηση των δικτυακών συσκευών.
- **Αυτοεξυπηρέτηση και Ορισμός των Υπηρεσιών:** Το YANG επιτρέπει την αυτοεξυπηρέτηση και τον καθορισμό των υπηρεσιών σε διάφορες πλατφόρμες.

Τα μοντέλα YANG περιγράφουν τις δομές δεδομένων ως διαφορετικούς τύπους δεδομένων και τις σχέσεις μεταξύ τους. Χρησιμοποιούνται σε πολλά πρωτόκολλα και τεχνολογίες, συμπεριλαμβανομένων των πρωτοκόλλων δικτύου, όπως το NETCONF, RESTCONF και άλλα, για την περιγραφή των δικτυακών υπηρεσιών, των παραμέτρων ρύθμισης και της κατάστασης των δικτυακών συσκευών.

4.1.4.BGP-SDN (Border Gateway Protocol).

Το BGP-SDN (Border Gateway Protocol - Software Defined Networking) περιγράφηκε για πρώτη φορά το 1989 στο RFC 1105 και χρησιμοποιείται στο Διαδίκτυο από το 1994. Το IPv6 BGP ορίστηκε για πρώτη φορά στο RFC 1654 το 1994 και βελτιώθηκε στο RFC 2283 το 1998 , αποτελεί μια συνδυαστική προσέγγιση που συνδυάζει το πρωτόκολλο δρομολόγησης BGP με την τεχνολογία Software Defined Networking (SDN). Το πρωτόκολλο BGP , το οποίο χρησιμοποιείται για τη διανομή πληροφοριών δρομολόγησης μεταξύ αυτόνομων συστημάτων, είναι ένα κρίσιμο στοιχείο της υποδομής δρομολόγησης του Διαδικτύου. Είναι ιδιαίτερα ευάλωτο σε διάφορες κακόβουλες επιθέσεις, λόγω της έλλειψης ενός ασφαλούς μέσου επαλήθευσης της αυθεντικότητας και της νομιμότητας της κίνησης ελέγχου BGP et al. Kent (Kent , 2000) .

Το BGP είναι ένα πρωτόκολλο δρομολόγησης που χρησιμοποιείται σε μεγάλη κλίμακα στο Διαδίκτυο Huston et al. (Huston,2006) . Χρησιμοποιείται για τη δρομολόγηση μεταξύ αυτονόητων συστημάτων (AS), τα οποία μπορούν να αντιστοιχούν σε ολόκληρους παροχείς υπηρεσιών Διαδικτύου ή μεγάλες επιχειρήσεις. Η λειτουργία του BGP είναι κρίσιμη για τη σταθερότητα και την αποδοτικότητα του Διαδικτύου, καθώς επηρεάζει το πώς τα δεδομένα πρέπει να προηγούνται μεταξύ διαφορετικών τμημάτων του δικτύου. Το BGP (Border Gateway Protocol) αποτελεί ένα από τα κύρια πρωτόκολλα δρομολόγησης στο Διαδίκτυο. Χρησιμοποιείται για την ανταλλαγή πληροφοριών δρομολόγησης μεταξύ διαφορετικών δικτύων, τα οποία ανήκουν σε διαφορετικά αυτόνομα συστήματα (AS). Τα AS είναι δίκτυα που διαχειρίζονται από μία μόνο οντότητα ή εταιρεία, και το BGP επιτρέπει την ανταλλαγή πληροφοριών μεταξύ αυτών των AS για να ληφθούν αποφάσεις δρομολόγησης.

Το BGP χαρακτηρίζεται από την πολυπλοκότητά του και το γεγονός ότι λαμβάνει αποφάσεις δρομολόγησης βασιζόμενο σε πολλούς παράγοντες, όπως η ποιότητα της διαδρομής, η διαθεσιμότητα του δικτύου και οι πολιτικές δρομολόγησης που έχουν οριστεί από τον διαχειριστή του δικτύου McPherson et al. (McPherson , 2002). Μέσω του BGP, οι διαχειριστές δικτύου μπορούν να ελέγχουν πώς τα δεδομένα κυκλοφορούν στο Διαδίκτυο και να λαμβάνουν αποφάσεις που εξυπηρετούν τις ανάγκες και τις προτιμήσεις τους. Ένας σημαντικός ρόλος του BGP είναι και η διαχείριση της διαφυγής εναλλακτικών διαδρομών. Σε περίπτωση που μια

διαδρομή γίνει μη διαθέσιμη, το BGP μπορεί να προσαρμόσει το δίκτυο ώστε να χρησιμοποιήσει μια εναλλακτική διαδρομή για να διατηρήσει τη συνδεσιμότητα. Συνολικά, το BGP αποτελεί ένα ουσιώδες στοιχείο της υποδομής του Διαδικτύου, παρέχοντας τη δυνατότητα ανταλλαγής πληροφοριών δρομολόγησης και τη δυνατότητα ελέγχου της διακίνησης των δεδομένων σε παγκόσμιο επίπεδο. Στην εικόνα 0-5 απεικονίζεται το αυτόνομο σύστημα BGP.



Εικόνα 0-5 BGP Autonomous System (Πηγή Huston, G. 2006)

4.1.5.OF-CONFIG

Το **OF-CONFIG** (OpenFlow Configuration and Management Protocol) είναι ένα πρωτόκολλο που χρησιμοποιείται στο πλαίσιο του οικοσυστήματος του Software Defined Networking (SDN) , Brandt et al. (Brandt , 2014) . Σκοπός του είναι η διαμόρφωση και διαχείριση των συσκευών που υποστηρίζουν το OpenFlow πρωτόκολλο. Το OF Config Protocol (OpenFlow Configuration Protocol) αποτελεί ένα κρίσιμο στοιχείο στο πλαίσιο των δικτύων SDN (Software-Defined Networking), που ανοίγει τον δρόμο για τη διαχείριση και τον έλεγχο των μεταγωγέων και άλλων δικτυακών συσκευών μέσω του πρωτοκόλλου OpenFlow. Το OF Config Protocol επιτρέπει στον ελεγκτή SDN να αλλάξει δυναμικά τις ρυθμίσεις των μεταγωγέων, προσφέροντας έτσι ευελιξία και έλεγχο στο δίκτυο. Μέσω του OF Config Protocol, ο ελεγκτής μπορεί να προγραμματίσει τη λειτουργία των μεταγωγέων σύμφωνα με τις ανάγκες και τις προτιμήσεις του δικτύου. Μπορεί να διαμορφώσει τους πίνακες δρομολόγησης, τους πίνακες αναμετάδοσης και άλλες ρυθμίσεις λειτουργίας των μεταγωγέων, εξασφαλίζοντας έτσι την αποτελεσματική διαχείριση της κίνησης των δεδομένων στο δίκτυο.

Η δυνατότητα διαχείρισης των ρυθμίσεων των μεταγωγέων μέσω του OF Config Protocol παρέχει στο δίκτυο μεγαλύτερη ευελιξία και απόκριση στις ανάγκες του, επιτρέποντας την προσαρμογή της λειτουργίας του δικτύου σε πραγματικό χρόνο McKeown et al.(McKeown , 2008) .Αυτό επιτρέπει την αντιμετώπιση διαφόρων

σεναρίων και την επίτευξη βέλτιστης απόδοσης και αξιοπιστίας του δικτύου. Με συνοπτικά λόγια, το OF Config Protocol συμβάλλει στη δημιουργία ευέλικτων και αυτοματοποιημένων δικτύων SDN.

Ορισμένα βασικά χαρακτηριστικά και σημαντικά σημεία σχετικά με το OF-CONFIG:

- **Διαχείριση Συσκευών SDN:** Το OF-CONFIG προορίζεται για τη διαχείριση συσκευών που λειτουργούν με το OpenFlow πρωτόκολλο. Αυτές οι συσκευές περιλαμβάνουν διακόπτες, δρομολογητές και άλλες εξοπλιστικές συσκευές που ανήκουν στην υποδομή SDN.
- **Διαμόρφωση και Παραμετροποίηση:** Το OF-CONFIG επιτρέπει την διαμόρφωση και παραμετροποίηση των συσκευών SDN. Αυτό μπορεί να περιλαμβάνει τον ορισμό κανόνων ροής των χαρακτηριστικών QoS (Quality of Service), των λειτουργιών ελέγχου, και άλλων παραμέτρων που αφορούν τη λειτουργία του δικτύου.
- **Επικοινωνία μεταξύ Ελεγκτή και Συσκευής:** Ο ελεγκτής SDN επικοινωνεί με τις συσκευές SDN μέσω του OF-CONFIG προκειμένου να προβεί σε διαμορφώσεις και ενημερώσεις σχετικά με τη λειτουργία τους.
- **Συμβατότητα με το OpenFlow:** Το OF-CONFIG σχεδιάστηκε για να συνδυάζεται με το OpenFlow. Αυτή η συμβατότητα επιτρέπει την ομαλή λειτουργία και διαχείριση του SDN οικοσυστήματος.

Συνολικά, το OF-CONFIG παίζει ένα σημαντικό ρόλο στην αποδοτική διαχείριση των συσκευών που υποστηρίζουν το OpenFlow, βοηθώντας έτσι στην διαμόρφωση, την αναβάθμιση και τον έλεγχο του SDN.

5. Ο ρόλος των ελεγκτών Ανοικτού και Κλειστού Λογισμικού.

Η έννοια των ελεγκτών ανοικτού και κλειστού λογισμικού στο πλαίσιο των δικτύων ξεκίνησε από ακαδημαϊκές και βιομηχανικές έρευνες στον τομέα των λογισμικών οριοθετημένων δικτύων (SDN). Μια από τις πρώτες και κυριότερες πρωτοβουλίες ήταν η ανάπτυξη του πρωτοκόλλου OpenFlow από το πανεπιστήμιο του Stanford το 2008. Οι καθηγητές Nick McKeown, Scott Shenker, Martin Casado και οι φοιτητές τους είχαν την πρωτοποριακή ιδέα να αποσυνδέσουν την επεξεργασία

των πακέτων δεδομένων (data plane) από την πολιτική δρομολόγησης και τη λήψη αποφάσεων (control plane), δημιουργώντας έτσι το SDN.

Στη συνέχεια, η ιδέα αυτή εξελίχθηκε και ενισχύθηκε από τη δημιουργία της Open Networking Foundation (ONF) το 2011, η οποία προωθεί την ανάπτυξη και την υιοθέτηση του SDN και του πρωτοκόλλου OpenFlow. Η ONF συγκέντρωσε πολλές εταιρείες του χώρου των τηλεπικοινωνιών και του δικτύου για να συνεργαστούν για την προώθηση της τεχνολογίας αυτής. Οι ελεγκτές σε ένα δίκτυο λειτουργούν ως το "εγκέφαλο" του συστήματος λογισμικού ορισμένου από την τεχνολογία SDN (Software-Defined Networking) , Salman et al. (Salman, 2016) .Αυτοί αναλαμβάνουν τον έλεγχο και τη διαχείριση των συσκευών δικτύου, όπως διακόπτες και δρομολογητές, μέσω μιας κεντρικής πλατφόρμας. Ας αναλύσουμε τον ρόλο τους σε σχέση με το ανοικτό και κλειστό λογισμικό:

Ελεγκτές ανοικτού λογισμικού (Open Source Controllers):

Οι ελεγκτές ανοικτού λογισμικού είναι ελεγκτές SDN οι οποίοι βασίζονται σε ανοικτό κώδικα. Το γεγονός ότι είναι ανοικτού λογισμικού τους επιτρέπει να προσαρμόζονται, να επεκτείνονται και να προσαρμόζονται στις ανάγκες του χρήστη. Μπορούν να προσφέρουν πλεονεκτήματα όπως ευελιξία, κοινότητα υποστήριξης, και δυνατότητα ανάπτυξης προσαρμοσμένων λύσεων , Shalimov et al .(Shalimov , 2013)

Ελεγκτές κλειστού λογισμικού (Closed Source Controllers):

Οι ελεγκτές κλειστού λογισμικού είναι ελεγκτές που βασίζονται σε κλειστό λογισμικό, όπου ο πηγαίος κώδικας δεν είναι προσβάσιμος στο κοινό. Αυτοί οι ελεγκτές προσφέρουν συνήθως εγγυημένη σταθερότητα, υψηλή ασφάλεια, και υποστήριξη από τον προμηθευτή. Ωστόσο, η περιορισμένη πρόσβαση στον πηγαίο κώδικα μπορεί να περιορίσει την προσαρμοστικότητα και την επεκτασιμότητα Ebeid et al .(Ebeid , 2018)

Σε κάθε περίπτωση, οι ελεγκτές αναλαμβάνουν τον συντονισμό των δικτυακών συσκευών, λαμβάνοντας αποφάσεις για τη δρομολόγηση των πακέτων, την ασφάλεια, την ποιότητα της υπηρεσίας και άλλες λειτουργίες του δικτύου βάση της κατάστασης του δικτύου και των πολιτικών που έχουν καθοριστεί. Οι ελεγκτές σε SDN δίκτυα, είτε ανήκουν στην κατηγορία του ανοικτού λογισμικού είτε στην κατηγορία του κλειστού λογισμικού, έχουν κοινό ρόλο στη λειτουργία του δικτύου και τη διαχείριση της επικοινωνίας. Ανεξάρτητα από την κατηγορία, οι ελεγκτές εκτελούν τις παρακάτω βασικές λειτουργίες:

- **Προγραμματισμός και Διαχείριση Ροών Δεδομένων:** Οι ελεγκτές αναλαμβάνουν τον προγραμματισμό και τον έλεγχο των ροών δεδομένων με

βάση τις ανάγκες του δικτύου. Αυτό επιτρέπει τη δυναμική αλλαγή της κατανομής των δεδομένων στο δίκτυο.

- **Διαχείριση Τοπολογίας:** Οι ελεγκτές παρέχουν ολοκληρωμένη άποψη της φυσικής τοπολογίας του δικτύου. Αυτό βοηθά στην εφαρμογή αλγορίθμων και πολιτικών για τη βελτιστοποίηση της επικοινωνίας.
- **Διαχείριση και Έλεγχος Ροών Επικοινωνίας:** Οι ελεγκτές διαχειρίζονται τη ροή των επικοινωνιακών δεδομένων, ελέγχοντας ποιες διαδρομές ακολουθούν και ποιος εξυπηρετητής θα χρησιμοποιηθεί για κάθε επικοινωνία.
- **Διαχείριση Πολιτικών και Ασφάλειας:** Οι ελεγκτές υποστηρίζουν την εφαρμογή και τη διαχείριση πολιτικών ασφαλείας στο δίκτυο. Αυτό εξασφαλίζει την προστασία του δικτύου από απειλές και παράνομες εισβολές.
- **Προγραμματισμός Δικτύου:** Οι ελεγκτές επιτρέπουν τον προγραμματισμό του δικτύου και των υπηρεσιών του μέσω λογισμικού, δίνοντας τη δυνατότητα δημιουργίας εξατομικευμένων λύσεων.
- **Εφαρμογή Επιπέδων Λογισμικού:** Οι ελεγκτές στρώνουν το λογισμικό επιπέδων στο δίκτυο, δημιουργώντας ένα περιβάλλον προσαρμοσμένο στις ανάγκες των εφαρμογών.
- **Διαχείριση Πόρων:** Οι ελεγκτές διαχειρίζονται τη χρήση πόρων, όπως εύρος ζώνης και επεξεργαστική ισχύ, με σκοπό τη βελτιστοποίηση της απόδοσης του δικτύου.

Ο ρόλος αυτός των ελεγκτών είναι κοινός για τους διάφορους ελεγκτές, ανεξάρτητα από το αν ανήκουν στην κατηγορία του ανοικτού ή του κλειστού λογισμικού.

5.1. Οι πιο διαδεδομένοι Ελεγκτές Ανοικτού κώδικα στον χώρο του SDN

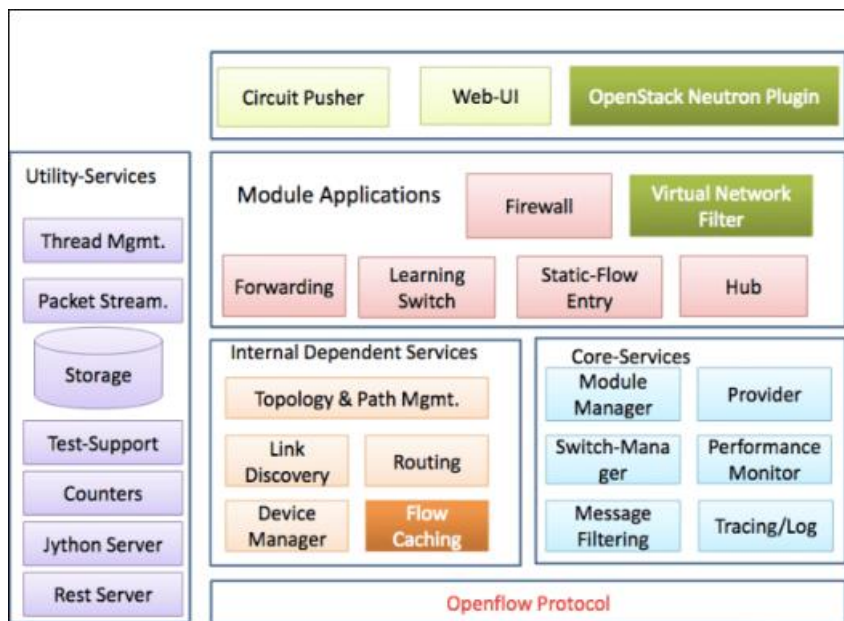
5.1.1. Floodlight

Ο Floodlight βασίζεται στον ελεγκτή Beacon από το Πανεπιστήμιο του Στάνφορντ και λειτουργεί με φυσικούς και εικονικούς μεταγωγείς OpenFlow είναι ένα από τα δημοφιλέστερα έργα λογισμικού στον κόσμο των ελεγκτών SDN Rowshanrad et al. (Rowshanrad , 2016). Επιτρέπει τη διαχείριση και τον έλεγχο των δικτύων, εκμεταλλευόμενος το πρότυπο OpenFlow για να αντιμετωπίσει διάφορες λειτουργικές ανάγκες. Ο ελεγκτής Floodlight έχει σχεδιαστεί ως σύστημα με έντονα ταυτόχρονη λειτουργία για επίτευξη της απόδοσης που απαιτείται από πολλαπλά κέντρα δεδομένων και δίκτυα επιχειρηματικής κλάσης. Δεδομένου ότι, το OpenFlow καθορίζει τα πρωτόκολλα μέσω ενός μεταγωγέα με δυνατότητα OpenFlow, ένας ελεγκτής που ενεργοποιείται εξ αποστάσεως μπορεί να τροποποιήσει τη

συμπεριφορά των βασικών συσκευών δικτύωσης μέσω ενός καλά καθορισμένου συνόλου εντολών προώθησης δεδομένων. Ο ελεγκτής Floodlight έχει σχεδιαστεί για να λειτουργεί με διαφορετικούς μεταγωγείς, δρομολογητές, σημεία πρόσβασης κ.λπ. που υποστηρίζουν τα πρότυπα OpenFlow. Ο ελεγκτής Floodlight θα μπορούσε επίσης να υποστηρίξει υβριδικά δίκτυα Idris et al. (Idris, 2017). Ορισμένα από τα κύρια χαρακτηριστικά του του ελεγκτή Floodlight παρατίθενται ως εξής:

- Προσφέρει ένα σύστημα φόρτωσης μονάδων που καθιστά απλή την επέκταση και τη βελτίωσή του.
- Είναι πολύ εύκολο να εγκατασταθεί με ελάχιστες εξαρτήσεις.
- Υποστηρίζει ένα ευρύ φάσμα φυσικών και εικονικών μεταγωγέων με δυνατότητα OpenFlow.
- Μπορεί επίσης να χειριστεί ένα δίκτυο υβριδικού περιβάλλοντος, το οποίο με τη σειρά του μπορεί να διαχειριστεί πολλαπλά τμήματα μεταγωγέων υλικού OpenFlow.

Επιπλέον, το Floodlight υποστηρίζει εικονικούς switches, διευκολύνοντας την ανάπτυξη και τη δοκιμή των πειραμάτων όσες φορές χρειάζεται σε ένα εικονικό περιβάλλον Morales et al. (Morales, 2015). Ένα από τα πλεονεκτήματα του Floodlight είναι η δυνατότητά του να λειτουργεί ως κεντρικό σημείο ελέγχου για να διαχειρίζεται τη ροή των πακέτων στο δίκτυο, καθιστώντας δυνατή τη διαμόρφωση της ροής των δεδομένων και τη διαχείριση του δικτύου σύμφωνα με τις ανάγκες της εφαρμογής ή του χρήστη. Μέσω της ευελιξίας του ανοιχτού κώδικα, ο Floodlight αποτελεί επίσης εργαλείο για τη δημιουργία καινοτόμων λύσεων στον τομέα των δικτύων, επιτρέποντας την εξέλιξη και την προσαρμογή του σε νέες τεχνολογικές ανάγκες και απαιτήσεις. Η εσωτερική αρχιτεκτονική του Floodlight ελεγκτή και των εφαρμογών που είναι διαθέσιμες, παρουσιάζεται στην εικόνα 0-6.

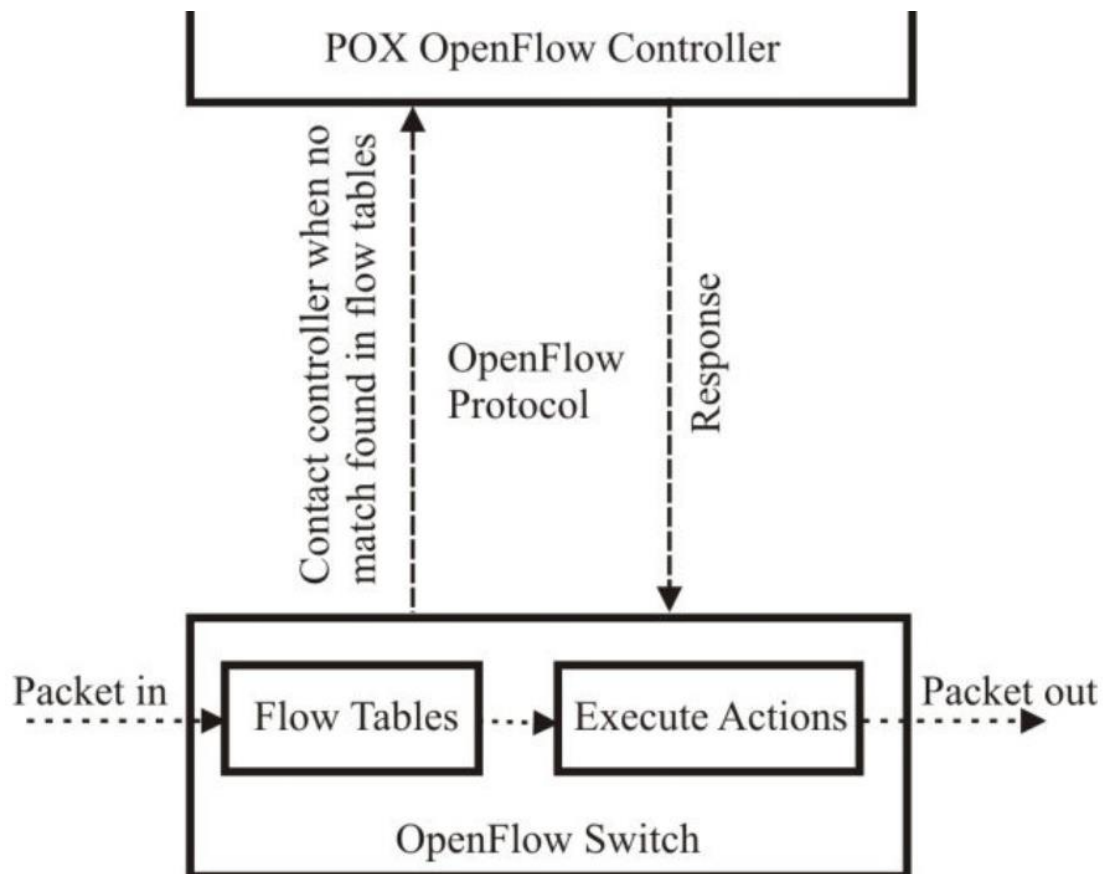


Εικόνα 0-6 Floodlight (Πηγή Bholebawa 2018)

5.1.2. POX

Ο ελεγκτής POX Ali et al. (Ali, 2018) αποτελεί ένα εύχρηστο και ευέλικτο εργαλείο στον χώρο του λογισμικού ορισμένου δικτύου (SDN). Το κυριότερο πλεονέκτημά του είναι η ευκολία χρήσης λόγω της Python, μιας προσιτής και ευέλικτης γλώσσας προγραμματισμού. Αυτό το χαρακτηριστικό τον καθιστά ιδανικό για προγραμματιστές ή ακόμη και για αρχάριους που θέλουν να αναπτύξουν τις ικανότητές τους στον τομέα των SDN.

Ένα ακόμη σημαντικό πλεονέκτημα είναι η ευελιξία και η ποικιλία λειτουργιών που παρέχει. Ο POX παρέχει ένα ευρύ φάσμα εργαλείων προγραμματισμού, επιτρέποντας στους χρήστες να προσαρμόσουν και να προγραμματίσουν τον ελεγκτή σύμφωνα με τις ανάγκες τους. Αυτό του επιτρέπει να προσφέρει προσαρμοσμένες λύσεις για διάφορα προβλήματα δικτύων. Επιπλέον, ο POX είναι ιδανικός για πειραματισμό και ανάπτυξη εφαρμογών SDN. Η ικανότητά του να προσφέρει προσαρμοσμένες λύσεις στον χώρο των δικτύων, σε συνδυασμό με την ευχρηστία και την ευελιξία της Python, τον καθιστούν ένα αξιόπιστο εργαλείο για προγραμματιστές και ερευνητές που εξερευνούν τον κόσμο των SDN. Στην εικόνα 0-7 απεικονίζεται η αρχιτεκτονική του POX OpenFlow .



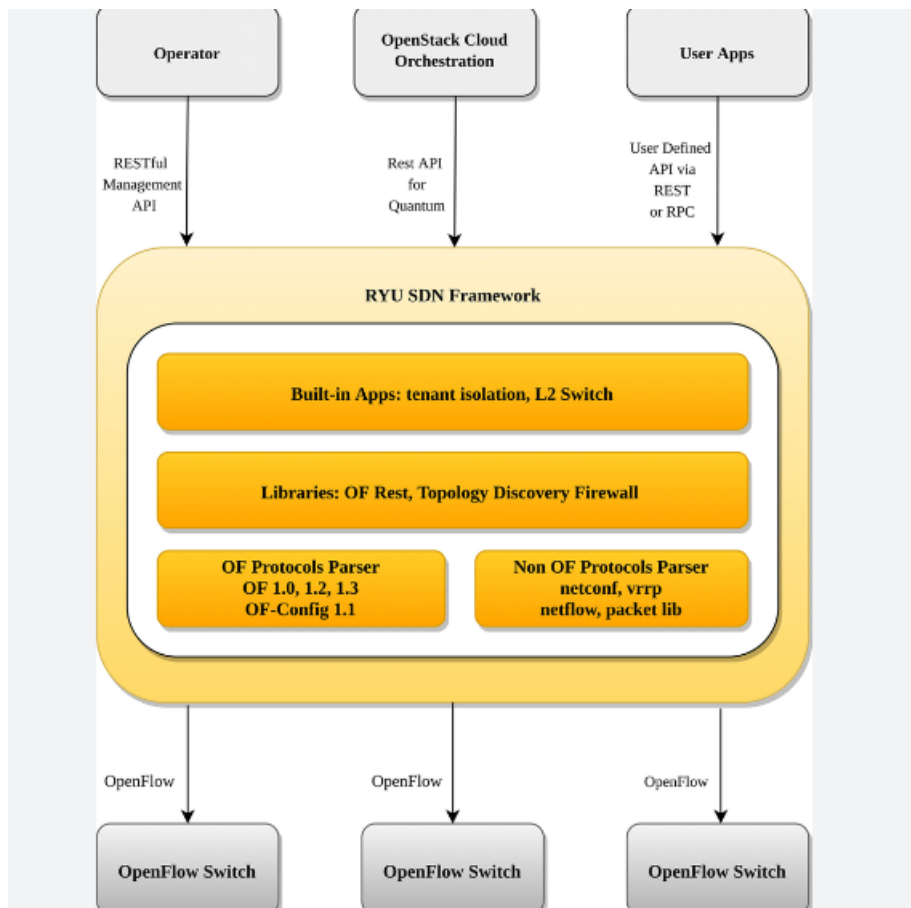
Εικόνα 0-7 POX Architecture (Πηγή Rani 2019)

Ο ελεγκτής POX (Python OpenFlow eXperimental) αντιπροσωπεύει μια ευέλικτη και εξαιρετικά προσαρμόσιμη λύση στον κόσμο των ελεγκτών λογισμικού ορισμένου δικτύου (SDN), Kaur et al. (Kaur , 2014). Γραμμένος σε Python, προσφέρει μια ευέλικτη πλατφόρμα που επιτρέπει στους χρήστες να δημιουργήσουν προσαρμοσμένες λύσεις SDN. Με τη χρήση βιβλιοθηκών Python, ο POX παρέχει ένα περιβάλλον προγραμματισμού που είναι φιλικό προς τον χρήστη και επιτρέπει την ανάπτυξη ελεγκτών που προσαρμόζονται στις ανάγκες του κάθε δικτύου. Με τη δυνατότητά του να αλληλεπιδρά με πρωτόκολλα όπως το OpenFlow και να διαχειρίζεται την επικοινωνία μεταξύ των συσκευών δικτύου, ο POX επιτρέπει στους προγραμματιστές να δημιουργήσουν προσαρμοσμένες λύσεις που εξυπηρετούν συγκεκριμένες απαιτήσεις δικτύων και εφαρμογές SDN. Οι δυνατότητες του POX τον καθιστούν ένα πολύτιμο εργαλείο για τη δημιουργία επιτυχημένων και εξατομικευμένων λύσεων SDN.

5.1.3. Ryu

Ο ελεγκτής Ryu (Md. Tariqul Islam, Node to Node Performance Evaluation through RYU SDN Controller, 2020) αποτελεί ένα ανοικτού κώδικα εργαλείο λογισμικού ορισμένου δικτύου (SDN), ο οποίος έχει ευρεία αποδοτικότητα και ευελιξία στην ανάπτυξη εφαρμογών δικτύων. Γράφεται σε Python και παρέχει ένα εύκολο στη χρήση πλαίσιο προγραμματισμού για τη δημιουργία λογισμικού ελέγχου δικτύων. Η αρχιτεκτονική του Ryu στηρίζεται στην επέκταση του πρωτοκόλλου OpenFlow όπως απεικονίζεται στην εικόνα 0-8, το οποίο επιτρέπει στους προγραμματιστές να δημιουργήσουν εφαρμογές SDN που ελέγχουν και διαχειρίζονται το δίκτυο. Ένα από τα κύρια πλεονεκτήματα του Ryu είναι η ευελιξία του στην προσθήκη προσαρμοσμένων λειτουργιών και συμπεριφορών στο δίκτυο, ανάλογα με τις απαιτήσεις της συγκεκριμένης εφαρμογής ή του περιβάλλοντος δικτύου.

Ο Ryu προσφέρει πολλές δυνατότητες για τη δημιουργία προσαρμοσμένων εφαρμογών SDN, ενώ παρέχει ένα ευέλικτο περιβάλλον ανάπτυξης και δοκιμής για νέες ιδέες στον χώρο της επικοινωνίας και δικτύων Askar et al. (Askar , 2021). Ο ελεγκτής Ryu ανήκει στην κατηγορία των ελεγκτών λογισμικού ορισμένου δικτύου (SDN controllers) και αποτελεί έναν πολύτιμο πόρο για την ανάπτυξη προηγμένων εφαρμογών SDN. Η βασική του λειτουργία είναι η παροχή ενός περιβάλλοντος ανάπτυξης που επιτρέπει στους προγραμματιστές να αλληλεπιδρούν με το δίκτυο μέσω του πρωτοκόλλου OpenFlow Md. et al.(Md. 2020) . Ένα από τα κύρια πλεονεκτήματα του ελεγκτή Ryu είναι η ευελιξία του επιτρέπει την εύκολη και γρήγορη ανάπτυξη νέων εφαρμογών .Επίσης, υποστηρίζεται από μια ενεργή κοινότητα που συνεχώς αναπτύσσει νέες λειτουργίες και βελτιώσεις.



Εικόνα 0-8 RYU (Πηγή Md, 2020)

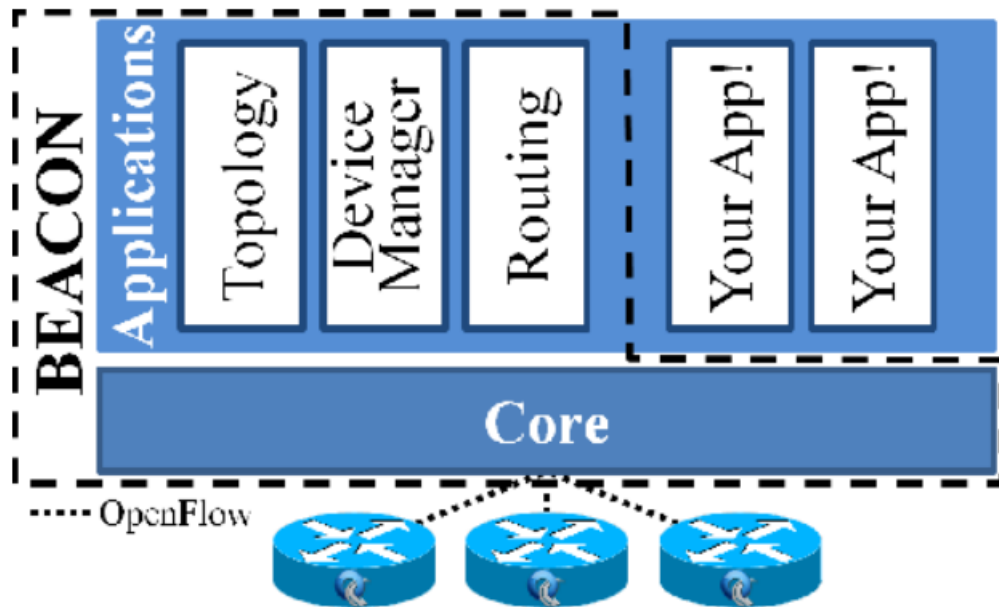
Οι κύριες χαρακτηριστικές πτυχές του RYU περιλαμβάνουν:

- **Ευελιξία και Προσαρμοστικότητα:** Ο RYU προσφέρει ένα ευέλικτο περιβάλλον προγραμματισμού που επιτρέπει την εύκολη δημιουργία και επέκταση εφαρμογών SDN. Οι προγραμματιστές μπορούν να προσαρμόσουν τον ελεγκτή σύμφωνα με τις ανάγκες τους.
- **Υποστήριξη Πολλαπλών Πρωτοκόλλων:** Ο RYU υποστηρίζει διάφορα πρωτόκολλα επικοινωνίας, όπως το OpenFlow, που είναι ένα από τα βασικά πρωτόκολλα του SDN.
- **Κοινότητα και Υποστήριξη:** Είναι ένα έργο ανοικτού κώδικα με μια ενεργή κοινότητα προγραμματιστών, προσφέροντας υποστήριξη και ανάπτυξη με νέες ενημερώσεις και βελτιώσεις.
- **Επιδόσεις:** Ο RYU σχεδιάστηκε να είναι αποδοτικός και να παρέχει υψηλές επιδόσεις για τις εφαρμογές SDN.
- **Ενσωματωμένες Βιβλιοθήκες και Παραδείγματα:** Ο RYU διαθέτει ενσωματωμένες βιβλιοθήκες και παραδείγματα που βοηθούν στην κατανόηση της ανάπτυξης εφαρμογών SDN.

5.1.4. Beacon

Ο ελεγκτής Beacon αναπτύχθηκε από το Πανεπιστήμιο της Στάνφορντ και αποτέλεσε έναν από τους πρώτους ελεγκτές SDN που δημιουργήθηκαν. Ο σχεδιασμός του επικεντρώθηκε στη δημιουργία ενός ευέλικτου ελεγκτή που μπορεί να διαχειριστεί αποτελεσματικά δίκτυα που υποστηρίζουν το πρωτόκολλο OpenFlow. Η κύρια του αρχή ήταν η απλότητα και η ευκολία χρήσης, επιτρέποντας στους χρήστες να δημιουργούν εφαρμογές SDN με αξιοπιστία και ευελιξία. Η δομή του είναι σχεδιασμένη για να παρέχει μια βασική λειτουργικότητα ελέγχου δικτύου OpenFlow, Erickson et al. (Erickson, 2013), ενώ παραμένει ανοικτός στην επέκταση και την προσαρμογή. Ο στόχος του Beacon είναι να προσφέρει έναν ελεγκτή που είναι ευέλικτος και εύκολος στη χρήση, επιτρέποντας σε προγραμματιστές και διαχειριστές δικτύων να δημιουργήσουν και να διαχειριστούν δίκτυα SDN χωρίς υπερβολική πολυπλοκότητα. Η ευελιξία του ελεγκτή Beacon δίνει τη δυνατότητα στους χρήστες να αξιοποιήσουν τις δυνατότητες του SDN σε διάφορες πτυχές της διαχείρισης δικτύων. Μέσω του ελεγκτή Beacon, οι χρήστες μπορούν να αναπτύξουν προσαρμοσμένες εφαρμογές SDN που προσαρμόζονται στις συγκεκριμένες ανάγκες τους, επιτρέποντάς τους να προσαρμόσουν και να αυτοματοποιήσουν τη λειτουργία του δικτύου τους. Επιπλέον, ο ελεγκτής Beacon προσφέρει πλούσιες δυνατότητες για την υλοποίηση διαφόρων αλγορίθμων δρομολόγησης και διαχείρισης της ροής δεδομένων, ενισχύοντας την απόδοση και την ασφάλεια του δικτύου. Με την αξιοποίηση του ελεγκτή Beacon, οι χρήστες έχουν τη δυνατότητα να επεκτείνουν τις γνώσεις τους στον τομέα των δικτύων SDN και να προωθήσουν την έρευνα και την καινοτομία στον εν λόγω τομέα.

Παρότι ο Beacon αποτελεί έναν από τους πρώτους ελεγκτές SDN, η συνεχής ανάπτυξη και οι αλλαγές στις απαιτήσεις δικτύων εξασφαλίζουν ότι συνεχίζει να εξελίσσεται για να ανταποκριθεί στις σύγχρονες ανάγκες δικτύων, Manuel et al. (Manuel, 2019). Στην εικόνα που 0-9 απεικονίζεται η αρχιτεκτονική του Beacon.



Εικόνα 0-9 Beacon (Πηγή Erickson 2013)

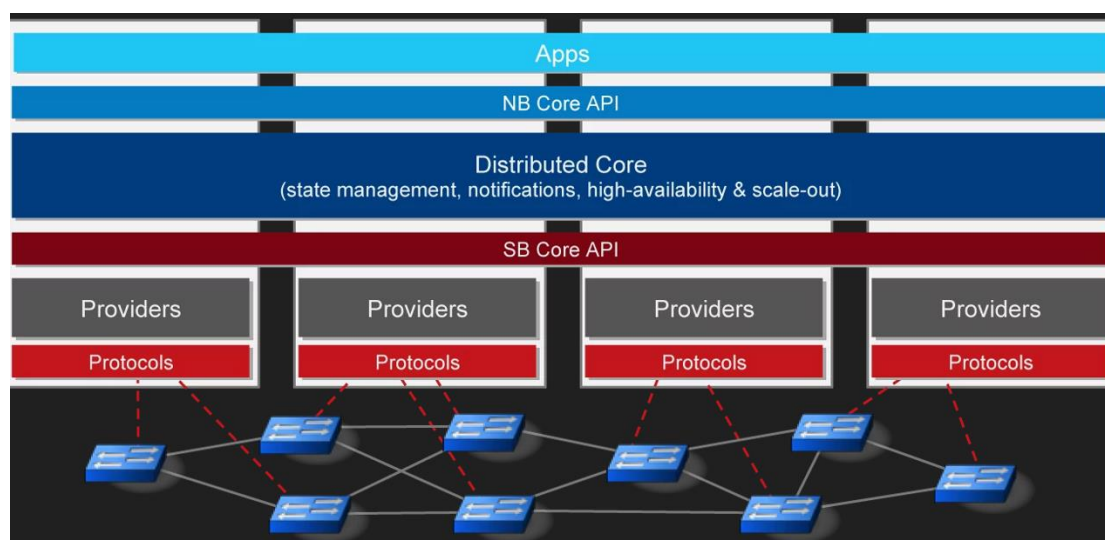
5.1.5. ONOS

Το ONOS (Open Network Operating System) είναι ένας ελεγκτής SDN ανοικτού κώδικα που αναπτύχθηκε αρχικά από το ερευνητικό εργαστήριο ON.Lab και αργότερα ανέλαβε την υποστήριξή του το Open Networking Foundation (ONF). Ο κύριος στόχος του ONOS είναι η δημιουργία ενός ελεγκτή SDN που να είναι κλιμακούμενος, αξιόπιστος και ευέλικτος για τη διαχείριση μεγάλων δικτύων. Έχει σχεδιαστεί για να παρέχει δυνατότητες ολοκληρωμένης διαχείρισης και ελέγχου για δίκτυα SDN, Sheikh et al. (Sheikh, 2019). Ο ελεγκτής ONOS (Open Network Operating System) αναπτύχθηκε με στόχο να παρέχει μια πλατφόρμα διαχείρισης δικτύων SDN που να είναι ανοιχτή, ευέλικτη και επεκτάσιμη. Εκτός από την ανάπτυξη εφαρμογών SDN, ο ONOS εστιάζει στη δημιουργία ενός αξιόπιστου και αποδοτικού λογισμικού για τη διαχείριση και τον έλεγχο πολύπλοκων δικτύων.

Ο ελεγκτής ONOS υποστηρίζει πολλές λειτουργίες υψηλής επίδοσης, συμπεριλαμβανομένης της διαχείρισης της ροής της κίνησης, της δρομολόγησης και της επίβλεψης του δικτύου. Το σύστημα χρησιμοποιεί ένα κατανεμημένο μοντέλο αρχιτεκτονικής για να διασφαλίσει την αποτελεσματική διαχείριση των πόρων του δικτύου και την αντιμετώπιση των προκλήσεων που προκύπτουν από την ανάπτυξη μεγάλης κλίμακας δικτύων. Επιπλέον, ο ελεγκτής ONOS παρέχει υποστήριξη για διάφορα πρότυπα και πρωτόκολλα, όπως το OpenFlow, το P4 και το NETCONF, επιτρέποντας την ενσωμάτωση σε διαφορετικές τεχνολογίες δικτύων Zinner et al

Zinner , 2017).Με αυτόν τον τρόπο, ο ελεγκτής ONOS συνδυάζει την ευελιξία και την αποδοτικότητα για να παρέχει ένα αξιόπιστο περιβάλλον διαχείρισης δικτύων SDN.

Έχει μια ευέλικτη αρχιτεκτονική όπως απεικονίζεται στην εικόνα 0-10 , η οποία του επιτρέπει να επεκταθεί και να προσαρμοστεί για να υποστηρίξει διάφορες εφαρμογές και περιβάλλοντα δικτύων. Έχει προσανατολιστεί στην υποστήριξη των σύγχρονων απαιτήσεων δικτύων, όπως η επιτάχυνση του Internet, τα έξυπνα δίκτυα, τα δίκτυα 5G και η διαχείριση μεγάλου όγκου δεδομένων. Έχει ευρεία χρήση σε διάφορους τομείς, όπως στις τηλεπικοινωνίες, τα κέντρα δεδομένων, τις smart cities και τις επιχειρήσεις, παρέχοντας ένα πλούσιο οικοσύστημα λογισμικού για την ανάπτυξη και τη διαχείριση σύγχρονων δικτύων SDN. Η ανοιχτή του φύση τον καθιστά ελκυστική επιλογή για ερευνητές, αναπτυσσόμενες εταιρείες και κοινότητες που θέλουν να υιοθετήσουν SDN σε διάφορους τομείς.



Εικόνα 0-10 Onos (Πηγή Mohammed Sammer 2018)

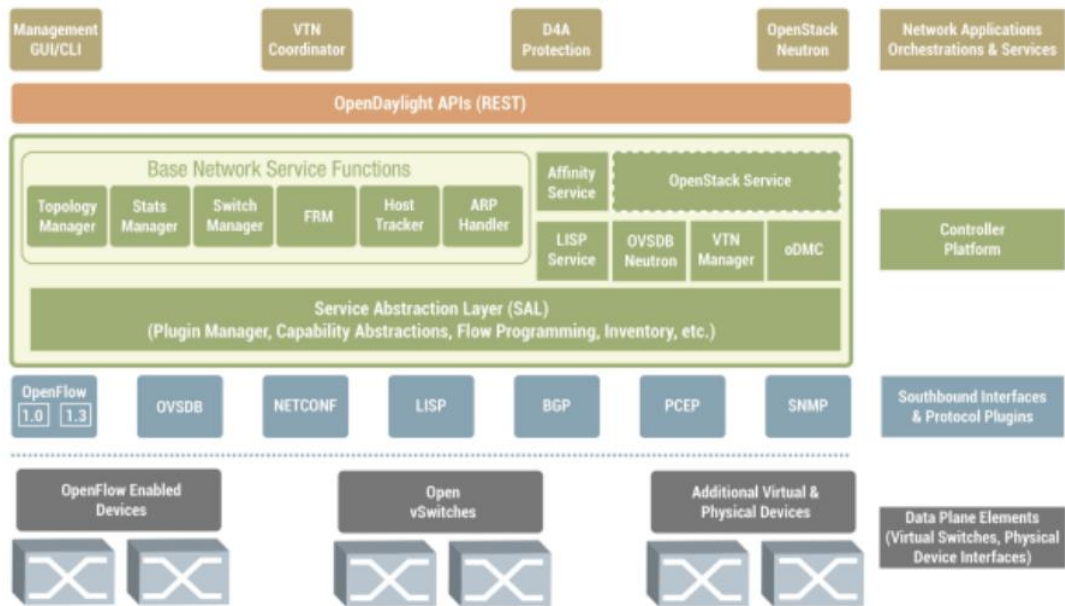
5.1.6. OpenDaylight

Το OpenDaylight (ODL) Badotra et al. (Badotra , 2017) αποτελεί έναν ελεγκτή SDN ανοικτού κώδικα που έχει αναπτυχθεί με τη συνεργασία πολλών εταιρειών, ερευνητικών οργανισμών και μελών της κοινότητας του ανοικτού λογισμικού. Το ODL προσφέρει ένα πλήρες σετ λειτουργιών για τη διαχείριση και τον έλεγχο δικτύων SDN. Η αρχιτεκτονική του ODL είναι βασισμένη σε ένα modifiable framework που επιτρέπει την επέκταση και την προσαρμογή των λειτουργιών του σε διάφορα περιβάλλοντα δικτύων. Χρησιμοποιείται ευρέως σε εφαρμογές που αφορούν την εικονικοποίηση λειτουργιών δικτύου, τις τηλεπικοινωνίες, τα κέντρα δεδομένων και τις υπηρεσίες cloud.

Το ODL παρέχει μια ευρεία γκάμα λειτουργιών , Khan et al. (Khan ,2010), συμπεριλαμβανομένων των δυνατοτήτων διαχείρισης δικτύου, ελέγχου της ροής

δεδομένων, εικονικοποίησης δικτύου και υπηρεσιών QoS. Έχει ανοιχτή αρχιτεκτονική, επιτρέποντας την ενσωμάτωση διαφορετικών προτύπων και λειτουργιών επικοινωνίας, κάτι που το καθιστά εύκολο να προσαρμοστεί σε διαφορετικές ανάγκες δικτύων και εφαρμογών. Επιπλέον, διαθέτει μια ενεργή κοινότητα που συνεισφέρει στην συνεχή βελτίωση και επέκτασή του.

Βασίζοντας στις τεχνολογίες που προτείνονται από τους Garcia και τους συνεργάτες τους (2015), το OpenDaylight (ODL) χρησιμοποιεί ένα συνδυασμό εργαλείων και γλωσσών προγραμματισμού για τη διευκόλυνση της ανάπτυξης και της λειτουργίας του. Το ODL εκμεταλλεύεται το Maven για την απλοποίηση των εξαρτήσεων του έργου και την αυτοματοποίηση των απαιτούμενων plugins, παρέχοντας στους προγραμματιστές τη δυνατότητα να διαχειρίζονται τα αρχικά πρότυπα του έργου. Η ανάπτυξη σε Java προσφέρει αξιόπιστη ασφάλεια και επιτρέπει την εύκολη υλοποίηση συγκεκριμένων υπηρεσιών. Επιπλέον, το OpenDaylight εκμεταλλεύεται το Open Service Gateway Interface (OSGi) ως βασικό συστατικό, δίνοντας τη δυνατότητα δυναμικής φόρτωσης δεσμών και πακέτων JAR (που συνθέτουν τις εφαρμογές) και τη σύνδεση μονάδων για την ανταλλαγή πληροφοριών. Επιπλέον, το ODL βασίζεται στο Karaf, μια πλατφόρμα εφαρμογών που βασίζεται στο OSGi, που απλοποιεί τη διαδικασία εγκατάστασης των εφαρμογών. Το ODL επιλέγει την YANG ως βασική τεχνολογία για την προσδιορισμό της συμπεριφοράς του ελεγκτή. Οι προγραμματιστές χρησιμοποιούν το YANG για τη μοντελοποίηση των λειτουργιών της εφαρμογής και τη δημιουργία APIs από τα μοντέλα αυτά, προκειμένου να υλοποιήσουν αργότερα τις λειτουργίες αυτές. Η τεχνολογία YANG υποστηρίζει τη μοντελοποίηση λειτουργικών και διαμορφώσιμων δεδομένων, καθώς και τη δημιουργία RPC και notifications. Στην εικόνα παρακάτω βλέπουμε την αρχιτεκτονική του OpenDaylight.



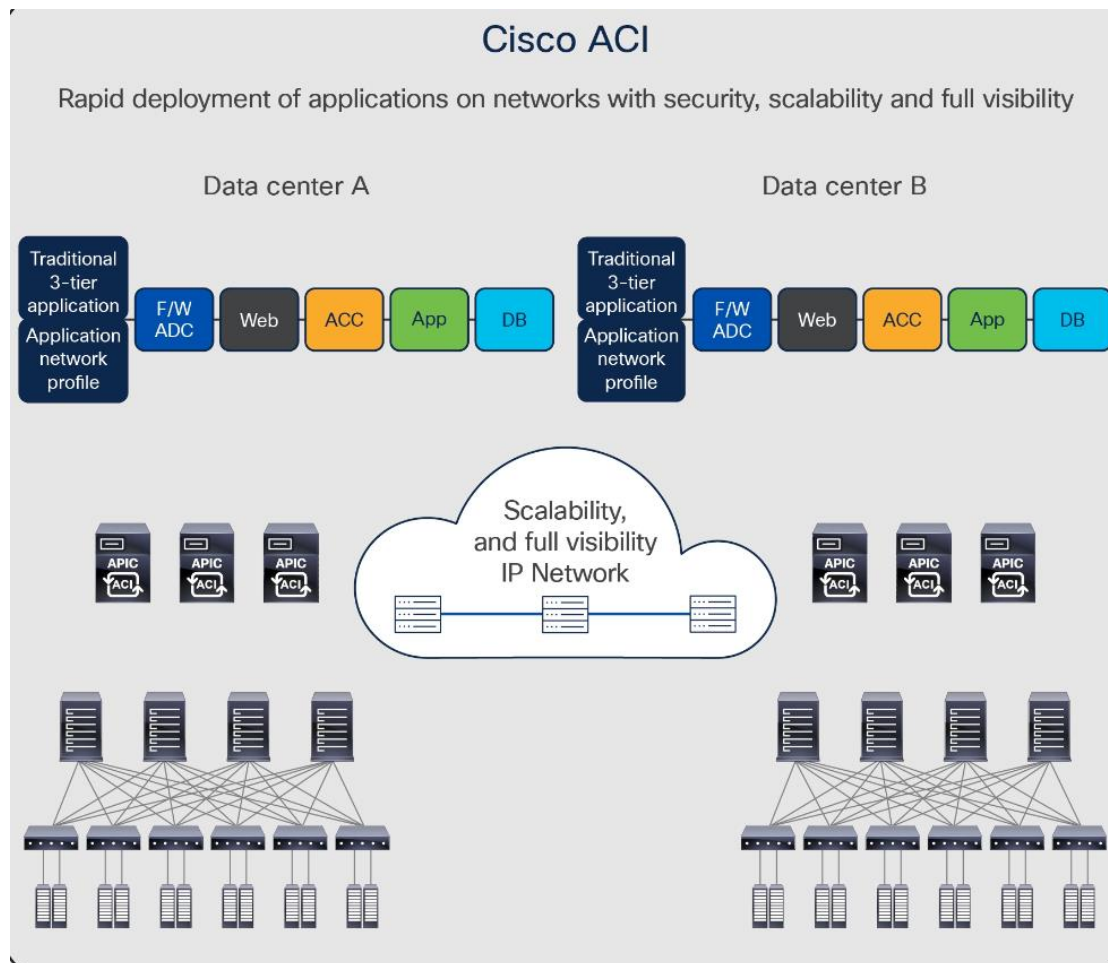
Εικόνα 0-11 OpenDaylight SDN Controller Architecture (Πηγή Muhammad Awais)

5.2. Οι πιο διαδεδομένοι Ελεγκτές Κλειστού κώδικα

5.2.1. Cisco Application Policy Infrastructure Controller

Το Cisco Application Policy Infrastructure Controller (APIC) είναι ένας ελεγκτής SDN που αναπτύχθηκε από την Cisco για τη διαχείριση σύγχρονων κέντρων δεδομένων, Gheorghe et al. (Gheorghe, 2017). Αυτός ο ελεγκτής προσφέρει μια ολοκληρωμένη πλατφόρμα διαχείρισης που επιτρέπει την ομαλή διαχείριση και παρακολούθηση των δικτύων SDN. Έχει μια πλούσια σουίτα εργαλείων για την παρακολούθηση των επιδόσεων του δικτύου, τη διαχείριση πολλαπλών συσκευών, και την εφαρμογή πολιτικών και κανόνων σε όλο το δίκτυο. Ο APIC επιτρέπει την εύκολη προσθήκη και απομάκρυνση συσκευών, την ολοκληρωμένη διαχείριση των ρυθμίσεων δικτύου, και την εφαρμογή διαφορετικών επιπέδων ασφάλειας. Ο APIC συνδέει τα επίπεδα εφαρμογών με τα φυσικά δίκτυα, επιτρέποντας στους διαχειριστές να δημιουργούν πολιτικές και να εφαρμόζουν αλλαγές στο δίκτυο μέσω ενός κεντρικού σημείου ελέγχου. Αυτός ο ελεγκτής προσφέρει επίσης εύκολες δυνατότητες επέκτασης και προσαρμογής στις ανάγκες ενός πολύπλοκου δικτύου. Με τη χρήση του APIC, οι διαχειριστές μπορούν να ολοκληρώσουν τη διαχείριση και

τον έλεγχο ενός μεγάλου δικτύου μέσα από μια ολοκληρωμένη και ενιαία πλατφόρμα . Η αρχιτεκτονική του Cisco ACI απεικονίζεται στη παρακάτω εικόνα 0-12.



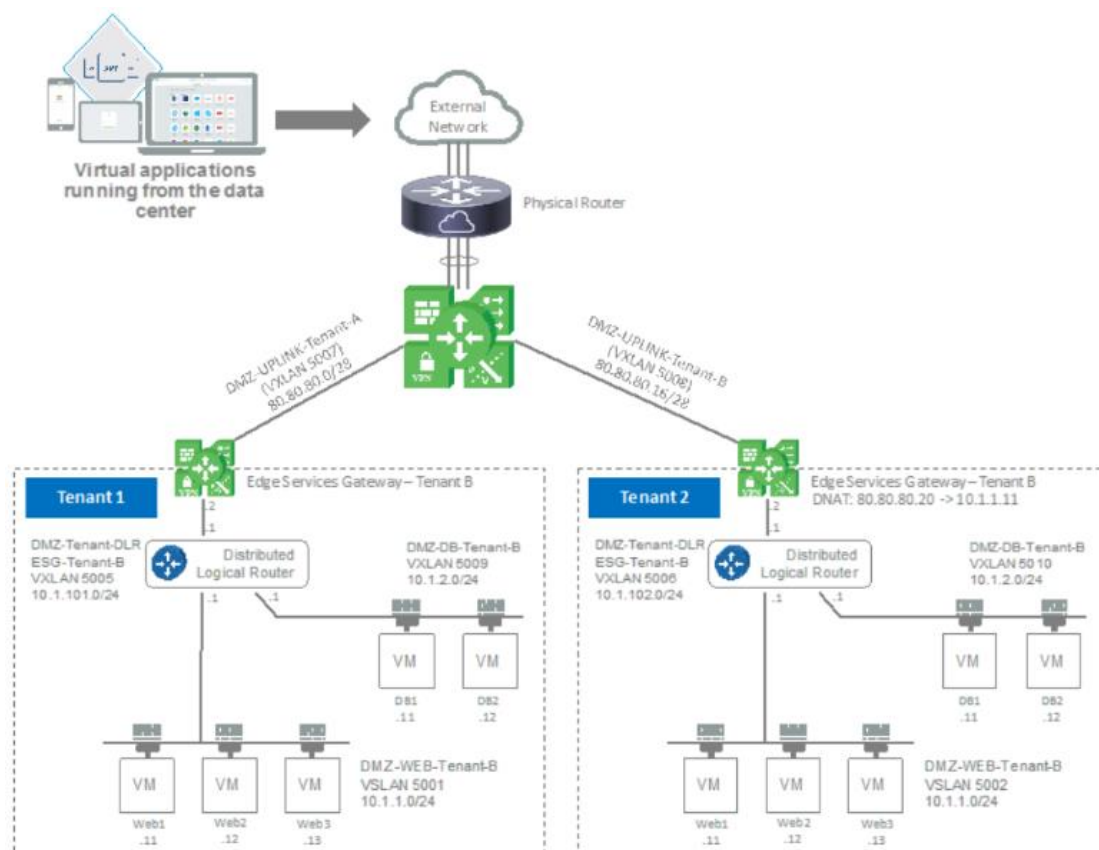
Εικόνα 0-12 Cisco ACI Architecture (Πηγή Cisco.com)

5.2.2.VMware NSX

Η πλατφόρμα VMware NSX αντιπροσωπεύει μια σημαντική εξέλιξη στον τομέα των δικτύων και της απεικόνισης Takasuo et al. (Takasuo, 2018). Αναπτυγμένη από την εταιρεία VMware, η NSX προέκυψε από την εξαγορά της Nicira το 2012, μιας startup εταιρείας που είχε αναπτύξει μια πρωτοποριακή τεχνολογία για το Software-Defined Networking (SDN). Το VMware NSX είναι μια πλατφόρμα απεικόνισης δικτύου που παρέχει λύσεις για το λογισμικό ορισμένου δικτύου (SDN) και την απεικόνιση του δικτύου λογισμικού ορισμένων λειτουργιών. Αποτελεί ένα σημαντικό εργαλείο στον χώρο της απεικόνισης δικτύου και των λύσεων ορισμένου δικτύου λογισμικού (SDN).

Το NSX Ammour et al. (Ammour , 2023), επιτρέπει τη δημιουργία εικονικών δικτύων στο επίπεδο του λογισμικού, ανεξάρτητα από την υποκείμενη υποδομή. Με το NSX, οι διαχειριστές μπορούν να δημιουργήσουν και να διαχειριστούν εικονικά δίκτυα, να εφαρμόσουν πολιτικές ασφαλείας και να παρέχουν προχωρημένες υπηρεσίες δικτύου, όπως δρομολόγηση, φόρτωση ισορροπίας φορτίου και προστασία από επιθέσεις, μέσω λογισμικού, ανεξάρτητα από τη φυσική υποδομή. Στην εικόνα 0-13 απεικονίζεται η αρχιτεκτονική του NSX. Ένα από τα βασικά χαρακτηριστικά του NSX είναι η δυνατότητα δημιουργίας ενός ενιαίου εικονικού δικτύου που εκτείνεται από το δεδομένο κέντρο δεδομένων μέχρι τον cloud και τα άκρα του δικτύου. Αυτό επιτρέπει στις επιχειρήσεις να δημιουργήσουν μια ευέλικτη, ασφαλή και ενοποιημένη υποδομή δικτύου που μπορεί να υποστηρίξει τις ανάγκες της ψηφιακής μετασχηματισμένης εποχής. Επιτρέπει τη δημιουργία ενός εικονικού δικτύου πάνω από υπάρχοντα υποδομές, ανεξάρτητα από το πού βρίσκονται οι φυσικοί πόροι. Αυτό το επιτυγχάνει με τη χρήση εικονικών μηχανών (VMs) για την αναπαράσταση της υποδομής του δικτύου και των λειτουργιών του, επιτρέποντας τη διαχείριση και τον έλεγχο του δικτύου μέσω λογισμικού. Η πλατφόρμα εστιάζει στην απλοποίηση των διαδικασιών ανάπτυξης, διαχείρισης και προστασίας του δικτύου .

Με το VMware NSX, οι διαχειριστές μπορούν να δημιουργήσουν εικονικά δίκτυα και να εφαρμόσουν πολιτικές ασφαλείας και άλλες ρυθμίσεις σε επίπεδο εφαρμογής, Abdullah et al. (Abdullah , 2018). Αυτό επιτρέπει ευελιξία στη διαχείριση του δικτύου, αυξάνοντας την ασφάλεια και την αποτελεσματικότητα της δικτύωσης σε ένα περιβάλλον εικονικού δικτύου. Το NSX αποτελεί ένα από τα ευρέως αποδεκτά εργαλεία για την επέκταση και την ενίσχυση της λειτουργικότητας του SDN σε επιχειρησιακό επίπεδο.

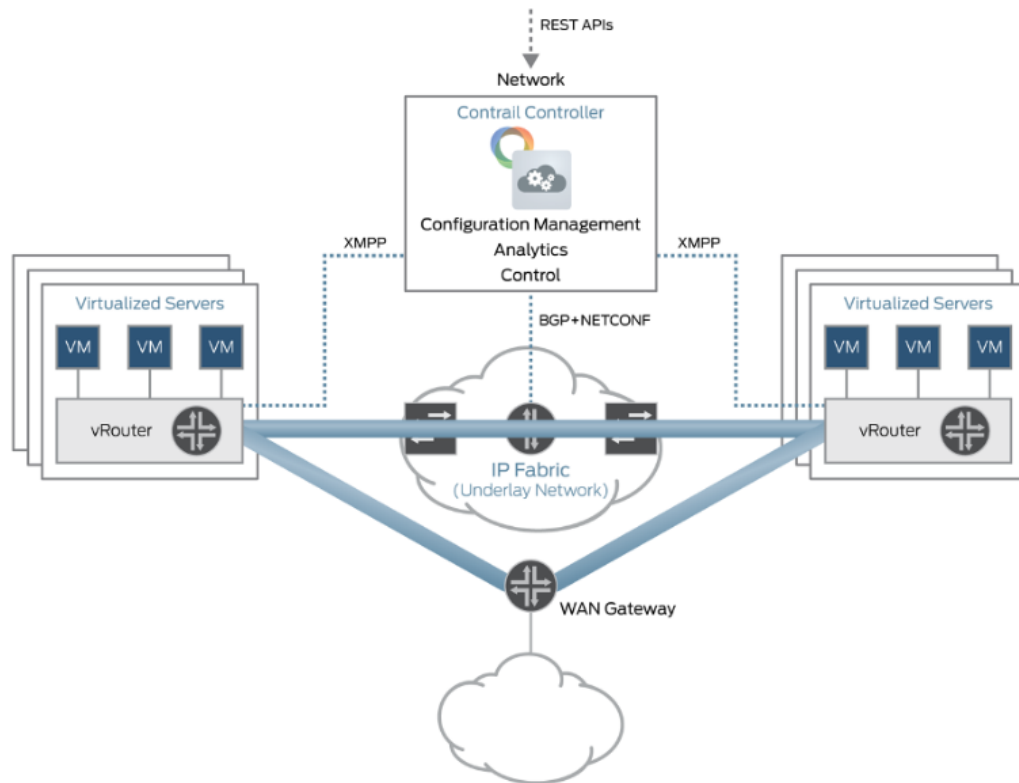


Εικόνα 0-13 VMware NSX Architecture(et al. Ammour M., 2023)

5.2.3. Juniper Contrail SDN

Το Juniper Contrail SDN Controller ανακοινώθηκε από την Juniper Networks τον Ιούνιο του 2013, Ελεγκτής SDN της Juniper, με εφαρμογή και έλεγχο δυναμικής διαμόρφωσης και βελτιστοποίησης από άκρη σε άκρη για οποιαδήποτε υποδομή cloud. Τα σημεία που ξεχωρίζουν είναι η εκτενής τεκμηρίωσή του, η ευρεία υποστήριξη τόσο σε SBI όσο και σε NBI, η ενσωμάτωση με τις περισσότερες υπηρεσίες cloud, όπως η υπηρεσία Contrail Cloud, καθώς και τα Kubernetes, Openshift και Mesos. Υποστηρίζει επίσης Network Functions Virtualization, Μια προδιαγραφή υλικού με τετραπύρρηνο επεξεργαστή x86 2.2ghz, 12gb RAM, 2 tb HDD πληροί τις ελάχιστες προδιαγραφές Neto et al.(Neto , 2021).Είναι μια πλατφόρμα λογισμικού που παρέχει λύσεις για τη διαχείριση και τον έλεγχο ενός δικτύου ορισμένου με λογισμικό (SDN). Κατασκευάζεται για να ενισχύσει την ευελιξία, την ασφάλεια και τη διαχείριση των δικτύων. Ο ελεγκτής αυτός βασίζεται σε ένα ολοκληρωμένο περιβάλλον που χρησιμοποιεί το ονομαστικό σύστημα ελέγχου Contrail της Juniper Networks. Αποτελεί ένα κεντρικό σημείο διαχείρισης για την εικονική και φυσική υποδομή του δικτύου, επιτρέποντας τη δημιουργία, τη διαχείριση και την ελεγχόμενη ενεργοποίηση των εικονικών δικτύων. Ένα από τα κύρια χαρακτηριστικά του Contrail

SDN Controller είναι η δυνατότητα διαχείρισης και ενοποίησης των εικονικών περιβαλλόντων και των φυσικών πλατφορμών, επιτρέποντας την ομαλή λειτουργία τους όπως φαίνεται στην εικόνα 0-14 . Αυτό επιτρέπει επίσης σημαντικές λειτουργίες όπως η δυναμική αντίθεση του δικτύου, η προστασία ασφαλείας και η ολοκληρωμένη διαχείριση των πόρων του δικτύου, προσφέροντας έτσι μια ολοκληρωμένη λύση SDN.



Εικόνα 0-14 Juniper Contrail SDN Controller(et al. Neto , 2021)

Ο Juniper Contrail SDN Controller προσφέρει μια πληθώρα λειτουργιών για τη διαχείριση και την ελεγχόμενη εκτέλεση των δικτύων Moledo et al. (Moledo, 2019). Με δυνατότητες όπως η ελεγχόμενη εκτέλεση δικτύου, η αυτοματοποιημένη παραμετροποίηση, η προηγμένη ασφάλεια, το ενιαίο εικονικό δίκτυο και η ορισμένη πολιτική, ο Contrail παρέχει μια ολοκληρωμένη λύση για τη διαχείριση των δικτύων. Επιπλέον, με εργαλεία αυτοματοποίησης και ευελιξία στη διαχείριση, προσφέρει αποτελεσματική λύση για τις ανάγκες των επιχειρήσεων στον τομέα των δικτύων.

Παρακάτω, Πίνακας 1, παραθέτουμε μια συνοπτική έρευνα που κάναμε, όσον αφορά διάφορα χαρακτηριστικά των SDN ελεγκτών, είτε αφορά ανοικτού κώδικα είτε κλειστού. Αυτά τα χαρακτηριστικά αναφέρονται βιβλιογραφικά στην εργασία μας, και για διευκόλυνση δημιουργήσαμε έναν συνοπτικό πίνακα.

Ελεγκτής	Χρονολογία	Γλώσσα	Αρχιτεκτονική	Προγραμματιστική Ευελξία	Ασφάλεια	Προσαρμοστικότητα	Απόδοση	Συνεχής Λειτουργία	Διαχείριση Πόρων	Κώδικας	Επίπεδο Διαχείρισης
pox	2011	Python	Κεντρική Αρχιτεκτονική	Περιορισμένη	Ανεπαρκής	Ανεπαρκής	Μέτρια	Περιορισμένη	Κλειστός	OpenFlow, NOX	Κεντρική διαχείριση
ryu	2011	Python	Κεντρική Αρχιτεκτονική	Υψηλή	Καλή	Υψηλή	Καλή	Περιορισμένη	Ανοιχτός	OpenFlow, OF- config	Κεντρική διαχείριση
OpenDaylight	2013	Java	Διανεμημένη Αρχιτεκτονική	Υψηλή	Άριστη	Υψηλή	Άριστη	Υψηλή	Ανοιχτός	OpenFlow, NETCONF, SNMP	Διανεμημένη διαχείριση
Floodlight	2011	Java	Κεντρική Αρχιτεκτονική	Υψηλή	Καλή	Υψηλή	Καλή	Περιορισμένη	Ανοιχτός	OpenFlow	Κεντρική διαχείριση
VMware	2013	Ποικίλες	Κεντρική Αρχιτεκτονική	Υψηλή	Ανεπαρκής	Άριστη	Άριστη	Περιορισμένη	Κλειστός	OpenFlow, VXLAN	Κεντρική διαχείριση
Juniper Contrail	2012	Python	Διανεμημένη Αρχιτεκτονική	Υψηλή	Άριστη	Υψηλή	Άριστη	Υψηλή	Κλειστός	BGP, XMPP	Διανεμημένη διαχείριση
Cisco	2013	Ποικίλες	Διανεμημένη Αρχιτεκτονική	Υψηλή	Άριστη	Υψηλή	Άριστη	Υψηλή	Κλειστός	OpenFlow	Διανεμημένη διαχείριση
Beacon	2012	Java	Κεντρική Αρχιτεκτονική	Υψηλή	Άριστη	Υψηλή	Άριστη	Υψηλή	Κλειστός	-	Κεντρική διαχείριση

Πίνακας 1 Χαρακτηριστικά SDN Ελεγκτών

5.3. Δείκτες απόδοσης Ελεγκτών

Οι δείκτες απόδοσης ελεγκτών στον χώρο του SDN αποτελούν ένα σημαντικό εργαλείο για την αξιολόγηση της απόδοσης και της αποτελεσματικότητας, Mamushiane et al.(Mamushiane, 2018). Είναι κρίσιμοι για την κατανόηση της λειτουργίας του ελεγκτή και την εξασφάλιση της αντοχής και της αποδοτικότητάς του σε διάφορες καταστάσεις λειτουργίας του δικτύου. Η ανάλυση αυτών των δεικτών μπορεί να προσφέρει βαθύτερη κατανόηση των αδυναμιών και των δυνατοτήτων του ελεγκτή, επιτρέποντας τη λήψη μέτρων για τη βελτίωση της απόδοσης. Επιπλέον, η συνεχής παρακολούθηση αυτών των δεικτών είναι κρίσιμη για την ανίχνευση πιθανών προβλημάτων και τη λήψη έγκαιρων μέτρων για την αντιμετώπισή τους, εξασφαλίζοντας τη σταθερή και αξιόπιστη λειτουργία του δικτύου. Ας εξετάσουμε αναλυτικά τους κύριους δείκτες

5.3.1. Throughput

Η απόδοση δικτύων είναι κρίσιμη για τη λειτουργία των διαδικτυακών συστημάτων Xu et al.(Xu. , 2017). Η μέτρηση του throughput, δηλαδή της ταχύτητας μεταφοράς δεδομένων από ένα σημείο σε ένα άλλο, είναι ζωτικής σημασίας για την αξιολόγηση της απόδοσης. Η απόδοση, ή η ταχύτητα με την οποία τα δεδομένα επεξεργάζονται και μεταφέρονται, είναι εξίσου σημαντική. Το throughput μετριέται συνήθως σε μονάδες όπως τα Mbps (megabits ανά δευτερόλεπτο) ή τα Gbps (gigabits ανά δευτερόλεπτο) και αφορά τον όγκο δεδομένων που μεταφέρονται από ένα σημείο σε ένα άλλο σε μια συγκεκριμένη χρονική περίοδο. Μπορεί να επηρεαστεί από πολλούς παράγοντες όπως η εκτεταμένη συνδεσιμότητα του δικτύου, η απόσταση μεταξύ των σημείων μετάδοσης, η κίνηση δεδομένων και ο τύπος των δεδομένων που μεταφέρονται. Η απόδοση περιγράφει την ταχύτητα επεξεργασίας των δεδομένων από την αρχική τους δημιουργία μέχρι την παράδοσή τους. Περιλαμβάνει τον χρόνο απόκρισης του δικτύου, τον χρόνο που απαιτείται για τη μετάδοση δεδομένων και τον χρόνο επεξεργασίας από τις συσκευές. Η σωστή ανάλυση του throughput και της απόδοσης είναι κρίσιμη για την αξιολόγηση της απόδοσης δικτύου, καθώς και για τη βελτίωση και την εξοικονόμηση των πόρων. Κατανοώντας αυτές τις έννοιες, οι διαχειριστές δικτύου μπορούν να βελτιστοποιήσουν την απόδοση, να προλάβουν προβλήματα και να εξασφαλίσουν τη σταθερή λειτουργία των συστημάτων τους.

Σε ένα δίκτυο, η βασική χωρητικότητα αντιπροσωπεύει τη μέγιστη ταχύτητα μετάδοσης δεδομένων υπό ιδανικές συνθήκες, ενώ οι παράμετροι του φυσικού επιπέδου, όπως η ευαισθησία του δέκτη και η απόσβεση σήματος, επηρεάζουν το μέγιστο εφικτό throughput , Zhu et al.(Zhu , 2019). Επίσης, παράγοντες όπως η

πολυπλοκότητα των αλγορίθμων και η απόδοση του ενεργού πρωτοκόλλου επικοινωνίας έχουν σημαντική επίδραση.

5.3.2.Bandwidth

Το bandwidth είναι μια μετρική που αναφέρεται στη μέγιστη ποσότητα δεδομένων που μπορούν να μεταφερθούν μέσα σε ένα δίκτυο σε ένα συγκεκριμένο χρονικό διάστημα. Yang et al.(Yang ,2021).Μπορεί να ερμηνευτεί ως η "χωρητικότητα" του δικτύου ή η "πλάτη" του δρόμου, καθώς ορίζει πόσα δεδομένα μπορούν να μεταφερθούν σε μια μονάδα χρόνου. Είναι σημαντικό να σημειωθεί ότι το bandwidth δεν αντιπροσωπεύει την πραγματική ταχύτητα μετάδοσης δεδομένων που επιτυγχάνεται πάντα, καθώς υπάρχουν πολλοί παράγοντες που μπορούν να επηρεάσουν την πραγματική ταχύτητα, όπως οι συγκρούσεις στο δίκτυο, οι παρεμβολές, κλπ . Το bandwidth είναι ένας κρίσιμος παράγοντας για τη σχεδίαση και τη διαχείριση των δικτύων, καθώς καθορίζει τη μέγιστη χωρητικότητα του δικτύου και επηρεάζει την απόδοση και την αποδοτικότητα της μετάδοσης δεδομένων. Η αύξηση του bandwidth μπορεί να βελτιώσει την απόδοση του δικτύου και να υποστηρίξει μεγαλύτερες ταχύτητες μετάδοσης δεδομένων και εφαρμογές υψηλού εύρους ζώνης. Όσο μεγαλύτερο είναι το bandwidth, τόσο περισσότερα δεδομένα μπορούν να μεταφερθούν ταυτόχρονα. Μετριέται συνήθως σε Bits ανά δευτερόλεπτο (bps), Kilobits (Kbps), Megabits (Mbps) ή Gigabits (Gbps). Το bandwidth επηρεάζει την ταχύτητα μεταφοράς δεδομένων στο δίκτυο Qin et al. (Qin ,2015). Αν ένα δίκτυο έχει χαμηλό bandwidth, μπορεί να υπάρχουν περιορισμοί στην ταχύτητα μετάδοσης δεδομένων, που μπορεί να οδηγήσουν σε καθυστερήσεις ή σε μειωμένη απόδοση. Μεγαλύτερο bandwidth επιτρέπει μεγαλύτερο όγκο δεδομένων να μεταφερθεί σε μικρότερο χρόνο, βελτιώνοντας την ταχύτητα και την απόδοση του δικτύου. Το bandwidth είναι σημαντικό σε όλα τα είδη δικτύων, από τα οικιακά δίκτυα μέχρι τις επιχειρηματικές υποδομές και το Διαδίκτυο. Επίσης, επηρεάζει την ικανότητα μεταφοράς δεδομένων σε διάφορες εφαρμογές, όπως το streaming βίντεο, οι τηλεδιασκέψεις ή η μεταφορά μεγάλων αρχείων. Το bandwidth αποτελεί σημαντικό παράγοντα στην συνολική απόδοση και λειτουργία ενός δικτύου, επηρεάζοντας την ταχύτητα, την αξιοπιστία και την απόδοσή του.

5.3.3. Καθυστέρηση (Delay)

Η καθυστέρηση (ή καθυστέρηση δικτύου), γνωστή και ως "delay" στα δίκτυα, αναφέρεται στο χρονικό διάστημα που απαιτείται για ένα πακέτο δεδομένων να διανύσει την διαδρομή από την αρχική του αποστολή (πηγή) μέχρι τον προορισμό του (παραλήπτη) Kumar et al. (Kumar , 2017). Αυτό το χρονικό διάστημα περιλαμβάνει τον χρόνο που απαιτείται για τη μετάδοση, την διαδρομή, καθώς και ενδεχόμενες συγκρούσεις σε ένα δίκτυο. Η καθυστέρηση είναι σημαντική στην απόδοση των δικτύων και μπορεί να επηρεάσει την αποδοτικότητα, την ευαισθησία στο χρόνο και την γενική εμπειρία των χρηστών.

Η Round-Trip Time (RTT), αποτελεί έναν σημαντικό δείκτη καθυστέρησης σε ένα δίκτυο Pathak et al. (Pathak , 2008). Στην πραγματικότητα, το RTT είναι μια συμβιβαστική λύση στις περισσότερες περιπτώσεις και χρησιμοποιείται για την εξαγωγή συμπερασμάτων σχετικά με τις καθυστερήσεις προς τα εμπρός και προς τα πίσω από πολλά πρωτόκολλα και εφαρμογές. Υποθέτουν ότι η εμπρόσθια και η αντίστροφη καθυστέρηση είναι ίσες με το μισό του RTT. Αναφέρεται στον χρόνο που απαιτείται για να μεταφερθεί ένα πακέτο από έναν αποστολέα σε έναν παραλήπτη και να επιστρέψει πίσω, δηλαδή τον χρόνο που απαιτείται για να γίνει η κυκλική διαδρομή των δεδομένων. Η RTT υπολογίζεται ως η διαφορά χρόνου μεταξύ της αποστολής ενός πακέτου από τον αποστολέα και της λήψης της απάντησης από τον παραλήπτη Kim et al. (Kim , 2019). Αυτό περιλαμβάνει το χρόνο που απαιτείται για τη μετάδοση στο δίκτυο, την επεξεργασία στους κόμβους, και την επιστροφή της απόκρισης στον αποστολέα. Οι καθυστερήσεις στο δίκτυο (όπως η απόσταση φυσικής μετάδοσης) και οι καθυστερήσεις στην επεξεργασία στους κόμβους μπορούν να επηρεάσουν το RTT . Οι χαμηλοί χρόνοι RTT σηματοδοτούν γρήγορη και αποτελεσματική μετάδοση δεδομένων, ενώ υψηλοί χρόνοι RTT μπορεί να είναι συνήθως αποτέλεσμα προβλημάτων στο δίκτυο, όπως συμφόρηση, πακέτα που χάνονται ή καθυστερήσεις στη μετάδοση. Η μείωση του RTT είναι ένας στόχος στη βελτίωση της απόδοσης του δικτύου, καθώς επηρεάζει την ταχύτητα και την αξιοπιστία της επικοινωνίας.

Η Καθυστέρηση Διάδοσης (Propagation Delay): Ο χρόνος που απαιτείται για ένα σήμα να διαδοθεί από ένα σημείο του δικτύου σε ένα άλλο λόγω της φυσικής απόστασης και της ταχύτητας μετάδοσης Chitre et al.(Chitre , 2012). Αυτή η καθυστέρηση επηρεάζεται από πολλούς παράγοντες, συμπεριλαμβανομένης της φυσικής απόστασης μεταξύ των σημείων στο δίκτυο, των χαρακτηριστικών του μέσου μετάδοσης και του φόρτου του δικτύου. Επιπλέον, η επεξεργαστική καθυστέρηση σε κάθε κόμβο του δικτύου μπορεί επίσης να επηρεάσει τη συνολική καθυστέρηση διαδρομής. Η διαχείριση και η βελτιστοποίηση αυτής της καθυστέρησης είναι κρίσιμη για τη βελτίωση της απόδοσης του δικτύου και την εξασφάλιση υψηλής ποιότητας υπηρεσιών, όπως οι φωνητικές κλήσεις και οι

βίντεοκλήσεις σε πραγματικό χρόνο. Κατά συνέπεια, οι διαχειριστές δικτύων επιδιώκουν συνεχώς να βελτιώσουν την απόδοση της διαδρομής και να μειώσουν την καθυστέρηση, εφαρμόζοντας κατάλληλες τεχνικές δρομολόγησης και διαχείρισης της κίνησης.

Transmission Delay : Η καθυστέρηση μετάδοσης αναφέρεται στον χρόνο που απαιτείται για να μεταφερθούν δεδομένα από έναν πόρο στο δίκτυο σε έναν άλλον, λαμβάνοντας υπόψη το μέγεθος του πακέτου και την ταχύτητα μετάδοσης του μέσου μετάδοσης Sheridan et al. (Sheridan , 1963).. Αυτή η καθυστέρηση είναι αποτέλεσμα της φυσικής διαδικασίας της μετάδοσης των δεδομένων μέσω του δικτύου και μπορεί να επηρεαστεί από πολλούς παράγοντες, όπως η ταχύτητα του μέσου μετάδοσης, η ποιότητα της σύνδεσης και ο όγκος της κίνησης στο δίκτυο. Καθώς ο χρόνος μετάδοσης είναι ανάλογος του μεγέθους του πακέτου δεδομένων και της ταχύτητας μετάδοσης του μέσου, οι υψηλότερες ταχύτητες μετάδοσης και τα μικρότερα μεγέθη πακέτων συνήθως οδηγούν σε μικρότερη καθυστέρηση μετάδοσης. Η καθυστέρηση μετάδοσης είναι σημαντική για τη συνολική απόδοση του δικτύου και επηρεάζει την αποτελεσματικότητα και την απόκριση των υπηρεσιών που παρέχονται στους χρήστες. Κατά συνέπεια, η διαχείριση και η βελτιστοποίηση της καθυστέρησης μετάδοσης είναι σημαντικές για την εξασφάλιση της υψηλής ποιότητας των υπηρεσιών δικτύου.

Η καθυστέρηση επεξεργασίας : αφορά τον χρόνο που απαιτείται για να επεξεργαστεί ένα πακέτο δεδομένων σε έναν κόμβο του δικτύου Ramaswamy et al. (Ramaswamy, 2004). Αυτή η καθυστέρηση περιλαμβάνει το χρόνο που απαιτείται για τη λήψη του πακέτου, την ανάλυση του, τη λήψη απόφασης σχετικά με τη δράση που πρέπει να ληφθεί και τη μετάδοσή του προς τον επόμενο κόμβο. Αυτή η καθυστέρηση επηρεάζεται από πολλούς παράγοντες, όπως η ισχύς του επεξεργαστή του κόμβου, η πολυπλοκότητα των αλγορίθμων επεξεργασίας, και η συνολική φόρτιση του συστήματος. Η καθυστέρηση επεξεργασίας μπορεί να επηρεάσει σημαντικά την απόδοση του δικτύου, ιδίως σε εφαρμογές που απαιτούν χαμηλή καθυστέρηση, όπως οι φωνητικές κλήσεις ή οι βίντεοκλήσεις σε πραγματικό χρόνο. Επομένως, η βελτιστοποίηση των διεργασιών επεξεργασίας σε κάθε κόμβο του δικτύου είναι κρίσιμη για την εξασφάλιση της υψηλής απόδοσης και της ποιότητας των υπηρεσιών που παρέχονται.

5.3.4.Jitter

Το Jitter είναι ένας σημαντικός δείκτης που παρακολουθεί τη διακύμανση στο χρόνο παράδοσης των πακέτων δεδομένων σε ένα δίκτυο Numan et al. (Numan , 2019). Στις τηλεπικοινωνίες και στην ανταλλαγή δεδομένων, η σταθερή, αξιόπιστη και ομαλή μετάδοση πακέτων είναι ουσιώδης. Ωστόσο, η μετάδοση δεδομένων δεν συμβαίνει πάντα με σταθερό τρόπο. Το Jitter μετρά τη διακύμανση στον χρόνο παράδοσης των πακέτων: αν ο χρόνος που χρειάζεται ένα πακέτο να φτάσει στον

προορισμό του διαφέρει από τον χρόνο άφιξης του προηγούμενου πακέτου, τότε έχουμε Jitter. Αυτή η διακύμανση μπορεί να οφείλεται σε πολλούς παράγοντες, όπως η κυκλοφορία δεδομένων στο δίκτυο, η συμφόρηση, η απώλεια πακέτων, ή ακόμα και η διαφορά στις διαδρομές που ακολουθούν τα πακέτα λόγω φορτίου. Ο Jitter είναι κρίσιμος για εφαρμογές που απαιτούν συνεχή και σταθερή μετάδοση, όπως οι φωνητικές κλήσεις ή οι τηλεδιασκέψεις. Ένα υψηλό επίπεδο Jitter μπορεί να οδηγήσει σε δυσλειτουργίες και προβλήματα στην επικοινωνία, ενώ ένα χαμηλό επίπεδο εξασφαλίζει την ομαλή μετάδοση δεδομένων. Οι προγραμματιστές δικτύων παρακολουθούν το Jitter για να διασφαλίσουν την ποιότητα και τη σταθερότητα των υπηρεσιών που παρέχουν. Το Jitter αναφέρεται στη διακύμανση στο χρόνο που απαιτείται για την άφιξη πακέτων δεδομένων σε ένα σημείο προορισμού. Σε μια ιδανική κατάσταση, όπου τα πακέτα μεταφέρονται στο δίκτυο με σταθερή ταχύτητα και δεν υπάρχουν καθυστερήσεις ή διακυμάνσεις, το Jitter είναι μηδενικό. Ωστόσο, στην πραγματικότητα, οι διάφοροι παράγοντες μπορούν να προκαλέσουν διακυμάνσεις στην άφιξη των πακέτων, δημιουργώντας έτσι το Jitter. Οι κύριοι παράγοντες που επηρεάζουν το Jitter, Sojan et al. (Sojan, 2022), περιλαμβάνουν:

- **Κίνηση Δικτύου:** Η υπερφόρτωση του δικτύου μπορεί να προκαλέσει καθυστερήσεις και αποκλίσεις στην άφιξη των πακέτων.
- **Διαφορετικές Διαδρομές:** Πακέτα που ακολουθούν διαφορετικές διαδρομές μπορεί να έχουν διαφορετικές καθυστερήσεις.
- **Διαχείριση Κίνησης (Traffic Management):** Οι μηχανισμοί διαχείρισης της κίνησης στο δίκτυο μπορούν να επηρεάσουν το Jitter.

Ο μετρικός όρος του Jitter συνήθως περιγράφεται μέσω της μέσης τιμής και του εύρους του, και παρέχει πληροφορίες σχετικά με την ποιότητα της μετάδοσης δεδομένων. Συχνά, χρησιμοποιείται σε συστήματα που απαιτούν σταθερή και αξιόπιστη μετάδοση δεδομένων, όπως τις φωνητικές κλήσεις και την βίντεο-διάδοση.

5.3.5.Απώλεια πακέτων

Η απώλεια πακέτων σε ένα δίκτυο αποτελεί σημαντικό πρόβλημα και επηρεάζει τη συνολική απόδοση του Sinha et al. (Sinha, 2018). Είναι μια μετρική που αντιπροσωπεύει το ποσοστό πακέτων που χάνονται κατά τη διαδικασία μετάδοσης σε ένα δίκτυο. Οι λόγοι απώλειας πακέτων μπορεί να είναι πολλοί, συμπεριλαμβανομένης της συμφόρησης στο δίκτυο, των σφαλμάτων σε δρομολογητές ή καλώδια, των προβλημάτων δικτύωσης ή ακόμη και της κακής ποιότητας της σύνδεσης. Η απώλεια πακέτων μπορεί να έχει καταστροφικές συνέπειες στην επικοινωνία. Σε εφαρμογές πραγματικού χρόνου, όπως φωνητικές ή βιντεοκλήσεις, η απώλεια πακέτων μπορεί να οδηγήσει σε διακοπές στην επικοινωνία ή σε μειωμένη ποιότητα ήχου και εικόνας. Σε δίκτυα που μεταφέρουν δεδομένα, η απώλεια πακέτων μπορεί να οδηγήσει σε ανεπαρκή διανομή δεδομένων, απώλεια πληροφοριών ή ακόμη και σε επαναλαμβανόμενα αιτήματα για

δεδομένα Mizrahi et al.(Mizrahi , 2016). Για να μειωθεί η απώλεια πακέτων, οι διαχειριστές δικτύων χρησιμοποιούν ποικίλα μέσα. Αυτά μπορεί να περιλαμβάνουν τη ρύθμιση αλγορίθμων ελέγχου συμφόρησης για να διαχειριστούν τη ροή δεδομένων, την επιβολή πολιτικών περιορισμού εύρους ζώνης για να μειώσουν την υπερφόρτωση του δικτύου, και την απόκριση σε προβλήματα συνδεσιμότητας ή σφαλμάτων σε πραγματικό χρόνο. Η επιτυχία στη μείωση της απώλειας πακέτων αποτελεί κρίσιμο παράγοντα για τη βελτίωση της αξιοπιστίας και της απόδοσης των δικτύων.

Αίτια απώλειας πακέτων

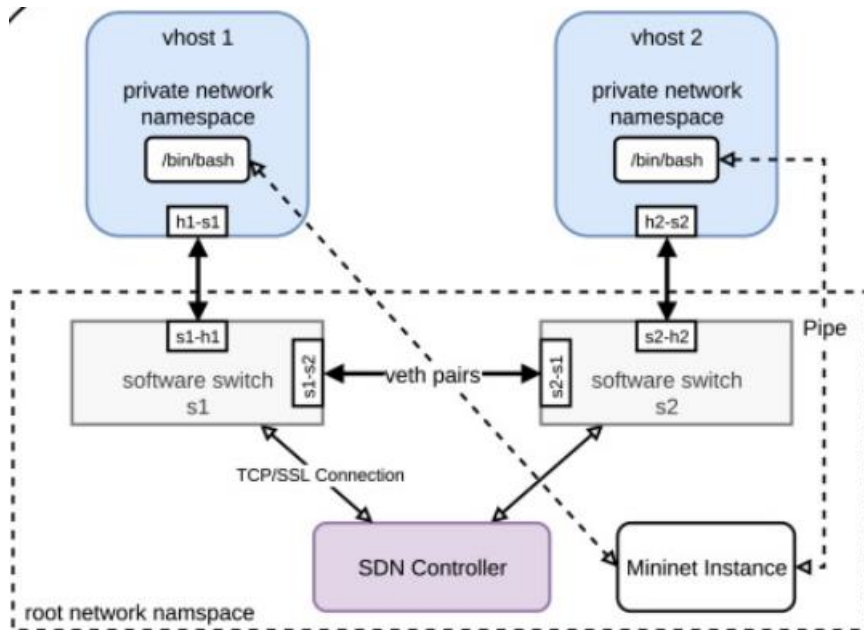
- **Υπερφόρτωση Δικτύου (Network Congestion):** Όταν το δίκτυο είναι υπερφορτωμένο, οι κόμβοι του δικτύου μπορεί να μην καταφέρνουν να χειριστούν όλα τα πακέτα και να τα χάσουν.
- **Συνθήκες Καναλιού (Channel Conditions):** Κακές συνθήκες στο κανάλι μετάδοσης, όπως πολλά παρεμβαλλόμενα σήματα ή αστάθεια στην ασύρματη επικοινωνία, μπορούν να προκαλέσουν απώλεια πακέτων.
- **Καταστροφή Πακέτων (Packet Corruption):** Σε κακή ποιότητα κανάλια μπορεί να παραμορφωθούν τα πακέτα, καθιστώντας τα ακατάλληλα για χρήση.
- **Επιπτώσεις της απώλειας πακέτων :** Χειρότερη Απόδοση: Η απώλεια πακέτων μπορεί να οδηγήσει σε χαμηλότερες ταχύτητες μετάδοσης και παρατεταμένη απόκριση (latency) στην επικοινωνία.
- **Επαναμετάδοση (Retransmission):** Η απώλεια πακέτων απαιτεί την επαναμετάδοση των πληροφοριών που περιείχαν τα πακέτα που χάθηκαν, αυξάνοντας την κίνηση στο δίκτυο.

6. MININET Πακέτο προσομοίωσης

6.1. MININET

Το Mininet Kaur et al.(Kaur ,2015) αναδεικνύεται ως ένας σημαντικός εξομοιωτής δικτύων που επιτρέπει την ανάπτυξη και πειραματισμό σε μεγάλη κλίμακα μέσα από περιορισμένους υπολογιστικούς πόρους. Ο εξομοιωτής αυτός δημιουργήθηκε ειδικά για την έρευνα στους τομείς της δικτύωσης που εστιάζουν στη δικτυακή εκτέλεση που καθορίζεται από λογισμικό (SDN) και το πρωτόκολλο OpenFlow. Οι εξομοιωτές, όπως το Mininet, επιτρέπουν την εκτέλεση του αυθεντικού λογισμικού χωρίς τροποποίηση σε εικονικό υλικό σε απλούς υπολογιστές. Το Mininet έχει ήδη τη δυνατότητα δημιουργίας εμπορευματοκιβωτίων καθώς και του δικτύου από ένα ενιαίο, απλό API Python. Με τη χρήση του Mininet αποφεύγεται η ανάγκη εγκατάστασης, διαμόρφωσης και διαχείρισης πολλαπλών συστημάτων ενορχήστρωσης. Επιπλέον, οι κεντρικοί υπολογιστές Mininet δεν εκτελούν περιττό επιπλέον λογισμικό, όπως πολλαπλούς πυρήνες, και δεν απαιτούν δυσκίνητες, ογκώδεις εικόνες εικονικών συστημάτων αρχείων. Για την υποστήριξη διαμορφώσεων που υπερβαίνουν τους πόρους ενός μόνο διακομιστή, η πειραματική υποστήριξη του Mininet μπορεί να χρησιμοποιηθεί για την εύκολη και απρόσκοπτη κατανομή του εικονικού περιβάλλοντος δοκιμών σε πολλούς φυσικούς (ή εικονικούς) διακομιστές Lantz et al.(Lantz , 2015). Το Mininet είναι εύκολο στη χρήση, ακριβές στις επιδόσεις και επεκτάσιμο. Η αυξανόμενη ανάγκη για μοντελοποίηση των κεντρικών υπολογιστών, των switches , των συνδέσεων και της τεχνολογίας SDN/Openflow τα τελευταία χρόνια, καθιστά το Mininet αναγκαίο εργαλείο.

Το Mininet είναι επίσης ένας πολύ καλός τρόπος για την ανάπτυξη και τον πειραματισμό με συστήματα Software-Defined Networking (SDN) χρησιμοποιώντας το OpenFlow Fontes et al.(Fontes , 2016). Ένα από τα κύρια πλεονεκτήματα του Mininet είναι η δυνατότητα δημιουργίας πολύ μεγάλων τοπολογιών με χιλιάδες κόμβους. Αυτό μπορεί να γίνει μέσω απλών εργαλείων γραμμής εντολών API που επιτρέπουν στους χρήστες να δημιουργούν, να προσαρμόζουν, να μοιράζονται και να δοκιμάζουν SDN δίκτυα όπως απεικονίζεται στην εικόνα 0-15 . Το Mininet αποδεικνύεται αξιόπιστο, παρέχοντας ρεαλιστικό περιβάλλον προσομοίωσης για την πειραματική έρευνα στον τομέα των SDN, επιτρέποντας την ανάπτυξη και τον έλεγχο εναλλακτικών εφαρμογών και πρωτοκόλλων. Επιπλέον, το Mininet παρέχει τη δυνατότητα να ενσωματώνει στοιχεία SDN, να διαμοιράζεται με άλλα δίκτυα και να αλληλεπιδρά με αυτά.



Εικόνα 0-15 Mininet(et al. Xiang ,2020)

Χρησιμοποιώντας το Mininet, είναι δυνατή η εξερεύνηση δικτύων SDN διαφόρων δομών Romanov et al. (Romanov, 2021). Τα κύρια πλεονεκτήματα του Mininet είναι τα εξής:

- **Γρήγορη δημιουργία δικτύου** με τη χρήση τυποποιημένων στοιχείων.
- **Δυνατότητα δημιουργίας δικτύων πολύπλοκης δομής.**
- **Δημιουργία εικονικών στοιχείων δικτύου**, όπως OpenFlow Switch, διακομιστές ιστού, εργαλεία παρακολούθησης, Wireshark.
- **Μεταφορά και εγκατάσταση διαμορφωμένων δομών δικτύου** από το Mininet σε μεταγωγείς υλικού.
- **Ανάπτυξη ενός δικτύου στο Mininet** σε φορητό υπολογιστή, διακομιστή, εικονική μηχανή ή νέφος.

Κάποια από τα χαρακτηριστικά του Mininet :

- **Ευελιξία:** με τη βοήθεια γλωσσών προγραμματισμού και κοινών λειτουργικών συστημάτων.
- **Εφαρμοστικότητα**
- **Αλληλεπιδραστικότητα:** το προσομοιωμένο δίκτυο πρέπει να αναπτύσσεται στο πραγματικό δίκτυο, σαν να συμβαίνει σε πραγματικά δίκτυα.

- **Επεκτασιμότητα :** μεγάλα δίκτυα πρέπει να κλιμακώνονται με τη βοήθεια του περιβάλλοντος χρησιμοποιώντας εκατοντάδες ή χιλιάδες switches σε έναν μόνο υπολογιστή.
- **Πρακτική:** η συμπεριφορά του πρωτοτύπου πρέπει να είναι ικανή για την αναπαράσταση της συμπεριφοράς σε πραγματικό χρόνο με υψηλό βαθμό εμπιστοσύνης, Patil et al. (Patil 2020) έτσι ώστε να μην απαιτείται τροποποίηση του κώδικα για τη χρήση εφαρμογών και στοίβες πρωτοκόλλων .
- **Κοινή χρήση:** οι άλλοι συνεργάτες πρέπει να είναι σε θέση να επαναχρησιμοποιήσουν τα δημιουργημένα πρωτότυπα, τα οποία μπορούν στη συνέχεια να εκτελέσουν και να τροποποιήσουν τα πειράματα.

Τέλος, το Mininet αποτελεί ένα εργαλείο που επιτρέπει τη δημιουργία και προσαρμογή στοιχείων SDN, μοιράζονται και αλληλεπιδρούν με άλλα δίκτυα, καθιστώντας το ένα χρήσιμο εργαλείο για την εξέλιξη της τεχνολογίας δικτύων.

6.1.1. Πλεονεκτήματα Mininet

Το Mininet προσφέρει πολλά πλεονεκτήματα και οφέλη για τους ερευνητές, τους αναπτυσσόμενους και τους εκπαιδευόμενους στον τομέα της δικτύωσης. Ορισμένα από τα βασικά πλεονεκτήματα του Mininet περιλαμβάνουν:

- **Ευελιξία και Ευκολία Χρήσης:** Το Mininet είναι εύκολο στη χρήση και επιτρέπει την εύκολη δημιουργία και προσομοίωση δικτύων Muelas et al . (Muelas , 2018). Οι χρήστες μπορούν να δημιουργήσουν ποικίλες τοπολογίες και να προσομοιώσουν διάφορες συνθήκες με λίγες εντολές.
- **Αποφυγή Κόστους και Πολυπλοκότητας:** Η προσομοίωση των δικτύων με το Mininet εξομοιώνει τη λειτουργία πραγματικών δικτύων χωρίς την ανάγκη για φυσικό υλικό Fontes et al .(Fontes , 2015). Αυτό μειώνει το κόστος και την πολυπλοκότητα που συνδέονται με την πραγματική αγορά, σύνδεση και συντήρηση υλικού δικτύων.
- **Ευελιξία Προγραμματισμού:** Το Mininet χρησιμοποιεί τη γλώσσα προγραμματισμού Python Kumar et al. (Kumar , 2019) για την προσαρμογή της συμπεριφοράς των δικτυακών συσκευών. Αυτό επιτρέπει στους χρήστες να προσαρμόσουν και να επεκτείνουν τα δίκτυα σύμφωνα με τις ανάγκες τους.

- **Προγραμματισμός Πραγματικού Χρόνου:** Το Mininet παρέχει τη δυνατότητα προσομοίωσης πραγματικού χρόνου Muelas et al .(Muelas , 2018) , επιτρέποντας την αναπαραγωγή πραγματικών συνθηκών λειτουργίας δικτύων. Αυτό είναι χρήσιμο για την εκτίμηση της απόδοσης του δικτύου και την αξιολόγηση των αλλαγών.
- **Ελεύθερο Λογισμικό Ανοικτού Κώδικα:** Το Mininet είναι ελεύθερο λογισμικό ανοικτού κώδικα, προσφέροντας ελευθερία προσαρμογής και επέκτασης για τους χρήστες Pakzad, et al.(Pakzad , 2016). Αυτό δίνει τη δυνατότητα σε κοινότητες να συμβάλουν στη βελτίωση και την εξέλιξη του εργαλείου.

Συνολικά, το Mininet αντιπροσωπεύει ένα ισχυρό εργαλείο που επιτρέπει την ανάπτυξη, τον έλεγχο και την αξιολόγηση των SDN δικτύων με ευελιξία, ευκολία και αποδοτικότητα.

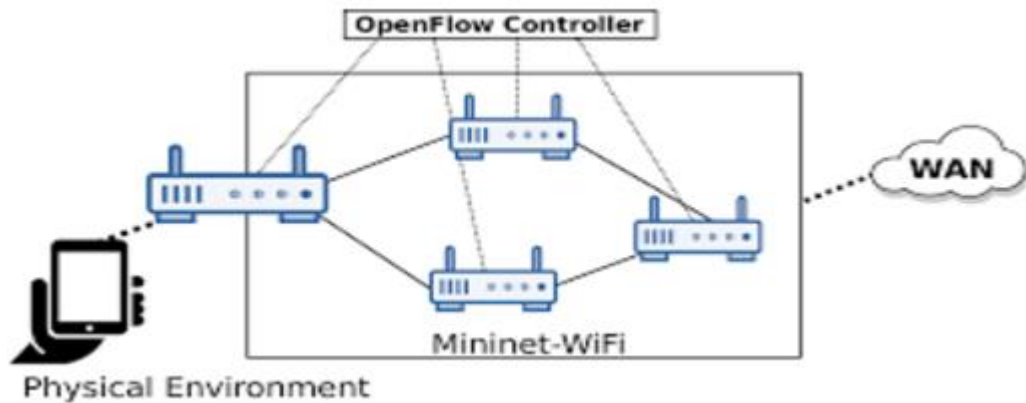
6.1.2. Μειονεκτήματα Mininet

Παρά τα πολλά πλεονεκτήματα που προσφέρει το Mininet, υπάρχουν και ορισμένα μειονεκτήματα που πρέπει να ληφθούν υπόψη:

- **Περιορισμένη Ακρίβεια:** Αν και το Mininet προσομοιώνει δίκτυα, οι πραγματικές συνθήκες λειτουργίας και οι μεταβολές στο πραγματικό περιβάλλον ενδέχεται να μην αποτυπώνονται ακριβώς.
- **Περιορισμένες Επιδόσεις:** Η προσομοίωση μέσω λογισμικού, όπως το Mininet, μπορεί να περιορίζει τις επιδόσεις και την απόδοση σε σύγκριση με πραγματικά δίκτυα. Αυτό είναι ιδιαίτερα εμφανές όταν προσπαθούμε να αντιμετωπίσουμε μεγάλα και πολύπλοκα δίκτυα .
- **Περιορισμένη Δυνατότητα Εξειδίκευσης:** Παρόλο που το Mininet είναι ευέλικτο, η προσομοίωση περιορίζεται στα όρια των δυνατοτήτων του εργαλείου Jarinder et al. (Jarinder , 2014) .Ορισμένες εξειδικευμένες απαιτήσεις μπορεί να απαιτούν προηγμένα εργαλεία ή προσομοιωτές.
- **Περιορισμένη Υποστήριξη Πρωτοκόλλων:** Το Mininet υποστηρίζει κυρίως τα πρωτόκολλα που σχετίζονται με την τεχνολογία SDN και το OpenFlow. Αν χρειάζεται να προσομοιώσετε πρωτόκολλα εκτός αυτής της κατηγορίας, μπορεί να είναι περιορισμένη η υποστήριξη.
- **Ανάγκη Υπολογιστικών Πόρων:** Παρότι το Mininet είναι αποδοτικό, η προσομοίωση μεγάλων και πολύπλοκων δικτύων μπορεί να απαιτεί σημαντικούς υπολογιστικούς πόρους, που ενδέχεται να περιορίζουν τη δυνατότητα προσομοίωσης σε μηχανήματα με περιορισμένους πόρους Oliveira et al . (Oliveira, 2014).

6.2. Mininet WiFi

Το Mininet-WiFi είναι ένας εξομοιωτής ασύρματου δικτύου για την υποστήριξη του SDWN, επεκτείνοντας το δημοφιλές Mininet με εξομοίωση ασύρματου καναλιού και υποστήριξη WiFi APs & Rothenberg et al. (Rothenberg, 2016). Το Mininet-WiFi επεκτείνει την αρχική λειτουργικότητα του Mininet, μιας πλατφόρμας προσομοίωσης δικτύων, προσθέτοντας τη δυνατότητα προσομοίωσης ασύρματων δικτύων. Αυτή η εξέλιξη ανοίγει νέες προοπτικές για την ανάπτυξη και δοκιμή δικτύων, επιτρέποντας στους χρήστες να προσομοιώσουν ασύρματες τεχνολογίες χωρίς την πραγματική παρουσία των συσκευών. Ο κύριος στόχος του είναι να εξομοιώνει ένα πλήρες δίκτυο από hosts, συνδέσεις και μεταγωγείς σε ένα μόνο μηχάνημα Castanheira et al. (Castanheira, 2018). Το Mininet-WiFi είναι μια προσθήκη κλάσεων στην κορυφή του mininet, υποστηρίζοντας όλες τις συνήθεις δυνατότητες εξομοίωσης SDN και απεικόνισης τόσο των σταθμών WiFi όσο και των σημείων πρόσβασης με τη χρήση τυποποιημένων οδηγών ασύρματου Linux. Από αυτές τις προσθήκες, υποστηρίζει μοντέλα κινητικότητας και διάδοσης. Αναλαμβάνει την προσομοίωση ασύρματων δικτύων όπως Wi-Fi, ενσωματώνοντας διάφορες συμπεριφορές όπως ασύρματα δίκτυα αισθητήρων ή mesh δίκτυα. Αυτό δίνει στους χρήστες τη δυνατότητα να πειραματιστούν με διάφορα πρωτόκολλα, πολιτικές δρομολόγησης, και συνδυασμούς δικτύων, παρέχοντας ένα ευέλικτο και ελεγχόμενο περιβάλλον προσομοίωσης. Στο Mininet-WiFi, οι ασύρματοι κόμβοι (όπως ασύρματα σημεία πρόσβασης ή κινητά τηλέφωνα) μπορούν να προστεθούν στο δίκτυο. Όπως απεικονίζεται στην εικόνα 0-16. Η αρχιτεκτονική του είναι παρόμοια με αυτήν του κανονικού Mininet, με τη διαφορά ότι υποστηρίζει επιπλέον την προσομοίωση ασύρματων συσκευών και των ασύρματων καναλιών. Μπορεί να χρησιμοποιηθεί για την εκπαίδευση, την έρευνα και την ανάπτυξη εφαρμογών σε ασύρματα δίκτυα, προσφέροντας μια πλατφόρμα για πειραματισμό και ανάλυση χωρίς την ανάγκη πραγματικού υλικού. Με την ευκολία χρήσης και την ευελιξία που προσφέρει, δίνει τη δυνατότητα για ευρεία ανακάλυψη και κατανόηση των πολύπλοκων χαρακτηριστικών των ασύρματων δικτύων.



Εικόνα 0-16 Mininet WiFi (et al.Karamjeet Kaur , 2015)

6.2.1. Χαρακτηριστικά του Mininet-WiFi:

Χαρακτηριστικά Mininet WiFi:

- **Mininet-WiFi:** Είναι ένα εργαλείο προσομοίωσης ασύρματων δικτύων, Kaur et al. (Kaur , 2014) διασυνδέοντας το Interface του Mininet με ασύρματες τεχνολογίες. Αυτό επεκτείνει την ικανότητα του Mininet να προσομοιώνει και να δοκιμάζει ασύρματα δίκτυα. Η κύρια δύναμή του είναι η δυνατότητά του να αναπαριστά την ασύρματη συμπεριφορά σε ένα ελεγχόμενο περιβάλλον.
- **Ευελιξία Συνδυασμών Δικτύων:** Η πλατφόρμα αυτή επιτρέπει στους χρήστες να δημιουργούν διάφορες τοπολογίες δικτύων, να εξερευνούν συνδυασμούς τεχνολογιών ασύρματων δικτύων, και να προσομοιώνουν διαφορετικά σενάρια δικτύων.
- **Ευέλικτος Προγραμματισμός:** Παρέχει εκτεταμένη υποστήριξη Python για τη δημιουργία, προσαρμογή, και εκτέλεση πειραμάτων δικτύου. Η χρήση Python επιτρέπει στους χρήστες να δημιουργήσουν ή να προσαρμόσουν εύκολα πειράματα δικτύων με σύνθετες λειτουργίες.
- **Συμβατότητα Mininet:** Το Mininet-WiFi είναι επεκτάσιμο από το Mininet και διατηρεί συμβατότητα με αυτό, Singh et al. (Singh 2014) επιτρέποντας στους χρήστες να χρησιμοποιούν γνώριμες δομές και εντολές από το Mininet.
- **Υποστήριξη Ασύρματων Συσκευών και Πρωτοκόλλων:** Υποστηρίζει ποικίλες ασύρματες συσκευές και πρωτόκολλα, επιτρέποντας στους χρήστες να μοντελοποιήσουν και να δοκιμάσουν διάφορες ασύρματες συσκευές και σενάρια.
- **Εκπαιδευτική Χρήση:** Παρέχει μια πλατφόρμα για την κατανόηση της συμπεριφοράς των ασύρματων δικτύων, και είναι χρήσιμο εκπαιδευτικό εργαλείο για φοιτητές και ερευνητές.

6.2.2.Πλεονεκτήματα του Mininet-WiFi:

Το Mininet WiFi είναι ένα περιβάλλον προσομοίωσης δικτύων λογισμικού ανοικτού κώδικα που χρησιμοποιείται ευρέως για την ανάπτυξη και τη δοκιμή δικτυακών εφαρμογών και πρωτοκόλλων Brito et al. (Brito, 2015). Το Mininet-WiFi αποτελεί ένα εργαλείο προσομοίωσης που επεκτείνει τη δυνατότητα του Mininet στον τομέα των ασύρματων δικτύων. Αυτό επιτρέπει στους ερευνητές και τους προγραμματιστές να αναπτύσσουν και να ελέγχουν εικονικά ασύρματα δίκτυα με ευκολία. Η δυνατότητα προσομοίωσης ασύρματων δικτύων επιτρέπει στους χρήστες να διερευνήσουν τη συμπεριφορά δικτύων σε διάφορες συνθήκες και να αναπτύξουν καινοτόμες λύσεις για τις προκλήσεις των ασύρματων δικτύων. Με το Mininet-WiFi, Singh et al. (Singh, 2014). οι χρήστες μπορούν να προσομοιώσουν διάφορες διαμορφώσεις του δικτύου, να πειραματιστούν με διαφορετικά πρωτόκολλα και να εξετάσουν την απόδοση και την αξιοπιστία των ασύρματων δικτύων. Αυτό επιτρέπει στους ερευνητές να εξερευνήσουν νέες τεχνολογίες και πρωτόκολλα, καθώς και να βελτιώσουν την απόδοση και την ασφάλεια των ασύρματων δικτύων.

Με βάση αυτές τις δυνατότητες, το Mininet-WiFi αποτελεί ένα ισχυρό εργαλείο για την ανάπτυξη και την εξέλιξη της έρευνας στον τομέα των ασύρματων δικτύων και του λογισμικού ορισμένου δικτύου. Παρέχει ένα περιβάλλον δοκιμών που είναι εύκολο στη χρήση και ευέλικτο, επιτρέποντας στους ερευνητές να αναπτύξουν νέες ιδέες και να εξερευνήσουν νέες προσεγγίσεις στον τομέα των ασύρματων επικοινωνιών. Με την ενσωμάτωση του υποσυστήματος ασύρματου δικτύου (Wi-Fi) στο περιβάλλον του Mininet, ανοίγει ένα νέο φάσμα δυνατοτήτων για τους ερευνητές και τους προγραμματιστές δικτύων. Μερικά από τα κύρια πλεονεκτήματα της χρήσης του Wi-Fi στο πλαίσιο του Mininet:

Πλεονεκτηματα Mininet WiFi

- **Προσομοίωση Ασύρματων Δικτύων:** Το Mininet-WiFi αποτελεί ένα εξαιρετικό εργαλείο για προσομοίωση ασύρματων δικτύων. Επιτρέπει τη δημιουργία περιβάλλοντος δοκιμής που μοιάζει με πραγματικά ασύρματα δίκτυα Kushi et al. (Kushi, 2019), επιτρέποντας τη διερεύνηση και την αξιολόγηση των εφαρμογών και των πρωτοκόλλων.
- **Ευκολία Προγραμματισμού:** Το Mininet-WiFi χρησιμοποιεί τη γλώσσα προγραμματισμού Python, που είναι ευέλικτη και διευκολύνει τη δημιουργία των τοπολογιών και την εκτέλεση των πειραμάτων. Οι χρήστες μπορούν να δημιουργήσουν, να προσαρμόσουν και να επεκτείνουν εύκολα τα πειράματά τους.
- **Επέκταση του Mininet:** Το Mininet-WiFi επιτρέπει τη σύνδεση ασύρματων κόμβων με τους ενσύρματους Jany et al. (Jany, 2017,) δημιουργώντας ολοκληρωμένες τοπολογίες που μπορούν να περιλαμβάνουν διαφορετικούς τύπους δικτύων.

- **Υποστήριξη Πολλών Πρωτοκόλλων:** Ο υπολογιστικός πυρήνας του Mininet-WiFi υποστηρίζει διάφορα ασύρματα πρωτόκολλα και τεχνολογίες, όπως 802.11a/b/g/n/ac, Mesh, Ad-hoc, έτσι ώστε οι χρήστες να μπορούν να ερευνήσουν τις επιδόσεις και τη συμπεριφορά των δικτύων σε διάφορες περιπτώσεις.
- **Εκπαιδευτική Χρήση:** Είναι πολύ χρήσιμο για εκπαιδευτικούς, φοιτητές και ερευνητές, καθώς επιτρέπει την πρακτική εξάσκηση σε ασύρματες τεχνολογίες δικτύων Enayet et al. (Enayet , 2019). ,βοηθώντας στην κατανόηση των αρχών και των πρωτοκόλλων που τα χαρακτηρίζουν.
- **Ενσωμάτωση Τεχνολογιών:** Η ενσωμάτωση ασύρματων τεχνολογιών στο Mininet επιτρέπει την εξέλιξη και την ανάπτυξη νέων τεχνολογιών στον τομέα των ασύρματων δικτύων.

6.2.3.Μειονεκτήματα Mininet WiFi

Παρά τα πλεονεκτήματα που έχει το Mininet WiFi πρέπει να ληφθούν υπόψη και τα ακόλουθα μειονεκτήματα :

- **Περιορισμένες Επιδόσεις:** Αν και το Mininet-WiFi παρέχει προσομοίωση ασύρματων δικτύων, οι επιδόσεις της προσομοίωσης μπορεί να μην αντικατοπτρίζουν πλήρως την πραγματικότητα. Αυτό οφείλεται στις απλοποιήσεις που γίνονται σε επίπεδο προσομοίωσης Manzoor et al. (Manzoor , 2020).
- **Απαιτήσεις Υπολογιστικών Πόρων:** Η δημιουργία περίπλοκων τοπολογιών ή η προσομοίωση μεγάλων ασύρματων δικτύων μπορεί να απαιτεί αρκετούς πόρους υπολογιστή, όπως CPU και μνήμη, ιδιαίτερα όταν το Mininet-WiFi τρέχει σε εικονικό περιβάλλον.
- **Περιορισμένη Υποστήριξη Ασύρματων Πρωτοκόλλων:** Παρόλο που υποστηρίζονται πολλά ασύρματα πρωτόκολλα, ενδέχεται να μην υποστηρίζονται όλες οι τελευταίες εκδόσεις ή χαρακτηριστικά πρωτοκόλλων, εξαρτάται από το επίπεδο υποστήριξης του εργαλείου.
- **Περιορισμένες Δυνατότητες Ανάλυσης:** Μπορεί να είναι περιορισμένη στην εκτέλεση προχωρημένων λειτουργιών ανάλυσης και μετρήσεων Purwita et al . (Purwita ,2022), καθώς επικεντρώνεται κυρίως στην προσομοίωση της συμπεριφοράς του δικτύου.
- **Απαιτεί Ειδικές Γνώσεις:** Για να εκμεταλλευτεί κανείς πλήρως τις δυνατότητες του Mininet-WiFi, απαιτούνται γνώσεις σε ασύρματα δίκτυα, ασύρματα πρωτόκολλα και προγραμματισμό δικτύων.

Παρόλα αυτά, αν και τα μειονεκτήματα αυτά πρέπει να ληφθούν υπόψη, το Mininet Wi-Fi παραμένει ένα ισχυρό εργαλείο για την ανάπτυξη, δοκιμή και αξιολόγηση εφαρμογών και πρωτοκόλλων σε ασύρματα δίκτυα.

6.3 Γενικός δείκτης επιδόσεων (GPI) για την αξιολόγηση του δικτύου SDWN

Γενικά, οι παράγοντες αξιολόγησης της απόδοσης μπορούν να χωριστούν σε δύο βασικές κατηγορίες: αυτοί που βελτιώνουν την απόδοση του δικτύου όταν αυξάνονται (π.χ. ρυθμός μετάδοσης) και αυτοί που βελτιώνουν την απόδοση του δικτύου όταν μειώνονται (π.χ. καθυστέρηση, κόστος κ.λπ.).

Ας δούμε πρακτικά τους παράγοντες της πρώτης ομάδας (μεγιστοποιημένοι) ως εξής: $m^{max} = m_1^{max}, m_2^{max}, \dots, m_p^{max}$ όπου p απεικονίζει τον αριθμό των μεγιστοποιημένων παραγόντων. Με τον ίδιο τρόπο, ας συμβολίσουμε τους παράγοντες της δεύτερης ομάδας (ελαχιστοποιημένοι) ως εξής: $m^{min} = m_1^{min}, m_2^{min}, \dots, m_r^{min}$ όπου r είναι ο αριθμός των ελαχιστοποιημένων παραγόντων. Η βασική ιδέα είναι να βρεθεί ένας γενικός δείκτης που να ενσωματώνει όλες τις τάσεις των επιμέρους συντελεστών και να μπορεί να μας υποδείξει με απλό τρόπο πόσο καλύτερο είναι ένα δίκτυο σε σχέση με ένα άλλο. Ας θεωρήσουμε δύο δίκτυα a και b που έχουν r αριθμό ελαχιστοποιημένων παραγόντων- μπορούμε να πούμε ότι αν $\sum_{j=1}^r (m_{a,j}^{min})^2 \leq \sum_{j=1}^r (m_{b,j}^{min})^2$, το δίκτυο a είναι καλύτερο από το δίκτυο b . Τα παραπάνω αθροίσματα αντιπροσωπεύουν την ευκλείδεια απόσταση των ελαχιστοποιημένων συντελεστών απόδοσης. Κάθε διάσταση απεικονίζει τον διανυσματικό χώρο ενός μεμονωμένου παράγοντα απόδοσης. Για να γίνει πιο συμπαγής η εμφάνιση αυτού του τύπου, μπορεί να ονομαστεί γενικός δείκτης απόδοσης (GPI) και η μορφή του θα είναι:

$$GPI = \sqrt{\sum_{i=1}^r (m_i^{min})^2}$$

Σε αυτή την περίπτωση, για δύο δίκτυα, δίκτυο a και δίκτυο b , εάν $GPI_a \leq GPI_b$, τότε το δίκτυο a είναι ισχυρότερο από το δίκτυο b . Ο όρος m_i^{min} είναι η τιμή

κανονικοποίησης και οι τιμές που προκύπτουν κυμαίνονται μεταξύ 0 και 1. Όταν χρησιμοποιούμε αυτόν τον τύπο για όλους τους μικρούς παράγοντες, τους κάνει όλους ίδιους. Έτσι, ακόμα κι αν οι παράγοντες μετρηθούν διαφορετικά, μπορούμε να τους συγκρίνουμε με τον ίδιο τρόπο. Αυτό μας βοηθά να καταλάβουμε τη συνολική απόδοση των παραγόντων. Ο GPI για τους ελαχιστοποιημένους παράγοντες μπορεί να οριστεί ως εξής:

$$GPI = \sqrt{\sum_{i=1}^r \left(\frac{m_i^{\min}}{\max(m_i^{\min})} \right)^2}$$

Ανάλογα το GPI για τους p μεγιστοποιημένους παράγοντες μπορεί να εκφραστεί ως εξής:

$$GPI = \sqrt{\sum_{j=1}^p \left(1 - \frac{m_j^{\max}}{\max(m_j^{\max})} \right)^2}$$

Για να συνδυαστούν και οι δύο ομάδες παραγόντων, ο GPI ορίζεται από την ακόλουθη εξίσωση:

$$GPI(w_i, w_j) = \sqrt{\frac{\sum_{i=1}^r w_i \left(\frac{m_i^{\min}}{\max(m_i^{\min})} \right)^2 + \sum_{j=1}^p w_j \left(1 - \frac{m_j^{\max}}{\max(m_j^{\max})} \right)^2}{\sum_{i=1}^r w_i + \sum_{j=1}^p w_j}}$$

Στους προηγούμενους τύπους, όλοι οι συντελεστές θεωρούνται ισοβαρείς. Ωστόσο, λόγω της φύσης ορισμένων προβλημάτων, συχνά ορισμένοι παράγοντες θεωρούνται πιο σημαντικοί από άλλους, βάσει των απαιτήσεων των εφαρμογών. Σε προβλήματα πολλαπλών κριτηρίων, η καθορισμένη βαρύτητα κάθε παραμέτρου αποτελεί ταυτόχρονα πρόβλημα λήψης αποφάσεων και θέμα σχεδιασμού. Έτσι, σε αυτές τις περιπτώσεις, κάθε παράγοντας πολλαπλασιάζεται με ένα ειδικό βάρος που αντιστοιχεί στη σημασία του. Ως αποτέλεσμα, ο τελικός τύπος μπορεί να περιγραφεί όπως απεικονίζεται από κάτω, όπου W_i και W_j αντιπροσωπεύουν τα βάρη των κανονικοποιημένων παραμέτρων του δικτύου. Ο GPI κυμαίνεται από 0 έως 1.

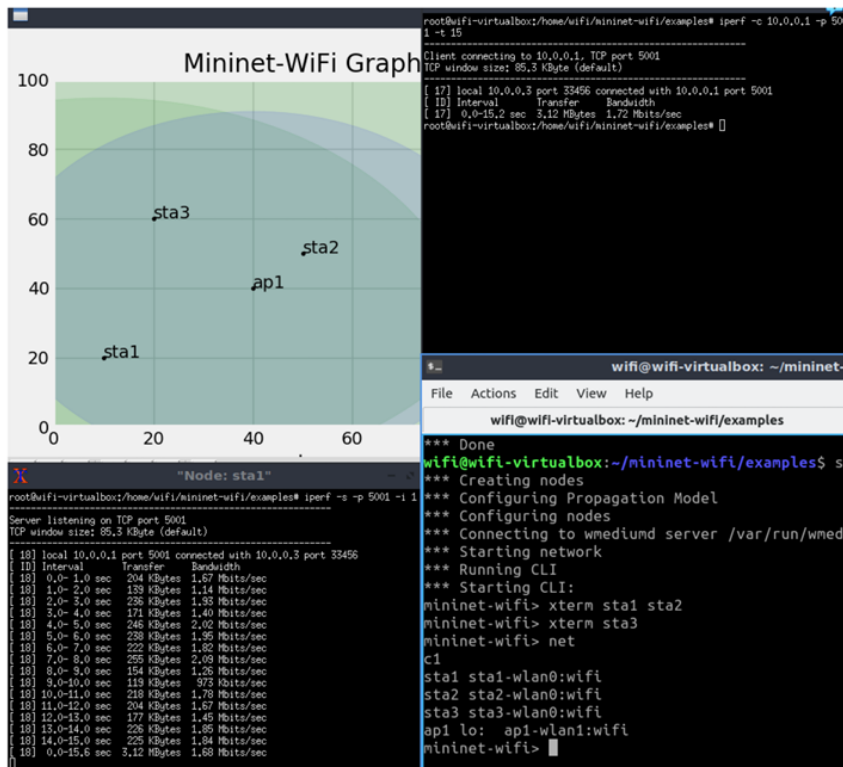
Συνεπώς, καθώς η τιμή του GPI μειώνεται, η συνολική απόδοση του δικτύου βελτιώνεται.

$$GPI(w_l, w_f) = \sqrt{\frac{\sum_{l=1}^r w_l \left(\frac{m_l^{\min}}{\max(m_l^{\min})} \right)^2 + \sum_{f=1}^p w_f \left(1 - \frac{m_f^{\max}}{\max(m_f^{\max})} \right)^2}{\sum_{l=1}^r w_l + \sum_{f=1}^p w_f}}$$

7. Προσομοίωση και αποτελέσματα

7.1 ΜΕΘΟΔΟΛΟΓΙΑ

Η τεχνολογία δικτύου που καθορίζεται από λογισμικό (SDN) μπορεί να προσφέρει στα ασύρματα δίκτυα τα πλεονεκτήματα του απλουστευμένου ελέγχου και της διαχείρισης του δικτύου. Αυτή η τεχνολογία υποκατηγορία SDN ονομάζεται ασύρματο δίκτυο καθορισμένο από λογισμικό (SDWN). Στην παρούσα μελέτη αξιολογείται η απόδοση τεσσάρων ελεγκτών σε περιβάλλον SDWN, δεδομένου ότι ο ελεγκτής είναι το σημαντικότερο στοιχείο ολόκληρου του δικτύου. Χρησιμοποιώντας την πλατφόρμα Mininet-WiFi, η απόδοση κάθε ελεγκτή αξιολογείται ως προς την απόδοση, την καθυστέρηση, το Jitter και την απώλεια πακέτων. Επιπλέον, εισάγεται και εφαρμόζεται μια αξιολόγηση με πολλαπλά κριτήρια για την παροχή μιας δίκαιης σύγκρισης μεταξύ των SDWN. Αυτή η μελέτη παρέχει μια κατάλληλη διαμόρφωση των SDWN που είναι χρήσιμη για τη μηχανική δικτύων και μπορεί να χρησιμοποιηθεί για τη βελτιστοποίηση της απόδοσης των SDWN. Όπως προαναφέραμε οι ελεγκτές που χρησιμοποιήθηκαν είναι οι ONOS, Ryu, POX και OpenDayLight (ODL). Για τα πειράματα μας χρησιμοποιήσαμε τη γραμμική τοπολογία (linear topology). Σε αυτή την τοπολογία, κάθε σημείο πρόσβασης συνδέεται με τον ελεγκτή και κάθε ασύρματος σταθμός συνδέεται με ένα σημείο πρόσβασης. Ο αριθμός των σημείων πρόσβασης και των ασύρματων σταθμών κυμαίνεται από 25 έως 100. Κατά τη δημιουργία της τοπολογίας, επιλέξαμε τυχαία ζεύγη κόμβων και εκτελέσαμε δοκιμές απόδοσης για ορισμένο χρονικό διάστημα. Η **εικόνα 0-1** παρακάτω, μας δείχνει ένα απλό παράδειγμα περιβάλλοντος προσομοίωσης.



Εικόνα 0-1 Mininet-WiFi και ελεγκτής POX

Για τη μέτρηση της απόδοσης χρησιμοποιείται ένα ενεργό εργαλείο μέτρησης, το iperf. Κάθε δοκιμή iperf δημιουργεί κίνηση TCP και οι μεταδόσεις πραγματοποιούνται για 60 s. Για την καταμέτρηση της καθυστέρησης, του jitter και της απώλειας πακέτων χρησιμοποιείται το εργαλείο δικτύου ring. Στην περίπτωση αυτή, ο πρώτος κόμβος στέλνει μια ακολουθία 10 πακέτων στον τελευταίο κόμβο. Η δοκιμή ring επαναλαμβάνεται 10 φορές και υπολογίζεται ο μέσος όρος κάθε μετρικής.

7.2 Μετρικές Πειραμάτων

- ✓ Throughput: Απόδοση
- ✓ RTT Latency: Μέσος όρος καθυστέρησης
- ✓ Packet Loss: Απώλεια πακέτων
- ✓ Average Jitter: Μέσος όρος Διακύμανσης

7.3 Πειραματικό Πλαίσιο

Για την πραγματοποίηση της έρευνας και των πειραμάτων, χρησιμοποιήθηκε υπολογιστής με τους εξής πόρους:

1. Επεξεργαστής: Intel Core i5-9400F 6-Core Processor στα 2.90 GHz
2. Μνήμη RAM: Corsair Vengeance LPX 16GB (2 x 8GB) DDR4 3200MHz
3. Κάρτα γραφικών: NVIDIA GeForce GTX 1650 4GB GDDR6
4. Μητρική: ASUS Prime B365M-A Micro ATX με Intel LGA1151 Socket
5. Σκληρός Δίσκος: Crucial MX500 500GB SATA SSD

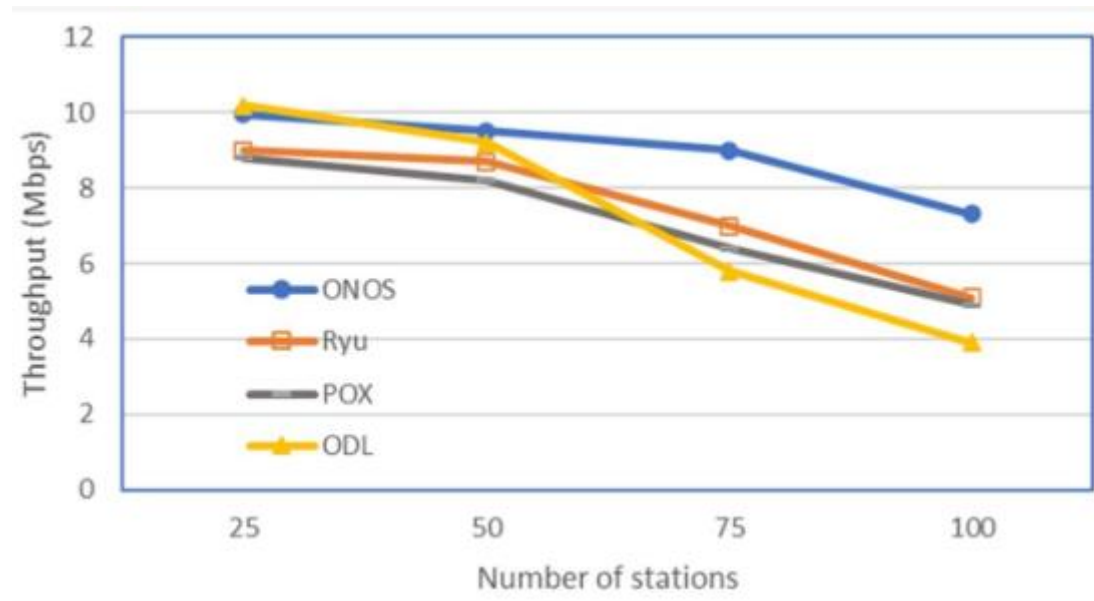
Το περιβάλλον όπου χρησιμοποιήσαμε για να πραγματοποιήσουμε τις μετρήσεις αλλά και να τρέξουμε τους ελεγκτές καθώς και το Mininet-WiFi, ήταν η μηχανή Ubuntu 22.04. Εδώ να επισημάνουμε πως μετά από κάθε εκτέλεση ενός πειράματος, πριν προχωρήσουμε στο επόμενο ακολουθήσαμε την διαδικασία εκκαθάρισης που μας προσφέρει το Mininet-WiFi. Συνοπτικά για να πάρουμε τις μετρήσεις μας, ακολουθήσαμε τα εξής βήματα:

- ✓ Εκτέλεση του ελεγκτή SDN.
- ✓ Ανάπτυξη της τοπολογίας δικτύου, χρησιμοποιώντας το Mininet-WiFi.
- ✓ Χρήση διαφόρων εργαλείων δικτύου, όπως το iperf και το ping, για τη συλλογή μετρήσεων απόδοσης.

7.4 Αποτελέσματα

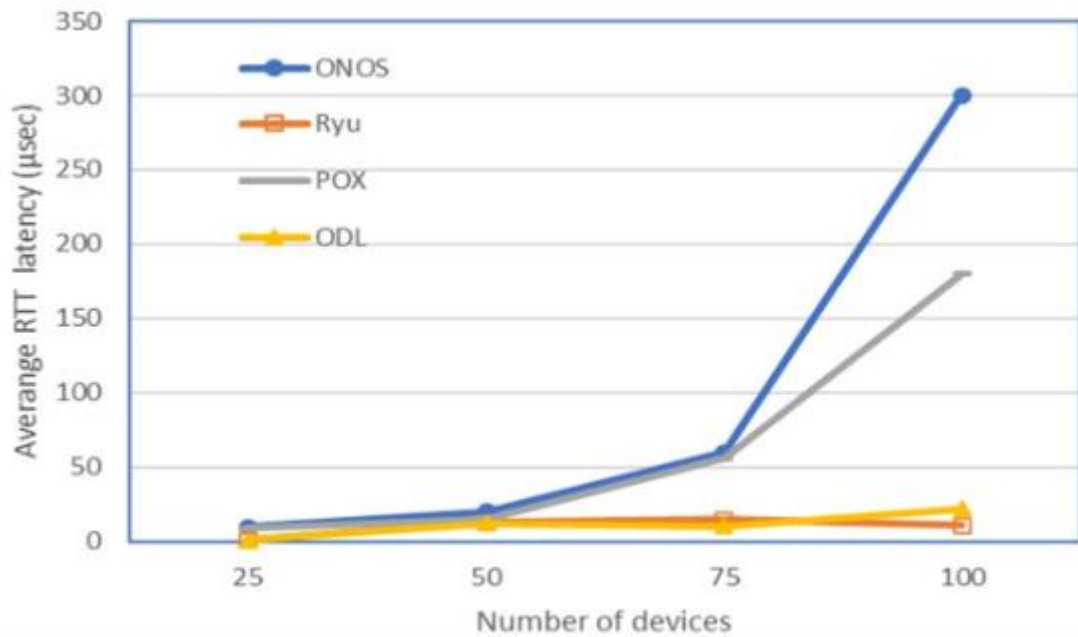
Σε αυτή την ενότητα παρουσιάζουμε τα αποτελέσματα και τις μετρικές που πήραμε από τα πειράματα μας, όσον αφορά θέματα καθυστέρησης και απόδοσης.

- **Throughput: Απόδοση**



Εικόνα 0-2 Ο μ.ό. απόδοσης σε συνάρτηση με τον αριθμό των ασύρματων συσκευών στο SDWN

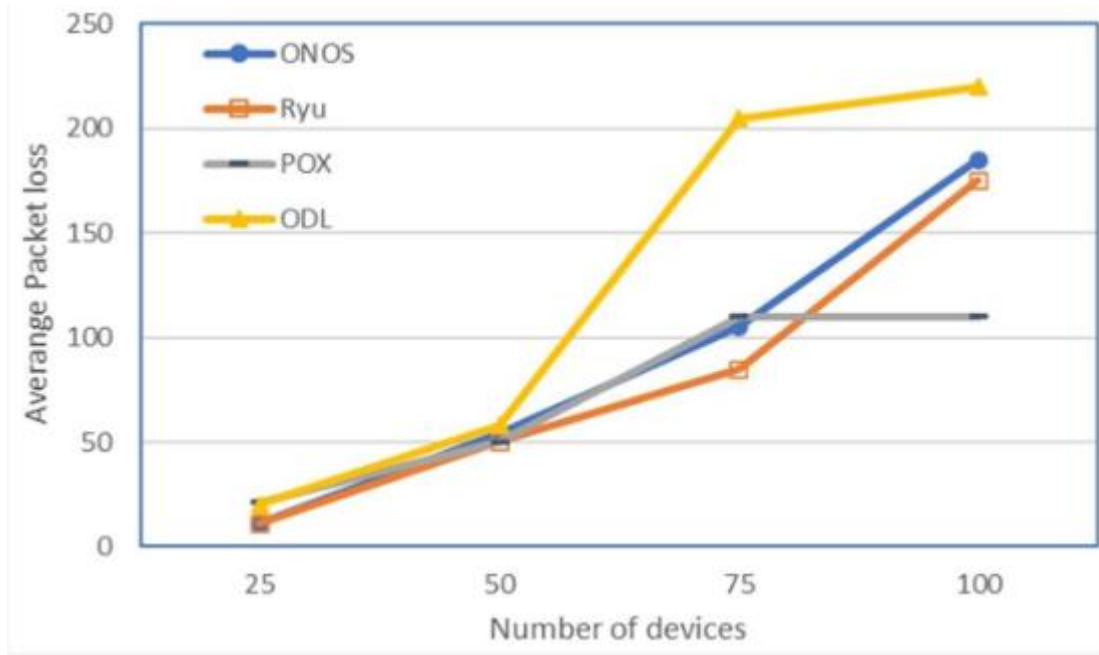
- **RTT Latency: Μέσος όρος καθυστέρησης**



Εικόνα 0-3 Μέση καθυστέρηση σε συνάρτηση με τον αριθμό των ασύρματων συσκευών στο SDWN

Το γράφημα (Εικόνα 0-3) παρουσιάζει τη μέση καθυστέρηση RTT των τεσσάρων ελεγκτών σε σχέση με τον πληθυσμό των συσκευών του SDWN. Σύμφωνα με τα δεδομένα, οι ελεγκτές Ryu και ODL εμφανίζουν τις καλύτερες (χαμηλότερες) τιμές καθυστέρησης RTT. Για παράδειγμα, για έναν πληθυσμό 100 συσκευών, οι τιμές είναι 10,8 ms και 22 ms αντίστοιχα. Αντίθετα, οι ελεγκτές ONOS και POX, ιδιαίτερα ο ελεγκτής ONOS (απεικονίζεται από τη μπλε γραμμή), δείχνουν ασυνήθιστα υψηλές τιμές καθυστέρησης πακέτων, οι οποίες αποτελούν τη χειρότερη περίπτωση.

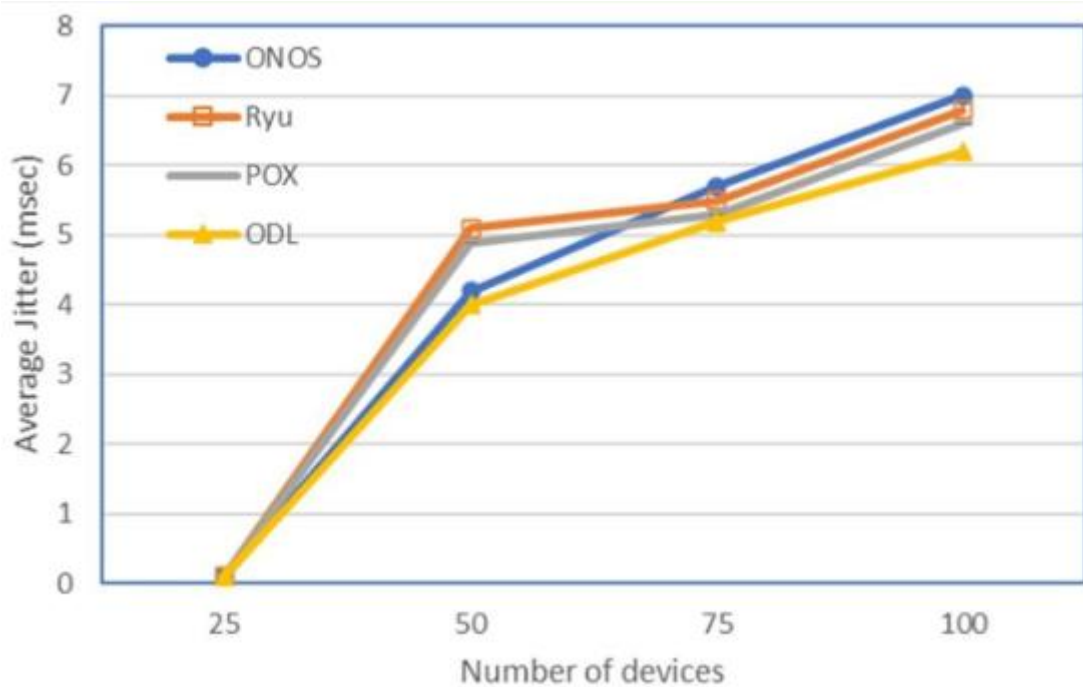
- **Packet Loss: Απώλεια πακέτων**



Εικόνα 0-4 Μέση απώλεια πακέτων σε συνάρτηση με τον αριθμό των ασύρματων συσκευών στο SDWN

Το διάγραμμα που παρουσιάζεται στην Εικόνα 0-4 αποτυπώνει τη μέση απώλεια πακέτων σε σχέση με τον αριθμό των ασύρματων συσκευών στο SDWN για τους τέσσερις ελεγκτές. Μια πρώτη ματιά στο διάγραμμα αποκαλύπτει ότι ο ελεγκτής ODL, που αναπαρίσταται από την κίτρινη γραμμή, εμφανίζει τη χειρότερη συμπεριφορά, καθώς παρουσιάζει τις υψηλότερες τιμές απώλειας πακέτων σε όλες τις περιπτώσεις. Ωστόσο, παρατηρείται ότι ο ελεγκτής POX δείχνει ένα σχετικά σταθερό ποσοστό απώλειας πακέτων για αριθμό συσκευών μεγαλύτερο από 75, το οποίο είναι επίσης ιδιαίτερα χαμηλό σε σύγκριση με τους άλλους ελεγκτές. Ενδιαφέρον παρουσιάζει και η ενδιάμεση ζώνη, όπου ο ελεγκτής Ryu, που απεικονίζεται από την πορτοκαλί γραμμή, παρέχει την καλύτερη συμπεριφορά με χαμηλότερη απώλεια πακέτων.

- Average Jitter: Μέσος όρος Διακύμανσης



Εικόνα 0-5 Μέσο Jitter σε σχέση με τον αριθμό των ασύρματων συσκευών στο SDWN

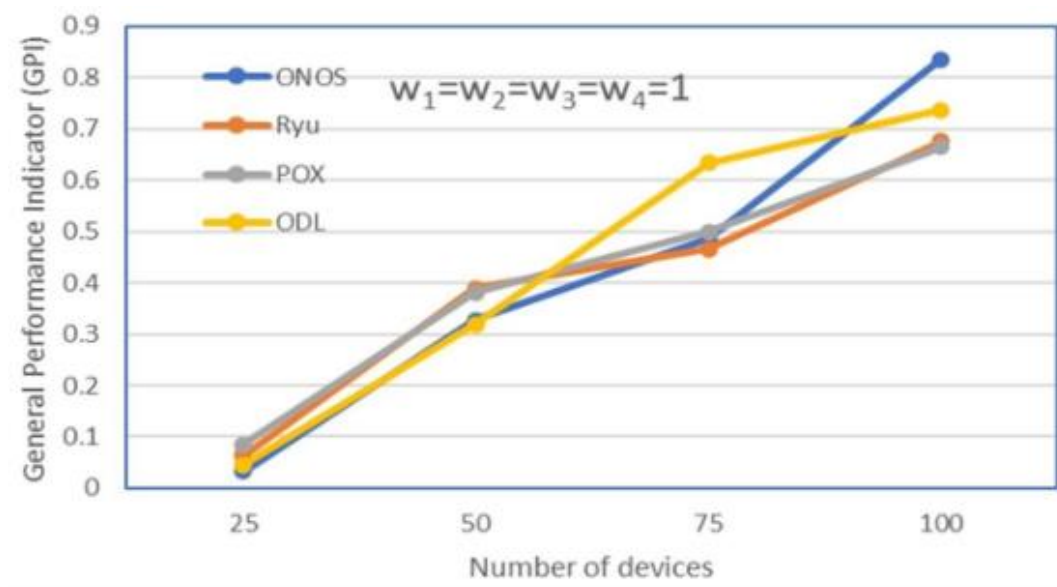
Το γράφημα παρουσιάζει το μέσο jitter (σε ms) σε σχέση με τον πληθυσμό των συσκευών του SDWN για τους τέσσερις ελεγκτές. Από τα δεδομένα φαίνεται ότι ο ελεγκτής ODL παρουσιάζει το χαμηλότερο jitter σε όλες τις περιπτώσεις (κίτρινη γραμμή). Επιπλέον, για πληθυσμό συσκευών μεγαλύτερο από 75, ο ελεγκτής ONOS θα πρέπει να αποφεύγεται εάν ο παράγοντας jitter είναι σημαντικός για μια συγκεκριμένη εφαρμογή.

Ωστόσο, για να αξιολογήσουμε τα διάφορα SDWN που περιγράφονται από διαφορετικούς παράγοντες απόδοσης, απαιτείται μια εξειδικευμένη μεθοδολογία προκειμένου να διαπιστώσουμε ποιο από τα δίκτυα εμφανίζει την ανώτερη συμπεριφορά. Για την αντιμετώπιση αυτού του προβλήματος, προτείνεται μια μεθοδολογία που μας βοηθά να αξιολογήσουμε ποιο δίκτυο εμφανίζει τις καλύτερες επιδόσεις σε σχέση με τον αριθμό των ασύρματων συσκευών.

7.5 Αποτελέσματα του γενικού συντελεστή απόδοσης (GPI)

Από τις αρχικές δοκιμές προέκυψε μια ενδιαφέρουσα συσχέτιση μεταξύ της απόδοσης των ελεγκτών SDWN και των διαφόρων παραμέτρων όπως η καθυστέρηση πακέτων RTT, το jitter και άλλες. Αυτή η συσχέτιση αναδεικνύει ότι όσο καλύτερες είναι οι επιδόσεις του ελεγκτή, τόσο χαμηλότερες είναι οι τιμές των παραμέτρων αυτών και αντιστρόφως. Επιπλέον, επισημαίνεται η σπουδαιότητα της κανονικοποίησης των παραγόντων απόδοσης προκειμένου να δημιουργηθεί ένα κοινό πλαίσιο αναφοράς για τη σύγκριση των ελεγκτών. Καθώς κάθε παράγοντας επιδόσεων έχει διαφορετική σημασία και εύρος τιμών, η κανονικοποίησή τους είναι αναγκαία για τη διαμόρφωση μιας δικαιολογημένης σύγκρισης. Με βάση αυτήν την προσέγγιση, ο τελικός δείκτης GPI είναι αντιπροσωπευτικός της συνολικής απόδοσης του δικτύου, όπου χαμηλότερες τιμές υποδεικνύουν καλύτερες επιδόσεις.

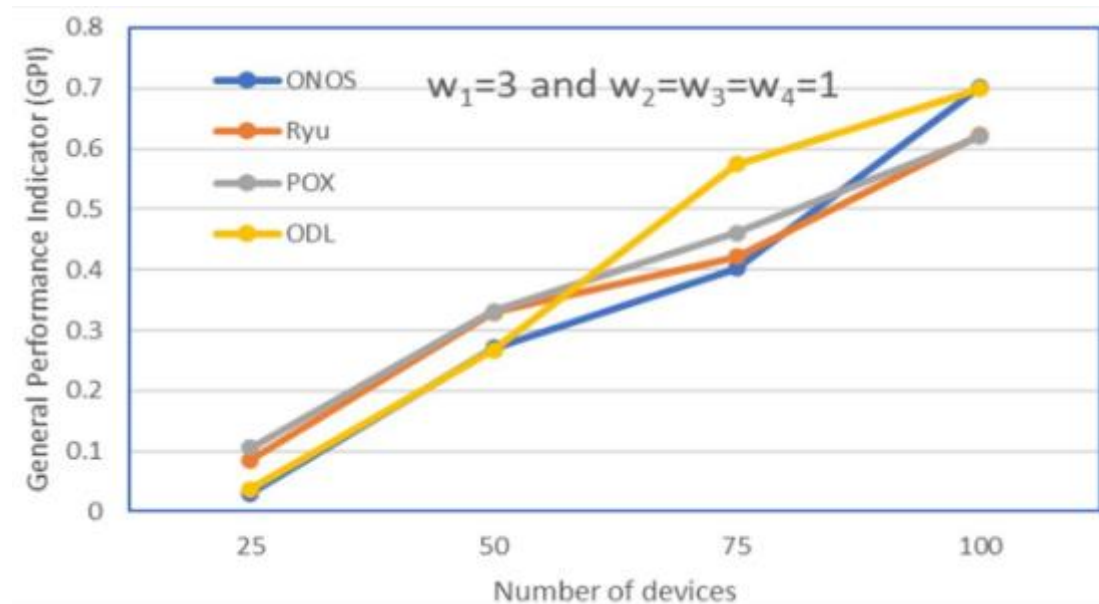
Το διάγραμμα στο Σχήμα 0-6 παρουσιάζει τις τιμές του Γενικού Δείκτη Απόδοσης (GPI) για ένα SDWN σε σχέση με τον πληθυσμό των ασύρματων συσκευών που διαθέτει το δίκτυο για τους τέσσερις ελεγκτές που εξετάζονται. Οι τιμές του GPI υπολογίστηκαν με την υπόθεση ότι οι τέσσερις παράγοντες απόδοσης έχουν ίσα βάρη.



Εικόνα 0-6 Τιμές γενικών δεικτών απόδοσης σε συνάρτηση με τον αριθμό των ασύρματων συσκευών θεωρώντας ότι οι τέσσερις παράγοντες απόδοσης έχουν ίση βαρύτητα

Από το διάγραμμα παρατηρούμε ότι για πληθυσμούς συσκευών μεγαλύτερους από 72, οι ελεγκτές Ryu και POX εμφανίζουν αξιόπιστη απόδοση. Αντίθετα, για μικρότερους πληθυσμούς συσκευών, οι ελεγκτές ONOS και ODL εμφανίζονται πιο κατάλληλοι ως προς την απόδοση. Στο Σχήμα 8 παρουσιάζονται οι τιμές του Γενικού

Δείκτη Απόδοσης (GPI) για ένα SDWN σε σχέση με τον πληθυσμό των ασύρματων συσκευών για τους τέσσερις ελεγκτές υπό μελέτη. Σε αυτήν την περίπτωση, υποθέτουμε ότι ο παράγοντας της απόδοσης θεωρείται ο πιο σημαντικός παράγοντας ($w_1 = 3, w_2 = w_3 = w_4 = 1$).

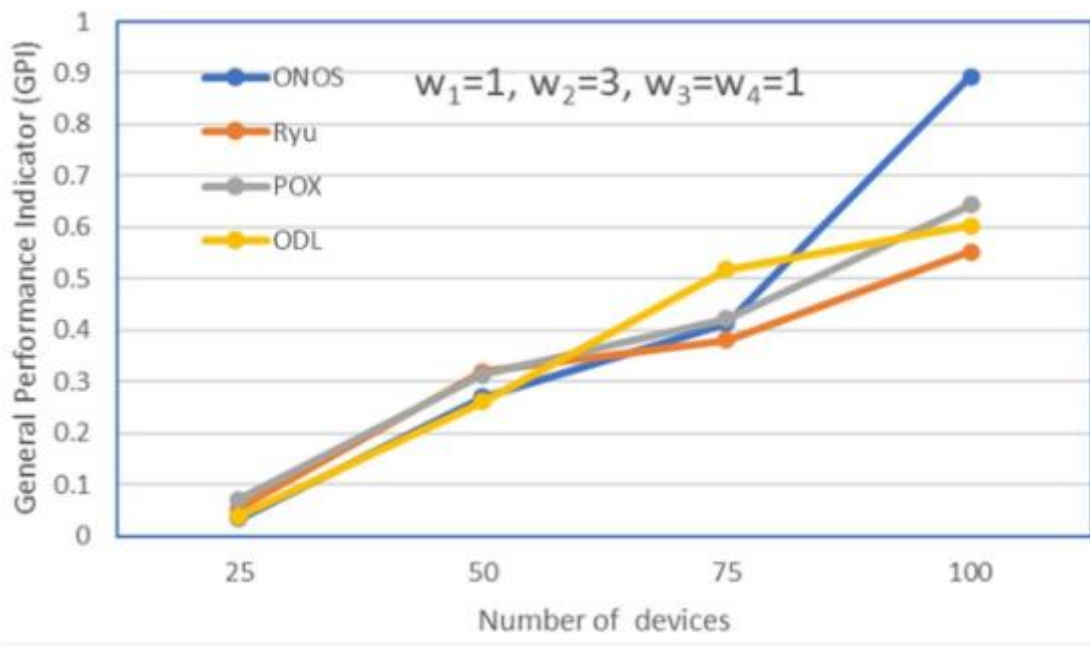


Εικόνα 0-7 Γενικός δείκτης απόδοσης ενός δικτύου SDWN σε σχέση με τον αριθμό των ασύρματων συσκευών, λαμβάνοντας υπόψη την απόδοση ως σημαντικό παράγοντα απόδοσης ($w_1 = 3$)

Από το διάγραμμα προκύπτει ότι οι ελεγκτές Ryu και POX διατηρούν την υψηλότερη συνολική απόδοση για πληθυσμούς συσκευών που υπερβαίνουν τις 80 μονάδες. Σε δίκτυα με πληθυσμό μεταξύ 50 και 78 συσκευών, ο ελεγκτής ONOS προσφέρει την υψηλότερη απόδοση όπου απεικονίζεται με μπλε γραμμή, ενώ για μικρότερα δίκτυα δηλαδή κάτω από πενήντα συσκευές, οι ελεγκτές ONOS και ODL συνεχίζουν να παρέχουν την καλύτερη απόδοση.

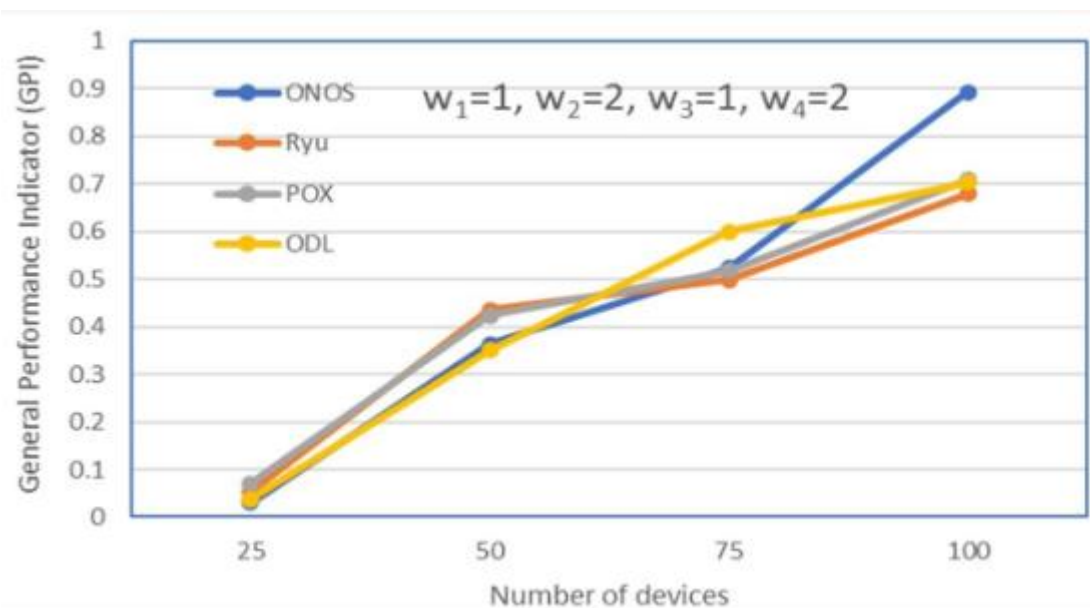
Από την άλλη πλευρά, υπάρχουν εφαρμογές που απαιτούν χαμηλή καθυστέρηση μετάδοσης πακέτων και χαμηλό jitter, όπως εφαρμογές πραγματικού χρόνου, ροή βίντεο, φωνητική επικοινωνία μέσω IP κ.λπ. Σε τέτοιες περιπτώσεις, η καθυστέρηση RTT των πακέτων και το jitter θεωρούνται κρίσιμοι παράγοντες. Το Σχήμα 0-8 δείχνει ότι για πληθυσμούς συσκευών άνω των 60, ο ελεγκτής Ryu προσφέρει την καλύτερη συνολική απόδοση (απεικονιζόμενη με πορτοκαλί γραμμή).

Ωστόσο, για μικρότερους πληθυσμούς συσκευών, οι ελεγκτές ONOS και ODL εμφανίζουν καλύτερες επιδόσεις.



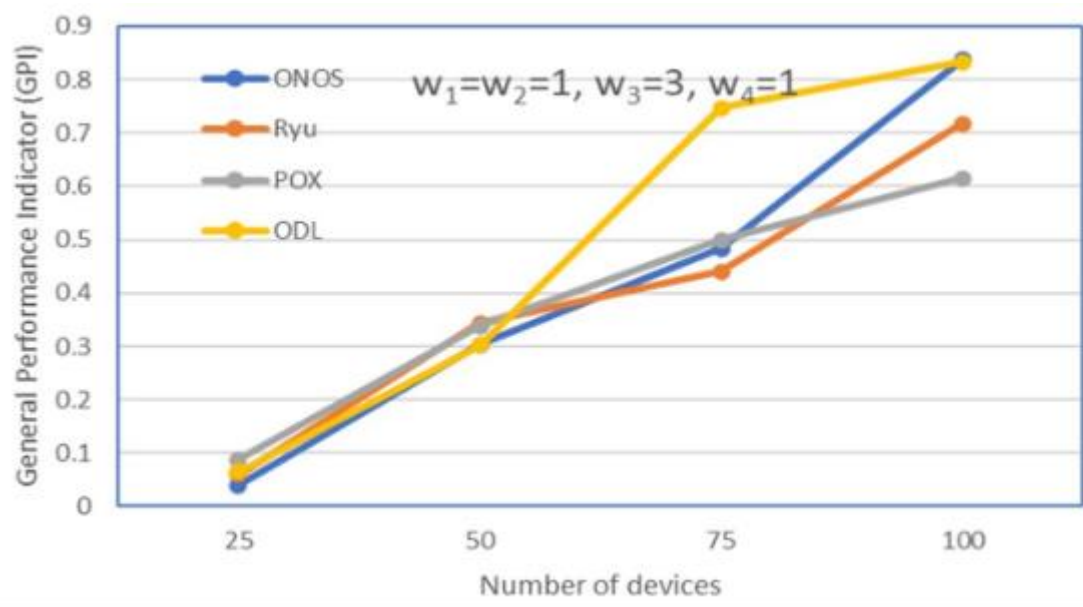
Εικόνα 0-8 Γενικές τιμές δεικτών απόδοσης ενός SDWN σε σχέση με τον αριθμό των ασύρματων συσκευών, λαμβάνοντας υπόψη ότι η καθυστέρηση RTT είναι ο σημαντικότερος παράγοντας απόδοσης ($w_2=3$)

Επιπλέον, το Σχήμα 0-9 εμφανίζει τις τιμές GPI που λαμβάνονται για τους τέσσερις ελεγκτές όταν η καθυστέρηση RTT και το jitter έχουν βάρη 2. Το διάγραμμα αποκαλύπτει ότι οι ελεγκτές Ryu και POX παραμένουν η καλύτερη επιλογή για πληθυσμούς συσκευών μεγαλύτερους από 70 (πορτοκαλί και γκρι γραμμές).



Εικόνα 0-9 Γενικές τιμές δεικτών απόδοσης ενός SDWN σε σχέση με τον αριθμό των συσκευών, λαμβάνοντας υπόψη την καθυστέρηση RTT και το jitter ως τους σημαντικότερους παράγοντες απόδοσης ($w_2 = 2$ και $w_4 = 2$)

Τέλος, υπάρχουν εφαρμογές που δεν μπορούν να ανεχθούν την απώλεια πακέτων λόγω της φύσης τους, όπως οι λογιστικές ή χρηματιστηριακές εφαρμογές. Είναι προφανές ότι αυτή η απαίτηση πρέπει να ικανοποιείται από το δίκτυο. Σε αυτά τα σενάρια, ο σημαντικότερος παράγοντας είναι η απώλεια πακέτων. Στο Σχήμα 0-10 παρουσιάζονται οι τιμές GPI για διάφορους πληθυσμούς συσκευών, όταν η απώλεια πακέτων έχει βαρύτητα 3.



Εικόνα 0-10 Γενικές τιμές δεικτών απόδοσης ενός SDWN σε σχέση με τον αριθμό των ασύρματων συσκευών, λαμβάνοντας υπόψη ότι η απώλεια πακέτων είναι ο πιο σημαντικός παράγοντας απόδοσης ($w_3 = 3$)

Αυτή η απεικόνιση δείχνει πως οι ελεγκτές Ryu και POX ξεχωρίζουν για τις αποδοτικές επιδόσεις τους σε σύγκριση με τους ONOS και ODL. Ειδικότερα, υπερτερούν όταν ο αριθμός των συσκευών ξεπερνά τις 70 περίπου. Το σημαντικότερο, ωστόσο, είναι ότι η χρήση του ελεγκτή ODL θα πρέπει να αποφεύγεται σε εφαρμογές που είναι ευαίσθητες στην απώλεια πακέτων λόγω του υψηλού κινδύνου απώλειας πακέτων που παρουσιάζει.

8 ΣΥΜΠΕΡΑΣΜΑΤΑ

Η παρούσα έρευνα εστιάζει στην αξιολόγηση των SDWN χρησιμοποιώντας τους πιο κοινούς ελεγκτές (ONOS, Ryu, POX και ODL). Χρησιμοποιώντας την πλατφόρμα εξομίωσης Mininet-WiFi, αναλύσαμε τέσσερις σημαντικές μετρήσεις απόδοσης για κάθε ελεγκτή (ρυθμό μετάδοσης, καθυστέρηση RTT, απώλεια πακέτων και jitter). Εφαρμόσαμε μια μεθοδολογία αξιολόγησης για τα SDWN, με έναν γενικό δείκτη επιδόσεων που παίζει σημαντικό ρόλο στη λήψη αποφάσεων για τη διαμόρφωσή τους. Από τη μελέτη αυτή είναι προφανές ότι οι ελεγκτές Ryu και POX είναι πιο ισχυροί για μεγάλα SDWN (αριθμός συσκευών μεγαλύτερος από περίπου 70) σε σύγκριση με τους άλλους δύο ελεγκτές (ONOS και ODL).

Παρά ταύτα, η μελέτη μας έχει κάποιους περιορισμούς. Διάφοροι παράγοντες που επηρεάζουν την απόδοση του δικτύου, όπως η δυναμική των ασύρματων δικτύων, η κινητικότητα των κόμβων και η ετερογένεια των συσκευών, δεν έχουν εξεταστεί πλήρως στην παρούσα έρευνα. Η τεχνολογία SDN προσφέρει πιθανές λύσεις και οφέλη για αυτούς τους περιορισμούς και μπορεί να αποτελέσει αντικείμενο μελλοντικών ερευνών.

Μελλοντικά θα μπορούσαμε να εστιάσουμε στην ανάλυση του προβλήματος της τοποθέτησης ελεγκτών (CPP) για την κατάλληλη τοποθέτηση και προσδιορισμό του αριθμού των ελεγκτών SDN σε μεγάλη κλίμακα δικτύων. Αυτός ο προσανατολισμός ερευνών θα επιτρέψει την βελτίωση της απόδοσης και την αποτελεσματική λειτουργία των SDN σε πιο σύνθετα περιβάλλοντα. Τα αποτελέσματα και η προσέγγιση της παρούσας μελέτης επιδόσεων μπορούν να αποτελέσουν πολύτιμα εργαλεία για την κατανόηση της επικοινωνίας, ειδικά στο πλαίσιο των SDN. Αυτά τα ευρήματα μπορούν να βοηθήσουν τους σχεδιαστές και τις ομάδες που ασχολούνται με την ανάπτυξη, την παρακολούθηση και τη βελτιστοποίηση των SDN, προσφέροντας σημαντική πληροφορία για την λήψη αποφάσεων και τη βελτίωση της απόδοσης των δικτύων.

9. Αναφορές

Amin, R., Reisslein, M., & Shah, N. (2018). *Hybrid SDN networks: A survey of existing approaches*. *IEEE Communications Surveys & Tutorials*, 20(4), 3259-3306.

Ahmad, S., & Mir, A. H. (2022). *SDN interfaces: protocols, taxonomy and challenges*. *Int. J. Wirel. Microwave Technol.(IJWMT)*, 12(2), 11-32.

Benzekki, K., El Fergougui, A., & Elbelrhiti Elalaoui, A. (2016). *Software-defined networking (SDN): a survey*. *Security and communication networks*, 9(18), 5803-5833.

Lantz, B., & O'Connor, B. (2015). *A mininet-based virtual testbed for distributed SDN development*. *ACM SIGCOMM Computer Communication Review*, 45(4), 365-366.

Kumar, A., Goswami, B., & Augustine, P. (2019). *Experimenting with resilience and scalability of wifi mininet on small to large sdn networks*. *International Journal of Recent Technology and Engineering*, 7(6S5), 201-207.

Keti, F., & Askar, S. (2015, February). *Emulation of software defined networks using mininet in different simulation environments*. In *2015 6th International Conference on Intelligent Systems, Modelling and Simulation* (pp. 205-210). IEEE.

Gelberger, A., Yemini, N., & Giladi, R. (2013, August). *Performance analysis of software-defined networking (SDN)*. In *2013 IEEE 21st International Symposium on Modelling, Analysis and Simulation of Computer and Telecommunication Systems* (pp. 389-393). IEEE.

Karakus, M., & Durresi, A. (2017). *A survey: Control plane scalability issues and approaches in software-defined networking (SDN)*. *Computer Networks*, 112, 279-293.

Raju, V. S. (2018, June). *SDN controllers comparison*. In *Proceedings of science globe international conference* (pp. 1-5).

Fontes, R. R., Afzal, S., Brito, S. H., Santos, M. A., & Rothenberg, C. E. (2015, November). *Mininet-WiFi: Emulating software-defined wireless networks*. In *2015 11th International Conference on Network and Service Management (CNSM)* (pp. 384-389). IEEE.

Dorsch, N., Kurtz, F., Georg, H., Hägerling, C., & Wietfeld, C. (2014, November). *Software-defined networking for smart grid communications: Applications, challenges and advantages*. In *2014 IEEE international conference on smart grid communications (SmartGridComm)* (pp. 422-427). IEEE.

Salman, O., Elhadj, I. H., Kayssi, A., & Chehab, A. (2016, April). *SDN controllers: A comparative study*. In *2016 18th mediterranean electrotechnical conference (MELECON)* (pp. 1-6). IEEE.

Valdivieso Caraguay, Á. L., Benito Peral, A., Barona Lopez, L. I., & Garcia Villalba, L. J. (2014). *SDN: Evolution and opportunities in the development IoT applications*. *International Journal of Distributed Sensor Networks*, 10(5), 735142.

- Al Mtawa, Y., Haque, A., & Lutfiyya, H. (2021). Migrating from legacy to software defined networks: A network reliability perspective. *IEEE Transactions on Reliability*, 70(4), 1525-1541.
- Al-Tarawneh, L., Alqatawneh, A., Tahat, A., & Saraereh, O. (2024). Evolution of optical networks: from legacy networks to next-generation networks. *Journal of Optical Communications*, 44(s1), s955-s970.
- Krikidis, I., Sun, Z., Laneman, J. N., & Thompson, J. (2009). Cognitive legacy networks via cooperative diversity. *IEEE Communications Letters*, 13(2), 106-108.
- Thirupathi, V., Sandeep, C. H., Kumar, N., & Kumar, P. P. (2019). A comprehensive review on sdn architecture, applications and major benefits of SDN. *International Journal of Advanced Science and Technology*, 28(20), 607-614.
- Latif, Z., Sharif, K., Li, F., Karim, M. M., Biswas, S., & Wang, Y. (2020). A comprehensive survey of interface protocols for software defined networks. *Journal of Network and Computer Applications*, 156, 102563.
- Ventre, P. L., Tajiki, M. M., Salsano, S., & Filsfils, C. (2018). SDN architecture and southbound APIs for IPv6 segment routing enabled wide area networks. *IEEE Transactions on Network and Service Management*, 15(4), 1378-1392.
- Shalimov, A., Zuikov, D., Zimarina, D., Pashkov, V., & Smeliansky, R. (2013, October). Advanced study of SDN/OpenFlow controllers. In *Proceedings of the 9th central & eastern european software engineering conference in russia* (pp. 1-6).
- Yu, J., & Al Ajarmeh, I. (2010, March). An empirical study of the NETCONF protocol. In *2010 Sixth International Conference on Networking and Services* (pp. 253-258). IEEE.
- Enns, R. (2006). NETCONF configuration protocol (No. rfc4741).
- Dorsch, N., Kurtz, F., Georg, H., Hägerling, C., & Wietfeld, C. (2014, November). Software-defined networking for smart grid communications: Applications, challenges and advantages. In *2014 IEEE international conference on smart grid communications (SmartGridComm)* (pp. 422-427). IEEE.
- Kent, S., Lynn, C., & Seo, K. (2000). Secure border gateway protocol (S-BGP). *IEEE Journal on Selected areas in Communications*, 18(4), 582-592.
- Huston, G. (2006). An Introduction to BGP—the Protocol. *The ISP Column*.
- McPherson, D., Gill, V., Walton, D., & Retana, A. (2002). Border gateway protocol (BGP) persistent route oscillation condition (No. rfc3345).
- Brandt, M., Khondoker, R., Marx, R., & Bayarou, K. (2014, July). Security analysis of software defined networking protocols—openflow, of-config and ovsdb. In *The 2014 IEEE fifth international conference on communications and electronics (ICCE 2014)*, DA NANG, Vietnam.
- Salman, O., Elhadj, I. H., Kayssi, A., & Chehab, A. (2016, April). SDN controllers: A comparative study. In *2016 18th mediterranean electrotechnical conference (MELECON)* (pp. 1-6). IEEE.

Shalimov, A., Zuikov, D., Zimarina, D., Pashkov, V., & Smeliansky, R. (2013, October). *Advanced study of SDN/OpenFlow controllers*. In *Proceedings of the 9th central & eastern european software engineering conference in russia* (pp. 1-6).

Ebeid, E., Skriver, M., Terkildsen, K. H., Jensen, K., & Schultz, U. P. (2018). *A survey of open-source UAV flight controllers and flight simulators*. *Microprocessors and Microsystems*, 61, 11-20.

Rowshanrad, S., Abdi, V., & Keshtgari, M. (2016). *Performance evaluation of SDN controllers: Floodlight and OpenDaylight*. *IIUM Engineering Journal*, 17(2), 47-57.

Bholebawa, I. Z., & Dalal, U. D. (2018). *Performance analysis of SDN/OpenFlow controllers: POX versus floodlight*. *Wireless Personal Communications*, 98, 1679-1699.

Kaur, S., Singh, J., & Ghumman, N. S. (2014, August). *Network programmability using POX controller*. In *ICCCS International conference on communication, computing & systems, IEEE* (Vol. 138, p. 70). sn.

Askar, S., & Ketii, F. (2021). *Performance evaluation of different SDN controllers: a review*.

Erickson, D. (2013, August). *The beacon openflow controller*. In *Proceedings of the second ACM SIGCOMM workshop on Hot topics in software defined networking* (pp. 13-18).

Manuel, T., & Goswami, B. H. (2019). *Experimenting with scalability of beacon controller in software defined network*. *International Journal of Recent Technology and Engineering*, 7(5S2), 550-555.

Sheikh, M. N. A., Halder, M., Kabir, S. S., Miah, M. W., & Khatun, S. (2019). *SDN-Based approach to evaluate the best controller: Internal controller NOX and external controllers POX, ONOS, RYU*. *Global Journal of Computer Science and Technology*, 19(1), 21-32.

Nguyen-Ngoc, A., Lange, S., Zinner, T., Seufert, M., Tran-Gia, P., Aerts, N., & Hock, D. (2017, November). *Performance evaluation of selective flow monitoring in the ONOS controller*. In *2017 13th International Conference on Network and Service Management (CNSM)* (pp. 1-6). IEEE.

Umeh, O. A., Akpado, K. A., Okechukwu, G. N., & Ejiogor, H. C. (2015). *Throughput and delay analysis in a real time network*. *International Journal of Engineering and Applied Sciences*, 2(12), 257775.

Tello-Oquendo, L., Akyildiz, I. F., Lin, S. C., & Pla, V. (2018, June). *SDN-based architecture for providing reliable Internet of Things connectivity in 5G systems*. In *2018 17th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net)* (pp. 1-8). IEEE.

Shah, S. A., Faiz, J., Farooq, M., Shafi, A., & Mehdi, S. A. (2013, June). *An architectural evaluation of SDN controllers*. In *2013 IEEE international conference on communications (ICC)* (pp. 3504-3508). IEEE.

OpenFlow: enabling innovation in campus networks. McKeown, Nick, et al. 2008, ACM

SIGCOMM Computer Communication Review, pp. 69-74.

Zuhran Khan Khattak, Muhammad Awais and Adnan Iqbal 2010

Gheorghe, C. M., Iurian, C. M., Luchian, E. F., Ivanciu, I. A., & Dobrota, V. (2017, September). *Applications of the Cisco APIC-EM software-defined networking controller for a virtualized testbed*. In *2017 16th RoEduNet Conference: Networking in Education and Research (RoEduNet)* (pp. 1-6). IEEE.

Cabaj, K., Wytrebowicz, J., Kuklinski, S., Radziszewski, P., & Dinh, K. T. (2014, September). *SDN Architecture Impact on Network Security*. In *FedCSIS (Position Papers)* (pp. 143-148).

Takasuo, T. (2018). *Software-Defined Networking*.

Abdullah, M. Z., Al-Awad, N. A., & Hussein, F. W. (2018). *Performance Comparison and Evaluation of Different Software Defined Networks Controllers*. *International Journal of Computing and Network Technology*, 6(2).

Neto, F. J. B. V., Miguel, C. J., de Jesus, A. C. D. S., & Sampaio, P. N. (2021, February). *SDN controllers-a comparative approach to market trends*. In *9th International Workshop on ADVANCES in ICT Infrastructures and Services (ADVANCE 2021)* (pp. 48-51).

AMMOUR, M. C., & DEBBAKH, F. *PERFORMANCE EVALUATION OF SOFTWARE DEFINED-NETWORK (SDN) CONTROLLER* (Doctoral dissertation, UNIVERSITY OF OUARGLA).

Pagola Moledo, S. (2019). *Vendor-Independent Software-Defined Networking: Beyond The Hype*.

Mamushiane, L., Lysko, A., & Dlamini, S. (2018, April). *A comparative evaluation of the performance of popular SDN controllers*. In *2018 Wireless Days (WD)* (pp. 54-59). IEEE.

Xu, H., Li, X. Y., Huang, L., Deng, H., Huang, H., & Wang, H. (2017). *Incremental deployment and throughput maximization routing for a hybrid SDN*. *IEEE/ACM Transactions on Networking*, 25(3), 1861-1875.

Zhu, L., Karim, M. M., Sharif, K., Li, F., Du, X., & Guizani, M. (2019). *SDN controllers: Benchmarking & performance evaluation*. *arXiv preprint arXiv:1902.04491*.

Yang, G., Yoo, Y., Kang, M., Jin, H., & Yoo, C. (2021, May). *Bandwidth isolation guarantee for SDN virtual networks*. In *IEEE INFOCOM 2021-IEEE Conference on Computer Communications* (pp. 1-10). IEEE.

Kumar, R., Hasan, M., Padhy, S., Evchenko, K., Piramanayagam, L., Mohan, S., & Bobba, R. B. (2017, December). *End-to-end network delay guarantees for real-time systems using SDN*. In *2017 IEEE Real-Time Systems Symposium (RTSS)* (pp. 231-242). IEEE.

Pathak, A., Pucha, H., Zhang, Y., Hu, Y. C., & Mao, Z. M. (2008). *A measurement study of internet delay asymmetry*. In *Passive and Active Network Measurement: 9th International Conference, PAM 2008, Cleveland, OH, USA, April 29-30, 2008. Proceedings 9* (pp. 182-191). Springer Berlin Heidelberg.

Chitre, M., Motani, M., & Shahabudeen, S. (2012). *Throughput of networks with large propagation delays*. *IEEE Journal of Oceanic Engineering*, 37(4), 645-658.

- Sheridan, T. B., & Ferrell, W. R. (1963). Remote manipulative control with transmission delay. *IEEE Transactions on Human Factors in Electronics*, (1), 25-29.
- Ramaswamy, R., Weng, N., & Wolf, T. (2004, November). Characterizing network processing delay. In *IEEE Global Telecommunications Conference, 2004. GLOBECOM'04.* (Vol. 3, pp. 1629-1634). IEEE.
- Numan, P. E., Yusof, K. M., Marsono, M. N. B., Yusof, S. K. S., Fauzi, M. H. B. M., Nathaniel, S., ... & Baharudin, M. A. B. (2019). On the latency and jitter evaluation of software defined networks. *Bulletin of Electrical Engineering and Informatics*, 8(4), 1507-1516.
- Sojan, J. K., & Haribabu, K. (2022, March). Monitoring Jitter in Software Defined Networks. In *International Conference on Advanced Information Networking and Applications* (pp. 635-645). Cham: Springer International Publishing.
- Sinha, Y., Vashishth, S., & Haribabu, K. (2018). Real time monitoring of packet loss in software defined networks. In *Ubiquitous Communications and Network Computing: First International Conference, UBICNET 2017, Bangalore, India, August 3-5, 2017, Proceedings 1* (pp. 154-164). Springer International Publishing.
- Mizrahi, T., & Moses, Y. (2016, April). Software defined networks: It's about time. In *IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications* (pp. 1-9). IEEE.
- Lantz, B., & O'Connor, B. (2015). A mininet-based virtual testbed for distributed SDN development. *ACM SIGCOMM Computer Communication Review*, 45(4), 365-366.
- Romanov, O. I., Saychenko, I. O., Marinov, A. I., & Skolets, S. S. (2021). Research of SDN network performance parameters using mininet network emulator.
- Patil, P. B., Bhagat, K. S., Kirange, D. K., & Patil, S. D. (2020). Software defined networks using mininet. *Int. J. Recent Technol. and Eng*, 9(1), 843-849.
- De Oliveira, R. L. S., Schweitzer, C. M., Shinoda, A. A., & Prete, L. R. (2014, June). Using mininet for emulation and prototyping software-defined networks. In *2014 IEEE Colombian conference on communications and computing (COLCOM)* (pp. 1-6). Ieee.
- Muelas, D., Ramos, J., & De Vergara, J. E. L. (2018). Assessing the limits of mininet-based environments for network experimentation. *IEEE network*, 32(6), 168-176.
- Fontes, R. R., Afzal, S., Brito, S. H., Santos, M. A., & Rothenberg, C. E. (2015, November). Mininet-WiFi: Emulating software-defined wireless networks. In *2015 11th International Conference on Network and Service Management (CNSM)* (pp. 384-389). IEEE.
- Ghosh, U., Chatterjee, P., Shetty, S., & Datta, R. (2020). An SDN-IoT- based framework for future smart cities: addressing perspective. In *Internet of Things and Secure Smart Environments* (pp. 441-468). Chapman and Hall/CRC.
- Pakzad, F., Layeghy, S., & Portmann, M. (2016, December). Evaluation of Mininet-WiFi integration via ns-3. In *2016 26th International Telecommunication Networks and Applications Conference (ITNAC)* (pp. 243-248). IEEE.

<https://mtechproject.com/computer-science/mininet-projects/>

Kaur, K., Singh, J., & Ghumman, N. S. (2014, February). *Mininet as software defined networking testing platform*. In *International conference on communication, computing & systems (ICCCS)* (pp. 139-42). IEEE.

Cabral, M., Silveira, M., & Urie, R. (2019). *SDN Advantages for Ethernet-Based Control*. Schweitzer Engineering Laboratories, Inc., Tech. Rep.

Castanheira, T. M. A. (2018). *Simulation of mobile edge-cloud applications using Mininet-WiFi*. Karamjeet Kaur, Japinder Singh, Navtej Singh Ghumman *Mininet as a Software Defined Networking Testing Platform ICCCS, 2014*

<https://github.com/Mininet/Mininet/wiki>

Manzoor, S., Karmon, P., Hei, X., & Cheng, W. (2020, May). *Traffic aware load balancing in software defined WiFi networks for healthcare*. In *2020 Information Communication Technologies Conference (ICTC)* (pp. 81-85). IEEE.

Purwita, A. A., Yesilkaya, A., & Haas, H. (2022, December). *Intelligent subflow steering in MPTCP-based hybrid Wi-Fi and LiFi networks using model-augmented DRL*. In *GLOBECOM 2022-2022 IEEE Global Communications Conference* (pp. 425-430). IEEE.

Assegie, S., & Nair, P. (2019). *Performance analysis of emulated software defined wireless network*. *Indonesian Journal of Electrical Engineering and Computer Science (IJECS)*, 16(1), 311-318.

Rajesh, M. (2021). *Study on SDN with security issues using Mininet*. *Recent Trends in Intensive Computing*, 39, 104.