Πανεπιστήμιο Πειραιώς – Τμήμα Πληροφορικής

Πρόγραμμα Μεταπτυχιακών Σπουδών

«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	Χρήση Λογισμικού Εξομοίωσης για την Εκμάθηση Προγραμματιζόμενων Δικτύων Using Simulation Software to Learn Programmable Networks
Ονοματεπώνυμο Φοιτητή	Αθανάσιος Τριλίβας
Πατρώνυμο	Γεράσιμος
Αριθμός Μητρώου	ΜΠΠΛ 13078
Επιβλέπων	Χρήστος Δουληγέρης, Καθηγητής

Ιούλιος 2020

Τριμελής Εξεταστική Επιτροπή

Χρήστος Δουληγέρης Καθηγητής	Δημήτρης Βέργαδος Καθηγητής	Μιχαήλ Ψαράκης Επίκουρος Καθηγητής

Περίληψη

Τα Προγραμματιζόμενα με Λογισμικό Δίκτυα (Software-Defined Networks) έχουν ήδη ενσωματωθεί σε κάθε πιθανή τεχνολογία μετάδοσης δεδομένων. Τα συναντάμε λιγότερο σε τοπικά δίκτυα, πιο συχνά σε δίκτυα ευρείας περιοχής και Data Centers, τα βρίσκουμε να λειτουργούν σε οικιακές δικτυακές συσκευές έως και συσκευές που αποτελούν τη ραχοκοκαλιά του Διαδικτύου. Ήταν μια ήσυχη επανάσταση που ξεκίνησε σχετικά πρόσφατα –το 2009 και που χάρη στην οποία διασώθηκε η οικονομική ζωή του πλανήτη στην εποχή του lockdown. Σε αυτά στηρίζεται και το πολυδιαφημισμένο 5G που θα φέρει επανάσταση στις ασύρματες κινητές επικοινωνίες και για αυτόν το λόγο όλοι οι πάροχοι κινητής αναβαθμίζουν τον πυρήνα του δικτυακού εξοπλισμού τους. Συνέπεια αυτού είναι η ανάγκη εκπαίδευσης των νέων μηχανικών και τεχνικών δικτύων στη νέα αυτή τεχνολογία η οποία δεν είναι επαναστατική αλλά σίγουρα τελείως διαφορετική από τα κατανεμημένα πρωτόκολλα που χρησιμοποιούνται και αντίστοιχα διδάσκονται στα τμήματα πληροφορικής και επικοινωνιών. Όσοι ασχοληθούν με το SDN, πέρα από την απλότητα του, θα ανακαλύψουν και τις τεράστιες δυνατότητες του που για να αξιοποιηθούν σε κάποιον βαθμό θα χρειαστεί οι ενδιαφερόμενοι να εντρυφήσουν σε όλο το φάσμα τις επιστήμης υπολογιστών. Η διατριβή αυτή ασχολείται με την αξιολόγηση ενός εργαλείου εξομοίωσης και εκμάθησης του SDN.

Abstract

Software Defined Networks already dominate the entire spectrum of computer networking either in Lans, Wans or Data Centers and we can find SDN running in SOHO network appliances and even in devices constituting the Internet's backbone. It has been a quiet revolution that started not long ago –in 2009 and thanks to it we managed to save most of this planet's financial activities during the covid-19 lockdown. Even the much-advertised 5G mobile wireless technology relies heavily on SDN and that is the reason most providers are in a process of updating their core networking equipment with SDN devices. Because of this, the need for training young network engineers and technicians has emerged in this new technology which cannot be described as revolutionary but is surely different from the distributed networking protocols that are used and in fact taught in computer and telecommunications classes around the world. Whoever delves into SDN will not only discover its simplicity but also its unlimited potential, making it imperative for them to further study all aspects of computer science. This postgraduate project is about evaluating a tool for emulating and learning SDN.

ΠΕΡΙΕΧΟΜΕΝΑ

Κατάλογος Εικόνων

Κατάλογος συντομογραφιών

AA	Active Application
ANTS	Active Networks Transport System
AP/MP	Application Plane/Management Plane
API	Application Programming Interface
ASN	Autonomous System Number
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BMC	Baseboard Management Controller
CDM	Code Division Multiplex
CLI	Command Line Interface
CP	Control Plane
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
DP	Data Plane
DSP	Digital Signal Processing
DWDM	Dense Wavelength Division Multiplexing
EE	Exeution Environment
EIGRP	Enhanced Interior Gateway Protocol
ETSI	European Telecommunications Standards Institute
EWBI	East-West Bound Interface
FDM	Frequency Division Multiplex
FIB	Forwarding Information Base
FIND	Future Internet Design
ForCes	Forwarding and Control Separation
GUI	Graphical User Inetrface
HTTP	HyperText Trasnsfer Protocol
I2RS	Interface to Routing System
ICP	Initial Connection Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
ISG	Industry Specification Group
JSON	Javascript Object Notation
LAN	Local Area Network
LSDB	Link State Database
MAN	Metropolitan Area Network
MD5	Message Digest 5
MGCP	Media Gateway Control Protocol
MPLS	Multi Protocol Label Switching

NBI	Northbound Interface
NCP	Network Control Program
NETCONF	NETWORK CONFIGURATION
NFV	Network Functions Virtualization
NMS	Network Management System
NOS	Network Operating System
ODL	OpenDaylight
OR/OR	Offline Routing/Online Reaction
OSI	Open Systems Interconnect
OSPF	OPEN SHORTEST PATH FIRST
OVS	Open vSwitch
OVSDB	Open vSwitch Database
PCC	Path Computation Communication Protocol
PCE	Path Computation Element
POF	Protocol Obvious Forwarding
PPP	Point to Point Protocol
QoS	Quality of Service
REST	Representational State Transfer
RFC	Request For Comments
RIB	Routing Information Base
RSVP	Resource Reservation Protocol
SBI	Southbound Interface
SDN	Software-Defined Networking
SDNC	SDN Controller
SD-WAN	Software Defined Wide Area Networking
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SRAM	Static Ram
SSH	Secure Shell
TCAM	Ternary Content –Addressable Memory
TCP	Transmission Control Protocol
TDM	Time Division Multiplex
TED	Traffic Engineering Database
VLAN	Virtual Local Area Network
VoIP	Voice over IP
VTEP	VXLAN TUNNEL ENDPOINT
VxLAN	Virtual eXtensible LAN
WAN	Wide Area Network
XML	eXtensible Markup Language
YAML	Ain't Markup Language

ΕΙΣΑΓΩΓΗ

Δικτυακή Αρχιτεκτονική

Το δίκτυο επικοινωνιών υφίσταται ώστε να συνδέσει έναν ή περισσότερους αποστολείς μηνυμάτων με έναν ή περισσότερους παραλήπτες. Η προέλευση της δικτυακής αρχιτεκτονικής που εξυπηρετεί αυτόν τον σκοπό εντοπίζεται στην εξέλιξη των δικτύων τηλεπικοινωνιών. Αρχικά ήταν απλά δίκτυα τηλεφωνίας και διαχειριζόντουσαν μόνο την φωνή. Αργότερα, με την έλευση της ψηφιακής τεχνολογίας αναπτύχθηκαν νέες αρχιτεκτονικές για τη μεταφορά ψηφιακών δεδομένων μεταξύ των δυο αντεπιστελλόντων μερών.

Κατηγοριοποίηση δικτύων:

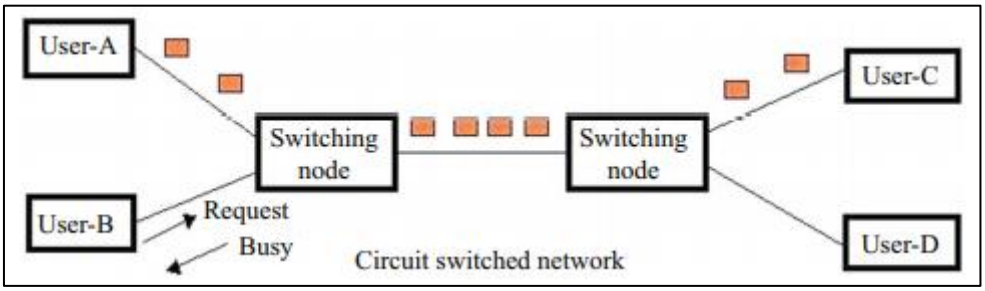
Τα δίκτυα διακρίνονται με διαφορετικά κριτήρια:

1. Μέγεθος:
    - Προσωπικό δίκτυο (Personal Area Network -PAN): που αποτελείται από έναν μόνο χρήστη και οι συσκευές συνδέονται αυτόματα.
    - Τοπικό δίκτυο (Local Area Network –LAN): που διασυνδέει προσωπικούς υπολογιστές και άλλες συσκευές όπως εκτυπωτές σε μια πανεπιστημιούπολη ή γραφείο.
    - Μητροπολιτικό δίκτυο (Metropolitan Area Network –MAN): το οποίο καλύπτει πόλη με έκταση έως και 100km προς μια κατεύθυνση. Κλασσικό παράδειγμα είναι τα δίκτυα καλωδιακής τηλεόρασης ή το υψίρρυθμο ασύρματο ίντερνετ σε αστικές περιοχές.
    - Δίκτυο ευρείας περιοχής (Wide Area Network): που καλύπτει χώρες και ηπείρους συμπεριλαμβάνοντας εκατομμύρια από συσκευές. Το δίκτυο αυτό διαιρείται σε υποδίκτυα και το μεγαλύτερο υπόδειγμα είναι το Διαδίκτυο.
2. Υπηρεσίες:
    - Η συνδεσμική (connection-oriented) υπηρεσία εγκαθιστά κάθε σύνδεση και διασφαλίζει την εγγυημένη παράδοση της πληροφορίας. Περιλαμβάνει αξιόπιστο έλεγχο ροής και συμφόρησης. Κλασσικό παράδειγμα της είναι η τηλεφωνία.
    - Η μη-συνδεσμική (connectionless) υπηρεσία όπου ο τερματικός χρήστης απλά στέλνει τα δεδομένα σε μια διεύθυνση. Λειτουργεί όπως το σύστημα των ταχυδρομείων και με παρόμοιο τρόπο τα δεδομένα διέρχονται από πολλές ενδιάμεσες συσκευές πριν φτάσουν στον προορισμό.
3. Τεχνολογία μετάδοσης:
    - Η ευρυεκπομπή σε διαμοιραζόμενο μέσο μετάδοσης αφορά τη δικτύωση με χρήση ενός μόνο καναλιού σε τοπολογία αρτηρίας ή αστέρα. Μόνο μια τερματική μηχανή επιτρέπεται να μεταδώσει κάθε φορά και το μήνυμα μπορεί να παραληφθεί και να διαβαστεί από όλους τους κόμβους. Το πακέτο διαθέτει ένα πεδίο διεύθυνσης που επίσης φαίνεται σε όλες τις τερματικές μηχανές οι οποίες με τη σειρά τους το συγκρίνουν με την δική τους διεύθυνση. Αν οι διευθύνσεις δεν ταιριάζουν, ο κόμβος αγνοεί το μήνυμα και το αφήνει να διέλθει. Αν η διεύθυνση κόμβου και παραλήπτη του πακέτου ταιριάζουν, ο κόμβος θα το επεξεργαστεί. Αυτά τα δίκτυα είναι εύκολο να υλοποιηθούν και δυσκολότερο να επεκταθούν.
    - Τα δίκτυα μεταγωγής από άκρο σε άκρο αποτελούν συλλογή από πολλές τέτοιες συνδέσεις. Ένα μήνυμα θα περάσει μέσα από αρκετές τέτοιες μηχανές κι έτσι ένα από τα μεγάλα ζητήματα είναι να βρει διαδρομή δρομολόγησης βελτιστοποιημένη όσον αφορά την χρονική καθυστέρηση, τον χρόνο παράδοσης και λοιπές παρόμοιες μετρικές. Αυτά τα δίκτυα είναι επεκτάσιμα αλλά δυσκολότερο να δημιουργηθούν,

Δίκτυα Μεταγωγής Κυκλώματος

Ιστορικά, η ιδέα της αρχιτεκτονικής μεταγωγής κυκλώματος προέκυψε από τα τηλεφωνικά δίκτυα. Όπως και με άλλες σημαντικές τεχνολογίες, η τηλεφωνία είχε ένα ταπεινό ξεκίνημα ως επικοινωνία μεταξύ δυο ατόμων. Οι ιδέες της μεταγωγής και του έλεγχου προέκυψαν μόλις προστέθηκε και ένα τρίτο μέλος.

Η λέξη «κύκλωμα» προκύπτει από την τεχνολογία διανομής ηλεκτρικού ρεύματος. Ως κύκλωμα ορίζεται μια αγώγιμη διαδρομή ηλεκτρικού ρεύματος μεταξύ δυο σημείων. Η ίδια λέξη «κύκλωμα» στα πλαίσια της τηλεφωνίας σημαίνει μια μόνιμη, αποκλειστική σύνδεση μεταξύ δυο μερών για τη διάρκεια μιας κλήσης. Πριν ο αποστολέας στείλει φωνή ή φαξ στον παραλήπτη πρέπει να εγκατασταθεί μια αποκλειστική σύνδεση μεταξύ τους η οποία αποκαλείται «κύκλωμα». Οι απαραίτητοι πόροι για την σύνδεση είναι αποκλειστικής χρήσης από τα δυο άκρα και δεν μπορούν να διαμοιραστούν. Η σύνδεση υφίσταται για το σύνολο της διάρκειας της κλήσης ακόμα και αν οι συνομιλητές δεν μεταδίδουν ενώ οι πόροι αποδεσμεύονται αφού τερματιστεί η κλήση. Στο σχήμα της Εικόνας 1 φαίνεται ότι υπάρχει κύκλωμα μεταξύ των χρηστών A και C το οποίο δεν διατίθεται ώστε να μιλήσουν οι B και D όσο διαρκεί η κλήση των πρώτων.



Εικόνα 1: Δίκτυο Μεταγωγής Κυκλώματος

Αρχικά η μεταγωγή κυκλώματος ήταν αποκλειστικό χαρακτηριστικό της αναλογικής τηλεφωνίας αλλά σήμερα το σύνολο των τηλεφωνικών συνομιλιών λαμβάνει χώρα στο ψηφιακό πεδίο. Το μεγαλύτερο μέρος της προετοιμασίας, συντήρησης και λοιπών λειτουργιών γίνεται με τη χρήση αποκλειστικού συστήματος δικτυακής διαχείρισης (Network Management Software – NMS). Το NMS ασκεί έλεγχο πάνω σε άλλες δικτυακές συσκευές που υπόκεινται σε εξατομικευμένη διαχείριση από ένα εγγενές στοιχειώδες διαχειριστικό σύστημα (Element Management System).

Το βασικό παράδειγμα μεταγωγής κυκλώματος αφορά τα τηλεφωνικά δίκτυα αλλά συναντιέται ακόμα στον πυρήνα του Διαδικτύου όπου χρησιμοποιούνται πρωτόκολλα όπως το Σύγχρονο Οπτικό Δίκτυο (Synchronous Optical NetWork –τυποποίηση κατά U.S) και η Σύγχρονη Ψηφιακή Ιεραρχία (μη U.S τυποποίηση) για τη μεταφορά οπτικών σημάτων πάνω από εξοπλισμό DWDM (Dense Wavelength Division Multiplexing). Το μέσο μετάδοσης μεταφέρει πολυπλεγμένα σήματα με κάθε μια από τις παρακάτω τεχνολογίες: πολυπλεξία συχνότητας (FDM), πολυπλεξία χρόνου TDM και πολυπλεξία κώδικα (CDM).

Λειτουργία του Δικτύου Μεταγωγής Κυκλώματος

Η από άκρου σε άκρο μεταγωγή σημάτων αποτελείται από τα παρακάτω βήματα:

1. Δέσμευση κυκλώματος: Ένα σήμα που περιέχει πληροφορίες ελέγχου αποστέλλεται πάνω από τη σύνδεση ώστε να δημιουργηθεί το κύκλωμα. Η λειτουργία αυτή εκλαμβάνεται ως πλεονασματική (overhead). Το εύρος ζώνης του καναλιού δεσμεύεται για τη ροή πληροφορίας (φωνή ή δεδομένα). Ο μηχανισμός ελέγχου διασφαλίζει ότι η χωρητικότητα του καναλιού είναι τουλάχιστον ίση με τον μέγιστο ρυθμό μετάδοσης που απαιτείται για τη ροή.

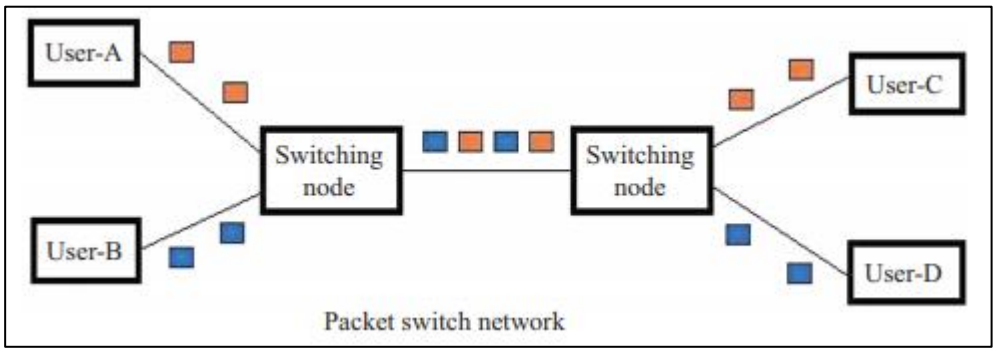
2. Μετάδοση: Το δεσμευμένο στο οποίο έχει ανατεθεί το μέγιστο εύρος μπορεί να διαθέσει συνδεσμική υπηρεσία (Connection-Oriented Service –Cons) με απόλυτη ποιότητα (QoS) όσον αφορά το εύρος ζώνης και το jitter. Αυτή η τεχνική είναι δαπανηρή αν η πηγή μετάδοσης είναι αδρανής ή ο ρυθμός ροής είναι μικρότερος του υψηλότερου. Οι λειτουργίες διαθέτουν επίσης μηχανισμό που αντιμετωπίζει τον ανταγωνισμό για εύρος ζώνης όταν το ίδιο κύκλωμα ζητείται ενώ είναι μια κλήση σε εξέλιξη.
3. Διακοπή (turn-off) κυκλώματος: Μετά το πέρας της κλήσης το κύκλωμα διακόπτεται και το εύρος ζώνης αποδίδεται πίσω στο δίκτυο.

Λοιποί παράγοντες που πρέπει να ληφθούν υπόψη:

- Συνήθως οι πηγές και οι προορισμοί των ροών τηλεφωνίας εντοπίζονται στους τερματικούς κόμβους. Η συνάθροιση πολλών τηλεφωνικών ροών σε μια μεγαλύτερη στο μέσον του δικτύου είναι επιτρεπτή.
- Αν δεν υπάρχουν αρκετά κανάλια ώστε να ικανοποιήσουν το αίτημα, πρέπει να καθυστερήσει η εγκατάσταση της σύνδεσης, να μπλοκαριστεί ή ακόμα και να απορριφθεί. Όταν τα κυκλώματα δίνουν το μέγιστο δυνατό εύρος, η μοναδική μετρική για το QoS είναι η πιθανότητα μπλοκαρίσματος μιας κλήσης.
- Οι υπάρχουσες κλήσεις δεν διαμοιράζονται πόρους με άλλες ροές. Αυτό εξαλείφει όποια αβεβαιότητα καθώς και την ανάγκη για ενδιάμεση αποθήκευση, επεξεργασία ή χρονοπρογραμματισμό της διαδρομής δεδομένων.
- Η πολυπλεξία πολλών κλήσεων σε ένα μόνο κανάλι αποτελεί σημαντική τεχνολογία των δικτύων μεταγωγής κυκλώματος. Υπάρχουν δυο τρόποι πολυπλεξίας: Πολυπλεξία διαίρεσης συχνότητας (Frequency Division Multiplexing –FDM) και Πολυπλεξία Διαίρεσης Χρόνου (Time Division Multiplexing –TDM). Στο FDM το διαθέσιμο εύρος ζώνης διαιρείται σε πολλά μικρότερα μέρη καθένα από τα οποία ανατίθεται σε διαφορετική κλήση. Στο TDM το σύστημα διαθέτει μια χρονοθυρίδα σε κάθε κλήση και το τερματικό μεταδίδει μόνο κατά τη διάρκεια αυτής.

Δίκτυα Μεταγωγής Πακέτου ή IP Δίκτυα

Η επικοινωνία μέσω πακέτων είναι σχετικά πρόσφατη τεχνική. Τα δεδομένα και η φωνή μετατρέπονται σε ψηφιακά πακέτα με το κάθε πακέτο να μεταφέρει πλεονάζουσα πληροφορία (μεταδεδομένα) στην αρχή του η οποία ονομάζεται «Επικεφαλίδα» Τα μεταδεδομένα μεταφέρουν πληροφορία σχετικά με την πηγή και τον προορισμό και αριθμούνται ακολουθιακά. Το μήνυμα προς παράδοση αποτελείται από σε σειρά αριθμημένα πακέτα τα οποία μπορούν να ταξιδέψουν μέσα από διαφορετικά κανάλια ενίοτε χάνοντας τη σειρά τους ανάλογα με το διαθέσιμο εύρος ζώνης κάθε καναλιού. Το πιο σχήμα της Εικόνας 2επιδεικνύει την αρχή αυτή με βάση τα χρωματισμένα πακέτα.



Εικόνα 2: Δίκτυο Μεταγωγής Πακέτων

Τα πακέτα συναθροίζονται στον προορισμό και ξαναμπαίνουν σε σειρά. Αυτή η μετάδοση αποκαλείται μετάδοση «βέλτιστης προσπάθειας» (best effort delivery) και σχεδόν όλες οι επικοινωνίες σήμερα στα ψηφιακά δίκτυα γίνονται με αυτόν τον τρόπο.

Η μεταγωγή πακέτων είναι σήμερα η προτιμώμενη δικτυακή τεχνολογία και αποτελεί το θεμέλιο του Διαδικτύου. Η βέλτιστης προσπάθειας παράδοση των πακέτων επαρκεί για τις περισσότερες εφαρμογές αλλά πάσχει σε περιπτώσεις κρίσιμων και πραγματικού χρόνου επικοινωνιών.

- Πρέπει να λαμβάνονται υπόψη περιορισμοί γύρω από την έγκαιρη και διασφαλισμένη παράδοση των πακέτων.
- Η εγγυημένη διαθεσιμότητα της υπηρεσίας είναι εξίσου σημαντική.

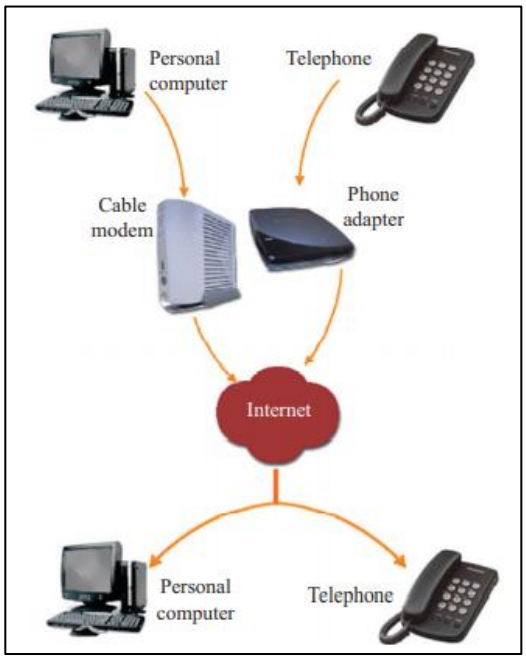
Για αυτές τις δυνατότητες η παράδοση των πακέτων πρέπει να υιοθετήσει πολλά από τα χαρακτηριστικά της μεταγωγής κυκλώματος. Για παράδειγμα, η τεχνολογία VPN συνδυάζει στοιχεία και από τα δυο είδη δικτύωσης.

Υβριδική Δικτύωση Μεταγωγής Κυκλώματος και Πακέτου: Το Παράδειγμα της Φωνής Πάνω Από το Πρωτόκολλο IP

Τα δίκτυα φωνής και δεδομένων ήταν αρχικά διακριτά και ανεξάρτητα. Σύντομα έγινε αντιληπτό ότι οι τεχνικές μετατροπής αναλογικής εισόδου σε ψηφιακά πακέτα μπορούν να εφαρμοστούν και στη φωνή. Απαιτήθηκε αρχικά ένα χρονικό διάστημα αλλά έγινε τελικά αντιληπτό ότι η πλέον συμφέρουσα μέθοδος διεξαγωγής τηλεφωνικών κλήσεων ήταν μέσω ευρυζωνικών συνδέσεων του Διαδικτύου. Οι παραδοσιακοί πάροχοι τηλεφωνίας μέσω του PSTN δικτύου έχουν ήδη ενσωματώσει την τεχνολογία VoIP (Voice over IP) και αυτό είναι ο κυριότερος λόγος για το οποίον οι τιμές τηλεφωνικών κλήσεων μέσω εφαρμογών όπως το WhatsApp έχουν μηδενιστεί. Μια αναπαράσταση δικτύου VoIP φαίνεται στην Εικόνα 3.

Το VoIP είναι ένα πρωτόκολλο επιπέδου 3 του OSI αλλά χρησιμοποιεί και διάφορα επιπέδου 2 πρωτόκολλα όπως PPP, Frame Relay ή ATM για τις λειτουργίες του. Χρησιμοποιεί ψηφιακούς επεξεργαστές σήματος (DSPs) ώστε να τεμαχίσει το σήμα φωνής σε πλαίσια τα οποία ενθυλακώνονται σε πακέτα φωνής που μετακινούνται χάρη σε IP τυποποιημένα πρωτόκολλα.Κάποια από αυτά είναι:

- H.323 –η τυποποίηση κατά ITU-T (International Telecommunications Union – Telecommunications Standardization Sector) για αποστολή φωνής, δεδομένων και video κατά μήκους ενός δικτύου συμπεριλαμβανομένων άλλων προτύπων όπως το H.225 για τον έλεγχο κλήσης, το H.235 για ασφάλεια, το H.245 για εύρεση διαδρομής και διαπραγμάτευση παραμέτρων και το H.450 για συμπληρωματικές υπηρεσίες.
- Το πρωτόκολλο MGCP (Media Gateway Control Protocol) είναι ένα πρωτόκολλο από την IETF για τον έλεγχο των πυλών φωνής των IP δικτύων.
- Το SIP (Session Initiation Protocol) καθορίζεται στο RFC 2543.



Εικόνα 3: Διαδίκτυο και τηλεφωνία

Τα βασικά βήματα στη μετατροπή φωνής σε πακέτα και στην εγκατάσταση μιας κλήσης αποδεικνύουν την υβριδική φύση της τεχνολογίας αυτής. Ως παράδειγμα δίνεται η ακολουθία βημάτων που περιγράφουν τη γενικευμένη ροή μιας κλήσης VoIP μεταξύ δυο αντεπιστελλόντων.

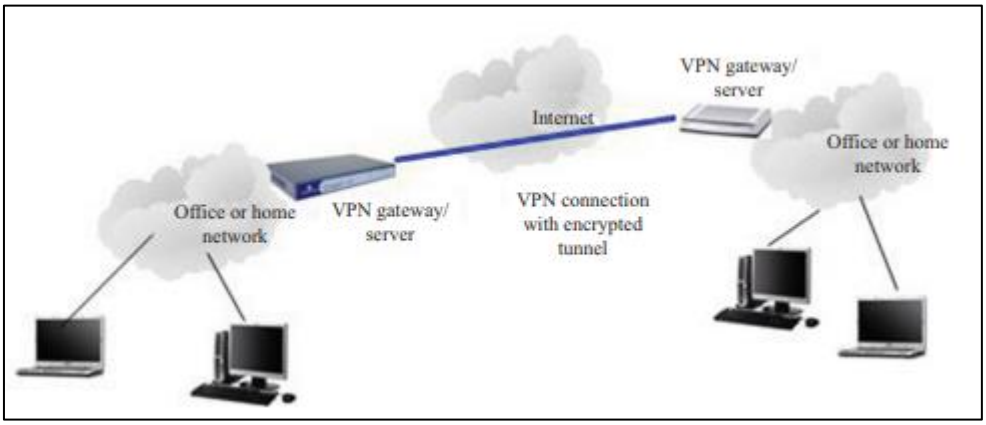
1. Ο καλών σηκώνει το ακουστικό προκαλώντας σηματοδοσία επιπέδου OSI 7 “Off-hook”.
2. Το πρωτόκολλο VoIP δημιουργεί ήχο κλήσης (επίπεδο 5 στο OSI) και αναμένει τον καλούντα να σχηματίσει τον αριθμό.
3. Ο καλών σχηματίζει τον αριθμό και τα ψηφία που πληκτρολογεί αποθηκεύονται ώσπου να κρατηθεί ολόκληρος ο αριθμός (και πάλι στο επίπεδο 5 OSI). Ο τηλεφωνικός αριθμός αντιστοιχίζεται μέσω του αντίστοιχου πίνακα σε ένα IP τερματικό με απευθείας σύνδεση στον προορισμό.
4. Το VoIP «τρέχει» το πρωτόκολλο συνεδρίας H.323 ώστε να εγκαταστήσει κανάλι μετάδοσης και λήψης προς κάθε κατεύθυνση στο IP δίκτυο (επίπεδο 5 του OSI). Στο σημείο αυτό χρησιμοποιείται το πρωτόκολλο RSVP (Resource Reservation Protocol) ώστε να επιτευχθεί το απαραίτητο QoS πάνω από το IP δίκτυο.
5. Οι ενεργοί κωδικοποιητές-αποκωδικοποιητές (codecs) και στα δυο άκρα της σύνδεσης ψηφιοποιούν, συμπιέζουν και πακετοποιούν τα σήματα φωνής σε διακριτά πακέτα. Αυτά μεταφέρονται πάνω από το δίκτυο και η συνομιλία συνεχίζει με χρήση RTP/UDP/IP πρωτοκόλλων.
6. Όλα τα σήματα δείκτες σχετικά με την εξέλιξη της κλήσης αφαιρούνται από την φωνητική κλήση και μεταφέρονται in-band από το IP δίκτυο. Ενθυλακώνονται στο RTCP (Real Time Conferencing Protocol) χρησιμοποιώντας τον μηχανισμό RTCP App.
7. Όταν οποιοδήποτε από τα δυο άκρα κατεβάσει το ακουστικό καταργούνται οι RSVP δεσμεύσεις (αν χρησιμοποιείται αυτό το πρωτόκολλο) και η σύνδεση τερματίζεται. Κάθε άκρο θα παραμείνει αδρανές περιμένοντας το σήκωμα του ακουστικού να δώσει έναυση σε μια ακόμα διαδικασία εγκατάστασης κλήσης.

Εικονικά Ιδιωτικά Δικτυα (Virtual Private Networking)

Η τεχνολογία VPN αποτελεί συνδυασμό της μεταγωγής κυκλώματος και της μεταγωγής πακέτων. Καθορίζεται ως μια ασφαλής και κρυπτογραφημένη σύνδεση μεταξύ των συσκευών

πηγής και προορισμού πάνω από ένα λιγότερο ασφαλές δίκτυο όπως το Διαδίκτυο. Το περιεχόμενο της επικοινωνίας παραμένει κρυφό από τους άλλους λόγω της κρυπτογράφησης.

Μια τυπική υπηρεσία VPN αποτελείται από τα βήματα που φαίνονται στο σχήμα της Εικόνας 4 και δημιουργεί ροές δεδομένων.



Εικόνα 4: Τα δίκτυα VPN

i. Ο χρήστης ξεκινά την VPN διαδικασία και εισαγάγει τα δεδομένα.
ii. Τα δεδομένα κρυπτογραφούνται και στέλνονται στον ISP ο οποίος τα προωθεί στον πλησιέστερο VPN διακομιστή στο δίκτυο.
iii. Τα δεδομένα παραμένουν κρυπτογραφημένα και στέλνονται στον διακομιστή VPN και εν συνεχεία στον ISP διακομιστή κοντινότερα στον προορισμό.
iv. Τα δεδομένα αποκρυπτογραφούνται και αποστέλλονται στο χρήστη-προορισμό.

Ο προορισμός αντιλαμβάνεται ως πηγή προέλευσης των δεδομένων τον VPN διακομιστή και όχι τη συσκευή του αποστολέα. Ο VPN διακομιστής δρα ως τρίτο μέρος που συνδέεται στο Διαδίκτυο εκ μέρους του χρήστη.

Η παρεχόμενη ασφάλεια εξαρτάται από την χρησιμοποιούμενη τεχνολογία και τους νομικούς και λοιπούς περιορισμούς ανάλογα με τη γεωγραφική θέση του διακομιστή. Για παράδειγμα η τεχνολογία αυτή δεν χρησιμοποιείται σε Τουρκία, Κίνα, Ιράκ, ΗΑΕ, Ρωσία, Λευκορωσία, Ομάν, Ιράν, Βόρειο Κορέα και Τουρκμενιστάν. Μερικές φορές ο πάροχος της VPN υπηρεσίας μπορεί να χρειαστεί να διατηρεί αρχείο καταγραφής που περιλαμβάνει τη δραστηριότητα του χρήστη, IP διευθύνσεις, χρονοσημάνσεις συνδέσεων και αποσυνδέσεων, συσκευές που χρησιμοποιήθηκαν, πληροφορίες πληρωμών κλπ κάνοντας λιγότερο ασφαλή τη σύνδεση.

Ακολουθεί λίστα με τα πιο σημαντικά πρωτόκολλα VPN.

a) PPTP (Point to Point Tunneling Protocol): σχεδιάστηκε από τη Microsoft και είναι μέρος του λειτουργικού συστήματος Windows. Είναι λιγότερο ασφαλές από τα άλλα πρωτόκολλα.
b) L2TP (Layer 2 Tunneling Protocol): αποτελεί συνδυασμό του PPTP με ιδιόκτητο πρωτόκολλο της Cisco. Χρησιμοποιεί κρυπτογραφικά κλειδιά και στα δυο άκρα της μετάδοσης δεδομένων ώστε να εγκαταστήσει τη σύνδεση. Υπάρχουν αμφιβολίες σχετικά με το πόσο ασφαλές είναι. Το L2TP/IPSec είναι το προεπιλεγμένο πρωτόκολλο των iPhone.
c) Το πρωτόκολλο SSTP (Secure Socket Tunneling Protocol) επίσης δημιουργήθηκε από τη Microsoft και χρησιμοποιεί SSL/TLS κρυπτογράφηση για να επιτύχει σύνδεση. Αυτή η μέθοδος βασίζεται σε συμμετρική κρυπτογραφία διασφαλίζοντας ότι μόνο ο αποστολέας και ο παραλήπτης μπορούν να διαβάσουν το μήνυμα.
d) Το πρωτόκολλο IKEV2 (Internet Key Exchange, version 2) φτιάχτηκε επίσης από τη Microsoft, είναι παρόμοιο με το SSTP αλλά παρέχει μεγαλύτερη ασφάλεια.

e) Το OpenVPN είναι ένα έργο ανοικτού κώδικα που συνδυάζει χαρακτηριστικά όλων των πιο πάνω πρωτοκόλλων. Βασίζεται στη συμμετρική κρυπτογράφηση και επί του παρόντος είναι το πιο πολύπλευρο και ασφαλές πρωτόκολλο για τεχνολογία VPN.

Ελλείμματα της Σημερινής Αρχιτεκτονικής Δικτύωσης

Ένα τυπικό δίκτυο αποτελείται από πολλούς κόμβους και ζεύξεις και είναι δύσκολο να αλλάξει αφού εγκατασταθεί. Τα τελευταία χρόνια έχει υπάρξει μια έκρηξη στην δικτυακή επικοινωνία λόγω του Διαδικτύου και των Μέσων Κοινωνικής Δικτύωσης. Αυτή η προσέγγιση έχει αποδειχτεί ότι έχει πολλές ελλείψεις.

- Στατικές παραμετροποιήσεις: υπάρχουν δυο σχετιζόμενα προβλήματα.
    a) Είναι κοπιαστικό και δύσκολο να παραμετροποιηθεί ένα δίκτυο σύμφωνα με τις προκαθορισμένες πολιτικές. Λόγω αυτού, όταν ολοκληρωθεί το δίκτυο υπάρχουν αντιδράσεις σε τυχόν αλλαγές αφού οι κόμβοι και οι ζεύξεις είναι προσαρτημένες στην εκάστοτε τεχνολογία και είναι πολύ δύσκολο να αλλάξουν.
    b) Είναι πολύ δύσκολο να αναδιαμορφωθεί ένα στατικό δίκτυο ώστε να ανταπεξέλθει σε αλλαγές στον φόρτο ή στην εμφάνιση σφαλμάτων. Οποιαδήποτε αλλαγή απαιτεί δαπάνη χρόνου από πλευράς διαχειριστή.
- Έλλειψη προγραμματισιμότητας: Τα δικτυακά στοιχεία σε ένα περιβάλλον με συσκευές ποικίλης προέλευσης, διαθέτουν διαφορετικό λογισμικό για έλεγχο το οποίο συνήθως ανήκει στους κατασκευαστές. Ο τρόπος λειτουργίας τους είναι ως «μαύρο κουτί» και δεν είναι εύκολο να αλλάξει η συμπεριφορά τους. Με εκατοντάδες τέτοια στοιχεία σε ένα τυπικό δίκτυο καθίσταται αδύνατο να γίνουν αλλαγές σε όλες ταυτόχρονα ή έστω σε ένα σύντομο χρονικό διάστημα.
- Μη βέλτιστη χρησιμοποίηση πόρων: Με εξαίρεση κάποιες χρονικές περιόδους έντονης κίνησης, τα κανάλια φωνής και δεδομένων δεν χρησιμοποιούνται στη μέγιστη χωρητικότητα τους. Θα ήταν ιδανικό να μετακινούνται οι πόροι σε πραγματικό χρόνο ώστε να αυξηθεί η χρήση αλλά δεν είναι δυνατό με τις σημερινές αρχιτεκτονικές.
- Έλλειψη ευελιξίας: Είναι πολύ δύσκολο να εισαχθούν νέες τεχνολογίες στα υπάρχοντα δίκτυα με πολυποίκιλη προέλευση. Κάθε αλλαγή απαιτεί δαπανηρές χειροκίνητες αλλαγές και φυσική πρόσβαση στο δίκτυο. Επίσης το δίκτυο δεν μπορεί να ανταπεξέλθει σε νέες απειλές όπως κυβερνοεπιθέσεις, αστοχίες συσκευών κα. Για παράδειγμα, έχει αποδειχτεί ότι είναι εξαιρετικά δύσκολο να αλλάξει το σημερινό IPv4 πρωτόκολλο στο IPv6.
- Εμπόδια στην καινοτομία:Δεν είναι δυνατό να επιτελεστούν πειραματισμοί σε δίκτυα παραγωγής καθώς είναι εξαιρετικά περιορισμένα όσον αφορά τις αλλαγές σε παραμετροποίηση και δυνατότητες. Μια τυπική ερευνητική ομάδα δεν διαθέτει ακριβό δικτυακό εξοπλισμό και την εμπειρία να τον διαχειριστεί. Είναι επίσης δύσκολο για ερευνητικές ομάδες να συνεργαστούν για ακριβώς τους ίδιους λόγους οδηγώντας σε χαμηλότερο ρυθμό καινοτομιών στον κλάδο των δικτύων σε σχέση με τους υπόλοιπους κλάδους της επιστήμης υπολογιστών.

Προδιαγραφές για Ένα Νέο Δικτυακό Μοντέλο

Κάθε νέα εξέλιξη στην τεχνολογία λαμβάνει χώρα όταν νέες ιδέες χρειάζονται ώστε:

- Να ανταπεξέλθουν στις απαιτήσεις της αγοράς
- Μειώσουν τα λειτουργικά κόστη
- Εκλεπτύνουν τη λειτουργία

Κάποιες από αυτές τις ανάγκες και ανησυχίες στη δικτύωση περιγράφονται παρακάτω:

1. Αυτοματοποίηση: τέτοιες δυνατότητες για συγκεκριμένες εργασίες πρέπει να αυξηθούν. Μερικές από αυτές είναι:
    - Μείωση των λειτουργικών εξόδων και του χρόνου εκτός λειτουργίας
    - Διευκόλυνση της αποτελεσματικότερης αποσφαλμάτωσης και της εφαρμογής των πολιτικών
    - Παροχή δικτυακών πόρων και φόρτων για τις εφαρμογές όποτε απαιτείται
    - χρήση τη δικτυακής προσομοίωσης ώστε να παρέχονται δικτυακοί πόροι χωρίς έγνοιες σχετικά με τη θέση των συσκευών όπως οι μεταγωγείς και οι δρομολογητές.
2. Δυναμική ανάθεση πόρων: δυνατότητα αλλαγής του μεγέθους του δικτύου, ενημέρωσης της τοπολογίας και των ήδη διατεθειμένων δικτυακών πόρων με δυναμικό τρόπο. Οι χειροκίνητες μέθοδοι απλά δεν μπορούν να ανταπεξέλθουν σε πολλές αλλαγές σε μικρό χρονικό διάστημα. Απαιτείται ενσωματωμένη και κατά περίπτωση διαχείριση πόρων ώστε να ενσωματώνονται πολλαπλές υπηρεσίες ανεμπόδιστα όπως κατανομείς φόρτου και παρακολουθητές πόρων. Πρέπει να είναι δυνατό αυτοί οι πόροι να διατίθενται κατά αίτημα και να τοποθετούνται στο δικτυακό πλέγμα όταν και όπου χρειάζεται.
3. Ενορχήστρωση: Τα κέντρα δεδομένων και το μεγάλης έκτασης δικτυακά περιβάλλοντα αναπτύσσουν εκατοντάδες ή και χιλιάδες διαφορετικές δικτυακές συσκευές. Υπάρχει η ανάγκη για ομαλότερη ενορχήστρωση και έλεγχο αυτών των οντοτήτων.
4. Πολλαπλή μίσθωση: Η υποδομή Νέφους επεκτείνεται με πολύ υψηλό ρυθμό. Οι πάροχοι υπηρεσιών Νέφους πρέπει να υποστηρίξουν τις αυξημένες ανάγκες για πολλαπλή μίσθωση των υπηρεσιών που προσφέρουν. Πρέπει επίσης να δώσουν στους πελάτες αυξημένο ή και πλήρη έλεγχο πάνω στις διευθύνσεις, τις τοπολογίες, τη δρομολόγηση και την ασφάλεια. Ο στόχος είναι ο διαχωρισμός της υποδομής του παρόχου από τις υποστηριζόμενες υπηρεσίες όσο το δυνατόν γίνεται.
5. API: Οι χρήστες πρέπει να αναπτύξουν προγραμματιστικές διεπαφές εφαρμογών (Application Programming Inetrfaces) ώστε να επιτελέσουν τις λειτουργίες τους. Τα δίκτυα πρέπει να διαθέτουν ανοικτά APIs δίνοντας τη δυνατότητα επιλογής προσθέτων (plugins), αφαιρέσεων (πολίτικές και προθέσεις) και καθορισμούς API εργασιών. Οι χρήστες δεν πρέπει να ασχολούνται συγκεκριμένα με τις λεπτομέρειες της υλοποίησης και το δίκτυο πρέπει να επιτρέψει την επικοινωνία μεταξύ δυο κόμβων χωρίς να προκαθορίζει το πρωτόκολλο αν είναι δυνατό.
6. Μεγαλύτερη προγραμματισιμότητα: Πρόκειται για μια από τις πιο σημαντικές νέες δυνατότητες που απαιτούνται για την αποτελεσματική διάθεση δικτυακών πόρων και χρειάζεται επίσης ώστε να αλλάζει η συμπεριφορά των συσκευών και παραμετροποίηση τους σε πραγματικό χρόνο σύμφωνα με τις δικτυακές συνθήκες.
7. Ασφάλεια: Η ασφάλεια των δικτυακών συσκευών πρέπει να ενσωματωθεί με την ασφάλεια της δικτυακής υποδομής. Αυτό θα οδηγήσει σε μεγαλύτερη ακρίβεια στον εντοπισμό περιστατικών ασφαλείας και σε μεγαλύτερη ικανότητα στην αντιμετώπιση τους.
8. Επιδόσεις: Αυξημένες επιδόσεις με σκοπό τη μείωση του αποτυπώματος διοξειδίου του άνθρακα της λειτουργίας του δικτύου είναι το σημερινό ζητούμενο. Ένα πλαίσιο απαιτείται ώστε να δοθεί η δυνατότητα ενσωμάτωσης καινοτόμων μεθόδων διαχείρισης της κίνησης, υπολογισμού της χωρητικότητας, ισοκατανομής φόρτου και υψηλότερο επίπεδο χρησιμοποίησης ώστε να ανταπεξέλθει σε αυτό το αίτημα.

9. Ευέλικτο επίπεδο ελέγχου: Μια κεντρικοποιημένη όψη του κατανεμημένου δικτύου μέσω του πεδίου ελέγχου παρέχει πιο αποτελεσματική ενορχήστρωση και αυτοματοποίηση των δικτυακών υπηρεσιών. Το πεδίο ελέγχου πρέπει να είναι σε θέση να προβλέψει επιπρόσθετες υπηρεσιακές προδιαγραφές, να λάβει προαιρετικά μέτρα για την κατανομή πόρων και να παραδώσει με υψηλή λεπτομέρεια καθορισμένες από τον χρήστη πολιτικές σε ροές δεδομένων ανά εφαρμογή.

Ως απάντηση, πολλές σχετικές αρχικές ιδέες και νέες προτάσεις συνδυάζονται ώστε να λύσουν τα προβλήματα αυτά και να προσφέρουν νέες δυνατότητες. Αυτό έχει οδηγήσει στο να γίνει αποδεκτό το SDN ως μια βιώσιμη τεχνολογία που ικανοποιεί τις απαιτήσεις.

Η ιδέα απομακρυσμένου ελέγχου του δικτύου μέσω λογισμικού δεν είναι καινούργια και χρονολογείται στις ημέρες της τηλεφωνίας. Η έρευνα στα δίκτυα έχει παραγάγει πολλά συστήματα λογισμικού που περιλαμβάνουν προγραμματισιμότητα στο επίπεδο δεδομένων και λοιπά χαρακτηριστικά SDN.

Πρώιμες Προσεγγίσεις στο Προγραμματιζόμενο Πεδίο Δεδομένων

Ο όρος Πεδίο Δεδομένων (Data Plane –DP) αναφέρεται σε μια αφαίρεση των δικτυακών συσκευών μέσω των οποίων διέρχονται τα πακέτα ή τα σήματα φωνής. Γενικά αυτές οι συσκευές έχουν δυο διακριτές ικανότητες. Όταν έχουν ικανότητα DP, προωθούν παθητικά τα δεδομένα χωρίς να τα αλλάζουν.

Η ανάγκη για αναπτυσσόμενες ικανότητες στο Data Plane έχει αναγνωριστεί από ερευνητές και διαχειριστές δικτύων.

1. Το επόμενης γενιάς δίκτυο αναμένετο να διαθέτει προγραμματιζόμενες λειτουργίες ώστε οι ερευνητές και οι διαχειριστές να μπορούν να εφαρμόζουν καινοτόμες ιδέες που θα το βελτίωναν. Είναι σχεδόν αδύνατον να γίνουν τέτοιοι πειραματισμοί σε λειτουργικό δίκτυο λόγω του φόβου παρεμπόδισης της ροής των δεδομένων της επιχείρησης. Αυτή η προσπάθεια οδήγησε σε δυο κατευθύνσεις προγραμματιζόμενων πεδίων ελέγχου και πεδίου μεταγωγής δεδομένων. Ο προγραμματισμός στο πεδίο δεδομένων επικεντρώνεται περισσότερο σε αλλαγές στο πακέτο και στις επικεφαλίδες αυτού σε αντιστοίχηση με τις εντολές στο πεδίο ελέγχου. Μετά από τον αρχικό θόρυβο αυτών των μεταβολών, το ενδιαφέρον έχει αναθερμανθεί λόγω των απαιτήσεων του NFV. (Network Function Virtualization – προσομοίωση δικτυακών λειτουργιών)
2. Η προσομοίωση των δικτυακών λειτουργιών απαιτεί την επιλογή διαφορετικού λογισμικού ανάλογα με την επικεφαλίδα του εκάστοτε πακέτου. Έχει ήδη δημιουργηθεί μια τέτοια πλατφόρμα όπως με το (a) Shared Node Operating System (NodeOS) για τη διαχείριση διαμοιραζόμενων πόρων. (β) ένα σύνολο από περιβάλλοντα εκτέλεσης (EEs) όπου το καθένα καθορίζει μια ιδεατή μηχανή για λειτουργίες στα πακέτα και (γ) ένα σύνολο από Ενεργές εφαρμογές (AAs) καθεμία εκ των οποίων εργάζεται εντός δεδομένου ΕΕ παρέχοντας μια από άκρου σε άκρο υπηρεσία. Η κατεύθυνση των πακέτων σε δεδομένη ΕΕ εξαρτάται από το γρήγορο ταίριασμα μορφής με τα πεδία της επικεφαλίδας και αν συνεχεία αποπολυπλέκεται στην κατάλληλη ΕΕ.
3. Άλλη οδηγήτρια δύναμη ήταν η ανάγκη για μια ενοποιημένη αρχιτεκτονική για διαχείριση των υποδομών η οποία δεν ήταν ακόμα εφικτή. Το βασικό όραμα είναι ακόμα ζωντανό στην ανάπτυξη κατά SDN-ελέγχου διαχείρισης των ενδιάμεσων συσκευών.

Αρχικά, οι συσκευές υπόκειντο σε ξεχωριστή διαχείριση και ήταν πρακτικά αδύνατο να προγραμματιστούν στο σύνολο τους ταυτοχρόνως. Οι αρχικές προσπάθειες να δοθούν ικανότητες προγραμματισιμότητας σε αυτές οδήγησαν σε δυο ενδιαφέρουσες προσεγγίσεις που χαρακτηρίζονται γενικότερα ως «Ενεργά Δίκτυα» (Active Networks):

1. Η προγραμματισιμότητα σε ποικίλο εύρος προστέθηκε στους μεταγωγείς και τους δρομολογητές μέσω εντολών εκτός εύρους ζώνης. Με αυτή την προσέγγιση η μορφή των πακέτων και τα περιεχόμενα τους μένουν αναλλοίωτα. Στις δικτυακές συσκευές προστέθηκε η ικανότητα καταφόπρτωσης προγραμμάτων που περιελάμβανα οδηγίες σχετικά με την επεξεργασία των πακέτων.
2. Στη δεύτερη προσέγγιση, προστέθηκαν πολύ μικρά τμήματα κώδικα στα ίδια τα πακέτα μετατρέποντας τα σε «κάπσουλες» οι οποίες εκτελόντουσαν εντός εύρους ζώνης στους δικτυακούς κόμβους. Αυτή η τεχνική οδηγούσε στην τροποποίηση της μορφής των πακέτων και των επικεφαλίδων οδηγώντας πρακτικά σε προγραμματιστικές εργασίες.

Ένας από τους σημαντικότερους καταλύτες των διεργασιών αυτών ήταν το πρόγραμμα Active Networks της αμερικάνικης D.A.R.P.A όπου καθοριστήκαν οι περισσότερες ορολογίες και τα απαραίτητα δομικά στοιχεία. Κάποια υποδείγματα αυτών των αρχικών τεχνολογιών είναι το ANTS και το IEEE P1520 (Standards Initiative for Programmable Networks).

Οι ιδέες αυτές αναπτύχθηκαν περαιτέρω και επί του παρόντος ενσωματώνονται σε προγράμματα όπως:

- Openflow
- ForCES (Forwarding and Control Element Separation) IETF RFC 5810
- POF (Protocol Oblivious Forwarding)
- P4 Programming Protocol-independent Packet Processors

Η προγραμματισιμότητα του Πεδίου Δεδομένων πιο συγκεκριμένα ήταν η πιο σημαντική ιδέα που ακολούθησαν οι ερευνητές της ενεργού δικτύωσης. Η αρχική ώθηση προέκυψε από τις δυσκολίες τσην εφαρμογή καινοτομιών σε ήδη λειτουργικά δίκτυα και από την ανάγκη να διατηρηθεί η πλατφόρμα δοκιμών ξέχωρα από αυτό το περιβάλλον. Η επίλυση παρόμοιων προβλημάτων επιχειρείται στα νεώτερα πρωτόκολλα όπως το OpenFlow και το ForCES.

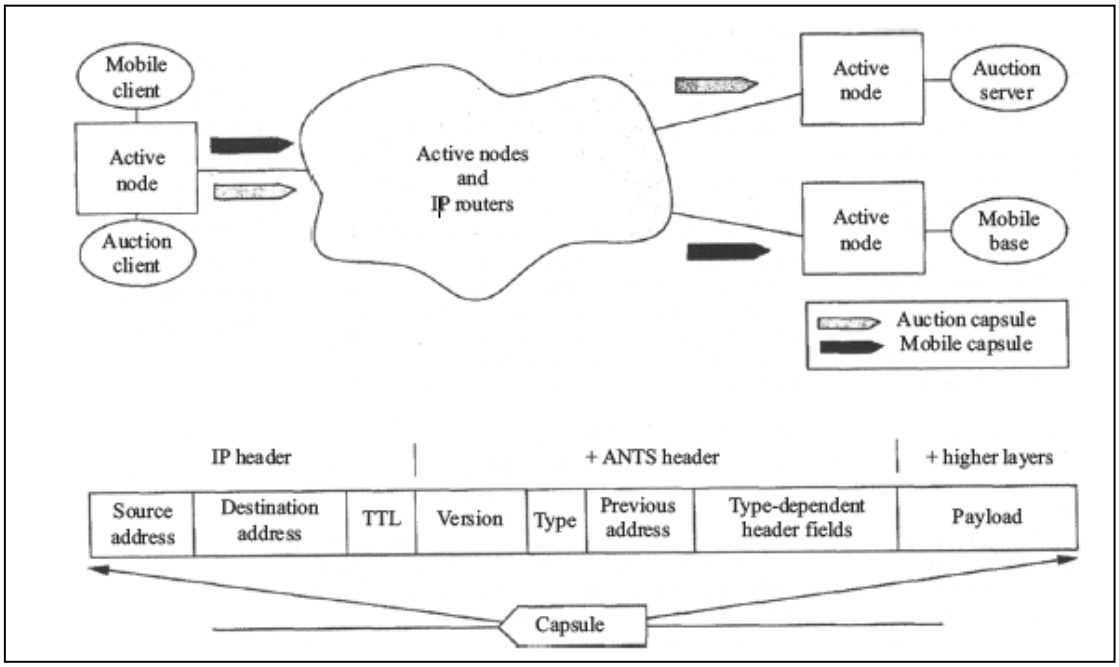
Μια σύντομη περιγραφή των τριών αυτών προσπαθειών δίνεται παρακάτω:

Active Networks Transport System (ANTS)

Η προσέγγιση του Active Network Transport System (ANTS) επικεντρωνόταν στο να δώσει στους χρήστες τη δυνατότητα να αναπτύξουν νέα πρωτόκολλα ή τροποποιημένα παλαιότερα πρωτόκολλα και να αντικαταστήσουν τη στατική δρομολόγηση με δυναμική και έξυπνη δρομολόγηση. Οι τρεις βασικοί στόχοι του ANTS προς τη κατεύθυνση αυτή ήταν η υποστήριξη:

- Μιας ποικιλίας υπαρχόντων πρωτοκόλλων
- Η δημιουργία νέων πρωτοκόλλων και
- Η ανάπτυξη των νέων πρωτοκόλλων

Μια νέα οντότητα που ονομάζεται «κάψουλα» δημιουργήθηκε αντικαθιστώντας μέρος του ωφέλιμου φορτίου IP από την αντίστοιχη επικεφαλίδα που περιείχε νέα πεδία όπως στο σχήμα που ακολουθεί:



Εικόνα 5: Η μορφή του πακέτου κατά ANTS (κάψουλα)

Τα νέα πεδία είναι τα ακόλουθα:

- Πεδίο “Version” που περιέχει την έκδοση του συστήματος ANT του κόμβου προέλευσης.
- Πεδίο “Type” το οποίο περιέχει την κατακερματισμένη τιμή (κατά MD5) του πρωτοκόλλου δρομολόγησης που επιθυμεί η κάψουλα.
- Το πεδίο “Previous Address” το οποίο είναι η διεύθυνση του προηγούμενου ενεργού κόμβου που επεξεργάστηκε την κάψουλα.

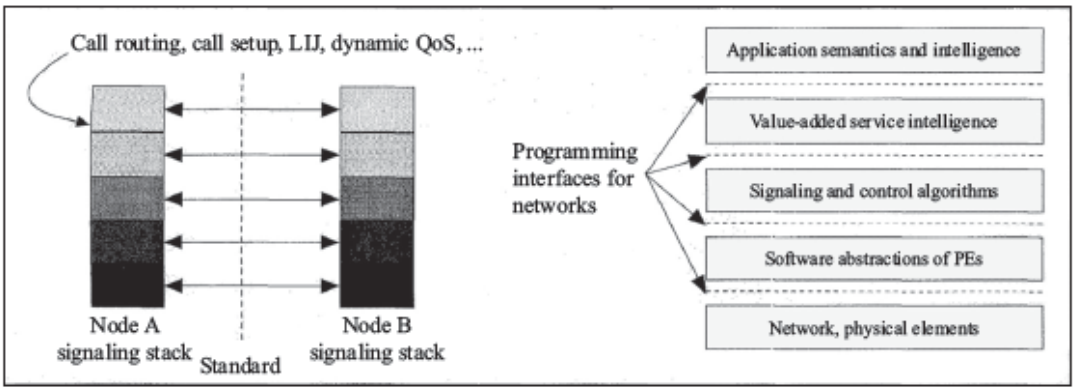
Η βασική ιδέα χρησιμοποιήθηκε αργότερα στο πρωτόκολλο OpenFlow και άλλα παρόμοια. Το δυσκολότερο πρόβλημα με το ANTS ήταν πώς να δουλέψουν τα νέα πρωτόκολλα με τις νέες IP επικεφαλίδες στα υπάρχοντα δίκτυα. Αργότερα ανακαλύφθηκε από τους ερευνητές ότι το

σχήμα αυτό ήταν ευάλωτο σε επιθέσεις DoS καθώς και σε προβλήματα διαχείρισης εύρους ζώνης.

IEEE P1520

Η πρόοδος των τεχνολογιών παρουσίασε την νέα και συναρπαστική ιδέα μεταχείρισης των δικτύων επικοινωνιών ως μια γιγαντιαία υπολογιστική πλατφόρμα. Αυτό έκανε επιτακτική την ανάπτυξη της δυνατότητας προγραμματισμού της και το πρότυπο IEEE P1520 ήταν το πρώτο βήμα προς αυτή την κατεύθυνση. Πιο συγκεκριμένα επικεντρώθηκε στον προγραμματισμό της σηματοδοσίας και των διεπαφών υπηρεσίας. Προϋποθέτει ένα δίκτυο υποδομής βασισμένο στην τεχνολογία ATM. Δυστυχώς το ATM αντικαταστάθηκε από την δικτύωση IP εγκαίρως οπότε οι συστάσεις του P1520 δεν εφαρμόστηκαν ποτέ στο σύνολο τους. Αλλά η βασική ιδέα του προγραμματισμού υιοθετήθηκε από τα πρωτόκολλα SDN όπως το OpenFlow ως κεντρική ιδέα στην εξέλιξη τους.

Στο μοντέλο αναφοράς του P1520 που παρουσιάζεται στην Εικόνα 6, υπάρχει μια διαστρωματοποιημένη αρχιτεκτονική με οντότητες σε κάθε επίπεδο και καθορισμένες διεπαφές μεταξύ των επιπέδων. Οι διεπαφές επιτρέπουν υπηρεσίας που επαυξάνουν την αξία του δικτύου, γενικευμένες υπηρεσίες δικτύου και διεπαφές στις φυσικές συσκευές.



Εικόνα 6: Τα επίπεδα του πρωτοκόλλου IEEE P1520

NETSCRIPT

Παρόμοιο με τις προηγούμενες προσεγγίσεις, το NetScript αναπτύχθηκε ως γλώσσα προγραμματισμού μοντελοποιημένη πάνω στην Javascript. Τα προγράμματα του διατίθεντο στους δικτυακούς κόμβους και εκτελούντο εκεί ώστε να αποκτήσουν νέες λειτουργίες δρομολόγησης και μεταγωγής. Παρείχε ευκολία στον προγραμματισμό τόσο για ενδιάμεσους καθώς και τερματικούς κόμβους στο δίκτυο. Το NetScript μπορεί να χρησιμοποιηθεί ώστε να χτίσει φίλτρα ροών πακέτων, δρομολογητών, αναλυτών πακέτων, επεξεργαστών πολυμεσικών ροών κοκ. Μια βασική παρακίνηση για το NetScript ήταν η ενσωμάτωση προηγμένων χαρακτηριστικών στο δίκτυο χωρίς να χρειαστεί αναμονή για την αργή και μερικές φορές μη βελτιστοποιημένη διαδικασία προτυποποίησης.

Αρχικές Προσεγγίσεις στον διαχωρισμό Πεδίου Ελέγχου (CP) και Πεδίου Δεδομένων (DP)

Ο όρος πεδίο ελέγχου αναφέρεται στη συλλογή αλγόριθμων και εντολών που χρησιμοποιούνται για την αλλαγή της συμπεριφοράς των πακέτων που διασχίζουν τους κόμβους του δικτύου. Στον κόσμο της τηλεφωνίας η ανάγκη διαχωρισμού των δεδομένων από τις εντολές που ελέγχουν την συμπεριφορά του δικτύου έγινε κατανοητό πολύ νωρίς και έγιναν προσπάθειες ώστε να ανακαλυφθούν νέες προσεγγίσεις προς αυτή την κατεύθυνση. Η AT&T είχε ένα πρόγραμμα (NCP – Network Control Program) που ενσωμάτωνε την ιδέα διαχωρισμού του πεδίου ελέγχου από το πεδίο δεδομένων πιθανότατα για πρώτη φορά. Αναπαριστούσε μια καθολική εικόνα της δικτυακής τοπολογίας και καθιστούσε τα δίκτυα περισσότερο διαχειρίσιμα.

Παρόμοιες προσπάθειες στην κατεύθυνση του διαχωρισμού του πεδίου δεμένων από το πεδίο ελέγχου υλοποιήθηκαν και σε άλλα είδη δικτύων:

- Tempest στο ATM
- ForCES στο Ethernet
- RCP στο BGP
- Path Computation Element (PCE) στο MPLS

Το NCP δημιουργήθηκε ώστε να λειτουργεί στο ARPANET (ο πρόδρομος του Internet) και παρείχε τα ενδιάμεσα επίπεδα της στοίβας πρωτοκόλλων που τρέχει στα τερματικά. Χρησιμοποιούσε δυο διευθύνσεις θυρών για να εγκαταστήσει δυο συνδέσεις με αμφίδρομη επικοινωνία και παρείχε έλεγχο ροής μεταξύ διεργασιών που έτρεχαν σε διαφορετικά τερματικά. Το NCP παρείχε το επίπεδο μεταφοράς του ARPANET όσον αφορά τα επίπεδα του OSI. Το επίπεδο αυτό αποτελείτο από δυο πρωτόκολλα: το ARPANET Host-to-Host Πρωτόκολλο (AHHP) και το Initial Connection Protocol (ICP). Το NCP είναι πρόδρομος του TCP όσον αφορά τη στοίβα TCP/IP. Την 1η Ιανουαρίου 1983 κατέστη παρωχημένο αφού το ARPANET άλλαξε τα κεντρικά του δικτυακά πρωτόκολλα από το NCP στην στοίβα TCP/IP δημιουργώντας το ξεκίνημα το σύγχρονου Διαδικτύου.

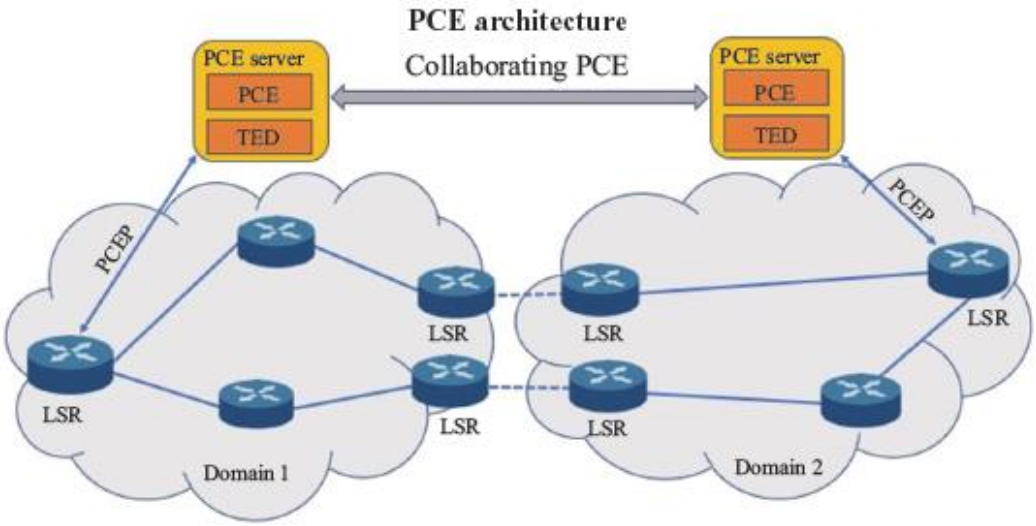
Path Computation Element Protocol (PCE)

Ο υπολογισμός της διαδρομής δρομολόγησης μεταξύ ενός δεδομένου ζευγαριού πηγής και προορισμού γίνεται επεξεργαστικά έντονο όταν λαμβάνονται υπόψη περιορισμοί QoS και διαχείρισης κίνησης (TE – traffic engineering). Το πρωτόκολλο PCE δημιουργήθηκε ώστε να βοηθήσει σε αυτήν την περίπτωση και μπορεί να ληφθείως παράδειγμα διαχωρισμού της δυνατότητας αυτής από τους δικτυακούς κόμβους ή το πεδίο δεδομένων και ανάθεσης στο πεδίο ελέγχου. Το PCE μπορεί να καθοριστεί ως μια οντότητα που είναι ικανή να υπολογίσει μια κατάλληλη δικτυακή διαδρομή για την μετάδοση δεδομένων μεταξύ πηγής και προορισμού εφαρμόζοντας επεξεργαστικούς περιορισμούς. Στα δίκτυα πριν το SDN μπορεί να είναι ένας μόνο εξωτερικός διακομιστής ή και ένας δρομολογητής. Το PCE πρωτόκολλο περιγράφεται στο RFC 4655 και στο RFC 5440.

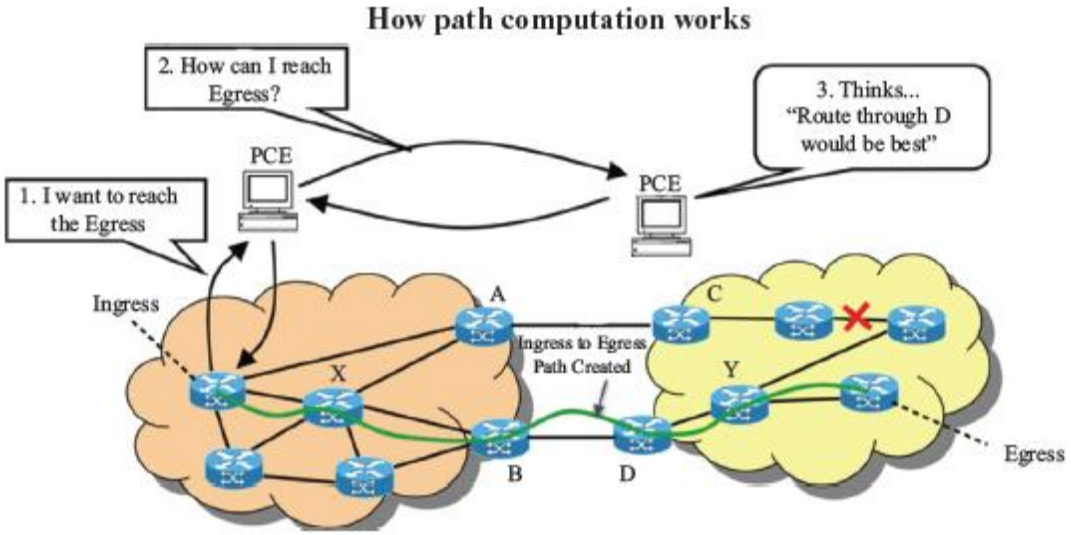
Η αρχιτεκτονική PCE περιλαμβάνει τα παρακάτω δομικά στοιχεία (Εικόνα 7):

1. Το Στοιχείο Υπολογισμού Διαδρομής (Path Computation Element –PCE): Υπολογίζει πολύπλοκες διαδρομές βασισμένο στην ζήτηση για κίνηση δεδομένων και δικτυακούς περιορισμούς.
2. Το Στοιχείο Υπολογισμού Διαδρομής Πελάτη (Path Computation Client – PCC): Ζητά να γίνει υπολογισμός μιας διαδρομής από το PCE.
3. Τη Βάση Δεδομένων Διαμόρφωσης Κίνησης (Traffic Engineering Database – TED): Περιλαμβάνει την τοπολογία, τους κόμβους, τις ζεύξεις τις σχέσεις, τις πληροφορίες πόρων και τις τιμές των πόρων του δικτύου.
4. Το Πρωτόκολλο Επικοινωνίας του Στοιχείου Υπολογισμού Διαδρομής (Path Computation Element Communication Protocol): Ένα TCP πρωτόκολλο επικοινωνίας για επικοινωνία PCC-PCE και PCE-PCE.

Ο πραγματικός υπολογισμός μπορεί να γίνει είτε με κεντρικοποιημένο ή κατανεμημένο τρόπο.



Εικόνα 7: Τυπική αρχιτεκτονική PCE



Εικόνα 8 Τυπική λειτουργία PCE

Ακολουθούνται τα παρακάτω βήματα στην λειτουργία του PCE (φαίνονται στο σχήμα της Εικόνας 8)

1. Το PCC εγκαθιστά σύνδεση TCP με τον PCE ώστε να φτάσει σε δοσμένο δικτυακό προορισμό.
2. Εγκαθίσταται μια PCEP σύνοδος με τη χρήση της σύνδεση TCP και ανταλλάσσονται μηνύματα “Session Open”.
3. Το PCC στέλνει “PCReq Message” ώστε να αιτηθεί διαδρομής έως το PCE. Περιλαμβάνει την πηγή της πληροφορίας, τον προορισμό της πληροφορίας, περιορισμούς διαδρομής (όπως απαιτούμενο εύρος ζώνης, κόμβοι που πρέπει να αποφευχθούν) και λοιπές TE προδιαγραφές,.
4. Το PCE απαντά στο PCC είτε με τις υπολογισμένες διαδρομές η με αρνητική απόκριση που συμπεριλαμβάνει τονν λόγο που δεν μπορούσε να υπολογιστεί η διαδρομή.
5. Ο ακραίος δρομολογητής στέλνει δεδομένα στον προορισμό χρησιμοποιώντας την κατά PCE υπολογισμένη διαδρομή.

Κατά τη διάρκεια αυτών των συναλλαγών η σύνοδος PCEP μπορεί να κλείσει από το PCE ή το PCC με αποστολή μηνύματος “Close Message”.

Πρώιμες Προσεγγίσεις στην Εικονικοποίηση Δικτυακών Λειτουργιών (Network Function Virtualization)

Οι ρίζες της εικονικοποίησης δικτύων εντοπίζονται στην ιδέα προγραμματιζόμενου Πεδίου Δεδομένων όπως στηρίχθηκε από το μοντέλο ενεργών δικτύων μέσω κώδικα κάψουλας. Επί του παρόντος το αρκτικόλεξο NFV σηματοδοτεί τη χρήση λογισμικού για πολλές δικτυακές λειτουργίες. Αυτό καθιστά δυνατή την αποδέσμευση των δικτυακών λειτουργιών από το υποκείμενο υλισμικό και επιτρέπει την αλληλοδέσμευση τους ώστε να δημιουργηθούν υπάρχουσες και νέες δικτυακές υπηρεσίες.

Η βασική ιδέα πίσω από την τεχνολογία NFV είναι η αποσύνδεση (απόζευξη) των δικτυακών υπηρεσιών από το υλικό στο οποίο τρέχουν. Είναι παρόμοιο με το διαχωρισμό Πεδίου Ελέγχου και Πεδίου Δεδομένων αλλά αφορά τις υπηρεσίες παρά την παραμετροποίηση και την τοπολογία. Οι επίσημες προσπάθειες ανάπτυξης του NFV ξεκίνησαν με τη δημιουργία του Industry Specification Group (ISG) σχετικά με το NFV από τον οργανισμό ETSI (European Telecommunications Standards Institute). Η σύσταση του ISG περιλαμβάνει κυρίως διεθνείς παρόχους υπηρεσιών τηλεφωνίας.

Μια γενικευμένη αρχιτεκτονική του NFV περιέχει τα ακόλουθα στοιχεία:

1. Στην κορυφή βρίσκονται οι προσομοιωμένες δικτυακές λειτουργίες (VNF –virtualized network functions)ως βασικά στοιχεία που πρέπει να συνδυαστούν κατάλληλα ώστε να αποδώσουν νέες δικτυακές υπηρεσίες.
2. Αυτό το επίπεδο επικοινωνεί με το επίπεδο εικονικών πόρων για επεξεργασία, αποθήκευση και δικτύωση. Η δικτυακή υπηρεσία τα παραμετροποιεί ώστε να επιτυγχάνονουν τους στόχους εικονικά.
3. Στο κάτω μέρος βρίσκεται το παρωχημένο υλικό διαμέσω του οποίου υλοποιείται ολόκληρη λογική υποδομή.

Είναι ξεκάθαρο ότι αυτή η προσέγγιση είναι παρόμοια με αυτή του SDN. Επικεντρώνεται στον προγραμματισμό του πεδίου δεδομένων σε αντίθεση με το SDN που ασχολείται κυρίως με τον προγραμματισμό του Πεδίου ελέγχου. Είναι πιθανό να συνδυαστούν οι τεχνολογίες SDN και NFV σε μια εννοποιημένη αρχιτεκτονική και πολλές ερευνητικές πρωτοβουλίες επικεντρώνονται σε αυτό ακριβώς.

GENI

Ένα από τα πιο λαμπρά παραδείγματα της τεχνολογίας NFV είναι το έργο Global Environment for Network Innovations (GENI) και συνδυάζει ιδέες τόσο από το NFV όσο και από το SDN ώστε να κάνει ένα μεγάλο δίκτυο προγραμματιζόμενο. Η νέα ιδέα της «τεμαχισμένης» δικτύωσης έχει εισαχθεί από το GENI. Ένα δικτυακό «τεμάχιο» είναι μια συλλογή από πόρους (επεξεργαστικούς, αποθηκευτικούς και δικτυακούς) που ανατίθενται προσωρινά σε ένα χρήστη για δικτυακό πειραματισμό. Μετά την ολοκλήρωση των πειραμάτων, οι πόροι επιστρέφονται στο δίκτυο. Η αρχιτεκτονική SDN έχει χρησιμοποιηθεί ώστε να εισαχθεί και ο προγραμματισμός. Η πρωτοβουλία GENI τελικά εξελίχθηκε σε μια πειραματική υποδομή που καλύπτει το σύνολο της Αμερικής με σκοπό την έρευνα στη δικτύωση και τα κατανεμημένα συστήματα.

Πρώιμες Προσεγγίσεις σε Δικτυακά Λειτουργικά Συστήματα (Network Operating Systems –NOS)

Καθώς τα παραδοσιακά δίκτυα τηλεπικοινωνιών γίνονταν όλο και πιο περίπλοκα, προέκυψε η ανάγκη για κάποιας μορφής κεντρικοποιημένη προσέγγιση στη διαχείριση των δικτυακών λειτουργιών. Η ανάπτυξη των υπολογιστών και του λογισμικού οδήγησε σε πολλές αρχικές προσπάθειες προς την κατεύθυνση αυτή. Ένα δικτυακό λειτουργικό σύστημα χτίζει μια εικόνα της κατάστασης του δικτύου από τις πληροφορίες που παρέχουν οι μεταγωγείς και λοιπά δικτυακά εξαρτήματα. Αυτό οδήγησε σε μια διαστρωματοποιημένη αναπαράσταση του δικτύου όπως αυτό δομείται από το πεδίο δεδομένων το πεδίο διαχείρισης δικτύου και το πεδίο λογικής ελέγχου. Μπορεί να εκληφθεί ως πρόδρομος του SDN.

ETHANE

Μια από τις περισσότερο υποσχόμενες προσεγγίσεις στη νέα αρχιτεκτονική που βασίζεται σε κεντρικοποιημένο ελεγκτή ήταν το πρωτόκολλο ETHANE που υλοποιήθηκε από το Πανεπιστήμιο Stanford. Μπόρεσε να δώσει λύση στο πρόβλημα του ελέγχου πρόσβασης σύμφωνα με τις εταιρικές πολιτικές ασφαλείας και βασίστηκε στις ροές των μεγάλων δικτύων. Η ιδέα της μείωσης της πολυπλοκότητας των μεταγωγέων ώστε να είναι απλοί περιέκτες των πινάκων ροής προέρχεται από το Ethane. Αυτό ήταν ο πρόδρομος του ελεγκτή SDN. Μια ενδιαφέρουσα όψη της προσέγγισης αυτής ήταν ο καθορισμός των πολιτικών ασφαλείας με πιο κατανοητά ονόματα όπως «διακομιστής μισθοδοσίας», “Bob” κοκ. Κάποιες από τις καινοτομίες του Ethane είναι οι κάτωθι:

1. Η καθολική πολιτική ασφαλείας εφαρμόζεται σε κάθε μεταγωγέα με τρόπο που δεν επιτρέπει την εξαπάτηση.
2. Όλα τα πακέτα μπορούν να ανιχνευθούν μέχρι τον αποστολέα και τη φυσική θύρα εισόδου. Αυτή η ιδιότητα μπ[ορεί να επεκταθεί και σε παλαιότερα πακέτα το οποίο είναι εξαιρετικά χρήσιμο για την ασφάλεια και εγκληματολογικούς ελέγχους.
3. Το Ethane χρησιμοποιεί πολύ απλούς μεταγωγείς.

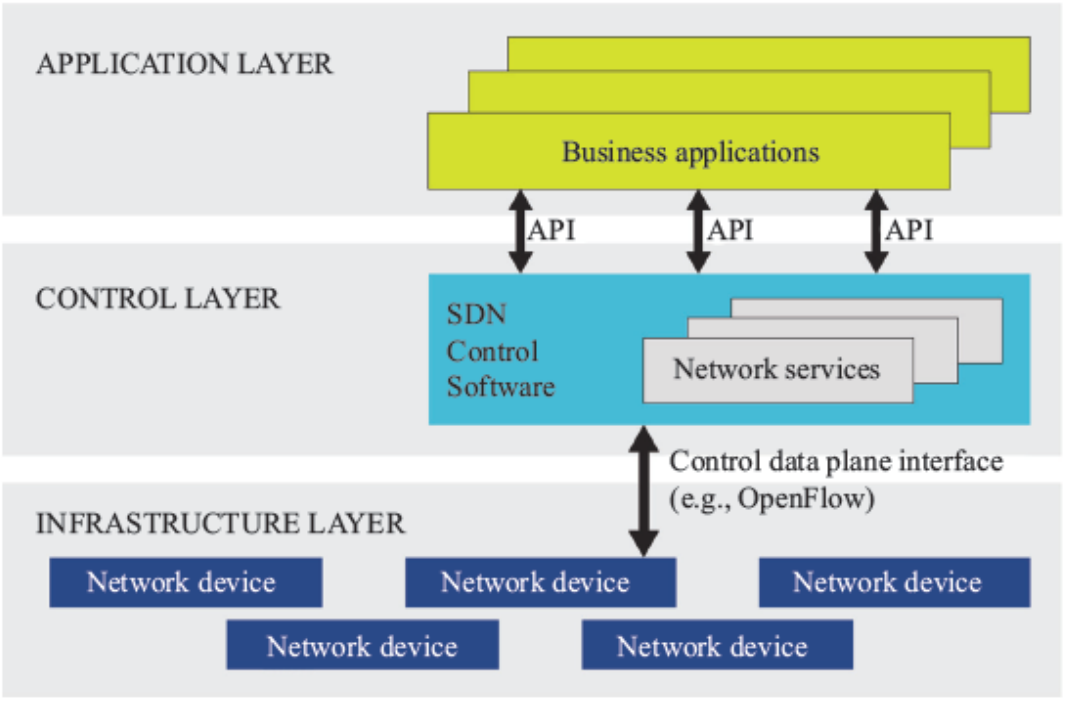
Όλα τα παραπάνω επιτυγχάνονται χάρη στην καινοτομία και την υλοποίηση ενός κεντρικού ελεγκτή Ethane ο οποίος εκλαμβάνεται ως πρόδρομος του ελεγκτή SDN. Ο ελεγκτής επιτελούσε όλες τις λειτουργίες δρομολόγησης, ονοματοδοσίας, δεδηλωμένων πολιτικών και ελέγχων ασφαλείας. Αυτό οδήγησε στην κατασκευή πολύ απλών μεταγωγέων με SRAM ολοκληρωμένα.

Άλλες πρωτοβουλίες:

Η πρωτοβουλία της Ευρωπαϊκή Ένωσης με όνομα FIRE (Future Internet Researh and Initiative) είναι παρόμοια στο πνεύμα αλλά και στο όραμα με τις προσπάθειες σχετικά με το SDN στην Αμερική. Στοχεύει σε δυο ερευνητικά έργα: την καλύτερη αρχιτεκτονική για το μελλοντικό διαδίκτυο και τον πειραματισμό σε μεγάλη κλίμακα. Ήταν παρόμοια με τα έργα του NSF “Future Internet Design” (FIND) και GENi. Η ιδέα της γεφύρωσης όλων των κενών μεταξύ έρευνας και εμπορικής χρήσης του διαδικτύου είναι πολύ ευρεία και φιλόδοξη αλλά οδήγησε στο κίνημα ανάπτυξης του SDN.

Επισκόπηση της Δικτύωσης Μέσω Λογισμικού

Το σχήμα της Εικόνας 9 μας δίνει μια όψη της ιεραρχίας SDN. Ο χρήστης αλληλεπιδρά με το δίκτυο στο επίπεδο υποδομής (infrastructure).



Εικόνα 9: Αφαιρετική απεικόνιση του SDN

Υπάρχουν πολλοί τρόποι με τους οποίους μπορεί να προσεγγιστεί η αρχιτεκτονική του SDN. Ο ρόλος των διαφορετικών επιπέδων (ονομάζονται και στοίβες –stacks ή πεδία –planes) εξηγείται παρακάτω ξεκινώντας από το χαμηλότερο επίπεδο.

1. **Επίπεδο Υποδομής ή Πεδίο Δεδομένων (DP)** Πρόκειται για το φυσικό και υλικό επίπεδο που αποτελείται από SDN-συμβατούς μεταγωγείς και δρομολογητές. Υπάρχει επίσης πιθανότητα υβριδικών δικτύων στα οποία υλικό που δεν είναι SDN-συμβατό μπορεί να συνυπάρξει στο SDN δίκτυο. Διαθέτει δυο υποεπίπεδα:
    - τη δικτυακή υποδομή που περιέχει το φυσικό υλικό
    - τη διεπαφή Southbound (Southbound Interface –SBI) που είναι λογισμικό εντός των δικτυακών συσκευών ώστε να επικοινωνούν με το Πεδίο Ελέγχου.
2. **Επίπεδο Ελέγχου ή Πεδίο Ελέγχου (CP)** Αυτό το επίπεδο έχει τρία υποεπίπεδα.
    - Επόπτη (hypervisor) που αλληλεπιδρά με τις δικτυακές συσκευές
    - Δικτυακό λειτουργικό Σύστημα (NOS) ή ελεγκτή SDN
    - Διεπαφή Northbound (Northbound Interface –NBI) που αλληλεπιδρά με το Πεδίο Εφαρμογής
3. **Επίπεδο εφαρμογής ή Πεδίο Εφαρμογής και Διαχείρισης (AP/MP)**
    Το πεδίο αυτό έχει τρια υποεπίπεδα.
    Είναι το κορυφαίο επίπεδο στην απλοποιημένη αρχιτεκτονική SDN και απαρτίζεται από τις εφαρμογές διαχείρισης δικτύου διαφορετικών ειδών. Αυτές είναι η καρδιά των SDN προγραμματιζόμενων δικτύων.
    - Η βασιζόμενη σε γλώσσα προγραμματισμού προσομοίωση αλληλεπιδρά με το NBI στο Πεδίο Ελέγχου.
    - Οι γλώσσες προγραμματισμού μεταφράζουν τις προδιαγραφές των εφαρμογών σε λογική για τον ελεγκτή.
    - Δικτυακές Εφαρμογές

Πεδίο Δεδομένων (Data Plane –DP)

Επίπεδο DP1 ή το κατώτερο επίπεδο του SDN: Δικτυακή Υποδομή

Περιλαμβάνει δικτυακές συσκευές όπως μεταγωγείς, δρομολογητές και προεπιλεγμένες πύλες οι οποίες είναι ως επί το πλείστον υλικό. Σε κανονικές δικτυακές αρχιτεκτονικές επιτελούν λειτουργίες τόσο μεταγωγής όσο και ελέγχου. Στο SDN, αφαιρούνται οι λειτουργίες ελέγχου και ενσωματώνονται στο SDNC. Το απομειωμένων δυνατοτήτων υλικό μεταπίπτει σε συσκευή προώθησης των δεδομένων. Στην ιδανική περίπτωση είναι απλά κουτιά του εμπορίου (commodity ή whiteboxes) που δεν περιλαμβάνουν κάποιο λογισμικό που ανήκει στον κατασκευαστή τους. Στο ενδιάμεσο φαίνεται ότι επικρατεί μια υβριδική κατάσταση η οποία θα περιλαμβάνει τόσο SDN-συμβατές (OpenVswitch) και μη συμβατές δικτυακές συσκευές (όπως από Cisco, Juniper κ.α)

Επίπεδο DP2 του SDN: Διεπαφή Southbound (SBI)

Όπως και όλα τα άλλα υποσυστήματα, πολλά από τα SBI που έχουν αναπτυχθεί προέρχονται από λογισμικά του παρελθόντος. Επί του παρόντος το κυρίαρχο πρωτόκολλο είναι το OpenFlow και αποτελεί το De facto πρότυπο. Αυτά τα πρωτόκολλα διαθέτουν ένα στοιχείο στο Πεδίο Ελέγχου και ένα στοιχείο στο εσωτερικό της δικτυακής συσκευής. Ακολουθεί μια σύντομη περιγραφή του ποιο σημαντικού SBI πρωτοκόλλου.

1. OpenFlow
   Αναπτύχθηκε από ερευνητές του πανεπιστημίου Stanford και σήμερα η εξέλιξη του διαχειρίζεται από το Open Network Foundation (ONF). Η τελευταία έκδοση του είναι η 1.4. Το λογισμικό πελάτης εδρεύει εντός των δικτυακών συσκευών ή μεταγωγέων και το λογισμικό εξηπηρετητή είναι μέρος του λογισμικού του ελεγκτή.
2. ForCES
   Το πρωτόκολλο Forwardind and Control Element Separation (ForCES) αποτελεί μια προσέγγιση από την IETF στα προγραμματιζόμενα δίκτυα. Οι στόχοι του είναι πιο ολοκληρωμένοι από ότι στο πρόγραμμα του OpenFlow αν και δεν είναι τόσο διαδεδομένο όσο αυτό. Καθορίζεται στο RFC 5810 (περιγραφή πρωτοκόλλου), RFC 5812 (μοντέλο στοιχείου μεταγωγής) και επικεντρώνεται περισσότερο στην διάθεση μιας προγραμματιστικής διεπαφής για δικτυακές συσκευές του εμπορίου. Ο καθορισμός των προδιαγραφών ολοκληρώθηκε το 2015.

Η τεχνολογία SDN για οπτικά και ασύρματα δίκτυα είναι λίγο περισσότερο περίπλοκη γιατί τα σήματα στο φυσικό επίπεδο είναι αναλογικά. Αφού ολοκληρωθεί η μετατροπή στο ψηφιακό πεδίο και η πακετοποίηση, μπορεί να εφαρμοστεί η γνωστή αρχιτεκτονική SDN.

Πεδίο Ελέγχου (Control Plane -CP)

Το πεδίο αυτό διαθέτει τις παρακάτω λειτουργίες:

1. Αναπαριστά μια καθολική όψη της τοπολογίας και του χώρου διευθύνσεων των δικτυακών συσκευών που συνδέονται στο SDNC.
2. Επιτρέπει τον τεμαχισμό του δικτύου. Ως τεμάχιο ορίζεται ένα εικονικό δίκτυο που περιλαμβάνει προκαθορισμένους δικτυακούς, επεξεργαστικούς και αποθηκευτικούς πόρους.

Έχουν αναπτυχθεί πολλές τέτοιες εφαρμογές που ονομάζονται «Επόπτες» (hypervisors) όπως για παράδειγμα τα Flow Visor, OpenVirteX, AutoSlice κλπ. Θα επικεντρωθούμε στον Flow Visor αφού επιτρέπει τη δημιουργία πολλών εικονικών δικτύων που περιλαμβάνουν OpenFlow-συμβατούς μεταγωγείς. Επιτρέπει σε πολλά λογικά δίκτυα να συνυπάρχουν σε μια φυσική υποδομή χωρίς να αλληλοπαρεμβάλλονται.

Επίπεδο CP2 του SDN:

Το επίπεδο αυτό περιλαμβάνει τον SDN ελεγκτή (SDNC) ο οποίος μπορεί να εκληφθεί ως ένα εξεζητημένο λειτουργικό σύστημα. Το πεδίο ελέγχου (CP) μεταφράζει τις δικτυακές προδιαγραφές σε εργασίες που πρέπει να υλοποιηθούν από τις δικτυακές συσκευές.

Ο ελεγκτής SDN (SDNC) βρίσκεται στην καρδιά της SDN αρχιτεκτονικής μεταφράζοντας τις απαιτήσεις από τις northbound εφαρμογές σε εντολές OpenFlow για τις αντίστοιχες ελεγχόμενες Southbound συσκευές. Έχουν αναπτυχθεί πολλοί SDN ελεγκτές από διαφορετικές οπτικές γωνίες και απαιτήσεις. Λόγω της απουσίας μιας προτυποποιημένης οντότητας η επιλογή εξαρτάται από το ποια βασική ικανότητα θεωρείται πρωτεύουσα σε σχέση με τις άλλες. Οι SDN ελεγκτές μπορούν να παραμετροποιηθούν ως κεντρικοποιημένα ή κατανεμημένα συστήματα.

1. Ο κεντρικοποιημένος ελεγκτής SDN είναι μοναδική οντότητα ελέγχου μεγάλου αλλά καθορισμένου αριθμού δικτυακών συσκευών. Το σκοπούμενο πεδίο εφαρμογής είναι τα κέντρα δεδομένων, οι υποδομές νέφους και τα δίκτυα των παρόχων. Μερικά υποδείγματα είναι τα Beacon, Floodlight, Maestro,Trema, Ryu, eridian κ.α.
2. Οι κατανεμημένοι ελεγκτές SDN μπορεί να είναι είτε συστοιχία ή μια οντότητα φυσικά κατανεμημένη σε μεγάλης έκτασης δίκτυο. Μπορούν να μεγεθυνθούν ώστε να ανταπεξέλθουν σε κάθε μεγέθους δίκτυο. Κάποια υποδείγματα είναι τα Onix, HyperFlow, ONOS, yanc, PANE κ.α

Στην παρακάτω λίστα περιγράφονται οι σημαντικότεροι ελεγκτές:

1. OpenDaylight:
   Βασίζεται στο πρότυπο OSGi και περιλαμβάνει πρόσθετο για διαλειτουργικότητα με το OpenFlow καθώς και OpenFlow βιβλιοθήκη πρωτοκόλλων, υποστήριξη πρωτοκόλλων διαχείρισης για βάση δεδομένων Open Vswitch (OVSDB) και εργαλεία για YANG. Θεωρείται ότι μπορεί να υποστηρίξει οποιοδήποτε SDN δίκτυο ανεξαρτήτως προέλευσης. Εκδόθηκε πρώτη φορά το 2014.
2. OpenContrail
   Ο ελεγκτής αυτός προέρχεται από την εταιρεία Juniper αλλά είναι ένα ανοικτό πρότυπο. Είναι αδειοδοτημένο κατά Apache 2.0 και υποστηρίζει την προσομοίωση δικτύων, τον προγραμματισμό τους, την αυτοματοποίηση και τις υποδομές Big Data. Πιο συγκεκριμένα, διαθέτει Northbound διεπαφές μαζί με μηχανή για analytics
3. Floodlight:
   Ο ελεγκτής αναπτύχθηκε από την εταιρεία Big Switch και γράφτηκε σε Java ενώ η άδεια του είναι επίσης Apache. Μπορεί να διαχειριστεί ανάμεικτα OpenFlow και μη OpenFlow δίκτυα και υποστηρίζει την πλατφόρμα νέφους OpenStack
4. Ryu:

   Υποστηρίζει το πλαίσιο SDN για την ανάπτυξη νέων εφαρμογών διαχείρισης και ελέγχου. Υποστηρίζει OpenFlow, NETCONF και OF-config.
5. FlowVisor:

   Μπορεί να συνδέσει OpenFlow μεταγωγείς σε πολλαπλούς OpenFlow ελεγκτές. Υποστηρίζει με ευκολία την προσομοίωση δικτύου διαιρώντας ένα φυσικό δίκτυο σε πολλαπλές λογικές τοπολογίες. Με αυτό τον τρόπο διασφαλίζει ότι το κάθε λογικό δίκτυο ελέγχει μόνο τους μεταγωγείς και τους πόρους που του έχουν ανατεθεί διαιρώντας και αναθέτοντας τον πίνακα ροής και το εύρος ζώνης του κάθε μεταγωγέα σε ανεξάρτητους ελεγκτές.
6. Open Network Operating System (ONOS):
   Πρόκειται για πρόγραμμα δημιουργίας λειτουργικού συστήματος για μεγάλα δίκτυα ανεξάρτητο από εταιρείες. Πιο συγκεκριμένα ικανοποιεί αυστηρές προδιαγραφές ικανοτήτων σχετιζόμενες με υψηλή απόδοση χαμηλές χρονοκαθυστερήσεις, μεγάλης έκτασης παγκόσμια δίκτυα, υψηλές διαθεσιμότητες κοκ.

Διεπαφή East-West Bound

Το επίπεδο 4 περιλαμβάνει επίσης το East-West Bound Interface (EWBI) διαμέσου του οποίου αλληλεπιδρά με SDN ελεγκτές του ιδίου επιπέδου. Αυτό συμβαίνει σε δίκτυο με κατανεμημένους ελεγκτές. Η διεπαφή EWBI δεν έχει προτυποποιηθεί ακόμα αν και πρωτόκολλα όπως το ForCES CE-CE και το SDNi αναπτύσσονται ώστε να ανταπεξέλθουν στην πρόκληση.

Επίπεδο CP3 του SDN: Διεπαφή NorthBound (NBI)

Η διεπαφή NBI εντός του SDN ελεγκτή αναπαριστά μια αφαιρετική όψη του δικτύου στο υποεπίπεδο Εφαρμογών της βασιζόμενης σε γλώσσα προσομοίωσης. Ικανότητες όπως ο υπολογισμός διαδρομής, η ασφάλεια, η δρομολόγηση κλπ, καθίστανται διαθέσιμες στις εφαρμογές μέσω αυτής της διεπαφής. Όπως και με πολλές άλλες διεπαφές και αυτή δεν είναι ακόμα προτυποποιημένη αφήνοντας πολλές δυνατότητες στην εξέλιξη της.

Πρωτόκολλα NBI και Προτυποποίηση

Δεν υπάρχει προτυποποιημένη προσέγγιση στο NBI επί του παρόντος αλλά αναδύεται ένα πλαίσιο. Τα δυο πιο κοινά πλαίσια είναι:

1. Restful State Transfer (REST) ή RESTful APIs. Αναπτύσσονται ως έργο ανοιχτού κώδικα. Η REST χρησιμοποιεί μηνύματα HTTP ώστε να επικοινωνήσει με τον ελεγκτή SDN, την εντολή GET για την ανάκτηση δεδομένων και την εντολή PUT για αποστολή. Οι δυο πιο κοινοί τρόποι διαχείρισης των RESTful APIs είναι η JSON (Javascript Object Notation) και η XML (eXtensible Markup Language).
2. Το πρωτόκολλο NETCONF (Network Configuration Protocol) περιγράφεται στο RFC 6241 της IETF. Το NETCONF βασίζεται στο SNMP και είναι γενικότερα μια εναλλακτική στο OpenFlow για την παραμετροποίηση των συσκευών μέσω SOUTHBOUND. Σε ορισμένες πλατφόρμες SDN όπως το OpenDaylight χρησιμοποιείται και ως διεπαφή NORTHBOUND. Η YANG (Yet Anoter Generation) είναι η γλώσσα μοντελοποίησης δεδομένων που αναπτύχθηκε για το NETCONF.

Πεδίο εφαρμογής και διαχείρισης

Επίπεδο AP1 του SDN: Προσομοίωση βασιζόμενη στη γλώσσα

Σε αυτό το επίπεδο, μια υψηλού επιπέδου αφαιρετική εικόνα του δικτύου είναι διαθέσιμη χάρη σε γλώσσες όπως η Pyretic. Ο «στατικός διαμερισμός» είναι μια ικανότητα του επιπέδου εφαρμογής η οποία είναι δυνατή χωρίς Επόπτη (Hypervisor).

Επίπεδο AP2 του SDN: Γλώσσες Προγραμματισμού

Γενικά, υφίστανται διαφορετικές γλώσσες που χρησιμοποιούνται για διαφορετικούς λόγους. Οι ελεγκτές SDN έχουν γραφτεί σε C, Python και Javascript.Οι γλώσσες διεπαφής με αυτούς είναι οι NETCONF και YANG αποδεικνύοντας ότι το πεδίο του προγραμματισμού SDN δεν έχει τυποποιηθεί ακόμα.

Επιπροσθέτως, το πλέον κοινά χρησιμοποιημένο πρωτόκολλο OpenFlow είναι γραμμένο με χαμηλού επιπέδου γλώσσα μηχανής και χρησιμοποιείται για τον έλεγχο δικτυακών συσκευών όπως οι μεταγωγείς και οι δρομολογητές. Αλλά όπως και στην περίπτωση των υπολογιστών, η προγραμματιζόμενη δικτύωση απαιτεί γλώσσες προγραμματισμού ώστε να ανταπεξέλθει σε πολλά θέματα όπως:

1. Τη χρησιμοποίηση υψηλού επιπέδου αφαιρέσεων ώστε να διαχειριστεί τον προγραμματισμό του υλικού.
2. Την αποφυγή αλληλοεπικαλύψεων και συγκρούσεων κατά την εκτέλεση διαφορετικών εργασιών

3. Την εισαγωγή της επαναχρησιμοποίησης και τμηματικοποίησης του κώδικα στο Πεδίο Ελέγχου.
4. Την ενσωμάτωση της προσομοίωσης δικτύων στο SDN
5. Την έκφραση υψηλότερου επιπέδου αφαιρέσεων όπως οι πολιτικές και οι προθέσεις.

Για τον λόγο αυτό αναπτύχθηκαν πολλές τέτοιες γλώσσες προγραμματισμού που εκφράζουν πολιτικές όπως για παράδειγμα η Frenetic, η Pyretic κα. Όλες έχουν τα δυνατά τους σημεία και τις αδυναμίες τους οπότε δεν υφίσταται μια σαφή λύση.

Επιπέδο AP3 ή κορυφαίο Επίπεδο του SDN: Δικτυακές Εφαρμογές

Μερικές βασικές κατηγορίες όπως οι εφαρμογές διαχείρισης δικτύου δίνονται παρακάτω:

1. Διαμόρφωση ροής δεδομένων: η ελαχιστοποίηση της κατανάλωσης ισχύος, η μεγιστοποίηση της χρήσης του δικτύου, η βελτιστοποίηση της κατανομής φόρτου, τα πρωτόκολλα δρομολόγησης, η προσομοίωση δικτύου κα.
2. Φορητότητα και ασύρματη μετάδοση: προγρμματισιμότητα της διαχείρισης των ασύρματων πόρων, τα ετερογενή δίκτυα, τα κινητά ad-hoc δίκτυα κλπ.
3. Μέτρηση και παρακολούθηση: εκτίμηση της ροής δεδομένων από άκρο σε άκρο, δειγματοληψία πακέτων, επιθέσεις και εντοπισμός ανωμαλιών κλπ
4. Δικτύωση Data Center: ζωντανή μεταφορά του δικτύου, αποφυγή αστοχιών, εντοπισμός μη κανονικής συμπεριφοράς κα.
5. Ασφάλεια και αξιοπιστία: εντοπισμός και αντίδραση σε κυβερνοεπιθέσεις, λίστες ελέγχου πρόσβασης (ACLs –Access Controlo Lists), εφαρμογή πολιτικών κα.

Ξεκινώντας από το κορυφαίο επίπεδο (αποκαλείται και NORTHBOUND τμήμα του SDN), βλέπουμε ότι το νέο αυτό δικτυακό υπόδειγμα επιτρέπει νέους τρόπους αλληλεπίδρασης με τον ελεγκτή SDN. Οι εφαρμογές που επικοινωνούν με το επίπεδο αυτό επιτρέπουν στον διαχειριστή δικτύου να συλλέξει δεδομένα ώστε να μετρήσει την υγεία του δικτύου και να κάνει αλλαγές ώστε να διατηρήσει την πολιτική QoS. Πρέπει να σημειωθεί ότι οι χρήστες δεν αλληλεπιδρούν άμεσα με τον SDNC.

Το NBI επιτρέπει στον ελεγκτή SDN (SDNC) να προγραμματίζεται και να ανταποκρίνεται στις προθέσεις του χρήστη. Το SBI επιτρέπει τον έλεγχο της μεταγωγής δεδομένων από τις δικτυακές συσκευές. Το EWBI χρησιμοποιείται στην επικοινωνία με άλλους ελεγκτές σε περιστάσεις πολλών τομών ή ιεραρχημένων δικτύων.

Ρόλος της ενορχήστρωσης στο SDN

Οι πάροχοι και άλλοι ανάλογου μεγέθους οργανισμοί χρειάζονται την ικανότητα να αυτοματοποιούν τις αλλαγές στο δίκτυο τους ώστε να μπορούν να διαθέσουν μια νέα υπηρεσία ή εφαρμογή σε μικρό χρονικό διάστημα. Η αντίστοιχη συμπεριφορά του λογισμικού και του υλικού πρέπει να συντονιστεί ώστε να ανταπεξέλθει στις απαιτήσεις των χρηστών και τις προκαθορισμένες QoS. Ο ενορχηστρωτής είναι η νέα οντότητα που επιτελεί το έργο αυτό και βρίσκεται πάνω από όλα τα SDN επίπεδα. Μεταφράζει την προδιαγραφή πόρων μιας εφαρμογής (όπως οι παράμετροι QoS για χρονοκαθυστέρηση, jitter, εύρος ζώνης κλπ) σε προδιαγραφές για τη δικτυακή τοπολογία και κανόνες δρομολόγησης για τον SDN ελεγκτή. Πρόκειται για βασικό συστατικό που χρειάζεται ώστε μεγάλα και ετερογενή δίκτυα να γίνονται προγραμματιζόμενα και να υποστηρίζουν εφαρμογές.

Η ενορχήστρωση περιλαμβάνει δυο είδη:

1. Ενορχήστρωση υπηρεσιών η οποία λαμβάνει χώρα ώστε να ικανοποιήσει τη ζήτηση από τον χρήστη συγκεκριμένης υπηρεσίας όπως για παράδειγμα VPN διαμέσω ανόμοιων τομέων.
2. Ενορχήστρωση υποδομής που εφαρμόζεται στη διαχείριση μεταγωγέων, διακομιστών και δεδομένων σε κέντρο αποθήκευσης.

Όταν πολλά ετερογενή δίκτυα με τους ενορχηστρωτές τους συμμετέχουν σε σενάριο εκπλήρωσης μιας υπηρεσίας απαιτείται ένας ενορχηστρωτής ενορχηστρωτών.

Ασφάλεια SDN

Όπως και με τις προηγούμενες δικτυακές αρχιτεκτονικές, το SDN είναι ευάλωτο σε διάφορα είδη επιθέσεων. Πολλές από τις αδυναμίες στην ασφάλεια είναι κοινές με τα παραδοσιακά μη SDN δίκτυα. Κάποιες όμως είναι καινούργιες όπως συμβαίνει σε κάθε νέα τεχνολογία.

Κοινές ή μη-SDN ευπάθειες

Αυτές οι ευπάθειες δεν είναι χαρακτηριστικές μόνο του SDN και αφορούν όλα τα δίκτυα. Η λίστα παρακάτω δεν είναι πλήρης παρά δίνει μια γενικευμένη εικόνα.

1. Κανάλι επικοινωνίας: από τον χρήστη έως τη δικτυακή συσκευή:
   Μπορούν να εισαχθούν από έναν χάκερ χαλκευμένες ροές δεδομένων στο σύστημα αποστερώντας πόρους από άλλες δικτυακές συσκευές.
2. Ευπάθειες μεταγωγέων και δρομολογητών
   Στα σύγχρονα SDN και μη-SDN δίκτυα οι μεταγωγείς αγοράζονται από ξένους κατασκευαστές δημιουργώντας υβριδικά δίκτυα που αποτελούνται από SDN και συμβατικές συσκευές. Πολλές φορές οι ευπάθειες των συσκευών επιτρέπουν την εγκατάσταση κακόβουλου λογισμικού και επιθέσεις DoS.
3. Ευπάθειες σταθμού διαχείρισης:
   Εμφανίζονται λόγω των αδυναμιών των σταθμών εργασίας από όπου ασκείται η διαχείριση του δικτύου.

Ευπάθειες χαρακτηριστικές του SDN

1. Στο κανάλι επικοινωνίας από τον χρήστη στην SDN συσκευή
   υπάρχουν παρόμοιες έννοιες με την πιο πάνω περίπτωση
2. Στο κανάλι επικοινωνίας από SDN συσκευή σε SDN συσκευή
   Ένας χάκερ μπορεί να αλλοιώσει τον πίνακα δράσεων εντός της συσκευής SDN και να αναδρομολογήσει τις ροές δεδομένων σε λάθος κατευθύνσεις.
3. Στο κανάλι επικοινωνίας από SDN συσκευή στον SDN ελεγκτή (SDNC)
   Οι σημερινές υλοποιήσεις του OpenFlow χρησιμοποιούν το TLS (Transport Layer Security) για την κρυπτογράφηση των καναλιών επικοινωνίας με τις δικτυακές συσκευές. Αυτό μπορεί να αποτελέσει το αντικείμενο επίθεσης στο άμεσο μέλλον καθότι βασίζεται σε υπολογιστές. Επίσης αυτό το κανάλι επικοινωνίας είναι εν δυνάμει ένας κόμβος συμφόρησης αφού μεταφέρει την σηματοδοσία από και προς τους κεντρικοποιημένους ελεγκτές. Ένας ελεγκτής διαθέτει περιορισμένους επεξεργαστικούς πόρους και αποθηκευτικό χώρο και γι αυτό τον λόγο μπορεί να διαχειριστεί ορισμένου μεγέθους δίκτυο. Αυτό το γεγονός μπορεί να χρησιμοποιηθεί ώστε να προκληθεί συμφόρηση στον ελεγκτή ώστε να μην μπορεί να λειτουργήσει.
4. Ευπάθειες ελεγκτή SDN (SDNC):

   Η αρχιτεκτονική του ελεγκτή περιλαμβάνει πολλά μέρη, καθένα εκ των οποίων έχει και τις αδυναμίες του. Πολλές φορές δεν είναι δυνατό να εντοπιστούν άμεσα και εμφανίζονται μόνο μετά από μεγάλα χρονικά διαστήματα εντατικής χρήσης.
5. Εμπιστοσύνη μεταξύ ελεγκτή SDN και των εφαρμογών:
   Οι εφαρμογές που τρέχουν στον ελεγκτή πρέπει να είναι έμπιστες αλλά επί του παρόντος δεν υφίσταται ένας παγκόσμια κατοχυρωμένος μηχανισμός για το σκοπό αυτό.
6. Κανάλι επικοινωνίας: Σταθμός διαχείρισης προς ελεγκτή SDN (SDNC):
   Οι σταθμοί διαχείρισης χρησιμοποιούνται για τον προγραμματισμό του ελεγκτή. Εάν ένας επιτιθέμενος καταλάβει τον σταθμό εργασίας που φιλοξενεί τον ελεγκτή το δίκτυο μπορεί να αναπρογραμματιστεί για κακόβουλο σκοπό. Επιπροσθέτως, αυτό το κανάλι επικοινωνίας δεν έχει προτυποποιηθεί ακόμα οπότε οι λύσεις έχουν ανόμοια επίπεδα ασφάλειας. Υπάρχει ελπίδα ότι θα λυθεί με την προτυποποίηση της αρχιτεκτονικής και τον αυστηρό καθορισμό των επιτρεπτών μηνυμάτων.

Επί του παρόντος εξελίσσεται έρευνα για την λύση των παραπάνω προβλημάτων και κάποιες λύσεις έχουν δοθεί για την αντιμετώπιση των ευπαθειών. Αναμένεται ότι τα μελλοντικά SDN δίκτυα θα είναι πιο σθεναρά και ικανά να αντιμετωπίσουν επιθέσεις.

1. Η ΕΞΕΛΙΞΗ ΤΩΝ ΔΙΚΤΥΩΝ

1.1 Έννοιες από την δρομολόγηση και την μεταγωγή δεδομένων

Κρίνεται πρώτα από όλα απαραίτητο να αναφερθούν τα τρία πρώτα επίπεδα του διαστρωματοποιημένου μοντέλου OSI (Open Systems Interconnect) στα οποία θα γίνεται συνεχώς αναφορά σε όλη την έκταση της εργασίας.

1. Layer 1 (L1): Πρόκειται για το φυσικό επίπεδο το οποίο περιλαμβάνει καλώδια όπως οι οπτικές ίνες και ο χαλκός, συνδετήρες, συγκεντρωτές και μετατροπείς σήματα.
2. Layer 2 (L2): Ονομάζεται και επίπεδο ζεύξης δεδομένων και περιλαμβάνει τα καθαρά δεδομένα που στέλνονται πάνω από το δίκτυο και διαχειρίζεται τις MAC διευθύνσεις του πρωτοκόλλου Ethernet. Οι κάρτες δικτύου και οι οδηγοί αυτών ανήκουν στο επίπεδο ζεύξης δεδομένων όπως και οι μεταγωγείς που δεν διαθέτουν ικανότητες δρομολόγησης (L2 switches)
3. Layer 3 (L3): Είναι το επίπεδο δικτύου και περιλαμβάνει τα πρωτόκολλα IPv4, IPv6, ICMPv4, ICMPv6 καθώς και όλα τα κατανεμημένα πρωτόκολλα δυναμικής δρομολόγησης. Όσον αφορά το υλικό, στο επίπεδο αυτό ανήκουν οι δρομολογητές και οι μεταγωγείς με ικανότητες δρομολόγησης (L3 switches)

Εφεξής στη διατριβή θα αναφέρονται τα επίπεδα του OSI ως Επίπεδο 1 ή L1, Επίπεδο 2 ή L2, Επίπεδο 3 ή L3 ώστε να γίνεται αντιληπτό η εκάστοτε εξεταζόμενη δικτυακή λειτουργία πόσο υψηλά ή χαμηλά επιτελείται.

1.1.1 Δρομολογητές και Μεταγωγείς

Σε ένα δίκτυο υπάρχουν συσκευές που μετάγουν και δρομολογούν τα δεδομένα. Ως Μεταγωγέας (Switch) ορίζεται η δικτυακή συσκευή που συνδέει πολλαπλά τερματικά όπως διακομιστές, παρέχει συνδεσιμότητα σε τοπικό επίπεδο και προσφέρει συνδεσιμότητα προς τον πυρήνα του δικτύου. Ο δρομολογητής είναι μια δικτυακή συσκευή που υπολογίζει διαδρομές προς απομακρυσμένες και τοπικές συσκευές και δίκτυα προσφέροντας συνδεσιμότητα σε όλη την έκταση του δικτύου. Οι μεταγωγείς και οι δρομολογητές χρησιμοποιούν καλώδια χαλκού και οπτικής ίνας στη διασύνδεση τους. Μια δικτυακή συσκευή αποτελείται από σχετικά λίγα μέρη: το ολοκληρωμένο προώθησης, η TCAM (ternary content-addressable memory) και τον επεξεργαστή δικτύου. Κάποιοι νεώτεροι μεταγωγείς διαθέτουν Baseboard Management Controllers (BMC's) που διαχειρίζονται την ισχύ, τους ανεμιστήρες και άλλο υλικό μειώνοντας τον φόρτο διαχείρισης του Δικτυακού Λειτουργικού Συστήματος για τις συσκευές αυτές.

Επί του παρόντος, οι δρομολογητές και οι μεταγωγείς είναι εξαιρετικά όμοιοι μεταξύ τους αφού υπάρχουν L3 ικανοί μεταγωγείς και L2 ικανοί δρομολογητές. Το να καταστεί ένας μεταγωγέας L2, δρομολογητής είναι σχετικά εύκολο αφού προστίθενται οι επιπλέον λειτουργίες. Από τη άλλη ένας δρομολογητής δεν κάνει μεταγωγή επιπέδου 2 γενικότερα και γι αυτό πρέπει να τροποποιηθεί ώστε να επιτρέψει στις θύρες του να προωθήσουν αντί να δρομολογήσουν.

1.1.2 VLAN/VXLAN

Ένα εικονικό τοπικό δίκτυο (VLAN) είναι τεχνική δημιουργίας ξεχωριστών λογικών δικτύων από ένα φυσικό δίκτυο. Τα VLAN γενικά χρησιμοποιούνται για να διαχωρίσουν/συνδυάσουν διαφορετικούς χρήστες ή στοιχεία του δικτύου όπως τηλέφωνα, διακομιστές και σταθμοί εργασίας. Ένα τμήμα του δικτύου μπορεί να διαχωριστεί σε έως και 4096 VLANs.

Virtual Extensible Lan (VXLAN): Δημιουργήθηκε για μεγάλα, δυναμικά απομονωμένα λογικά δίκτυα, προσομοιωμένα δίκτυα και δίκτυα με πολλούς ενοίκους. Ένα τμήμα δικτύου μπορεί να διαχωριστεί σε δεκαέξι εκατομμύρια VXLAN σε σχέση με τα μόλις 4096 VLAN.

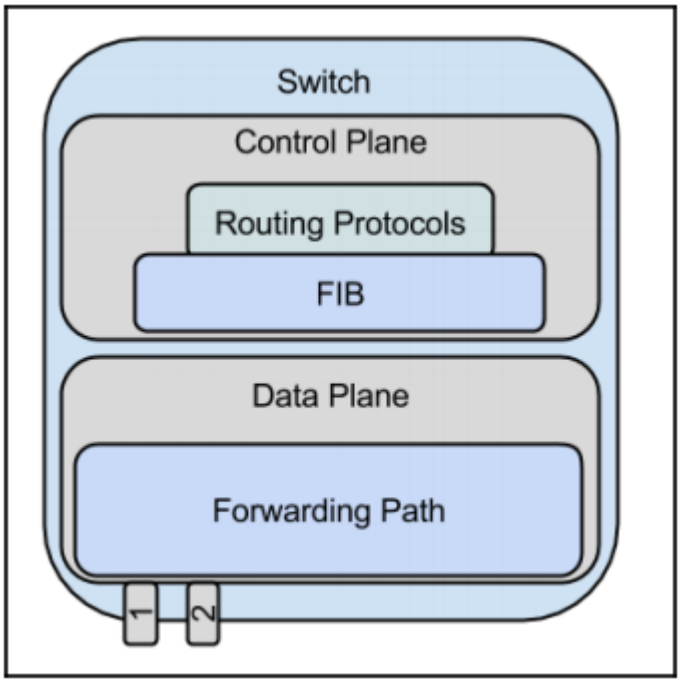
VXLAN Tunnel Endpoint (VTEP): είναι σύνολο από δυο λογικές διεπαφές: την διεπαφή εισόδου που ενθυλακώνει την εισερχόμενη κίνηση δεδομένων σε VXLANs και τη διεπαφή εξερχομένων που αφαιρεί την ενθυλάκωση των VXLAN από τα εξερχόμενα πακέτα ώστε να τα επαναφέρει στην αρχική τους μορφή.

1.1.3 Πεδίο Ελέγχου (Control Plane ή CP)

Το πεδίο ελέγχου είναι το μέρος όπου διατηρούνται όλες οι πληροφορίες σχετικά με τον χειρισμό των πακέτων. Τα πρωτόκολλα δρομολόγησης εδρεύουν στο Πεδίο Ελέγχου και επεξεργάζονται συνεχώς τις ληφθείσες πληροφορίες ώστε να καθορίζουν τη βέλτιστη διαδρομή που πρέπει να ακολουθήσουν τα δεδομένα. Η πληροφορία που προκύπτει συμπεριλαμβάνεται σε έναν πίνακα και παραδίδεται στο Πεδίο Δεδομένων.

1.1.4 Πεδίο Δεδομένων

Στο Πεδίο Δεδομένων λαμβάνει χώρα η προώθηση των πακέτων. Σε έναν δρομολογητή λογισμικού αυτό λαμβάνει χώρα στον επεξεργαστή της συσκευής και σε έναν δρομολογητή αυτό λαμβάνει χώρα στο ολοκληρωμένο προώθησης πακέτων και τις συναφείς μνήμες:



Εικόνα 10 Ο διαχωρισμός CP και DP σε σχέση με την FIB

1.1.5 Ελεγκτές δικτύου

Ως ελεγκτής ορίζεται ένας υπολογιστής που ανήκει στο δίκτυο και διαχειρίζεται μια ή περισσότερες δικτυακές συσκευές. Ο ελεγκτής μπορεί να είναι ενσωματωμένος σε μια συσκευή όπως το Cisco Supervisor Module ή να δουλεύει ανεξάρτητα όπως οι ελεγκτές OpenFlow.

Ο ελεγκτής είναι υπεύθυνος για τη διαχείριση όλων των δεδομένων του Πεδίου Ελέγχου και να αποφασίζει τι να αποστέλλεται στο Πεδίο Δεδομένων.

Γενικά, ένας ελεγκτής διαθέτει διεπαφή γραμμής εντολών (CLI –Command Line Interface) και οι πιο πρόσφατοι διεπαφή παραμετροποίησης μέσω ιστοσελίδας. Κάποιοι ελεγκτές διαθέτουν προγραμματιστική διεπαφή (API Application Programming Interface).

1.1.6 Ο ελεγκτής OpenFlow

Ως ελεγκτής OpenFlow ορίζεται το μηχάνημα που χρησιμοποιεί το πρωτόκολλο OpenFlow για να επικοινωνήσει με δικτυακές συσκευές. Οι πιο κοινοί OpenFlow ελεγκτές είναι οι OpenDaylight και ONOS ενώ λιγότερο γνωστοί είναι οι Floodlight και RYU.

1.1.7 Η μονάδα Supervisor

Ένας επεξεργαστής δρομολόγησης είναι ένας υπολογιστής που φιλοξενείται στο μεταλλικό σασί μιας δικτυακής συσκευής. Κάποιες φορές ο επεξεργαστής δρομολόγησης είναι ενσωματωμένος στο σύστημα ενώ άλλες φορές είναι διακριτή μονάδα που μπορεί να αντικατασταθεί και ή να αναβαθμισθεί. Πολλά συστήματα κατασκευαστών δικτυακού εξοπλισμού διαθέτουν πολλαπλές θύρες επέκτασης ώστε να εφοδιαστούν με αντίστοιχα πολλαπλούς τέτοιους επεξεργαστές για πλεονασμό.

Χαρακτηριστικό παράδειγμα είναι ο αφαιρούμενος επεξεργαστής δρομολόγησης της μονάδας Supervisor της σειράς Cisco 9500. Υπάρχουν πολλαπλές εκδόσεις, μεταξύ τους και η έκδοση A με τετραπύρηνο επεξεργαστή και 16 GB RAM και η έκδοση B με εξαπύρηνο επεξεργαστή και 24 GB RAM.

Προηγούμενα συστήματα όπως το Cisco Catalyst 7600 διέθεταν επιλογές όπως η μονάδα Supervisor 720 (SUP720) η οποία προσφερόταν σε πολλαπλές εκδόσεις: η τυπική διέθετε περιορισμένο πλήθος από διαδρομές που μπορούσε να υποστηρίξει (256k) ενώ η SUP720XL μπορούσε να υποστηρίξει ένα εκατομμύριο διαδρομές.

1.2 (Κατανεμημένα) Πρωτόκολλα Δυναμικής Δρομολόγησης

Ένα πρωτόκολλο δρομολόγησης είναι μια διεργασία (daemon) που εκτελείται σε έναν ελεγκτή και επικοινωνεί με άλλες δικτυακές συσκευές ώστε να ανταλλάξει δικτυακές πληροφορίες.

1.2.1 Border Gateway Protocol (BGP) –Πρωτόκολλο Συνοριακών Πυλών

Το BGP είναι ένα πρωτόκολλο συνοριακών πυλών (External Gateway Protocol –EGP) που λαμβάνει αποφάσεις δρομολόγησης βασιζόμενο σε διαδρομές, δικτυακές πολιτικές ή κανόνες (χάρτες διαδρομών για την Cisco). Αν και σχεδιάστηκε σαν EGP μπορεί να χρησιμοποιηθεί σαν εσωτερικό (iBGP) ή εξωτερικό πρωτόκολλο (eBGP). Χρησιμοποιεί σηματοδοσία πακέτων keepalive ώστε να διαπιστώσει ότι οι γείτονες είναι ακόμα ενεργοί. Το BGP είναι το πρωτόκολλο που χρησιμοποιείται για να δρομολογήσει δεδομένα κατά μήκους του Διαδικτύου, ανταλλάσσοντας πληροφορίες μεταξύ διαφορετικών Αυτόνομων συστημάτων (ASNs). Ένα ASN συμπεριλαμβάνει όλα τα συνδεόμενα δίκτυα στον έλεγχο μιας κεντρικής οντότητας όπως μια συσκευή L3 με Αυτόνομο Σύστημα 1 (AS1) ή π.χ. Sprint (AS1239).

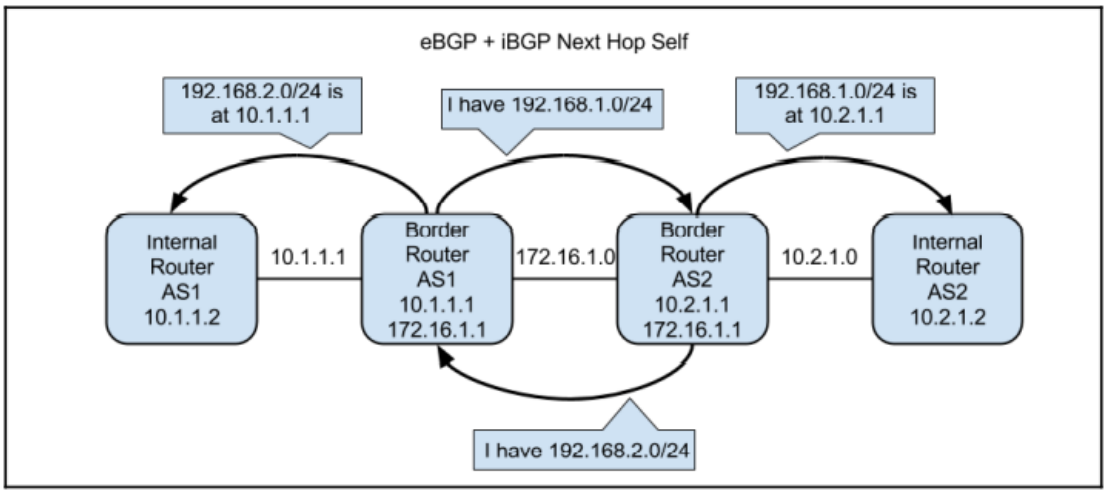
Όταν διασυνδέονται δυο διαφορετικά ASNs, εγκαθίστανται συνεδρίες μεταξύ δυο ή και περισσοτέρων δικτυακών συσκευών που διαθέτουν άμεσες συνδέσεις μεταξύ τους.

Σε ένα σενάριο eBGP για παράδειγμα, ο AS1 και ο AS1239 θα εγκαθιστούσαν σύνοδο που θα τους επέτρεπε να δρομολογήσουν μεταξύ των αυτόνομων συστημάτων τους.

Σε ένα σενάριο iBGP, το ίδιο AS θα συνδεόταν με άλλους δρομολογητές που ανήκουν στο ίδιο AS και θα μετέφερε διαδρομές που καθορίζονται από το σύστημα. Αν και το iBGP χρησιμοποιείται εσωτερικά στα περισσότερα δίκτυα, προτιμάται στα μεγάλης έκτασης εταιρικά δίκτυα διότι τα πρωτόκολλα εσωτερικών πυλών (IGPs) δεν μπορούν να ανταπεξέλθουν.

Για παράδειγμα:

- iBGP με επόμενο άλμα τον συνοριακό δρομολογητή: Στο σενάριο αυτό (Εικόνα 1) τα AS1 και AS2 συνδέονται μεταξύ τους και ανταλλάσσουν από ένα δίκτυο με το αντίστοιχο πρόθεμα το καθένα: Ο AS1 διαφημίζει το 192.168.1.0/24 και ο AS2 διαφημίζει το 192.168.2.0/24. Κάθε δίκτυο έχει δυο δρομολογητές, έναν συνοριακό που συνδέεται με άλλα ASNs (αυτόνομα συστήματα και έναν εσωτερικό δρομολογητή που μαθαίνει διαδρομές από τον συνοριακό δρομολογητή. Οι διαδρομές διαφημίζονται εσωτερικά με επόμενο στη σειρά άλμα τον συνοριακό δρομολογητή. Αυτό είναι και το τυπικό σενάριο όταν στο εσωτερικό δεν τρέχει κάποιο IGP πρωτόκολλο, ώστε να διανεμηθούν οι διαδρομές για τις εξωτερικές διεπαφές του συνοριακού δρομολογητή.

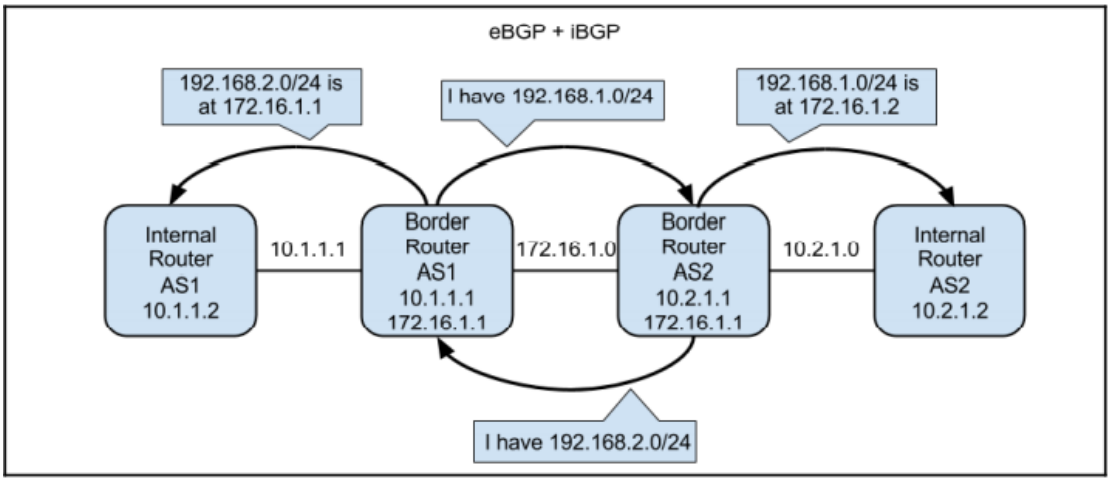


Εικόνα 11: Σεναριο iBGP με επόμενο κόμο τον συνοριακό δρομολογητή

η συνδιαλλαγή έχει ως εξής:
AS1->AS2 (ο AS1 συστήνεται στον AS2)
AS2->AS1 (ο AS2 συστήνεται στον AS1)
AS1->AS2 (ο AS1 ενημερώνει τον AS2 για το δίκτυο 192.168.1.0/24)
AS2->AS1 (ο AS2 ενημερώνει τον AS1 ότι έλαβε τη διαδρομή και τον ενημερώνει για το δίκτυο 192.168.2.0)
AS1->AS2 (ο AS1 ενημερώνει τον AS2 ότι έλαβε τη διαδρομή)
AS1->Εσωτερικό δρομολογητή AS1 (AS1 ενημερώνει εσωτερικό δρομολογητή του AS1 ότι διαθέτει διαδρομή προς το 192.168.2.0/24 δίκτυο και μπορεί να φτάσει σε αυτό μέσω του ιδίου στο 10.1.1.1)
AS2->Εσωτερικό δρομολογητή του AS2 (AS2 ενημερώνει εσωτερικό δρομολογητή του AS1 ότι διαθέτει διαδρομή προς το 192.168.1.0/24 δίκτυο και μπορεί να φτάσει σε αυτό μέσω του ιδίου στο 10.2.1.1)

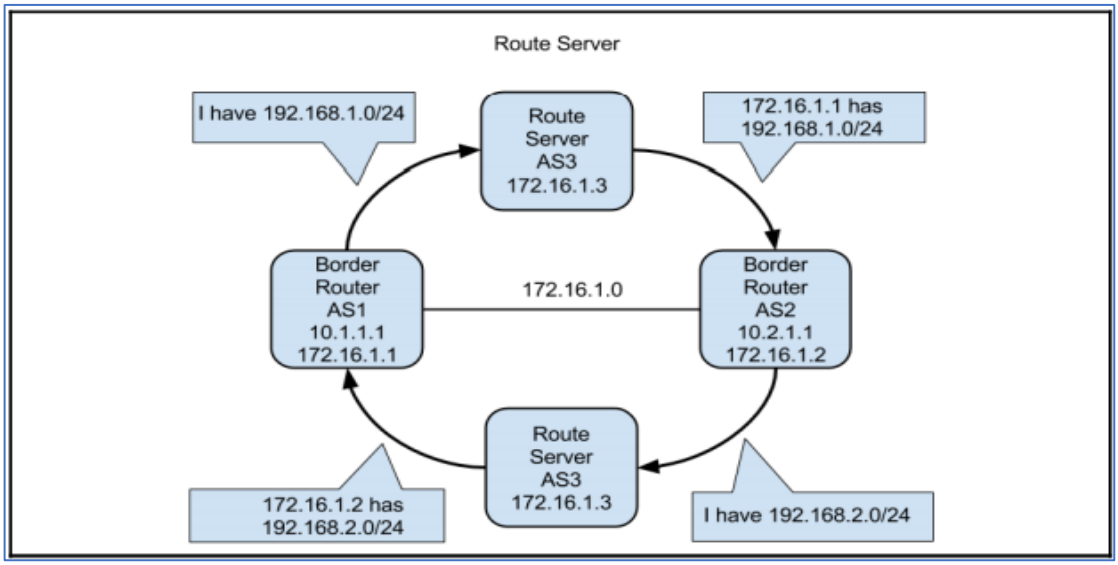
- iBGP με αμετάβλητο τον δρομολογητή του επόμενου άλματος: Στην περίπτωση αυτή οι συνοριακοί δρομολογητές είναι ίδιοι αλλά οι εσωτερικοί δρομολογητές μαθαίνουν ότι ως επόμενο άλμα για το απομακρυσμένο δίκτυο είναι ο εξωτερικός (από άλλο AS)

δρομολογητής.



Εικόνα 12: Σενάριο iBGP με αμέταβλητο τον δρομολογητή επόμενου άλματος

- Το τελευταίο σενάριο (Εικόνα 13),αφορά την διασύνδεση με διακομιστή που ασχολείται με την δρομολόγηση και έχει ιδιαίτερη σημασία γιατί είναι ακριβώς μια από τις τοπολογίες που εμφανίζουν κοινά σημεία με το SDN και τις οποίες το δεύτερο δύναται να αντικαταστήσει. Ο διακομιστής φιλτράρει τις διαδρομές που έχουν επιλεχθεί προς κοινοποίηση στα υπόλοιπα AS και ενημερώνει σχετικά τους συνοριακούς δρομολογητές ορίζοντας τον εαυτό του ως επόμενο άλμα.



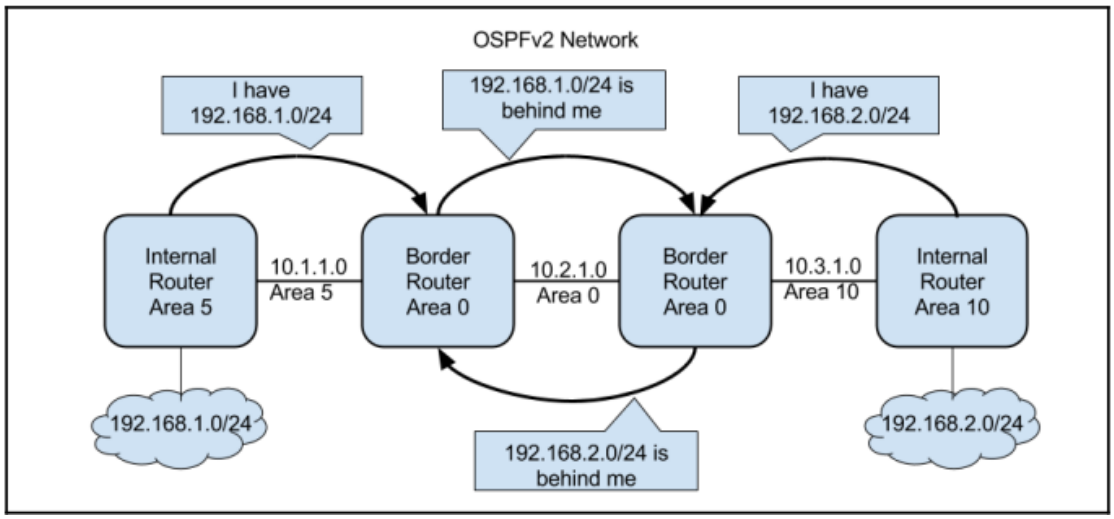
Εικόνα 13: BGP παρουσία διακομιστή δρομολόγησης

1.2.2 Open Shortest Path First (OSPF) –Πρωτόκολλο Προτεραιότητας Ανοίγματος της Συντομότερης Διαδρομής

Το OSPF είναι ένα πρωτόκολλο εσωτερικών πυλών (IGP) το οποίο χρησιμοποιεί έναν αλγόριθμο κατάστασης συνδέσμων για να διαδίδει πληροφορίες δρομολόγησης. Κάθε δρομολογητής που συμμετέχει στο OSPF πρέπει να βολιδοσκοπεί περιοδικά τους γειτονικούς δρομολογητές και έπειτα να εκπέμπει ένα μήνυμα κατάστασης συνδέσμων. Το πρωτόκολλο OSPF βελτιστοποιεί τη μέθοδο, αναθέτοντας σε έναν μόνο δρομολογητή να εκπέμπει στο

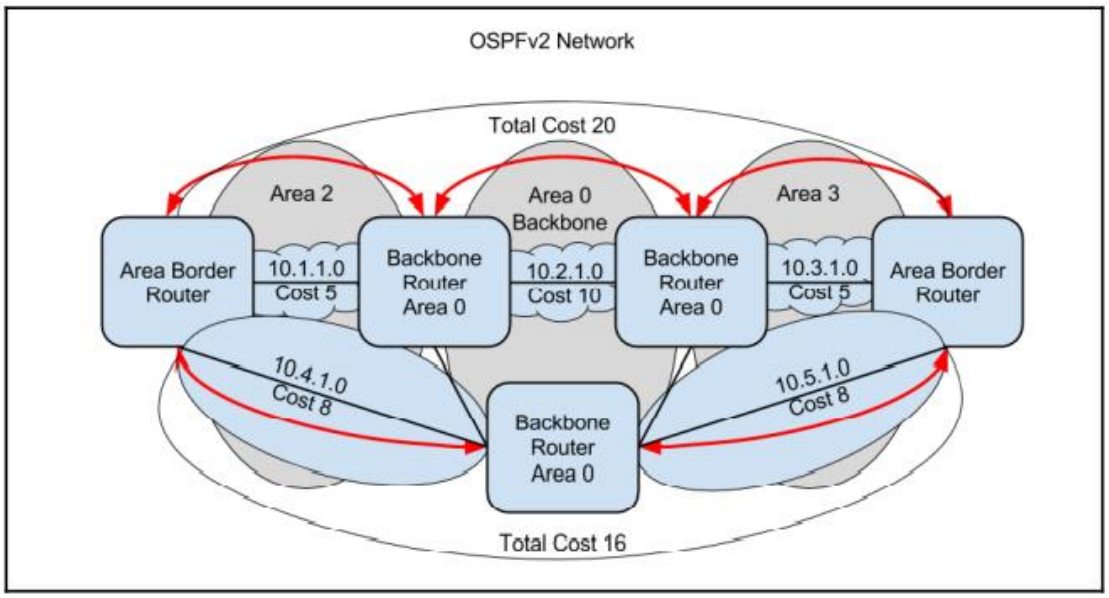
δίκτυο. Το OSPF χρησιμοποιεί την έννοια των περιφερειών (areas) ώστε να περιορίζει τον αριθμό των περιττών μεταδόσεων και των ευρυεκπομπών. Οι περιφέρειες φαίνονται στην Εικόνα 14.

Υπάρχουν δυο εκδόσεις του OSPF: η v2 για το πρωτόκολλο IPv4 που υποστηρίζει και υποδικτύωση και η v3 για τα IPv6 δίκτυα:



Εικόνα 14 Multi-Area OSPF

Όταν μπορούν να χρησιμοποιηθούν πολλαπλές διαδρομές όπως στην Εικόνα 15, πρέπει να λαμβάνεται υπόψη το κόστος κάθε συνδέσμου. Στο πιο κάτω διάγραμμα υπάρχουν δυο διαδρομές, μια με συνολικό κόστος 20 (5+5+10) και μια με κόστος 16 (8+8) και για αυτό τα δεδομένα θα ακολουθήσουν τον σύνδεσμο μικρότερου κόστους:

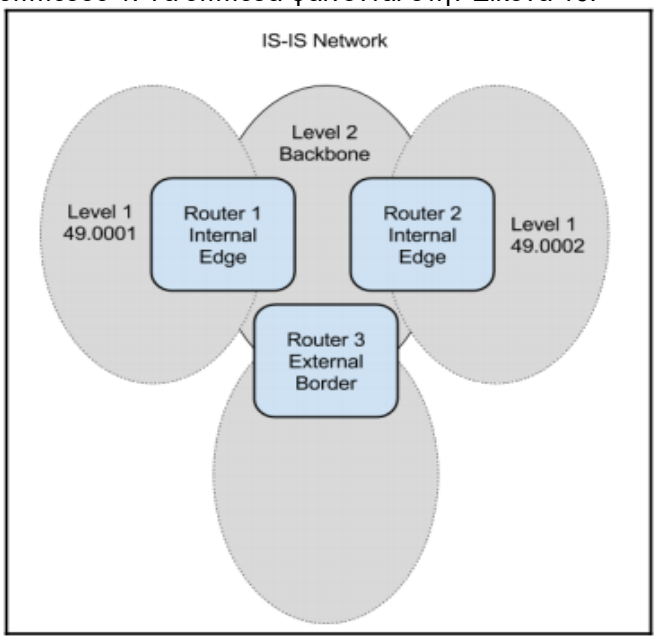


Εικόνα 15 Multi-Area OSPF με πολλαπλές διαδρομές

Intermediate System to Intermediate System (IS-IS) –Ενδιάμεσο Σύστημα προς Ενδιάμεσο Σύστημα

Πρόκειται για ένα πρωτόκολλο κατάστασης συνδέσμων όπως και το OSPF που λειτουργεί διαχέοντας τις πληροφορίες κατάστασης σε ολόκληρο το δίκτυο χρησιμοποιώντας Network Entity Titles (NETs). Κάθε δρομολογητής IS-IS διαθέτει και τη δικιά του βάση δεδομένων τις δικτυακής τοπολογίας που χτίζεται κομμάτι-κομμάτι συναθροίζοντας τις πληροφορίες που έχουν κατακλύσει το δίκτυο. Το IS-IS χρησιμοποιείται από εταιρείες που επιζητούν γρήγορη σύγκλιση, επεκτασιμότητα και τη γρήγορη διάχυση των νέων πληροφοριών δικτύωσης.

Το IS-IS χρησιμοποιεί τις έννοιες των επιπέδων (levels) αντί για τις περιφέρειες (areas) στο OSPF. Υπάρχουν δυο επίπεδα στο IS-IS, το επίπεδο 1 (περιφέρεια) και το επίπεδο 2 (κορμός). Ένα επιπέδου 1 Intermediate System (IS) καταγράφει τους προορισμούς εντός της περιφέρειας του ενώ ένα επιπέδου 2 IS καταγράφει τις διαδρομές στις περιφέρειες του επιπέδου 1. Τα επίπεδα φαίνονται στην Εικόνα 16:



Εικόνα 16 Τοπολογία IS-IS

1.2.3 Enhanced Interior Gateway Protocol (EIGRP) – Βελτιωμένο Πρωτόκολλο Εσωτερικής Πύλης

Το EIGRP είναι ένα ιδιόκτητο από τη Cisco πρωτόκολλο εσωτερικών πυλών. Δεν χρησιμοποιείται συχνά στα σημερινά δίκτυα και προτείνεται η αντικατάσταση του με το OSPF ώστε να υπάρχει διαλειτουργικότητα μεταξύ μη-Cisco συσκευών.

1.2.4 Routing Information Protocol (RIP) –Πρωτόκολλο Πληροφοριών Δρομολόγησης

Πρόκειται για ένα από τα αρχικά πρωτόκολλα δρομολόγησης και χρησιμοποιεί το πλήθος των αλμάτων μεταξύ της προέλευσης και του προορισμού ώστε να καθορίσει τη βέλτιστη διαδρομή. Το RIP αποστέλλει ολόκληρο των πίνακα δρομολόγησης από κάθε ενεργή διεπαφή του δρομολογητή κάθε 30 δευτερόλεπτα. Όταν οι πίνακες δρομολόγησης ήταν μικροί, πριν 30 χρόνια, το RIP δούλευε άψογα. Με τους σημερινούς όμως μεγάλου μεγέθους πίνακες δρομολόγησης, τις ριπές στην μετάδοση δεδομένων και τον συνεχή επανυπολογισμό από άλλους δρομολογητές στο δίκτυο, οι επεξεργαστές τρέχουν στο 100% όλο τον χρόνο.

2. Η ΑΝΑΓΚΗ ΓΙΑ ΠΡΟΓΡΑΜΜΑΤΙΖΟΜΕΝΑ ΔΙΚΤΥΑ

2.1 Η εμφάνιση του SDN

Καθώς τα δίκτυα είναι πλέον απαραίτητα στην λειτουργία των επιχειρήσεων και ολοένα και πιο πολύπλοκα στη λειτουργία έχουν γίνει επίσης ακριβά στη δημιουργία και τη διαχείριση. Αυτή η διαπίστωση έχει οδηγήσει τη δικτυακή κοινότητα στην αναζήτηση πέρα από τα πεδία της δικτυακής διαχείρισης και των πρωτοκόλλων προς μια νέα έννοια που ονομάζεται SDN (Software-Defined Network)

Τι ακριβώς είναι ένα Προγραμματιζόμενο Δίκτυο (SDN) πως λειτουργεί και τι επιτελεί; Οι απαντήσεις στις ερωτήσεις αυτές εξαρτώνται από την αλληλεπίδραση μεταξύ σχεδιασμού, επιχειρησιακών απαιτήσεων και δικτύου.

Ένας προτεινόμενος ορισμός:

Ως SDN προσδιορίζεται ένα δίκτυο όπου ένα API (Application Programming Interface) επιτρέπει στις εφαρμογές να αντιλαμβάνονται την κατάσταση του και να αντιδρούν σε αυτήν σε σχεδόν πραγματικό χρόνο. Τρία βασικά σημεία διαφοροποιούν το SDN από τα πρωτόκολλα διαχείρισης δικτύου:

- Το SDN αποτελεί διεπαφή με το δίκτυο παρά μια ακόμα δικτυακή συσκευή.
- Το SDN αλληλεπιδρά άμεσα με κάποιο επίπεδο του πεδίου δεδομένων (ή με τον πίνακα προώθησης) αντί με την παραμετροποίηση και την τωρινή κατάσταση λειτουργίας.
- Το SDN επικεντρώνεται στην διακίνηση των δεδομένων διαμέσου του δικτύου ή του πεδίου ελέγχου και δεν ασχολείται με το σύνολο της λειτουργίας του δικτύου.

Αν και δεν είναι εύκολο να καθοριστεί επακριβώς τι είναι το SDN, είναι ακόμα δυσκολότερο να καθοριστεί ποια τεχνολογία είναι αξιοπρόσεκτη και ποια όχι. Είναι οι υλοποιήσεις που κεντρικοποιούν κάθε έλεγχο σε σχέση με τον ρόλο των κατανεμημένων πεδίων ελέγχου το πραγματικό SDN; Και τι γίνεται με εφαρμογές που τροποποιούν μόνο την κίνηση εγκαθιστώντας στατικές διαδρομές μέσω της γραμμής εντολών;

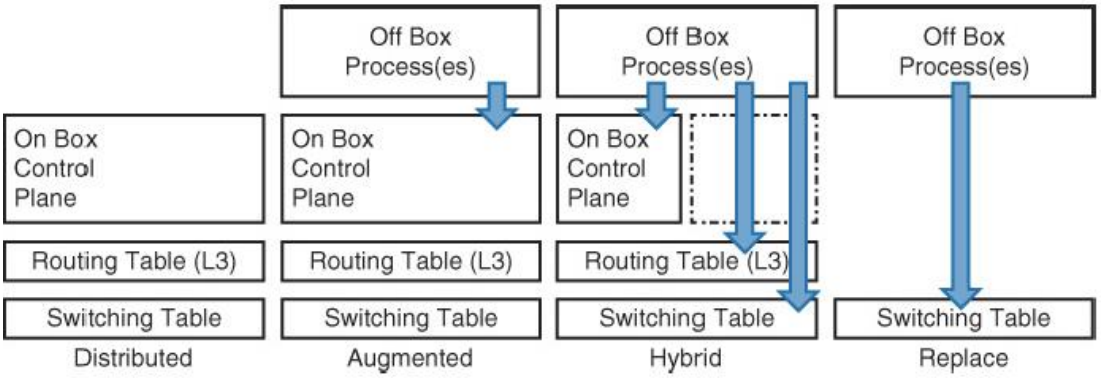
Προτεινόμενο πλαίσιο

Το πλαίσιο που παρουσιάζεται εδώ δεν προορίζεται να αντικαταστήσει όλες τις υπόλοιπες ταξονομίες παρά να δώσει στον κόσμο μια άλλη οπτική που μπορεί να φανεί χρήσιμη ιδιαιτέρως σε σχεδιαστές και αρχιτέκτονες δικτύων. Αντί να επικεντρωθούμε σε λεπτομέρειες πως δουλεύει το κάθε πρωτόκολλο, με το μοντέλο αυτό αποπειρόμαστε να αναδείξουμε ως η κάθε λύση αλληλεπιδρά με τις εφαρμογές και με άλλα δικτυακά στοιχεία.

Το πλαίσιο βασίζεται σε δυο σημεία:

- Το σημείο όπου το SDN εγχέει πληροφορίες σε δρομολογητές και μεταγωγείς (συσκευές πρώθησης)
- Ο τρόπος με τον οποίον οι πληροφορίες εγχέονται από το SDN αλληπεδρά με άλλα επίπεδα ελέγχου.

Η Εικόνα 17 αναπαριστά το υπόβαθρο όπου φαίνεται το σημείο όπου η πληροφορία εγχέεται στις συσκευές προώθησης.



Εικόνα 17: Αλληλεπίδραση Πεδίου Ελέγχου με τις διεργασίες δρομολόγησης και μεταγωγής

Προγραμματιζόμενα δίκτυα:

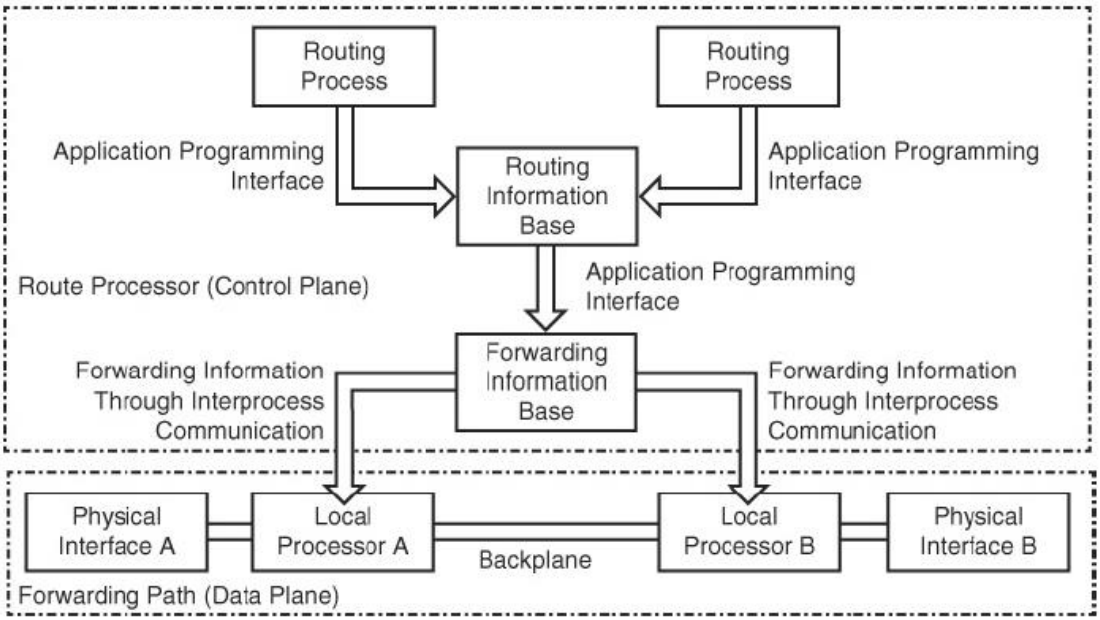
- Το κατανεμημένο μοντέλο «δένει» το υλικό μεταγωγής σε ένα πλήρως κατανεμημένο πεδίο ελέγχου.
- Το ενισχυμένο μοντέλο χρησιμοποίει ένα πλήρως ψηφιακό πεδίο ελέγχου που είναι ενισχυμένο ή διαχειρίσιμο με κάποιο τρόπο από διεργασίες εκτός συσκευής.
- Το υβριδικό μοντέλο χρησιμοποιεί διεργασίες που τρέχουν πάνω στις δικτυακές συσκευές και εκτός αυτών σε παραλληλία.
- Ο μοντέλο αντικατάστασης μετακινεί το πεδίο έλεγχου εντελώς εκτός των συσκευών προώθησης σε διεργασίες που τρέχουν σε άλλες συσκευές.

Παρακάτω ακολουθεί πιο αναλυτική περιγραφή του κάθε μοντέλου:

2.2 Το Κατανεμημένο Μοντέλο

Δεν θεωρείται μορφή του SDN καθότι διαφέρει στα κεντρικά σημεία του. Δεν υπάρχει API στο πεδίο ελέγχου που είναι σχεδιασμένο να υπάρχει στενή σύνδεση μεταξύ των εφαρμογών και τις μεταγωγής των δεδομένων στο δίκτυο. Η έλλειψη μιας τέτοιας διεπαφής σημαίνει ότι δεν υπάρχει τρόπος διανομής πολιτικών στο επίπεδο προώθησης είτε αυτό αφορά πρωτόκολλο δρομολόγησης, πίνακα δρομολόγησης ή οποιαδήποτε συσκευή μέσα στο δίκτυο. Εξετάζοντας παρ' όλα αυτά το μοντέλο αυτό θα μπορέσουμε να κατανοήσουμε καλύτερα τα υπόλοιπα.

Αν και τείνουμε να θεωρούμε τον υπολογιστή η το μεταγωγέα ως έναν συνδυασμό λογισμικού /υλικού που δουλεύει ως μια οντότητα, η πραγματικότητα είναι τελείως διαφορετική. Στο εσωτερικό των περισσότερων δρομολογητών και μεταγέων υπάρχει σαφής διαχωρισμός μεταξύ του Πεδίου Ελέγχου και του Πεδίου Δεδομένων. Το σχήμα της Εικόνας 18 αποδίδει την αρχιτεκτονική των περισσοτέρων δρομολογητών και μεταγωγέων.



Εικόνα 18: Τυπική Αρχιτεκτονική δρομολογητή

2.2.1 Μοντέλο Λειτουργίας Δρομολογητή

Η διαδικασία μεταγωγής ενός πακέτου καθώς περνά από την συσκευή έχει ως εξής:

1. Το πακέτο εισέρχεται στη φυσική θύρα Α, που είναι υπεύθυνη για την ανάγνωση του πακέτου από το μέσο μεταδοσης στην τοπική μνήμη.
2. Η φυσική θύρα Α εν συνεχεία στέλνει ένα σήμα λογισμικού (διακοπή) στον τοπικό επεξεργαστή Α σημειώνοντας ότι υπάρχει διαθέσιμο ένα νέο πακέτο προς επεξεργασία.
3. Ο τοπικός επεξεργαστής Α ελέγχει τον τοπικό πίνακα ώστε να καθορίσει τη θύρα εξόδου. Αν η πληροφορία αυτή δεν είναι διαθέσιμη σε τοπικό πίνακα (αν ο τοπικός πίνακας είναι ενδιάμεση μνήμη) τότε το πακέτο (ή πληροφορίες σχετικά με το πακέτο) πρέπει να εισαχθούν στον Επεξεργαστή Δρομολόγησης ώστε να δημιουργήσουν σωστές καταχωρήσεις στον τοπικό πίνακα.
4. Ο τοπικός επεξεργαστής Α αντικαθιστά την παρούσα επικεφαλίδα πακέτου με νέα, κατάλληλη για τη φυσική θύρα εξόδου (αυτό αποκαλείται επανεγγραφή MAC Header)
5. Το πακέτο τοποθετείται στην αρτηρία της πλακέτας ώστε να μπορεί να μεταφερθεί τοπικό Επεξεργαστή Β από όπου θα συνεχίσει στην μνήμη που εξυπηρετεί την αντίστοιχη κάρτα.
6. Ο τοπικός επεξεργαστής Β επιτελεί ότι επιπρόσθετη επεξεργασία χρειάζεται και τοποθετεί το στην σωστή ουρά για την έξοδο.
7. Η φυσική διεπαφή Β διαβάζει το πακέτο από την μνήμη και το τοποθετεί στο μέσο μετάδοσης.

Ο επεξεργαστής δρομολόγησης που συνιστά το πραγματικό σύνολο από διεργασίες όπου εκτελούνται τα κατανεμημένα πρωτόκολλα πεδίου ελέγχου όπως το OSPF και το EIGRP δεν συμμετέχει στη μεταγωγή πακέτων από τη μια διεπαφή στην άλλη παρά τρέχει στο υλικό πλησίον της περιοχής στη πλακέτα που λαμβάνει χώρα η μεταγωγή. Η εγγύτητα μεταξύ πεδίου ελέγχου και πεδίου δεδομένων στο υλικό παρέχει κάποια πλεονεκτήματα συμπεριλαμβανομένων των πολύ μικρών καθυστερήσεων μεταξύ πεδίου ελέγχου και πεδίου δεδομένων επιτρέποντας τους να επικοινωνούν σε σχεδόν πραγματικό χρόνο. Η διανομή της κατάστασης του δικτύου σε ολόκληρη την έκταση του δικτύου επιτρέπει στο πεδίο ελέγχου να αντιδρά σε αλλαγές σε σχεδόν πραγματικό χρόνο.

Οι αρνητικές επιπτώσεις της στενής ζεύξης μεταξύ πεδίου ελέγχου και πεδίου δεδομένων και της μεθόδου διανομής των δεδομένων κατά μήκους του συνολικού δικτύου είναι οι εξής:

- Δεν υφίσταται μια μόνο όψη του δικτύου από άκρου σε άκρο, από το επίπεδο εφαρμογής έως το επίπεδο μεταφοράς σε μια μόνο συσκευή οπουδήποτε σε ένα κατανεμημένο πεδίο ελέγχου κάνοντας δύσκολή την κατανόηση και τη προσαρμογή στις εκάστοτε δικτυακές συνθήκες σε συνθήκες σχεδόν πραγματικού χρόνου.
- Η πολιτική ή διαφορετικά οι εξαιρέσεις στους κανονικούς κανόνες δικτύωσης πρέπει να ακολουθήσουν το κατανεμημένο πεδίο ελέγχου κατά μήκος του δικτύου υπό τη μορφή της παραμετροποίησης ξεχωριστά δρομολογητών και μεταγωγέων. Δεν υπάρχει συγκεκριμένο μέρος ή σημείο ελέγχου όπου μπορεί να εγχυθεί η πολιτική ώστε να εφαρμόζεται στα σωστά μέρη στον σωστό χρόνο.

Το πρώτο βήμα της μετακίνησης από ένα πλήρως κατανεμημένο μοντέλο, σε κάποια μορφή SDN είναι να μεταφερθεί μέρος του πεδίου ελέγχου εκτός της φυσικής δικτυακής συσκευής όπου τα πακέτα μετάγονται ώστε να σπάσει η ισχυρή ζεύξη μεταξύ πεδίου ελέγχου και δεδομένων. Το ποσοστό του επιβαλλόμενου διαχωρισμού κυμαίνεται αλλά ένα δίκτυο τεχνολογίας SDN θα διαθέτει περισσότερη απόσταση μεταξύ των πεδίων ελέγχου και δεδομένων σε σχέση με το κατανεμημένο μοντέλο.

2.3 Το επαυξημένο μοντέλο

Το επαυξημένο μοντέλο παρέχει ένα εξωτερικό στοιχείο επόπτευσης και ελέγχου σε περιορισμένο μέρος του δικτύου (τυπικά σε έναν ή σε λίγους δρομολογητές), χρησιμοποιώντας ένα ετερόκλητο σύνολο εργαλείων. Συνήθως η κατανεμημένη δρομολόγηση επαυξάνεται τροποποιώντας την παραμετροποίηση της πολιτικής σε ξεχωριστές συσκευές το οποίο με τη σειρά του επηρεάζει την λειτουργία του κατανεμημένου πεδίου ελέγχου με κάποιον τρόπο.

Αν για παράδειγμα ληφθούν συσκευές οι οποίες αντιδρούν σε μια επίθεση Στερήσεως Υπηρεσίας (Denial of Service) μέσω της εισαγωγής πληροφοριών στο πρωτόκολλο δρομολόγησης ώστε να εμποδίσουν την σε όλες τις εισόδους ταυτόχρονα. Μια τέτοια συσκευή θα έτρεχε ένα πρωτόκολλο δρομολόγησης όπως το BGP αποκλειστικά με σκοπό την εισαγωγή των πληροφοριών πολιτικής στο σύστημα δρομολόγησης και όχι ώστε να παρέχει πληροφορίες προσβασιμότητας. Ένα άλλο παράδειγμα θα ήταν μια συσκευή που παρακολουθεί διάφορες διαθέσιμες ζεύξεις για επιδόσεις, κόστη και άλλους παράγοντες και εν συνεχεία χρησιμοποιεί διάφορα μέσα ώστε να παραμετροποιήσει στατικές πληροφορίες δρομολόγησης σε μια συσκευή ώστε να αλλάξει την επιλεχθείσα διαδρομή.

Για παράδειγμα το Performance Routing της Cisco πλησιάζει περισσότερο την ιδέα του SDN από την αλλαγή σε πολιτικές δρομολόγησης μέσω του φιλτραρίσματος ή της εισαγωγής δρομολογητών «μαύρες τρύπες». Το PfR χρησιμοποιεί αποκλειστικό API ώστε να αλληλεπιδρά με τον δρομολογητή. Το αποκλειστικής χρήσης API μπορεί να χρησιμοποιηθεί ώστε να εξεταστεί ένα περιορισμένο σύνολο καταστάσεων του δρομολογητή όπως καθορισμένες διαδρομές ή πληροφορίες διεπαφών και να διοχετεύσει τις διαδρομές αυτές στον πίνακα δρομολόγησης δημιουργώντας στατικές διαδρομές.

Λόγω τις μικρής επίδρασης στα υπάρχοντα δικτυακά πεδία ελέγχου και το στενό εύρος των πιθανών λύσεων, τα Επαυξημένα μοντέλα χρησιμοποιούνται ευρέως σε πολλά δίκτυα. Το ερώτημα που τίθεται είναι αν το Επαυξημένο μοντέλο συνιστά SDN. Αν και φαίνεται να πλησιάζει το SDN, η στενότητα του βρόχου ανάδρασης –φιλοξενείται σε αυτόνομες εφαρμογές σε μικρά μέρη του δικτύου- οδηγεί πολλούς μηχανικούς δικτύων στο συμπέρασμα ότι δεν αποτελεί στη πραγματικότητα μέρος του SDN.

2.4 Το Υβριδικό μοντέλο

Στόχος του Υβριδικού μοντέλου είναι να επιτρέψει στην κατανεμημένη δρομολόγηση να επιτελέσει το μεγαλύτερο μέρος του έργου της δημιουργίας μιας τοπολογίας άνευ βρόχων και να παρέχει πληροφορίες προώθησης για την πλειοψηφία της κίνησης επιτρέποντας στην πολιτική να διαμορφώνεται με περισσότερο κεντρικοποιημένο τρόπο.

Το Υβριδικό μοντέλο καλύπτει τα δυο βήματα που έχουν καλυφθεί έως τώρα – τη μετακίνηση μέρους του Πεδίου Ελέγχου εκτός της δικτυακής συσκευής με εφαρμογή πολιτικών σε σχεδόν πραγματικό χρόνο- ώστε οι εφαρμογές να μπορούν να αλληλεπιδράσουν απευθείας με το δίκτυο. Αυτό είναι και το πρώτο «πραγματικό» SDN μοντέλο με κάτι το οποίο μπορεί να κατηγοριοποιηθεί ως API εντός του δικτύου συμπεριλαμβανομένου ενός βρόχου ανάδρασης και τη διαθεσιμότητα πληροφόρησης σχεδόν πραγματικού χρόνου σχετικά με τις από άκρου σε άκρο συνθήκες στο δίκτυο.

Το υβριδικό μοντέλο ανοίγει ένα API άμεσα στον πίνακα δρομολόγησης (RIB – Routing Information Base) και πιθανώς στον μηχανισμό προώθησης παρέχοντας στις εξωτερικές διεργασίες τη δυνατότητα να αλληλεπιδράσουν με τον πίνακα δρομολόγησης με παρόμοιο τρόπο όπως και με τις κατανεμημένες διεργασίες δρομολόγησης. Οι εξωτερικές διεργασίες δρουν επί της ουσίας ως διεργασίες δρομολόγησης αλληλεπιδρώντας με τον πίνακα δρομολόγησης και λοιπές διεργασίες δρομολόγησης που τρέχουν στην δικτυακή συσκευή στη περίπτωση αυτή , το API μεταξύ του πίνακα δρομολόγησης και της διεργασίας δρομολόγησης εκτελείται εντός RPC (Remote Procedure Call) έτσι ώστε διεργασίες που δεν εντοπίζονται στη συσκευή να μπορούν αν αλληλεπιδράσουν άμεσα με τον πίνακα δρομολόγησης.

Η άμεση αλληλεπίδραση με τον πίνακα δρομολόγησης όχι μόνο επιτρέπει στην απομακρυσμένη διεργασία να εγκαταστήσει διαδρομές στον πίνακα δρομολόγησης όπως ακριβώς θα έκανε και μια τοπική διεργασία, επιτρέπει επίσης στην απομακρυσμένη διεργασία την αναδιανομή διαδρομών από και προς άλλες διεργασίες δρομολόγησης έσω της RIB και την ανακάλυψη της όψης που διατηρεί η κάθε συσκευή από την δική της γωνία.

2.4.1 Διεπαφή προς το Σύστημα δρομολόγησης (Interface to the Routing System)

Ένα παράδειγμα του υβριδικού μοντέλου είναι η διεπαφή RIB του I2RS της IETF.

Η διεπαφή I2RS περιλαμβάνει:

- Προτιμήσεις διαδρομής ώστε ο πίνακας δρομολόγησης να δύναται να αποφασίσει μεταξύ όσων διαδρομών προσφέρονται από διαφορετικά πρωτόκολλα ποιες να εγκαταστήσει.
- Μετρικές διαδρομών ώστε πολλαπλές διαδρομές εντός της εξωτερικής διεργασίας δρομολόγησης να μπορούν να παραμετροποιηθούν (συμπεριλαμβανομένων εναλλακτικών διαδρομών και για γρήγορη αναδιαμόρφωση)
- Ταυτοποιητές των διεργασιών δρομολόγησης που καθιστούν δυνατή την αναδιανομή πληροφορίας μεταξύ διεργασιών που επιτελούνται εντός και εκτός της συσκευής.
- Αλληλεπίδραση κατά την εισαγωγή και εξαγωγή διαδρομών.
- Αλληλεπίδραση μεταξύ VLANs, VRFs κλπ.
- Επανακλήσεις για την εγκατάσταση, αφαίρεση διαδρομών και λοιπά γεγονότα.

Από την άποψη του RIB η εξωτερική διεργασία του I2RS συμπεριφέρεται ακριβώς όπως και η εσωτερική διεργασία. Η εξωτερική διεργασία μπορεί να είναι οτιδήποτε από μηχανή πολιτικής δρομολόγησης έως εξειδικευμένη υλοποίηση του BGP.

Αναλόγως με την υλοποίηση από τον εκάστοτε κατασκευαστή, είναι πιθανό για την εξωτερική διεργασία να διαθέτει τοπική βάση διαδρομών όπως είναι ο BGP πίνακας μια βάση κατάστασης ζεύξεων (Link State Database –LSDB) ή έναν πίνακα τοπολογίας του EIGRP. Αυτού του είδους ο τοπικός πίνακας επιτρέπει γρηγορότερες αναζητήσεις, την εγκατάσταση εναλλακτικών διαδρομών, την αναδιανομή γεγονότων και άλλες αλληλεπιδράσεις με την RIB όπως η παροχή τοπικά πόρων ώστε να διαχειρίζεται και να αποσφαλματώνεται ο εξωτερικός πίνακας δρομολόγησης

2.4.2 Cisco OnePK

Άλλο παράδειγμα του υβριδικού μοντέλου είναι η διεπαφή OnePK της Cisco (η οποία θεωρείται υπερσύνολο του SDN παρά κλασικό υπόδειγμα). Το OnePK API είναι επί της ουσίας ένα

σύνολο από βιβλιοθήκες που ένας προγραμματιστής μπορεί να τραβήξει σε έναν Compiler της γλώσσας C ή σε εικονική μηχανή Java, το οποίο δίνει άμεση επίδραση σε πλήθος από δομές δεδομένων σε έναν δρομολογητή Cisco. Οι δομές δεδομένων περιλαμβάνουν τα εξής:

- Την Routing Information Base (RIB)
- Στατιστικά διεπαφών και λοιπές πληροφορίες
- Πληροφορίες πρωτοκόλλου Netflow
- Πολιτικές δρομολόγησης.

Το OnePK επιτρέπει την παρακράτηση ροών δεδομένων ώστε κάποια από τα πακέτα τους να τροποποιηθούν. Είναι για παράδειγμα να δημιουργηθεί μια μικρή εφαρμογή που κρατά την κίνηση του πρωτοκόλλου Telnet που διέρχεται μέσα από δρομολογητή ώστε να κάνει μικρές αλλαγές όπως την κρυπτογράφηση των περιεχομένων.

Τα μέρη του OnePK που είναι τα πλέον ενδιαφέροντα από άποψη SDN είναι εκείνα που εμπλέκονται στην αλληλεπίδραση του I2RS με τον πίνακα δρομολόγησης. Πιο συγκεκριμένα με τη δυνατότητα εγκατάστασης διαδρομών και την εξέταση των περιεχομένων του πίνακα δρομολόγησης, την τροποποίηση της πολιτικής στο Πεδίο Ελέγχου και λοιπές παρόμοιες δυνατότητες.

2.5 Υβριδική Λειτουργία και το Πρόβλημα του Σχοινιού

Το κυριότερο μειονέκτημα του υβριδικού τρόπου είναι ότι δρα σαν ένα εξωτερικό πρωτόκολλο δυναμικής δρομολόγησης –τουλάχιστον όσον αφορά την οπτική ενός δυναμικού πεδίου ελέγχου. Όπως και όλες οι άλλες διεργασίες δρομολόγησης, κάθε εξωτερικός υβριδικός ελεγκτής πρέπει να λαμβάνει υπόψη τις υπάρχουσες συνθήκες δρομολόγησης πριν προσθέσει ο ίδιος διαδρομές ή αλλαγές σε αυτές στην τοπική RIB.

Ο απλούστερος τρόπος να γίνει αντιληπτή η λειτουργία είναι να εκληφθεί ότι τα δυο πρωτόκολλα δρουν συνεργατικά δημιουργώντας ένα μόνιμο βρόχο ανάδρασης στο κομμάτι δρομολόγησης του πεδίου ελέγχου. Οι στατικές διαδρομές αποτελούν εξέχον παράδειγμα. Τα υβριδικά SDN πρέπει να αποφεύγουν τη «στατικότητα» αλληλεπιδρώντας με τον πίνακα δρομολόγησης σε σχεδόν πραγματικό χρόνο αντί απλά να εγχύουν πληροφορίες δρομολόγησης αγνοώντας την τωρινή κατάσταση του δικτύου.

2.5.1 Το μοντέλο Αντικατάστασης (REPLACE)

Πρόκειται για το μοντέλο που έρχεται στο μυαλό των περισσότερων μηχανικών δικτύου όταν σκέφτονται το SDN εφόσον αφορά την μετακίνηση ολόκληρου του πεδίου ελέγχου από συγκεκριμένους δρομολογητές και μεταγωγείς σε κεντρικοποιημένο σύστημα ελέγχου. Το σύστημα μπορεί να απαρτίζεται από έναν μόνο ελεγκτή ή να είναι κατανεμημένο σύστημα διάσπαρτων ελεγκτών σε όλο το δίκτυο που εκτελούν πρωτόκολλα μεταξύ τους ώστε να κατανείμουν τις πολιτικές και τις απαραίτητες πληροφορίες προώθησης. Το μοντέλο REPLACE ανοίγει API μεταξύ της FIB (Forwarding Information Base) και των ελεγκτών υλικού ή μεταξύ της RIB και της FIB επιτρέποντας έτσι στον ελεγκτή να προγραμματίσει τις ξεχωριστές εγγραφές στις συσκευές μεταγωγή καθαυτές. Η ομάδα της IETF FORCES και το πρωτόκολλο OpenFLOW αποτελούν παραδείγματα αντικατάστασης εξολοκλήρου του πεδίου έλεγχου των συσκευών από σύστημα εξωτερικών ελεγκτών κατανεμημένων κατά μήκος του δικτύου.

Τα SDN του μοντέλου REPLACE μπορούν να αναπτυχθούν με ποικίλους τρόπους, κάποιοι εκ των οποίων είναι παρόμοιοι με πιο παραδοσιακά μοντέλα δικτύωσης και άλλοι που είναι τελείως ξένοι με τους παραδοσιακούς τρόπους δικτύωσης.

2.5.2 Δρομολόγηση Χωρίς Σύνδεση / Αντίδραση με Σύνδεση (OR/OR –Offline Routing – Online Reaction)

Τα παραδοσιακά μοντέλα δικτύωσης θέτουν το πεδίο ελέγχου στη ροή δεδομένων χρήστη (in-band) που σημαίνει ότι τα πακέτα του πεδίου ελέγχου μεταφέρονται μέσω των ιδίων ζεύξεων με τα δεδομένα. Αυτό επιτρέπει στο πεδίο ελέγχου να αντιδρά σε αλλαγές στην τοπολογία

επαναϋπολογίζοντας τη βέλτιστη διαδρομή προς δοσμένο προορισμένο σε σχεδόν πραγματικό χρόνο. Όταν αστοχεί μια ζεύξη ή ένας κόμβος, το πρωτόκολλο δρομολόγησης ανακαλύπτει τη βλάβη και τελικά υπολογίζει ένα νέο σύνολο από διαδρομές κατά μήκους του δικτύου που δρομολογούν πέριξ της βλάβης.

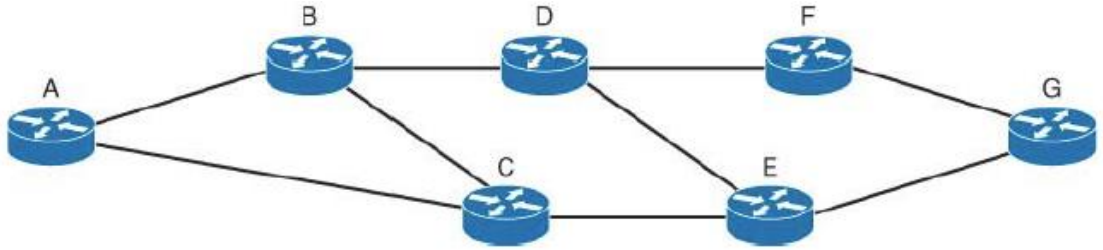
Οι υπέρμαχοι του μοντέλου αυτού ισχυρίζονται ότι το κατανεμημένο μοντέλο είναι θεμελιωδώς ελαττωματικό. Ένα πεδίο ελέγχου που αντιδρά σε αλλαγές στην δικτυακή τοπολογία δεν μπορεί να αντιδράσει αρκετά γρήγορα ώστε να αποτρέψει μεγάλες απώλειες πακέτων χωρίς να αυξήσει υπερβολικά την πολυπλοκότητα, το οποίο κάνει το δίκτυο δύσκολο στον σχεδιασμό, την ανάπτυξη και τη διαχείριση.

Απαιτείται εξαιρετικά εξειδικευμένος συντονισμός των χρονομετρητών μαζί με περίπλοκες προσθήκες στο σύστημα δρομολόγησης ώστε το σύστημα δρομολόγησης να αντιδρά σε αλλαγές στη τοπολογία σε σχεδόν πραγματικό χρόνο.

Το σύστημα OR/OR επιλύει αυτό το πρόβλημα υπολογίζοντας όλες τις πληροφορίες του Πεδίου Ελέγχου, συμπεριλαμβανομένου ενός συνόλου από εναλλακτικές διαδρομές που μπορούν να χρησιμοποιηθούν σε περίπτωση αστοχίας της βέλτιστης διαδρομής για οποιαδήποτε ροή δεδομένων. Αυτό μοιάζει με ένα MPLS-TE δίκτυο με ταχεία αναδρομολόγηση όπου υπολογίζεται πρώτα η βασική διαδρομή προς τον οποιονδήποτε προορισμό και εν συνεχεία μια εναλλακτική διαδρομή. Και οι δυο διαδρομές εγκαθίστανται στον πίνακα δρομολόγησης της κάθε συσκευής του δικτύου την ώρα του υπολλογισμού.

Αν αστοχήσει η πρωτεύουσα διαδρομή σε οποιοδήποτε σημείο του δικτύου , η συσκευή που θα ανιχνεύσει τη βλάβη μπορεί άμεσα να μεταγάγει τα δεδομένα στην εναλλακτική διαδρομή και εν συνεχεία να ειδοποιήσει το Πεδίο Ελέγχου ότι πρέπει να γίνει υπολογισμός εναλλακτικής διαδρομής για τον συγκεκριμένο προορισμό. Αυτό είναι με την ευρύτερη έννοια ταυτόσημο μ ε τον υπολογισμό εναλλακτικών διαδρομών από ένα παραδοσιακό πρωτόκολλο δρομολόγησης. Το EIGRP για παράδειγμα, μπορεί να ανακαλύψει εναλλακτικές διαδρομές χωρίς βρόχους (Feasible Successors – Εν δυνάμει διάδοχοι) και να τις εγκαταστήσει στον πίνακα δρομολόγησης για άμεση χρήση όταν αστοχεί η κύρια διαδρομή.

Η προφανής απλότητα του προϋπολογισμού διαδρομών δεν είναι παρ' όλα αυτά τόσο απλή υπόθεση. Το σχήμα της Εικόνας 19 επιδεικνύει κάποια από την πολυπλοκότητα που περιλαμβάνει ο προϋπολογισμός εναλλακτικών διαδρομών:



Εικόνα 19: Παράδειγμα πολυπλοκότητας προϋπολογισμού διαδρομών

Ας υποτεθεί ότι ένας ελεγκτής εκτός σύνδεσης καθορίζει ότι η βέλτιστη διαδρομή μεταξύ A και G είναι (A,B,D.F,G) και εγκαθιστά τη σωστή πολιτική προώθησης σε κάθε συσκευή κατά μήκους αυτής. Ο ελεγκτής λογισμικού επίσης καθορίζει ότι μια καλή εναλλακτική διαδρομή είναι η (A,C,E,G) και γ αυτό εγκαθιστά την εναλλακτική πληροφόρηση προώθησης σε κάθε έναν από αυτούς τους δρομολογητές ώστε να διαθέτουν εναλλακτική διαδρομή για την κίνηση δεδομένων.

Αυτή η προφανώς απλή λύση περιλαμβάνει τρία διακριτά προβλήματα:

- Πρώτον η πληροφορία δρομολόγησης του δικτύου έχει διπλασιαστεί. Ένας απλός υπολογισμός των διαδρομών για κάθε ζεύγος πηγής/προορισμού είναι ήδη επιβαρυντικός –τα παραδοσιακά δίκτυα υπολογίζουν την διαδρομή μόνο προς κάθε προορισμό και για αυτό η κατάσταση δρομολόγησης επαυξάνεται καθώς πλησιάζουμε τον προορισμό. Δεν πρέπει όμως κάθε ζεύγος πηγής /προορισμού να υπολογίζεται σε αυτήν τη λύση και οι πληροφορίες προώθησης να εγκαθίστανται σε κάθε ζεύγος πηγής/προορισμού, οι πληροφορίες για τις εναλλακτικές διαδρομές πρέπει επίσης να εγκατασταθούν σε κάθε συσκευή κατά μήκους της εναλλακτικής διαδρομής. Ως εκ

τούτου ο δρομολογητής C πλέον διατηρεί μια διαδρομή για το (A,G), που κανονικά δεν θα είχε σε ένα παραδοσιακό δίκτυο.

- Δεύτερον, πώς θα έπρεπε ο δρομολογητής C να εκλάβει αυτές τις πληροφορίες δρομολόγησης; Υπήρχαν κάποτε δυο καταστάσεις στους πίνακες δρομολόγησης και προώθησης της κάθε συσκευής –μια διαδρομή είναι ενεργή ή είναι εναλλακτική για άλλη διαδρομή που χρησιμοποιείται τοπικά. Ο δρομολογητής C όμως δεν έχει τοπική διαδρομή για το (A,G) και θα χρειαστεί ξεχωριστή καταχώρηση που να υποδεικνύει ότι η εγκατεστημένη διαδρομή είναι εναλλακτική που δεν υφίσταται τοπικά.
- Τρίτον, πως πρέπει να αντιμετωπίσουμε με μη-τοπικές αστοχίες κατά μήκους της κύριας διαδρομής; Στο σενάριο του σχήματος, αν η ζεύξη μεταξύ των δρομολογητών A και B αστοχήσει, ο A μπορεί απλά να αναδρομολογήσει μέσω της εναλλακτικής διαδρομής, δηλαδή του δρομολογητή C. Αλλά τι γίνεται αν η ζεύξη μεταξύ των δρομολογητών και C αστοχήσει; Πως μπορεί ο A να γνωρίζει πώς να αναδρομολογήσει; Υπάρχουν μόνο δυο πιθανές λύσεις σε αυτό το πρόβλημα.

Ο δρομολογητής B μπορεί να εξετάσει τον τοπικό πίνακα δρομολόγησης και να αποστείλει κάποιο σήμα σε κάθε κόμβο που χρησιμοποιεί τον δρομολογητή B ως ενδιάμεση συσκευή. Αυτό σημαίνει την προσθήκη ενός πρωτοκόλλου σηματοδοσίας που θα παρέχει αυτή τη λειτουργία πληροφόρησης στο δίκτυο. Αυτή η τεχνική όμως χρειάζεται χρόνο, το ίδιο ποσό χρόνου που θα χρειαζόταν ένα παραδοσιακό πρωτόκολλο να ανιχνεύσει και να διαχύσει την πληροφορία σχετικά με την ίδια ακριβώς δικτυακή αλλαγή. Τα σήματα ενημέρωσης δεν είναι μόνο πολύπλοκα, οδηγούν και σε χρόνους σύγκλισης που είναι σχετικά ίσοι με αυτούς που προκύπτουν από τα ενσωματωμένα στις συσκευές Πεδία Ελέγχου. Μια άλλη επιλογή είναι για τον δρομολογητή B να ειδοποιήσει των εξωτερικό ελεγκτή σχετικά με την αστοχία της ζεύξης. Ο ελεγκτής μπορεί εν συνεχεία να σηματοδοτήσει τον δρομολογητή A ότι πρέπει να χρησιμοποιήσει την εναλλακτική διαδρομή για αυτή τη ροή δεδομένων. Αλλά ο καθοριστικός παράγοντας για μεταγωγή μεταξύ των ζεύξεων στη περίπτωση αυτή είναι η διαδρομή σηματοδοσίας από τον δρομολογητή B στον ελεγκτή και ξανά πίσω στον δρομολογητή A και όχι το ποσό του χρόνου που χρειάζεται ο ελεγκτής να υπολογίσει και να εγκαταστήσει την εναλλακτική διαδρομή. Αν αυτό αληθεύει γιατί αν υπολογίζεται και εν συνεχεία να εγκαθίσταται η δευτερεύουσα διαδρομή; Δεν μπορεί η δευτερεύουσα διαδρομή να υπολογιστεί και να εγκατασταθεί σε πραγματικό χρόνο όπως και με τα παραδοσιακά πρωτόκολλα δρομολόγησης που χρησιμοποιούν τις ζεύξεις δεδομένων;

Είναι επίσης πιθανό για τον ελεγκτή να υπολογίσει όχι μια αλλά δυο εναλλακτικές διαδρομές διαμέσου του δικτύου. Η εναλλακτική διαδρομή για τον δρομολογητή A θα μπορούσε να είναι η (A,C,F,G) και η εναλλακτική διαδρομή για την ίδια ροη B θα ήταν η (A,B,F,G). Αν τώρα αστοχήσει η ζεύξη μεταξύ των δρομολογητών B και D, η οποιαδήποτε κίνηση μπορεί να αναδρομολογηθεί απευθείας από τον B –με κόστος την αύξηση της πολυπλοκότητας στη κατάσταση του δικτύου,

Τελικά προκύπτει το ερώτημα του τι συμβαίνει στα δεδομένα εν κινήσει όταν εμφανίζεται αστοχία. Αν καταρρεύσει η ζεύξη μεταξύ των δρομολογητών F και G, ο δρομολογητής F πρέπει να ανατρέξει προς τα πίσω τη διαδρομή σηματοδοτώντας τον δρομολογητή A ή να ειδοποιήσει τον ελεγκτή ο οποίος πρέπει εν συνεχεία να πει στον δρομολογητή A να ανατρέξει στην εναλλακτική διαδρομή. Το ερώτημα στην περίπτωση αυτή είναι τι συμβαίνει με τα πακέτα στους ενδιάμεσους δρομολογητές B και D, απλά θα απορριφθούν;

Τα πρωτόκολλα δυναμικής δρομολόγησης επιλύουν όλα τα ανωτέρω προβλήματα επιτρέποντας σε κάθε κόμβο στο δίκτυο να υπολογίσει εναλλακτική διαδρομή για κάθε προορισμό. Οι μηχανισμοί IP ταχείας αναδρομολόγησης μπορούν να σχεδιαστούν ώστε να προσθέτουν λίγη ή και καθόλου πλεονασματική πληροφορία στο δίκτυο και να αντιδρούν αρκετά γρήγορα ώστε να μειωθούν η χρόνοι σύγκλισης ώστε μόνο τα πακέτα εν κινήσει ή αυτά που βρίσκονται στη μνήμη του κόμβου που αστοχεί να χαθούν.

Αν και η αντιπαράθεση σχετικά με το καλύτερο δυνατό δικτυακό μοντέλο –τη παραδοσιακή δρομολόγηση ή το OR/OR- θα συνεχιστεί εσαεί, δεν υπάρχει αμφιβολία ότι είναι θέμα των τωρινών τεχνολογιών και των πλεονεκτημάτων τους και όχι αν κάποιο μοντέλο επικρατεί του άλλου σε καθαρά τεχνικό επίπεδο.

2.6 OpenFlow

Το OpenFlow καθορίζει ένα σύνολο από κανόνες αλληλεπίδρασης μεταξύ ενός μεταγωγέα (στην πραγματικότητα πρόκειται απλά για ένα Πεδίο Προώθησης χωρίς συνοδεία Πεδίου Ελέγχου) και έναν εξωτερικό ελεγκτή. Αυτές οι αλληλεπιδράσεις μοντελοποιούνται ως ένα σύνολο καταστάσεων στον πίνακα προώθησης του μεταγωγέα, ένα σύνολο από πρωτόκολλα στη σύνδεση μεταξύ μεταγωγέα και ελεγκτή και ως ένα σύνολο από αντικείμενα στον ελεγκτή. Η τροποποίηση αντικειμένων στο μοντέλο δεδομένων του ελεγκτή προκαλεί την αποστολή OpenFlow μηνυμάτων από τον ελεγκτή στον μεταγωγέα που εν συνεχεία οδηγεί σε αλλαγή της κατάστασης στο πεδίο Προώθησης του μεταγωγέα.

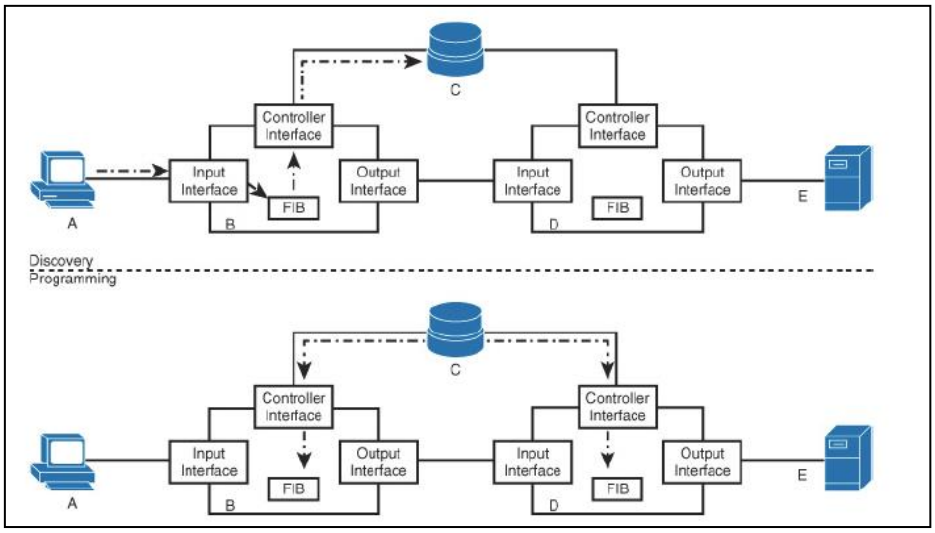
Οι αλληλεπιδράσεις αυτές βασίζονται σε διακριτές ροές δεδομένων, καθορισμένες από ένα σύνολο από πλειάδες, όπως η παραδοσιακή πενταπλή καταχώρηση ροής (IP αποστολέα, IP παραλήπτη, αριθμός πρωτοκόλλου, θύρα εισόδου, θύρα παραλήπτη) ο αριθμός των πλειάδων που χρησιμοποιούνται για την ταυτοποίηση μιας ροής είναι μεταβλητός με κάποιες υλοποιήσεις να υποστηρίζουν μια δωδεκάδα (συμπεριλαμβανομένων των L2 MAC διευθύνσεων, τους αριθμούς πρωτοκόλλου, τους αριθμούς L4 θυρών κλπ) .Ένα σύνολο από ροές μπορεί να υποδειχθεί με την χρήση χαρακτήρων «μπαλαντέρ» -wildcards σε διαφορετικά πεδία: για παράδειγμα όλη η κίνηση μεταξύ 192.0.2.1 και 198.51.100.1 περιγράφεται χρησιμοποιώντας: (192.0.2.1., 198.51.100.1,*,*,*).

Σε κάθε ροή (ή ομάδα από ροές) ανατίθεται μια από άκρου σε άκρο διαδρομή από τον εξωτερικό ελεγκτή που κατέχει μια καθολική όψη του δικτύου. Ο ελεγκτής πρέπει να διασφαλίσει ότι η κίνηση δεν εκτελεί βρόχο μεταξύ διαφόρων κόμβων στο δίκτυο εκτελώντας κάποιον υπολογισμό ελάχιστης διαδρομής (shortest path όπως χρησιμοποιείται στο SPF και στο IS-IS). Αν αστοχήσει μια ζεύξη ή δικτυακή συσκευή, πρέπει η κίνηση να σταματήσει έως ότου ο ελεγκτής ανακαλύψει τη βλάβη και ανταποκριθεί εγκαθιστώντας νέα διαδρομή στο δίκτυο.

2.6.1 Λειτουργία OpenFlow

Όσον αφορά τις πληροφορίες δρομολόγησης, το OpenFlow μπορεί να λειτουργήσει προληπτικά ή αντιδραστικά. Στον προληπτικό τρόπο λειτουργίας, ο πίνακας δρομολόγησης συμπληρώνεται σύμφωνα με τις πληροφορίες για την δικτυακή τοπολογία που διαθέτει ο ελεγκτής πριν οποιοδήποτε πακέτο φτάσει στις δικτυακές συσκευές καθαυτές. Επειδή αυτός ο τρόπος είναι παρόμοιος μ το παραδοσιακό μοντέλο δρομολόγησης με το οποίο είναι και εξοικειωμένοι οι περισσότεροι αρχιτέκτονες δικτύων, εξετάζεται περισσότερο το αντιδραστικό μοντέλο.

Στο αντιδραστικό μοντέλο (Εικόνα 20), το πεδίο προώθησης συμπληρώνεται καθώς νέες ροές ξεκινούν από τα τερματικά που είναι συνδεδεμένα στο δίκτυο, αντί να γίνεται προσπάθεια να καταγράφονται όλοι οι πιθανοί προσβάσιμοι προορισμοί σε κάθε χρονική στιγμή. Στο παρακάτω σχήμα αποδίδεται η διαδικασία του αντιδραστικού μοντέλου κατά τη δημιουργία ενός OpenFlow δικτύου.



Εικόνα 20: Reactive Μοντέλο SDN Δικτύου

2.6.2 OpenFlow μοντέλο σε αντιδραστική Λειτουργία

Η λειτουργία του OpenFlow διαχωρίζεται στα δυο βασικά μέρη από τα οποία αποτελείται το κάθε αντιδραστικό Πεδίο Ελέγχου: ανακάλυψη και προγραμματισμός. Για να εκκινήσει η διαδικασία, ο Host A στέλνει ένα πακέτο στο Server E. Ο μεταγωγέας B λαμβάνει το πακέτο και ελέγχει τον τοπικό πίνακα προώθησης (FIB) για πληροφορίες σχετικά με την συγκεκριμένη ροή. Θα υποτεθεί για αυτό το παράδειγμα ότι δεν υπάρχει καταχώρηση για τη ροή αυτή στην τοπική FIB.

Με την παραλαβή ενός πακέτου για μια ροή για την οποία δεν υπάρχουν πληροφορίες προώθησης, ο μεταγωγέας OpenFlow, B ενθυλακώνει ολόκληρο το πακέτο και το αποστέλλει μέσω ξεχωριστού καναλιού πίσω στον ελεγκτή C για περαιτέρω επεξεργασία. Στο σημείο αυτό ο ελεγκτής έχει δυο επιλογές:

- Πρώτα από όλα ο ελεγκτής θα μπορούσε απλά να επεξεργαστεί το πακέτο συμπεριλαμβανομένης της τοποθέτησης οποιασδήποτε απαραίτητης πληροφορίας για την προώθηση του πακέτου στον τελικό προορισμό να το στείλει στον μεταγωγέα B για περαιτέρω επεξεργασία. Ο μεταγωγέας B θα λάμβανε το πακέτο, θα ανακάλυπτε την πληροφορία που απαιτείται για την προώθηση του πακέτου στις επικεφαλίδες OpenFlow που έχουν προστεθεί από τον ελεγκτή C και θα το προωθούσε σύμφωνα με τις οδηγίες αυτές.
- Δεύτερον, ο ελεγκτής θα μπορούσε να επεξεργαστεί το πακέτο και να το στείλει πίσω στον μεταγωγέα B για προώθηση και εν συνεχεία να προγραμματίσει μια καταχώρηση στον πίνακα προώθησης κάθε μεταγωγέα κατά μηκος της διαδρομής μέσω του καναλιού επικοινωνίας με τον ελεγκτή όπως φαίνεται στο πιο πάνω σχήμα. Με αυτόν τον τρόπο, το δεύτερο πακέτο που στέλνει ο Host A στον διακομιστή E θα προωθηθεί μέσω των μεταγωγέων B και D χρησιμοποιώντας επεξεργασία υλικού. Αυτή η διαδρομή ροής που χτίζεται δυναμικά από τον ελεγκτή ως απάντηση στο πρώτο πακέτο της ροής, μπορεί να εκληφθεί ως μια από άκρου σε άκρο πολιτική δρομολόγησης για τη συγκεκριμένη ροή.

Αυτή η διαδρομή ροής διατηρείται μέχρις ότου κάποια τοπική πολιτική στο δίκτυο ή τους ανεξάρτητους μεταγωγείς την αφαιρέσει. Η διαδικασία αφαίρεσης συνήθως βασίζεται σε έναν απλό χρονομέτρη (αν μια επικεφαλίδα ροής δεν έχει χρησιμοποιηθεί ώστε να προωθηθεί ένα συγκεκριμένο πακέτο μέσα σε δοθέν πλήθος δευτερολέπτων, τότε αφαιρείται), ή μπορεί να βασίζεται σε πιο εξεζητημένο μηχανισμό που αναζητά την κατακλείδα πολύ γνωστών πρωτοκόλλων. Για παράδειγμα, ένας μεταγωγέας μπορεί να παραμετροποιηθεί να προωθεί την κίνηση που εμπίπτει σε συγκεκριμένη ροή αλλά και να αντιγράφει όσα πακέτα TCP διαθέτουν συγκεκριμένα bit ή μηνύματα ελέγχου στον ελεγκτή. Αυτό θα επέτρεπε στον ελεγκτή να

παρακολουθεί την κατάσταση και την υγεία της κάθε σύνδεσης TCP και να απομακρύνει κάθε καταχώρηση ροής για TCP συνεδρίας που έχει λήξει ή έχει τερματίσει.

Ολόκληρο το δίκτυο SDN από άκρη OpenFlow σε άκρη λαμβάνεται ως ένας μονός τομέας επιπέδου 2 (L2) από πλευράς δρομολόγησης όπως ακριβώς ένα μονό ζευγνύον δέντρο ή τομέας TRILL.

2.6.3 Αντιρρήσεις και Σημεία Προσοχής

Οι περισσότερες από τις αντιρρήσεις στην τεχνολογία SDN αφορούν την επεκτασιμότητα, την πολυπλοκότητα, τον διαχωρισμό των Πεδίων Ελέγχου και Δεδομένων καθώς και την αντιδραστική φύση του Πεδίου Ελέγχου όπως θα φανεί στα παρακάτω εδάφια.

Επεκτασιμότητα

Η πιο συνηθισμένη αντίρρηση στο SDN είναι ότι δεν διαθέτουν επεκτασιμότητα. Αυτή είναι και μια τυπική αντίρρηση σε κάθε τεχνολογία στον τομέα των δικτύων και γι αυτό πρέπει να εμβαθύνουμε σε αυτήν την αντίρρηση ώστε να την κατανοήσουμε καθώς και τις απαντήσεις σε αυτήν. Τι σημαίνει τελικά δεν επεκτείνεται; Γενικά , σημαίνει ότι το εν λόγω πρωτόκολλο ή σύστημα δεν θα μπορεί να διαχειριστεί μεγάλους αριθμούς από τερματικά λόγω της αύξησης της πλεονάζουσας πληροφορίας ή της λειτουργίας.

Στην περίπτωση των SDN, υπάρχουν τρεις συγκεκριμένες κατηγορίες όσων αφορά την επεκτασιμότητα. Η πρώτη αντίρρηση είναι ότι απλά δεν είναι δυνατόν να δημιουργηθεί υλικό που να υποστηρίζει εκατοντάδες ή χιλιάδες από ροές ή μικρο-ροές. Σήμερα οι OpenFlow μεταγωγείς μπορούν να υποστηρίξουν εκατοντάδες ή χιλιάδες καταχωρήσεις πίνακα προώθησης. Φαίνεται δύσκολο να βρεθεί επεξεργαστική ισχύς που να χτίσει και γρήγορα να βρίσκει καταχωρήσεις σε πίνακα με εκατομμύρια από καταχωρήσεις των 5 ή 12 πεδίων.

Κοιτάζοντας πίσω στην ιστορία της δικτύωσης υπολογιστών, ανακαλύπτουμε ότι το μέλημα της επεκτασιμότητας έχει ξαναεμφανιστεί και αντίστοιχα αντιμετωπιστεί πολλές φορές στο παρελθόν. Πριν από 10 χρόνια ένας πίνακας δρομολόγησης με 5000 καταχωρήσεις θα θεωρείτο υπερβολικός εκτός του πυρήνα του Διαδικτύου και ο ίδιος ο πυρήνας διαδρομών του Διαδικτύου με 100000 εγγραφές θεωρείτο υπερβολικά μεγάλος. Σήμερα οι δρομολογητές υποστηρίζουν εκατομμύρια διαδρομές στους πίνακες δρομολόγησης τους με αντίστοιχους πίνακες μεταγωγής των ίδιων μεγεθών.

Οι κατασκευαστές υλικού, οι σχεδιαστές πρωτοκόλλων και οι αρχιτέκτονες δικτύων έμαθαν πώς να «πειράζουν» το υλικό , τα πρωτόκολλα, το λογισμικό και το ίδιο το σχέδιο του δικτύου ώστε να δημιουργούν και να διαχειρίζονται δίκτυα. Δεν ήταν εύκολο φυσικά αλλά τα δίκτυα μεταγωγής πακέτου μεγενθύνονται πέρα από τις προβλέψεις πριν 10 με 15 χρόνια.

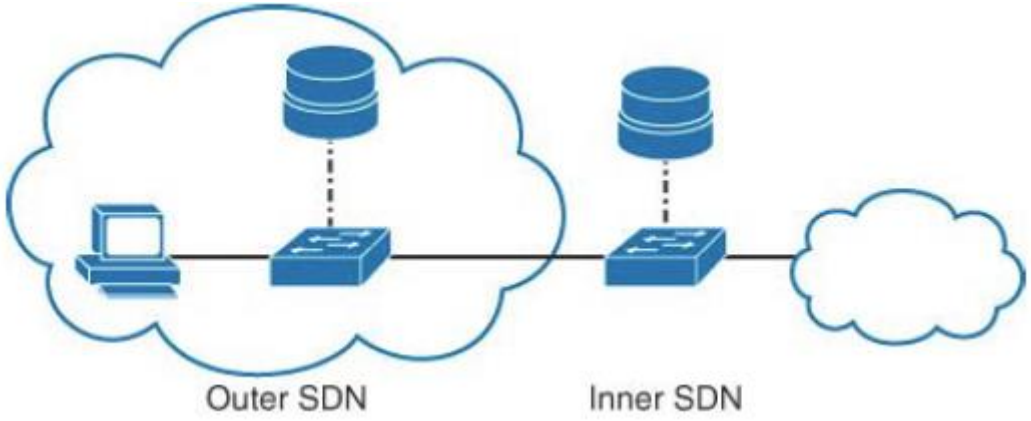
Καθώς αυξανόταν η ζήτηση, οι μηχανικοί έμαθαν πώς να χτίζουν το ζητούμενο. Το SDN είναι πιθανότατα η απάντηση στο πρόβλημα της επέκτασης όπως και οι κατασκευαστές υλικού θα μάθουν να δημιουργούν μεγάλης κλίμακας πεδία προώθησης, βελτιστοποιημένα για τις απαιτήσεις του SDN. Οι αλγόριθμοι, το υλικό και άλλα εξαρτήματα θα διαμορφωθούν γύρω στις τωρινές απαιτήσεις κάνοντας τα προβλήματα επεκτασιμότητας μια μακρινή ανάμνηση. Η δεύτερη αντίρρηση σχετικά με την επεκτασιμότητα είναι ότι ένα SDN δίκτυο αποτελεί έναν επίπεδο τομέα –ότι η ιεραρχία και τα μαθήματα που πήραμε από αυτήν πετάγονται από το παράθυρο. Σε αντίθεση με την πρώτη αντίρρηση το πρόβλημα πλέον είναι δομικό. Μόνο με τον χρόνο θα φανεί αν η αλλαγή στη φιλοσοφία σχεδίασης μπορεί να υπερβεί αυτήν την αντίρρηση. Οι αρχιτέκτονες δικτύου μπορεί να ρουν ότι το πεδίο των SDN είναι περιορισμένο σε μεγέθη υπολογιστικών κέντρων ή σε πάρκα και ότι η δρομολόγηση μεταξύ των SDN πρέπει να λαμβάνει χώρα όπως διαχειρίζεται σήμερα το πρωτόκολλο BGP την δρομολόγηση μεταξύ τομέων. Απλά δεν υπάρχει τρόπος να το προβλέψουμε επί του παρόντος.

Για να το δούμε στην πράξη, θα λάβουμε το πρόβλημα του δικτύου πλήρους πλέγματος όσον αφορά τα τερματικά. Αν κάθε τερματικό στο δίκτυο μπορεί να συνδεθεί με όλα τα άλλα τερματικά μέσω του δικτύου, τότε πρέπει να γίνουν n*(n-1)/2 ζεύξεις. Στο επίπεδο όπου το OpenFlow διαχειρίζεται το δίκτυο, το πρόβλημα δεν είναι ανά ζευγάρι τερματικών αλλά ανά ζεύγος socket και ο τύπος πρέπει να εφαρμοστεί ανά διεργασία ή ανά ροή που διέρχεται το δίκτυο. Η επέκταση σε τοπολογία πλήρους πλέγματος απλά δεν μπορεί να υποστηριχθεί. Δεν αφορά το πλήθος των καταχωρήσεων στον εκάστοτε πίνακα, ούτε και τη διαχείριση της ροής

στο πεδίο ελέγχου παρά εγγενή προβλήματα σε κάθε μορφής περιβάλλον μετάδοσης πλήρους πλέγματος.

Το πρόβλημα πρέπει τελικά να λυθεί με τον ίδιο τρόπο που λύνεται και στα παραδοσιακά δίκτυα –συναθροίζοντας τις πληροφορίες του Πεδίου Ελέγχου. Το μοναδικό ερώτημα που πρέπει να απαντηθεί είναι πώς θα λάβει χώρα αυτή η συνάθροιση. Υπάρχουν επί του παρόντος τουλάχιστον τρεις επιλογές.

- Περιοχές του δικτύου όπου τα SDN μοντέλου Replacement έχουν αναπτυχθεί μπορούν να αντιμετωπιστούν ως ένας μεγάλος L2 τομέας εντός του δικτύου, όπως και ένας τομέα ζευγνύοντος δέντρου είναι σε ένα παραδοσιακό σχέδιο IP. Αυτό περιορίζει το μέγεθος του τομέα SDN, διασπώντας πιθανούς τομείς αστοχιών χάρη σε σημεία IP διασύνδεσης. Για να δουλέψει αυτό το σχέδιο, οι ελεγκτές SDN πρέπει να τρέξουν ένα πρωτόκολλο δρομολόγησης και α εγχύσουν πληροφορίες προσβασιμότητας στο δρομολογούμενο πεδίο ελέγχου στο άκρο του SDN τομέα.
- Μπορούν να αναπτυχθούν πολλαπλά επίπεδα από Replacement SDNs σε ένα δίκτυο με κάποιας μορφής ακριανό κόμβο να λειτουργεί ως host σε υψηλότερο επίπεδο, ή σε επικαλυπτόμενο SDN δίκτυο. Το παρακάτω σχήμα επιδεικνύει την ιδέα:



Εικόνα 21 Πολλαπλά επίπεδα Replacement SDNs

- Ιεραρχημένο Μοντέλο Αντικατάστασης SDN: Στην Εικόνα 21, το εξωτερικό SDN εμφανίζεται ως μια μόνο συσκευή στο εσωτερικό SDN ενώ το εξωτερικό SDN μπορεί στην πραγματικότητα να εκπροσωπεί χιλιάδες συσκευές. Αυτού του είδους η ιεραρχία είναι γνωστή στους μηχανικούς που έχουν ήδη αναπτύξει L2VPN, L2VPN και άλλες συσκευές προσομοίωσης.
- Τα πεδία ελέγχου SDN μπορούν να τροποποιηθούν ώστε να συναθροίσουν πληροφορίες όπως πράττουν τα πρωτόκολλα δρομολόγησης στα παραδοσιακά δίκτυα. Μπορεί για παράδειγμα να επεκταθεί η χρήση από bit μπαλαντέρ ώστε να συμπεριληφθεί η έννοια της μάσκας υποδικτύωσης ώστε πληροφορίες σχετικά με σύνολα από προσβάσιμους προορισμούς να μπορούν να διαφημίζονται και να εγκαθίστανται αντί για τον κάθε προορισμό ξεχωριστά. Αυτού του είδους συνάθροιση Πεδίου Ελέγχου είναι ήδη ευρέως κατανοητή και είναι σχετικά εύκολο να αναπτυχθεί και να την διαχειριστούμε σε περίπτωση μεγάλης μοντέλων Αντικατάστασης SDN.

Η εμπειρία λέει ότι θα αναπτυχθούν και τα τρία μοντέλα SDN και ίσως και περισσότερα. Τελικά θα εξαρτηθεί από τους κατασκευαστές εξοπλισμού και τους αρχιτέκτονες δικτύων ο τρόπος αντιμετώπισης της μεγέθυνσης των δικτύων πλήρους πλέγματος.

2.7 Πολυπλοκότητα

Το πρόβλημα της πολυπλοκότητας των δικτύων βασισμένων σε λογισμικό μπορεί να συνοψισθεί στα εξής:

- Οι μηχανικοί λογισμικού αντικρίζοντας τα δίκτυα σκέφτονται ότι είναι εξαιρετικά πολύπλοκα και ότι θα ήταν πιο απλό να γράψουν λίγες γραμμές κώδικα που τα διαχειρίζονται.
- Οι μηχανικοί δικτύων επίσης σκέπτονται ότι και το λογισμικό είναι εξαιρετικά πολύπλοκο με όλες αυτές τις γραμμές κώδικα και όλες αυτές τις αλληλεπιδράσεις μεταξύ προγραμμάτων που πιθανώς περιέχουν ευπάθειες ασφάλειας, σφάλματα (bugs) και θεωρούν ότι οι σημερινές δικτυακές εφαρμογές είναι απλούστερες και σαφέστερες.

Το πρόβλημα είναι ότι και οι δυο έχουν δίκιο αφού εξετάζουν απλοποιημένες εκδοχές του προβλήματος. Ο μηχανικός λογισμικού βλέπει ένα μεγάλο, περίπλοκο δίκτυο με εκατοντάδες από διαφορετικά είδη συσκευών και εκατοντάδες διαφορετικά πρωτόκολλα όλα να αλληλεπιδρούν μεταξύ τους μέσω εκατοντάδων διαφορετικών εκδόσεων λογισμικού και υποεκδόσεων υλικού ώστε τους φαίνεται πολύ δυσκολότερο από έναν αλγόριθμο. Αντίστοιχα ο μηχανικός δικτύων βλέπει έναν υπολογιστή και πως τα διαφορετικά μέρη λογισμικού και σκέφτεται ότι είναι πολύ δυσκολότερο από ένα πρωτόκολλο OSPF.

Η πραγματικότητα είναι πως τόσο τα δίκτυα όσο και το λογισμικό είναι περίπλοκα γιατί υπάρχουν ώστε να αντιμετωπίσουν περίπλοκα συστήματα. Το βασικό ερώτημα που τίθεται όταν λαμβάνεται υπόψη η πολυπλοκότητα του SDN (και οποιασδήποτε άλλης λύσης) είναι: περίπλοκο σχετικά με τι; Είναι ένα δίκτυο 5000 VLAN περισσότερο περίπλοκο από ένα SDN; Είναι ένα κατανεμημένο πρωτόκολλο δρομολόγησης περισσότερο περίπλοκο από τον κώδικα που χρειάζεται ώστε να υπολογιστούν βέλτιστες και χωρίς βρόχους διαδρομές στον ελεγκτή.

2.8 Διαχωρισμός των Πεδίων Δεδομένων και Ελέγχου

Σε αυτή την παράγραφο αναλύονται δυο ενστάσεις. Η πρώτη αφορά την περίπτωση ταχείας σύγκλισης σε περίπτωση αστοχίας του δικτύου και έχει καλυφθεί ήδη στην περίπτωση Δρομολόγησης εκτός σύνδεσης/Αντίδρασης με σύνδεση.

Η δεύτερη ένσταση αφορά αστοχίες μεταξύ της σύνδεσης του πεδίου δεδομένων μιας συσκευής και του πεδίου ελέγχου που εδρεύει σε άλλη συσκευή. Είναι πιθανό να δημιουργηθούν πρωτόκολλα που να δύνανται να ελέγχουν και να διαχειρίζονται σε πραγματικό χρόνο εκατομμύρια ροές με συνδέσεις εκτός της συσκευής; Είναι ευρέως γνωστό ότι οι δικτυακές διεπαφές και οι αντίστοιχες συσκευές απορρίπτουν πακέτα σε καταστάσεις υψηλού φόρτου. Τι θα συμβεί όταν ο ελεγκτής στείλει ένα μήνυμα και αυτό χαθεί σε κάποιο σημείο της διαδρομής προς τον μεταγωγέα; Ακόμα χειρότερα τι θα συμβεί αν διακοπεί πλήρως η επικοινωνία μεταξύ της συσκευής προώθησης πακέτων και τον ελεγκτή αυτής;

Μέρος αυτής της ανησυχίας οφείλεται στην αντίληψη μας των συσκευών αυτών ως «ένα κουτί» ενώ στην πραγματικότητα αποτελούν μια συλλογή από επεξεργαστές που τρέχουν διαφορετικές διεργασίες και διασυνδέονται μέσω μιας κεντρικής αρτηρίας. Πολλοί λίγοι μηχανικοί χρειάστηκε να αντιμετωπίσουν βλάβες στις εσωτερικές αρτηρίες γιατί οι σχεδιαστές τους έχουν μάθει πλέον να τις κάνουν αρκετά ανθεκτικές ώστε να μπορούν να αντέξουν τον φόρτο και να αστοχούν με κάποια «χάρη».

Άρα το ζήτημα είναι να μάθουμε να σχεδιάζουμε σωστά το λογισμικό, το υλικό και την αρχιτεκτονική που κάνει ένα μοντέλο Αντικατάστασης SDN να δουλέψει. Ανατρέχοντας στην εμπειρία των παραδοσιακών πεδίων ελέγχου, τα πρωτόκολλα link state έχουν σχεδιαστεί ώστε να καθαρίζουν και να κατακλύζουν το δίκτυο με τα link states σε τακτικά χρονικά διαστήματα. Αντίστοιχα, το EIGRP σχεδιάστηκε ώστε να έχει περισσότερο ενεργή οπτική του δικτύου. Αυτά τα μέτρα σχεδιάστηκαν στα δικτυακά πρωτόκολλα ώστε να αντιπαρέρχονται σε κοινές αστοχίες ζεύξεων και συσκευών αλλά και για ακραίες καταστάσεις. Τα πρωτόκολλα link-state λειτουργούν πλέον με τα χρονικά διαστήματα για αυτοκαθαρισμό και ανανέωση ορισμένα στο μέγιστο δυνατό ή με τους χρονομετρητές απενεργοποιημένους και το EIGRP είναι μόνιμα σε ενεργό κατάσταση ώστε να εκμεταλλεύεται τα νεώτερα δίκτυα και τις δυνατότητες τους.

Αυτό είναι ένα ακόμα πεδίο όπου αναμένεται οι σχεδιαστές SDN πρωτοκόλλων, υλικού και λογισμικού να μάθουν σε βάθος χρόνου να αντιμετωπίζουν το πρόβλημα αυτό.

2.9 Αντιδραστικά Πεδία Ελέγχου

Ένας πλήθος από αντιρρήσεις σχετικά με τα αντιδραστικά πεδία ελέγχου αφορά τα SDN που λειτουργούν αντιδραστικά. Η βασική αντίρρηση και η πιο δύσκολη να ξεπεραστεί, είναι ότι η προσωρινή αποθήκευση στο πεδίο δεδομένων αφορά συγκεκριμένα μορφότυπα ροών δεδομένων. Η προσωρινή αποθήκευση βασίζεται σε σχετικά μικρό αριθμό όλων των πιθανών τερματικών να εκκινούν ροές δεδομένων μεταξύ τους σε οποιαδήποτε χρονική στιγμή. Αν η κίνηση αποκλίνει από τα συγκεκριμένα μορφότυπα σε μεγάλο βαθμό, τότε η προσωρινή αποθήκευση αποτυγχάνει ολοκληρωτικά.

Για παράδειγμα, αν μια προσωρινή μνήμη αποθήκευσης μπορεί να κρατήσει δέκα καταχωρήσεις, σε κανονική λειτουργία είναι ασφαλές να διατηρούνται τέσσερις με πέντε θέσεις συμπληρωμένες στην προσωρινή μνήμη. Αν η μνήμη γεμίσει κατά 80%, οι παλαιότερες καταχωρήσεις πρέπει να απομακρυνθούν γρηγορότερα ώστε να προλάβουν πιθανή άρνηση συνδέσεων λόγω έλλειψης χώρου.

Αυτό το είδος αστοχίας της προσωρινής μνήμης έχει προκαλέσει αρκετές ολικές αστοχίες δικτύου, ειδικότερα όταν η κίνηση του Πεδίου Ελέγχου (συμπεριλαμβανομένης της σηματοδοσία σχετικά με την κατάσταση των ζεύξεων) μεταδίδεται μαζί με τα δεδομένα των χρηστών. Η Cisco για παράδειγμα επανασχεδιάζει ολόκληρη την υποδομή του πεδίου προώθησης, μετακινούμενη από την γρήγορη ενδιάμεση αποθήκευση στο CEF (Cisco Express Forwrding) ώστε να επιλύσει τα συχνά εμφανιζόμενα προβλήματα του είδους. Αν και ένα πλήθος από πιθανές λύσεις έχουν προταθεί ώστε να λυθεί αυτού του είδους το πρόβλημα, υπάρχει βαθειά επιφυλακτικότητα στην κοινότητα των μηχανικών δικτύων ως προς την επιστροφή σε προσωρινά αποθηκευμένους πίνακες προώθησης.

2.10 Συμπέρασμα

Τα δίκτυα βασισμένα σε λογισμικό εμφανίζονται εξαιρετικά ελπιδοφόρα όσον αφορά τη μείωση της πολυπλοκότητας των κατανεμημένων δικτυακών μοντέλων ενώ παρέχουν οδηγό για την ανάπτυξη δικτυακών τεχνολογιών στο άμεσο μέλλον. Αν και δεν υπάρχει σαφής ερώτηση σχετικά με το ποιο είναι το καλύτερο μοντέλο ή αν τα δίκτυα βασιζόμενα σε λογισμικό τελικά καταλάβουν τον κόσμο, η κατανόηση των διαφορετικών προτάσεων και του τρόπου με των οποίο μπορούν να συνεργαστούν ώστε να υπάρξουν σωστές αποφάσεις.

Η επιλογή εγκατάστασης ενός δικτύου SDN εξαρτάται από τις επιχειρησιακές ανάγκες παρά τεχνολογικές. Ο καλύτερος τρόπος να γίνει η επιλογή είναι να ληφθούν υπόψη οι θετικές και οι αρνητικές όψεις της εν λόγω τεχνολογίας σε συγκεκριμένες περιστάσεις, να καθοριστεί ποια προβλήματα μπορεί να αντιμετωπίσει, να ληφθούν υπόψη όλες οι πιθανές παρενέργειες και επιπτώσεις και να αποφασιστεί ο τρόπος υλοποίησης της.

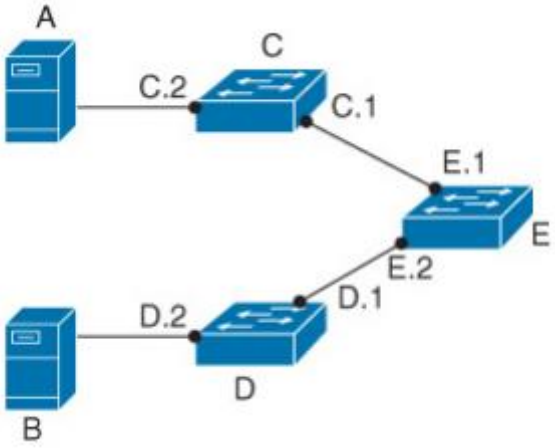
2.11 Το SDN στο υπολογιστικό κέντρο

Το περιβάλλον των υπολογιστικών κέντρων αποτελεί περιοχή έρευνας και ανάπτυξης τα τελευταία χρόνια. Συγκεκριμένα πρωτόκολλα και τεχνολογίες έχουν αναπτυχθεί ώστε να διαχειριστούν τις τεράστιες ανάγκες επέκτασης και διαχείρισης μεγάλων δικτύων (δεκάδες έως και εκατοντάδες χιλιάδες συσκευών σε ένα μόνο κτίριο). Οι εγκαταστάσεις τέτοιου μεγέθους φέρνουν και ποικίλα περίπλοκα προβλήματα διαχείρισης του πεδίου ελέγχου στον κόσμο της σχεδίασης δικτύων συμπεριλαμβανομένης της διαχείρισης μεγάλης έκτασης δικτυακής προσομοίωσης, πολιτικές διαχείρισης και της διαχείρισης της παραμετροποίησης μεγάλου αριθμού δικτυακών συσκευών. Για παράδειγμα θα ληφθεί υπόψη πως το OpenFlow μπορεί να λύσει τέτοια προβλήματα και από την άλλη, ποιες προκλήσεις θα αντιμετωπίσει.

2.11.1 Τι φέρνει το OpenFlow

Τα μεγάλης κλίμακας υπολογιστικά κέντρα σχεδιάζονται ώστε να εξυπηρετούν πολλούς ενοικιαστές, όπως πολλαπλές εταιρικές μονάδες εντός μιας επιχείρησης, πολλές επιχειρήσεις με κοινή ιδιοκτησία ή μια εταιρία που πουλά υπηρεσίες νέφους σε άλλες εταιρείες. Το πρόβλημα των πολλών ενοικιαστών αναπαριστά στον αρχιτέκτονα δικτύων ένα πρόβλημα διαχωρισμού των δεδομένων. Τα δεδομένα του κάθε ενοικιαστή πρέπει κάπως να διαχωριστούν από όλους τους υπολοίπους, ακόμα και καθώς τα δεδομένα μετακινούνται εντός του δικτύου ώστε να βελτιστοποιηθεί η χρήση των πόρων και η ροή των δεδομένων.

Κανονικά αυτός ο διαχωρισμός επιτυγχάνεται με την ανάθεση ενός VLAN ανά ενοικιαστή ή σε πιο πρόσφατες εγκαταστάσεις, με την παροχή σε κάθε ενοικιαστή ενός L3VPN ή L2VPN με χρήση πρωτοκόλλου MPLS εντός του υπολογιστικού κέντρου. Παρ' όλα αυτά και οι δύο λύσεις είναι δύσκολες στην υλοποίηση και στη διαχείριση. Πως μπορεί ένα δίκτυο SDN βασισμένο στο OpenFlow να λύσει τα προβλήματα αυτά; Ένα κεντρικοποιημένο πεδίο ελέγχου είναι πολύ χρήσιμο στην δυναμική διαχείριση της ροής των δεδομένων από και προς ποικίλες θέσεις του δικτύου ενός υπολογιστικού κέντρου σχεδιασμένου για παραχώρηση σε πολλούς χρήστες όπως φαίνεται στο παρακάτω σχήμα:



Εικόνα 22: Απλό υπόδειγμα υπολογιστικού κέντρου

Μετακίνηση δεδομένων στο Υπολογιστικό Κέντρο

Όταν μια υπηρεσία μετακινείται από έναν διακομιστή στο ικρίωμα A (Εικόνα 22) σε άλλον διακομιστή στο ικρίωμα B, οι θύρες E.1,C.1 και C.2 πρέπει να αναδιαμορφωθούν ώστε να απομακρυνθούν από το VLAN στο οποίο υπάγεται η εν λόγω υπηρεσία. Για να αποφευχθεί μεγάλο μέρος του έργου της παραμετροποίησης σε ένα παραδοσιακό δίκτυο, κάθε VLAN διοχετεύεται σε κάθε ικρίωμα (ή σε μεγάλο υποσύνολο ικριωμάτων όπου επιτρέπεται η λειτουργία της υπηρεσίας). Η διατήρηση όλων των VLANs, υπηρεσιών και των πιθανών τους συνδυασμών είναι βαρύ έργο όσον αφορά τη διαχείριση.

Σε μια εγκατάσταση OpenFlow όμως, η μετακίνηση της υπηρεσίας θα γινόταν με ένα κεντρικοποιημένο σύστημα που δεν μετακινεί μόνο την σωστή διεργασία από το ένα σύστημα

στο άλλο, αλλά μετακινεί και τις κατάλληλες θύρες στα αντίστοιχα VLANs. Με άλλα λόγια, τις κατάλληλες ροές από ένα σύνολο ροών σε άλλο απλοποιώντας τη διαχείριση του δικτύου και το σχέδιο του.

Άλλα δύσκολα προβλήματα που θα λυνόντουσαν πιο εύκολα σε περιβάλλον SDN υπολογιστικού κέντρου είναι τα εξής:

- Η μεταγωγή άγνωστων ροών, ή ροών που έχουν στιγματιστεί ως πιθανές απειλές ασφαλείας σε υλικό που έχει σχεδιαστεί να εξαλείφει ιούς και να αντιμετωπίζει DDoS επιθέσεις.
- Το χτίσιμο της κατάστασης προωθήσεων σε συνδυασμό με συστήματα αυθεντικοποίησης και εξουσιοδότησης ώστε οι χρήστες να έχουν διαδρομές προς διακομιστές όπου τους επιτρέπεται η πρόσβαση.

2.11.2 Προκλήσεις στη λύση με OpenFlow

Το SDN στο υπολογιστικό κέντρο, όπως όλες οι τεχνολογίες προσφέρει στον αρχιτέκτονα δικτύων τόσο θετικές όσο και αρνητικές όψεις. Ατέλειες στους αλγόριθμους που συνδέουν τα συστήματα μεταξύ τους μπορούν να προκαλέσουν βρόχο θετικής ανάδρασης επιτρέποντας στην αστοχία σε ένα σύστημα να εισχωρήσει σε άλλο ή και να προκαλέσει γενικευμένη κατάρρευση του δικτύου. Η ανθεκτικότητα δεν αφορά την ύπαρξη πολλαπλών ελεγκτών αλλά και την απομόνωση των τομέων σφαλμάτων. Τα SDN μοντέλου αντικατάστασης με τα κεντρικοποιημένα Πεδία Ελέγχου, αποτελούν πρόκληση στο πεδίο του διαχωρισμού των τομέων σφαλμάτων.

Ένα άλλο ζήτημα είναι ότι και οι SDN ελεγκτές πρέπει πλέον να διασφαλίζονται. Κάθε επίθεση σε έναν SDN ελεγκτή αποτελεί μακράν χειρότερη απειλή από την επίθεση και την καταβολή ενός μόνοδρομολογητή. Τα κατανεμημένα πεδία ελέγχου είναι εξαιρετικά ανθεκτικά σε αστοχίες μοναδικών κόμβων ή και ζεύξεων αφού κάθε κόμβος στο δίκτυο παίζει σχετικά ισότιμο ρόλο στη λειτουργία του ίδιου του δικτύου.

Η εξοικονόμηση μεγάλων κεφαλαίων που πολλοί διαχειριστές δικτύων αναμένουν με τη μετακίνηση τους σε μια λύση SDN, πιθανότατα 0δεν θα εμφανιστεί μακροπρόθεσμα. Το υλικό που θα υποστηρίζει το πλήθος των ροών για ένα μεγάλης κλίμακας υπολογιστικό κέντρο με τη δυνατότητα διαχείρισης εκατομμυρίων ροών δεν αναμένεται να είναι λιγότερο ακριβό από τις τυπικές πλατφόρμες δρομολόγησης και μεταγωγής που χρησιμοποιούμε σήμερα.

SDN σε πυρήνα δικτύου ευρείας περιοχής (WAN)

Αν και το μοντέλο SDN αντικατάστασης δείχνει να κατέχει τις περισσότερες προοπτικές για χρήση στα υπολογιστικά κέντρα και σε άλλα περιβάλλοντα που ταιριάζουν σε συγκεκριμένο σύνολο προδιαγραφών, τα μοντέλα παράλληλου SDN εμφανίζονται ως τα περισσότερ υποσχόμενα για εφαρμογές ευρείας περιοχής και δικτυακού πυρήνα.

Είναι συχνά επιθυμητό στα δικτυακά άκρα, όπου η κίνηση εξέρχεται από δυο πιθανές διαδρομές, να επιλέγεται η διαδρομή με βάση περισσότερες πληροφορίες από αυτές που παρέχει το BGP. Για παράδειγμα, ένας χειριστής δικτύου μπορεί να θέλει να λάβει υπόψη το κόστος χρήσης μιας ζεύξης ανά μονάδα δεδομένων, που μπορεί να περιλαμβάνει περιορισμούς σχετικά με την ώρα της ημέρας (η τιμολόγηση σε ώρα αιχμής αυξάνει ή επιβαρύνει), επιπλέον κόστη ανά μονάδα δεδομένων επί της βασικής μονάδας ή και το κόστος της αποστολής δεδομένων σε συγκεκριμένο προορισμό. Το κόστος χρήσης μιας ζεύξης πρέπει να ισοσκελίζεται με το οικονομικό όφελος, συμπεριλαμβανομένων των γρηγορότερων αντιδράσεων στις συνθήκες τις αγοράς σε συγκεκριμένες χρονικές περιόδους.

Οι είσοδοι σε ένα τέτοιο σύστημα μπορεί να περιλαμβάνουν τα ακόλουθα:

- Κόστος αποστολής ανά μονάδα δεδομένων
- Ώρα της ημέρας
- Πόσο επείγοντα είναι τα δεδομένα ή η ροή
- Οι επιδόσεις του σημείου εξόδου συμπεριλαμβανομένου του jitter, της χρονοκαθυστέρησης και του διαθέσιμου εύρους ζώνης, πιθανώς ανά προορισμό

- Διαθεσιμότητα συγκεκριμένου προορισμού μέσω δεδομένης ζεύξης ανά προορισμό (περισσότερο καθορισμένη απ΄ότι με πρωτόκολλο δρομολόγησης)

Οι μετρικές μπορούν να προστεθούν στο BGP ή σε οποιοδήποτε άλλο δικτυακό πρωτόκολλό, παρέχοντας επιπλέον πληροφορίες. Οι λεπτομερώς ρυθμισμένοι αλγόριθμοι μπορούν να αναπτυχθούν εντός των υλοποιήσεων δικτυακών πρωτοκόλλων αλλά αυτό θα απαιτούσε μαζικές αλλαγές στον τρόπο λειτουργίας τους σε μια προσπάθεια να προσμετρηθεί ο κάθε πιθανός συνδυασμός παραμέτρων που μπορεί να προκύψουν σε ένα δίκτυο για ένα μικρό σχετικά σύνολο περιπτώσεων χρήσης. Αυτό είναι μη πρακτικό και καταστροφικό για την επέκταση των πρωτοκόλλων.

Ένα πρόβλημα αυτού του τύπου με πολλαπλές ανεξάρτητες μεταβλητές επιλύεται μέσω της συλλογής δεδομένων σε εξωτερική συσκευή και εν συνεχεία με τροφοδότηση των αποφάσεων δρομολόγησης πίσω στο σύστημα δρομολόγησης. Οι εξωτερικές συσκευές που παρέχουν τέτοιου είδους επεξεργασία συνήθως ανακαλύπτουν τις πληροφορίες τοπολογίας επερωτώντας κάθε δικτυακή συσκευή μέσω πρωτοκόλλου SNMP ή κάποιου άλλου μηχανισμού, ή συνδέονται απευθείας στο σύστημα δρομολόγησης σχηματίζοντας σχέση γειτονίας με κάθε μια από τις δικτυακές συσκευές. Για να εγχύσουν πληροφορίες διαδρομών πίσω στο σύστημα δρομολόγησης, ενσωματώνονται σε αυτό ή τις εγχέουν άμεσα στους πίνακες δρομολόγησης των συσκευών μέσω SNMP, αντιγραφής κλπ.

Όλες αυτές οι λύσεις έχουν μια σειρά από μειονεκτήματα:

- Η ανακάλυψη της τοπολογίας μέσω άμεσης αλληλεπίδρασης με το σύστημα δρομολόγησης συχνά καταλήγει σε μη πλήρη ή ελλιπώς ανεπτυγμένη όψη του δικτύου. Ο εξωτερικός ελεγκτής στην περίπτωση αυτή δεν μπορεί να αναπαραστήσει την ίδια όψη δικτύου όπως οι περιμετρικές συσκευές και ως εκ τούτου θα παραγάγει αποφάσεις δρομολόγησης που δεν είναι πάντα βέλτιστες για τις περιμετρικές συσκευές. Για παράδειγμα, το SNMP δεν μπορεί να αναφέρει πολλαπλές διαδρομές ίσου κόστους από τον πίνακα δρομολόγησης και γι αυτό ένας ελεγκτής που βασίζεται στο SNMP δεν θα ήταν ποτέ ικανός να σχηματίσει πλήρη εικόνα της τοπολογίας του δικτύου και του πίνακα δρομολόγησης κατά την διαδικασία ανάγνωσης.
- Οι μηχανισμοί που εγχέουν πληροφορίες δρομολόγησης μέσω αντιγραφής, SNMP και λοιπές ιδιωτικές τεχνολογίες δεν επιτρέπουν στην εγχυμένη διαδρομή να αλληλεπιδράσει με άλλες διαδρομές που έχουν εγκατασταθεί στον πίνακα δρομολόγησης με πιο παραδοσιακούς τρόπους. Για παράδειγμα, οι στατικές διαδρομές που προστίθενται με οποιονδήποτε τρόπο, πρέπει, από τη φύση τους να αλλάξουν την παραμετροποίηση της συσκευής, το οποίο μπορεί να είναι προβληματικό όταν οι χειριστές δικτύου προσπαθούν να καταλάβουν την λειτουργία του δικτύου ή να αποσφαλματώσουν πρόσφατα προβλήματα. Οι εγκατεστημένες διαδρομές μέσω της στατικής μεθόδου είναι δύσκολο να αναδιανεμηθούν σε άλλα πρωτόκολλα ώστε να έλξουν κίνηση σε συγκεκριμένο σημείο εξόδου και μπορεί να είναι δύσκολο να ρυθμιστεί με ακρίβεια ο τρόπος που αυτές οι εγχυμένες διαδρομές αλληλεπιδρούν με διαδρομές που μαθαίνονται μέσω άλλων διαδικασιών δρομολόγησης.
- Οι μηχανισμοί που προσπαθούν να επηρεάσουν τη δρομολόγηση της κίνησης δεδομένων μεταβάλλοντας διαδρομές στο ίδιο το σύστημα δρομολόγησης συχνά δεν καταφέρνουν σημαντικά αποτελέσματα. Η δρομολόγηση λειτουργεί οδηγώντας την κίνηση προς την συσκευή που διαφημίζει τον προορισμό και είναι δύσκολο για μια τρίτη οντότητα να μετακινήσει δεδομένα μεταξύ δυο ζεύξεων στις οποίες δεν συνδέεται.

Με το σύστημα I2RS η καλύτερη διαδρομή θα μπορούσε να υπολογιστεί χρησιμοποιώντας οποιονδήποτε αριθμό από κατά περίπτωση γραφθέντες μηχανισμούς και οι διαδρομές που προστίθενται στα σωστά σημεία στο δίκτυο ώστε να προκαλέσουν την πιο αποτελεσματική καθοδήγηση των δεδομένων στο καλύτερο σημείο εξόδου. Οι αλλαγές στο δικτυακό περιβάλλον θα μπορούσαν εύκολα να προκαλέσουν την οδήγηση της κίνησης σε εναλλακτικά σημεία εξόδου όταν οι περιστάσεις το απαιτούν.

2.12 Τελικές σκέψεις πάνω στο SDN

Είναι δύσκολο να καθοριστούν τα δίκτυα SDN γιατί δεν είναι στην πραγματικότητα μια αλλά συλλογή από τεχνολογίες που αλληλεπιδρούν με τα υπάρχοντα συστήματα πεδίων ελέγχου τα οποία και πιθανώς θα αντικαταστήσουν. Τα SDN πεδία ελέγχου μπορούν να λειτουργήσουν με κάθε τρόπο που λειτουργούν και τα κατανεμημένα πεδία ελέγχου.

Τα SDN επί της ουσίας είναι ένας διαφορετικός τρόπος αντιμετώπισης και επίλυσης του προβλήματος των πεδίων ελέγχου σε δίκτυα μεγάλης κλίμακας.

Οι αρχιτέκτονες δικτύων και οι επιχειρήσεις θα έπρεπε να ανατρέξουν στο SDN ώστε να επιλύσουν συγκεκριμένα προβλήματα με τρόπο που μειώνει το πλεονάζον κόστος εγκατάστασης και διαχείρισης ενός δικτύου. Το κόστη του υλικού (CAPEX) δεν αναμένεται να αποτελέσουν το βασικό σημείο μείωσης του κόστους σε SDN εγκαταστάσεις. Το ανθρώπινο σφάλμα θα είναι πάντα παράγοντας στον χειρισμό των δικτύων. Τα δίκτυα SDN δεν διαφέρουν στον τομέα αυτό από όλα τα άλλα επίπεδα ελέγχου.

Πάνω από όλα τα δίκτυα SDN παρουσιάζουν μοναδικές ευκαιρίες και προκλήσεις στην δικτυακή βιομηχανία και τις επιχειρήσεις που βασίζονται σε δίκτυα, οποιοδήποτε κι αν είναι το μέγεθος τους. Έχουν τη δυνατότητα να αλλάξουν δραματικά τη μηχανική των δικτύων όπως την ξέρουμε από τη πλευρά των πρωτοκόλλων, της διαχείρισης αλλά δεν θα αλλάξουν ιδιαίτερα τα αποδεδειγμένα μοντέλα, θεωρίες και σχεδιαστικά παραδείγματα (όπως ο διαχωρισμός σε τομείς αστοχίας) που επιτρέπουν τη λειτουργία των δικτύων.

3. ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΤΟΥ OPENFLOW

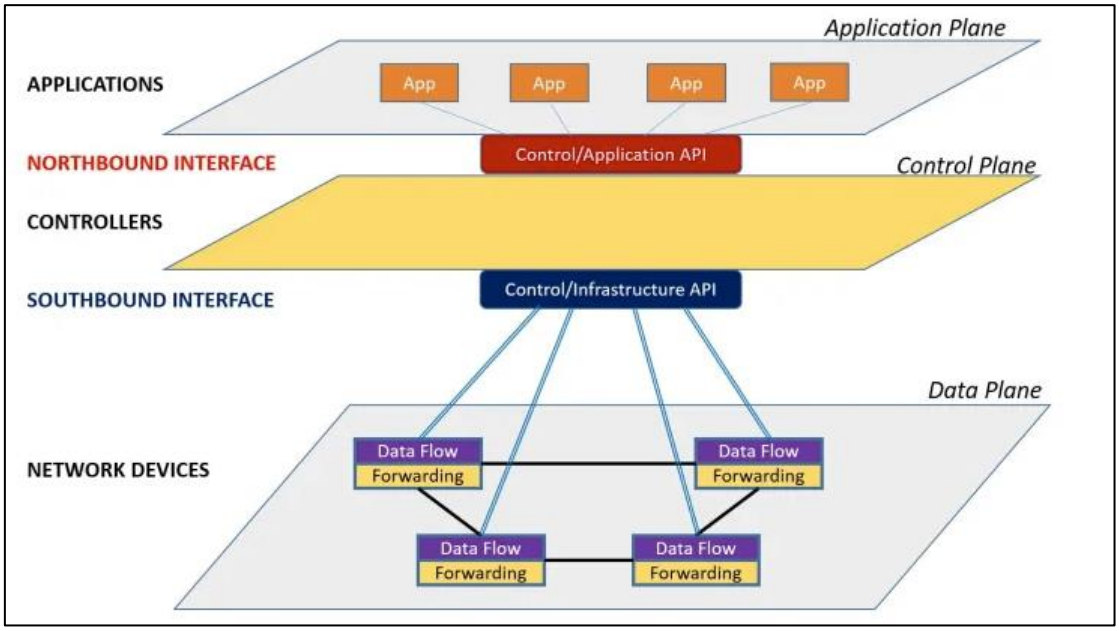
Το OpenFlow είναι ένα ανοικτό πρότυπο για πρωτόκολλο επικοινωνιών που επιτρέπει στο Πεδίο ελέγχου να αποσχιστεί από το Πεδίο Ελέγχου και συνάμα να αλληλεπιδρά με τα Πεδία Ελέγχου Πολλαπλών συσκευών από ένα κεντρικό σημείο, αποζευγνύοντας τους ρόλους για υψηλότερη αποτελεσματικότητα και προγραμματισιμότητα.

1. Το SDN δεν είναι OpenFlow
2. Το SDN είναι πολύ περισσότερο από ένας διαχωρισμός του Πεδίου Ελέγχου από το Πεδίο Δεδομένων

3.1 Η ανάγκη για αφαιρετική εικόνα των δικτύων

Οι προγραμματιστές εφαρμογών συνήθως δεν χρειάζεται να ανησυχούν για το υποκείμενο υλικό όταν γράφουν κώδικα αφού το υλικό κρύβεται από το λειτουργικό σύστημα. Πολλές φορές ακόμα και το λειτουργικό σύστημα κρύβεται από το υλικό με επόπτες και containers. Αυτό το επίπεδο αφαίρεσης είναι σχετικά καινούργιο στην βιομηχανία των δικτύων με το OpenFlow να παρέχει μια ανοικτή σε όλους διεπαφή για επίπεδα αφαίρεσης δικτύου.

Αυτή η δυνατότητα αφαίρεσης θα μπορούσε να γίνει με ένα επίπεδο ελεγκτή χάρη στο οποίο δύναται η διαχείριση πινάκων ροής και αντίστοιχων καταχωρήσεων σε δικτυακές συσκευές χωρίς να συνδέεται απευθείας σε αυτές. Ο προγραμματιστής εφαρμογών μπορεί να χρησιμοποιήσει APIs ώστε να επικοινωνήσει με τον ελεγκτή και ο ελεγκτής μπορεί αναλαμβάνει τις απαραίτητες λεπτομέρειες ώστε να ενημερώνει τους πίνακες ροών των δικτυακών συσκευών. Η ομορφιά του SDN είναι βρίσκεται στο Επίπεδο Εφαρμογής. Το OpenFlow είναι μια από τις πολλές διαθέσιμες μορφές αφαίρεσης του SDN.



Εικόνα 23: SDN-μια υψηλού επιπέδου αρχιτεκτονική δικτύων

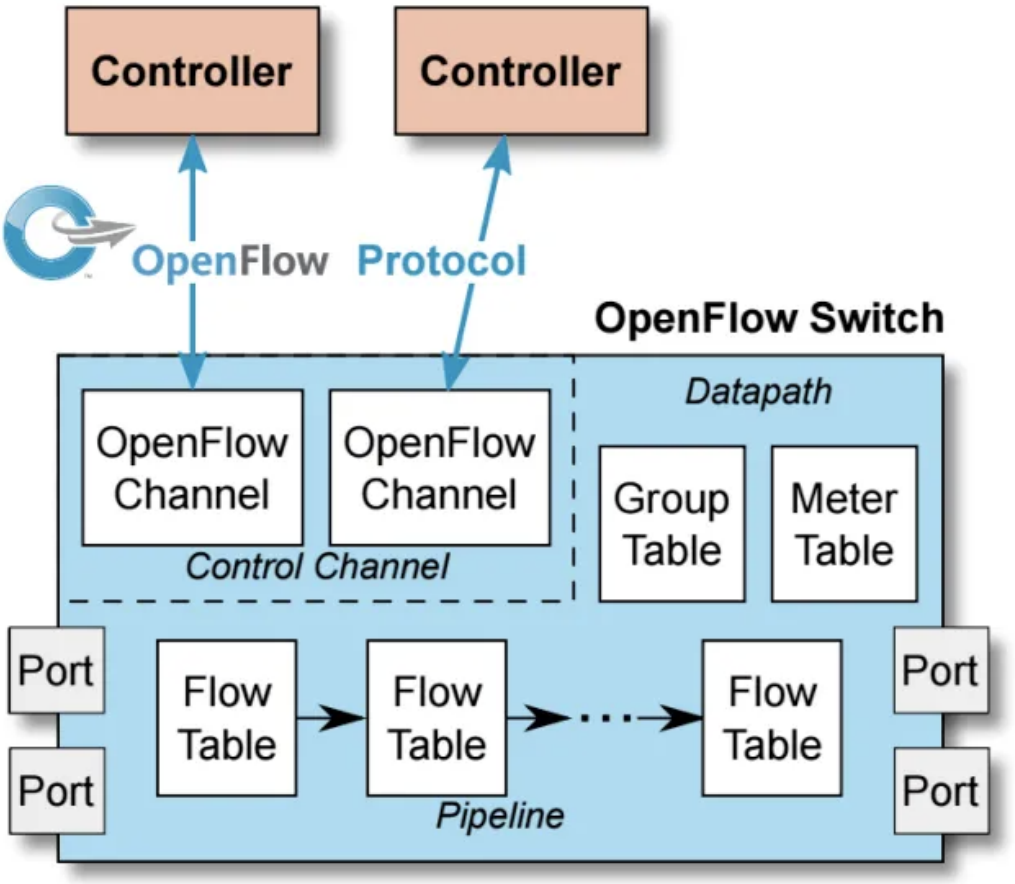
Είναι σημαντικό να σημειωθεί ότι το OpenFlow δεν ενημερώνει τις παραμέτρους των δικτυακών συσκευών αλλά τους πίνακες ροής δεδομένων. αν χρειάζεται για παράδειγμα να παραμετροποιηθεί το πρωτόκολλο NTP, δεν θα γίνει με το OpenFlow αλλά με ένα πρωτόκολλο όπως το SNMP, NETCONF, OVSDB κλπ.

3.2 Συστατικά ενός OpenFlow μεταγωγέα

«Ένας OpenFlow λογικός μεταγωγέας αποτελείται από έναν ή και περισσότερους πίνακες ροής και έναν πίνακα συνόλου, που επιτελούν αναζήτηση πακέτων και προώθηση και έναν ή και

περισσότερους ελεγκτές σε έναν εξωτερικό ελεγκτή. Ο μεταγωγέας επικοινωνεί με τον ελεγκτή και ο ελεγκτής διαχειρίζεται τον μεταγωγέα μέσω του πρωτοκόλου OpenFlow»

Όλα τα παραπάνω απεικονίζονται στην Εικόνα 24:



Εικόνα 24: Βασικά συστατικά ενός μεταγωγέα OpenFlow

3.2.1 Πίνακες ροής

Χάρη στο πρωτόκολλο OpenFlow, ο ελεγκτής μπορεί να προσθέσει, να ενημερώσει και να καταργήσει καταχωρήσεις ροής στους πίνακες ροής τόσο αντιδραστικά όσο και προληπτικά.

Οι αντιδραστικές καταχωρήσεις ροής δημιουργούνται όταν ο ελεγκτής δυναμικά μαθαίνει που βρίσκονται οι συσκευές τις τοπολογίας και πρέπει να ενημερώσει τους πίνακες ροής των συσκευών αυτών ώστε να επιτρέψει την από άκρου σε άκρο συνδεσιμότητα. Για παράδειγμα, αφού οι μεταγωγείς σε ένα καθαρά OpenFlow περιβάλλον απλά δρουν ως προωθητές της κίνησης, όλη η λογική πρέπει να υπαγορεύεται και να προγραμματίζεται από τη πλευρά του ελεγκτή. Γι αυτό αν ένα τερματικό στο μεταγωγέα Α χρειάζεται να μιλήσει στο μεταγωγέα Β, τα μηνύματα θα αποσταλλούν στον ελεγκτή ώστε να βρεί πως θα φτάσουν σε αυτό το τερματικό. Ο ελεγκτής θα μάθει τους πίνακες διευθύνσεων MAC των τερματικών από τους μεταγωγείς και πως συνδέονται, προγραμματίζοντας τη λογική στους πίνακες ροών σε κάθε μεταγωγέα. Αυτή είναι μια αντιδραστική καταχώρηση ροής.

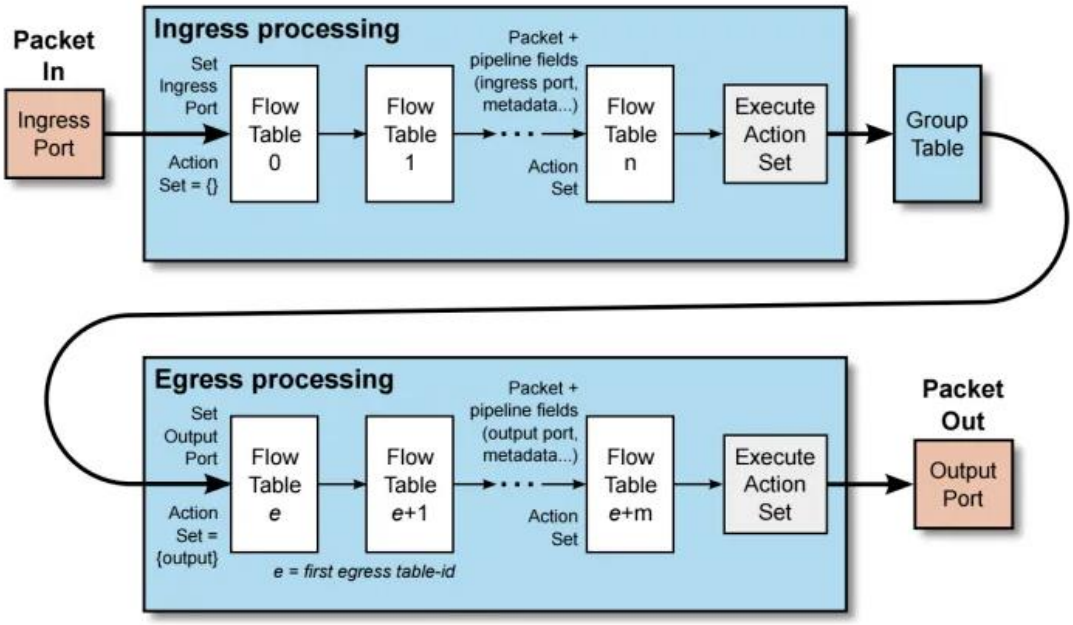
Οι προληπτικές καταχωρήσεις ροής προγραμματίζονται πριν αφιχθούν οι ροές. Είναι ήδη γνωστό αν δυο συσκευές θα πέπρεπε ή όχι να επικοινωνήσουν και ο ελεγκτής μπορεί να προγραμματίσει τις ροές αυτές στα τερματικά OpenFlow εκ των προτέρων.

3.2.2 Ταίριασμα κίνησης δεδομένων, επεξεργασία σωλήνωσης και πλοήγηση στον πίνακα ροών

Σε ένα δίκτυο OpenFlow, κάθε μεταγωγέας περιλαμβάνει τουλάχιστον έναν πίνακα ροής και ένα σύνολο από καταχωρήσεις ροής εντός του πίνακα. Αυτές οι καταχωρήσει ροής περιέχουν πεδία ταιριάσματος, μετρητές και οδηγίες που εφαρμόζονται στα πακέτα που ταιριάζονται.

Τυπικά υπάρχει πάνω από ένας πίνακας ροής και για αυτό είναι σημαντικό να σημειωθεί ότι η διαδικασία ταιριάσματος ξεκινά στον πρώτο πίνακα ροής και μπορεί να συνεχιστεί σε επιπλέον πίνακες ροής του αγωγού. Το πακέτο θα ξεκινήσει από τον πίνακα 0 και θα αντιπαραβληθεί με όλες τις καταχωρήσεις βάσει προτεραιότητας η υψηλότερη προτεραιότητα θα ελέγχεται πρώτα (π.χ 200, μετά 100 και τέλος 1). Αν η ροή πρέπει να εξεταστεί και με βάση άλλον πίνακα, η δήλωση goto λέει στο πακέτο να πάει στον πίνακα που καθορίζεται στις οδηγίες.

Η επεξεργασία σωλήνωσης λαμβάνει χώρα σε δυο φάσεις όπως φαίνεται στην Εικόνα 25, την επεξεργασία εισερχομένων και την επεξεργασία εξερχομένων.

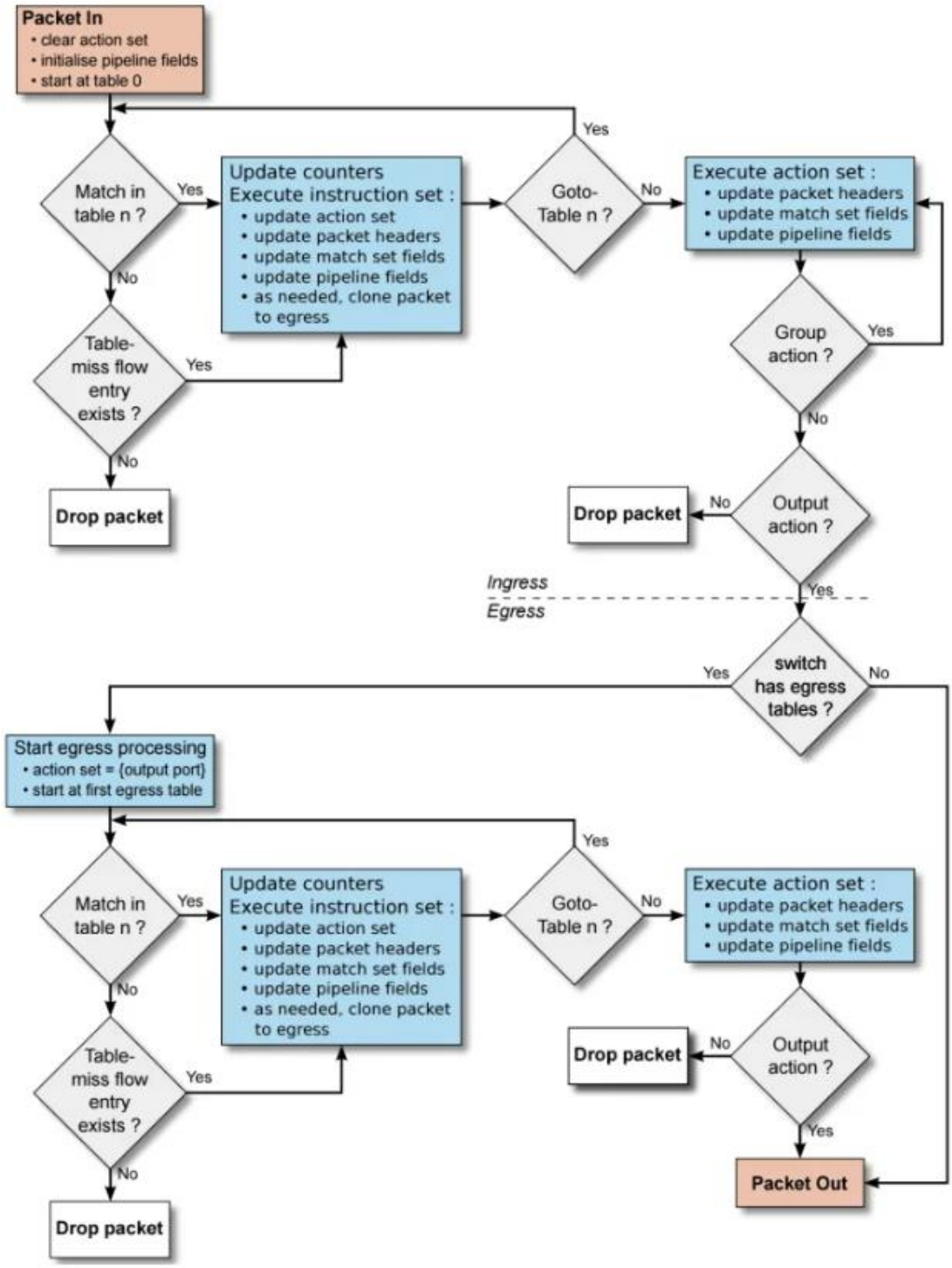


Εικόνα 25: Επεξεργασία πακέτων στη διαδικασία σωλήνωσης του SDN

Αν βρεθεί καταχώρηση που ταιριάζει στην κίνηση εκτελούνται οι εντολές της συγκεκριμένης ροής. Αν δεν υπάρξει ταίριασμα σε έναν πίνακα ροής, το απαοτέλεσμα εξαρτάται από την διαμόρφωση της καταχώρησης σε περίπτωση αστοχίας στον πίνακα.

3.2.3 Αστοχία καταχώρησης ροής

Η αστοχία καταχώρησης ροής είναι η τελευταία στον πίνακα, έχει προτεραιότητα 0 και ταιριάζει με οτιδήποτε. Είναι ένας μπαλαντέρ και οι ενέργειες που θα λάβουν χώρα εξαρτώνται από τις επιλογές του δαιχειριστή. Το πακέτο μπορεί να προωθηθεί στον ελεγκτή μέσω του καναλιού OpenFlow ή το πακέτο μπορεί να απορριφθεί ή να συνεχίσει στον επόμενο πίνακα ροής. Η διαδικασία απόρριψης παρουσιάζεται στην Εικόνα 26.



Εικόνα 26: Επεξεργασία πακέτου κατά τη SDN σωλήνωση

3.2.4 Θύρες OpenFlow

Οι θύρες OpenFlow είναι οι δικτυακές θύρες που κομίζουν τα πακέτα από την επεξεργασία του OpenFlow στο υπόλοιπο δίκτυο. Οι OpenFlow ελεγκτές συνδέονται λογικά μεταξύ τους μέσω των OpenFlow θυρών.

Υπάρχουν τρία είδη θυρών σε έναν OpenFlow μεταγωγέα: φυσικές, λογικές και κρατημένες θύρες.

- **Φυσικές θύρες**

  Οι φυσικές θύρες αντιστοιχούν στις πραγματικές θύρες του μεταγωγέα. Αυτό σημαίνει ότι υπάρχει μια-προς-μια αντιστοίχιση των φυσικών θυρών του OpenFlow στις Ethernet θύρες του υλικού. Μερικές φορές οι μεταγωγείς OpenFlow μπορούν να έχουν θύρες που είναι εικονικές και να απεικονίζουν μια εικονική αναπαράσταση φυσικής θύρας. Αυτό είναι παρόμοι με την εικονικοποίηση υλικών δικτυακών θυρών σε υπολογιστικά περιβάλλοντα.

- **Λογικές θύρες**

  Οι λογικές θύρες καθορίζονται από τον μεταγωγέα και δεν αντιχτοιχίζονται σε πραγματικές θύρες στο υλικό. Παράδειγμα αυτών είναι τα LAGs, τα tunnels και οι loopback. Οι μοναδικές διαφορές μεταξύ φυσικών θυρών και λογικών είναι ότι ένα πακέτο που σχετίζεται με λογική θύρα μπορεί να διαθέτει ένα πεδίο σωλήνωσης (Tunnel-id) και όταν τα πακέτα λαμβάνονται σε λογικές θύρες που απαιτούν επικοινωνία στον ελεγκτή, τόσο η λογική θύρα και η υποκείμενη φυσική θύρα αναφέρονται σε αυτόν.

- **Δεσμευμένες θύρες**

  Οι θύρες αυτές καθορίζουν γενικευμένες ενέργειες προώθησης όπως η αποστολή στον ελεγκτή, πλημμυρίδα, ή προώθηση χωρίς μεθόδους OpenFlow όπως Ethernet μεταγωγή.

  Υπάρχουν ποικίλα είδη απαιτούμενων δεσμευμένων θυρών όπως *ALL, CONTROLLER, TABLE, IN_PORT, ANY, UNSET, LOCAL.* Η θύρα CONTROLLER αντιπροσωπεύει το OpenFlow κανάλι που χρησιμοποιείται για επικοινωνία μεταξύ μεταγωγέα και ελεγκτή.

  Σε υβριδικά περιβάλλοντα, υπάρχουν και οι θύρες *NORMAL* και *FLOOD* που επιτρέπουν αλληλεπίδραση μεταξύ της σωλήνωσης OpenFlow και της σωλήνωσης του υλικού του μεταγωγέα.

3.3 OpenFlow μεταγωγείς vs υβριδικοί μεταγωγείς

Υπάρχουν δυό ειδών μεταγωγείς: οι αποκλειστικά OpenFlow και οι υβριδικοι OpenFlow – Ethernet

Οι μεταγωγείς OpenFlow είναι «χαζοί» μεταγωγείς που διαθέτουν μόνο πεδίο προώθησης δεδομένων και κανέναν τρόπο να λάβουν αποφάσεις προώθησης. Όλα τα πακέτα επεξεργάζονται στην σωλήνωση OpenFlow και μόνο.

Οι υβριδικοί μεταγωγείς OpenFlow-Ethernet υποστηρίζουν την λειτουργία του OpenFlow και τη μεταγωγή Ethernet. Αυτό σημαίνει ότι μπορεί να χρησιμοποιηθεί παραδοσιακή L2 Ethernet μεταγωγή, απομόνωση VLAN, L3 δρομολόγηση, ACLs και επεξεργασία QoS μέσω του εγγενούς Πεδίου ελέγχου του μεταγωγέα ενώ παράλληλα αλληλεπιδρά με τη σωλήνωση OpenFlow χρησιμοποιώντας ποικίλους μηχανισμούς κατάταξης.

Για παράδειγμα μπορεί ένας μεταγωγέας να χρησιμοποιεί τις μισές θύρες του για παραδοσιακή μεταγωγή και δρομολόγηση ενώ το άλλο μισό να είναι ρυθμισμένο για OpenFlow. Το δεύτερο μισό μάλιστα το διαχειρίζεται OpenFlow ελεγκτής και το άλλο μισό, το Πεδίο Ελέγχου του μεταγωγέα. Η διακίνηση δεδομένων μεταξύ των σωληνώσεων αυτών απαιτεί χρήση των δεσμευμένων θυρών NORMAL και FLOOD.

3.4 Μηνύματα OpenFlow

Τα OpenFlow έχει τρία είδη μηνυμάτων, το καθένα με δικά του υπο-είδη

- Ελεγκτής προς μεταγωγέα
- Ασύγχρονα
- Συμμετρικά

3.4.1 Μηνύματα ελεγκτή προς μεταγωγέα

Τα μηνύματα ελεγκτή προς τον μεταγωγέα εκκινούν στον ελεγκτή και χρησιμοποιούνται για απευθείας διαχείριση ή επίβλεψη του μεταγωγέα. Περιλαμβάνουν:

- Features (χαρακτηριστικά) – ο μεταγωγέας ζητά την ταυτότητα
- Configuration (διαμόρφωση) – θέτει και αναζητά παραμέτρους διαμόρφωσης
- Modify-State (τροποποίηση κατάστασης) – αποκαλείται και “flow-mod”, χρησιμοποιείται για να προσθέσει, διαγράψει και μεταβάλλει ροές/καταχωρήσεις συνόλων
- Read-States (ανάγνωση κατάστασης) – ζητά στατιστικά
- Packet Outs – Ο ελεγκτής στέλνει μήνυμα στον μεταγωγέα, είτε πλήρες πακέτο είτε ταυτότητα ενδιάμεσης μνήμης
- Barrier (φράγμα) – αιτήσεις ή απαντήσεις που χρησιμοποιούνται ώστε να διασφαλιστεί ότι οι αλληλεξαρτήσεις των μηνυμάτων είναι έγκυρες και λαμβάνει ειδοποίηση
- Role-request (αίτημα ρόλου) – ορίζει τον ρόλο του καναλιού OpenFlow
- Asynchronous-configuration (ασύγχρονη διαμόρφωση) - ορίζει επιπλέον φίλτρο στο ασύγχρονο μήνυμα που επιθυμεί να λάβει στο κανάλι OpenFlow

3.4.2 Ασύγχρονα μηνύματα

Τα ασύγχρονα μηνύματα εκκινούνται από το μεταγωγέα και χρησιμοποιούνται ώστε να ενημερώσουν τον ελεγκτή για δικτυακά συμβάντα και αλλαγές στην κατάσταση του μεταγωγέα. Αυτά τα μηνύματα περιλαμβάνουν:

- Packet-in – μεταφέρουν τον έλεγχο ενός πακέτου στον ελεγκτή
- Flow-Removed – ενημερώνουν τον ελεγκτή ότι η ροή έχει αφαιρεθεί
- Port Status – ειδοποιούν τον ελεγκτή ότι ο μεταγωγέας δεν δουλεύει
- Error – ειδοποιούν τον ελεγκτή για προβλήματα

3.4.3 Συμμετρικά Μηνύματα

Τα συμμετρικά μηνύματα εκκινούν είτε από το μεταγωγέα ή τον ελεγκτή και στέλνονται χωρίς αίτημα. Αυτά τα μηνύματα περιλαμβάνουν:

- Hello – εισαγωγή σε μηνύματα keep-alive που ανταλλάσσονται μεταξύ ελεγκτή και μεταγωγέα
- Echo – στέλνεται από το μεταγωγέα ή τον ελεγκτή για να επιβεβαιώσει ότι είναι ενεργή σύνδεση και να μετρήσει χρονική υστέρηση ή εύρος ζώνης
- Experimenter – τυπικός τρόπος με τον οποίο οι μεταγωγείς OpenFlow προσφέρουν επιπλέον λειτουργικότητα στον χώρο μηνυμάτων OpenFlow

3.5 Διαδικασία Έναρξης Σύνδεσης Πρωτοκόλλου OpenFlow

- Ο μεταγωγέας εκκινεί την σύνδεση με την IP του ελεγκτή στη προεπιλεγμένη θύρα (TCP 6633 πριν το OpenFlow 1.3.2, TCP θύρα 6653 για μετέπειτα εκδόσεις), ή σε θύρα καθορισμένη από τον διαχειριστή
- Ο ελεγκτής μπορεί να εκκινήσει αίτημα σύνδεσης αλλά σπανιότερα
- Εγκαθίσταται σύνδεση TCP ή TLS
- Και οι δυο συσκευές θα στείλουν OFPT_HELLO με συμπληρωμένο πεδίο έκδοσης πρωτοκόλλου
- Και οι δυο συσκευές υπολογίζουν ποια έκδοση θα χρησιμοποιήσουν
- Αν δεν επιτύχει αυτό, αποστέλλεται μήνυμα OFPT_ERROR
- Αν η κάθε μια υποστηρίζει την ίδια έκδοση , ο ελεγκτής στέλνει OFPT_FEATURES_REQUEST για να εντοπίσει την Datapath ID του μεταγωγέα, καθώς και τις ικανότητες του.

4. ΠΡΑΚΤΙΚΟ ΜΕΡΟΣ

Για την εξομοίωση ενός SDN δικτύου συμπεριλαμβανομένου ενός OpenFlow μεταγωγέα και του αντίστοιχου ελεγκτή επιλέχθηκε το λογισμικό Mininet. Ο λόγος είναι σχετικά απλός και δεν περιγράφεται στα πλεονεκτήματα χρήσης του αλλά κρίνεται σκόπιμο να αναφερθεί εξαρχής: Το Mininet δημιουργήθηκε πρωτίστως για να εξομοιώσει δίκτυα προγραμματιζόμενα με λογισμικό (SDN) και λιγότερο για να δημιουργεί παραδοσιακές δικτυακές τοπολογίες. Εξάλλου εργαλεία εξομοίωσης (emulation) και προσομοίωσης (simulation) δικτύων υπήρχαν αρκετά ήδη από το 2011 που εμφανίστηκε η πρώτη σταθερή έκδοση του Mininet. Το Mininet τέλος υλοποιεί άψογα το πρωτόκολλο OpenFlow στους μεταγωγείς και είναι απόλυτα παραμετροποιήσιμο από γραμμή εντολών, ενίοτε και με την χρήση της γλώσσας Python.

4.1 Το σενάριο

Θα δημιουργηθούν δύο εικονικές μηχανές: Η πρώτη θα φιλοξενήσει Linux όπου θα τρέχει ένας από τους πιο διαδεδομένους SDN ελεγκτές, ο OpenDaylight. Στην δεύτερη εικονική μηχανή θα τρέξει εικόνα επίσης λειτουργικού συστήματος Linux και θα φιλοξενείται το Mininet όπου έχει υλοποιηθεί μια σχετικά απλή τοπολογία τοπικού δικτύου αποτελούμενη από έναν OpenFlow μεταγωγέα και τρία τερματικά. Σκοπός είναι η επικοινωνία του ελεγκτή με τον μεταγωγέα μέσω του OpenFlow ώστε ο πρώτος να μπορέσει να διαβάσει την τοπολογία και να χειριστεί τον δεύτερο, ενώ γίνεται και σύλληψη πακέτων OpenFlow ώστε να διαβαστούν οι επικεφαλίδες τους και να αναδειχτεί η διαφορά τους με τις έως τώρα γνωστές επικεφαλίδες Επιπέδων 1 και 2.

Μια δευτερεύουσα αλλά πολύ σημαντική όψη της εργασίας αυτής αφορά την παραμετροποίηση αλλά και την ταυτόχρονη εκτέλεση δυο εικονικών μηχανών οι οποίες μάλιστα τρέχουν 64 bit λειτουργικό Linux Server v16.04.6. Η επικοινωνία τους επιτυγχάνεται χάρη στο εικονικό δίκτυο που δημιουργεί το λογισμικό-επόπτης VirtualBox της εταιρείας Oracle. Το εικονικό δίκτυο μεταξύ των δυο εικόνων του Linux είναι ένα τυπικό /24 δίκτυο το οποίο στις περισσότερες περιπτώσεις είναι το 192.168.56.0. Χάρη στον εικονικό προσαρμογέα που εγκαθίσταται στο υπολογιστικό σύστημα –οικοδεσπότη, καταχωρείται στον πίνακα δρομολόγησης του διαδρομή στο 192.168.56.0 δίκτυο και μπορεί ο διαχειριστής να επικοινωνήσει με τις εικονικές μηχανές με πρόγραμμα εξομοίωσης τερματικού όπως το putty και πρωτόκολλο SSH.

Ο μεταγωγέας επικοινωνεί με τον ελεγκτή OpenDaylight στη θύρα 6633 ενώ είναι δυνατή και η χρήση συνηθισμένων δικτυακών εργαλείων όπως η ping του πρωτοκόλλου ICMP ώστε να διαπιστωθεί μια καταρχήν ελάχιστη επικοινωνία. Το Mininet εξοπλίζεται με επιπλέον εργαλεία που βρίσκονται στο GitHub όπως είναι ο Wireshark OpenFlow Dissector και ο ελεγκτής με εργαλεία γραφικής αναπαράστασης της τοπολογίας, RestFul API για επικοινωνία μέσω του Northbound interface και όχι μόνο του Southbound, Yang UI (User Interface) που βασίζεται στη γλώσσα μοντελοποίησης Yang ώστε να δώσει δυνατότητα λεπτομερέστατης διαχείρισης του ελεγκτή κ.α

4.2 Το εργαλείο εξομοίωσης Mininet

Το Mininet είναι ένας *εξομοιωτής* δικτύων, ή για περισσότερη ακρίβεια ένα σύστημα ενορχήστρωσης δικτυακής εξομοίωσης. Τρέχει ως μια συλλογή από τερματικές συσκευές, μεταγωγείς, δρομολογητές και ζεύξεις σε έναν πυρήνα Linux. Χρησιμοποιεί ελαφριά εικονικοποίηση ώστε να εμφανίσει ένα σύστημα ως ένα πλήρες δίκτυο που τρέχει τον ίδιο πυρήνα, σύστημα και κώδικα χρήστη. Ένα τερματικό Mininet συμπεριφέρεται ακριβώς όπως ένας πραγματικός υπολογιστής. Ο χρήστης μπορεί να συνδεθεί σε αυτό με ssh και να τρέξει σε αυτό προγράμματα –ειδικότερα όσα συνοδεύουν το Linux υποσύστημα. Τα προγράμματα μπορούν να στείλουν πακέτα μέσα από μια εξομοιωμένη θύρα Ethernet με συγκεκριμένο ρυθμό μετάδοσης και την αντίστοιχη χρονοκαθυστέρηση. Τα πακέτα υφίστανται επεξεργασία σε σχεδόν πραγματικούς Ethernet μεταγωγείς, δρομολογητές και ενδιάμεσες συσκευές με δεδομένη ουρά αναμονής. Όταν δυο προγράμματα όπως ένα ζεύγος πελάτη και διακομιστή επικοινωνούν μέσω του Mininet, οι μετρούμενες επιδόσεις ταιριάζουν στην πιο αργή από τις δυο μηχανές όπως και στον πραγματικό κόσμο.

Με λίγα λόγια, τα εικονικά τερματικά, μεταγωγείς, σύνδεσμοι και ελεγκτές είναι πραγματικά. Απλά δημιουργούνται με λογισμικό αντί υλικού και η συμπεριφορά τους είναι παρόμοια με αυτή διακριτών στοιχείων υλικού. Συνήθως είναι δυνατόν να δημιουργηθεί δίκτυο στο Mininet που να μοιάζει με δίκτυο υλικού ή και το αντίστροφο και να τρέξει κώδικας και εφαρμογές σε κάθε μια από τις διαφορετικές πλατφόρμες.

4.2.1 Τα πλεονεκτήματα του Mininet:

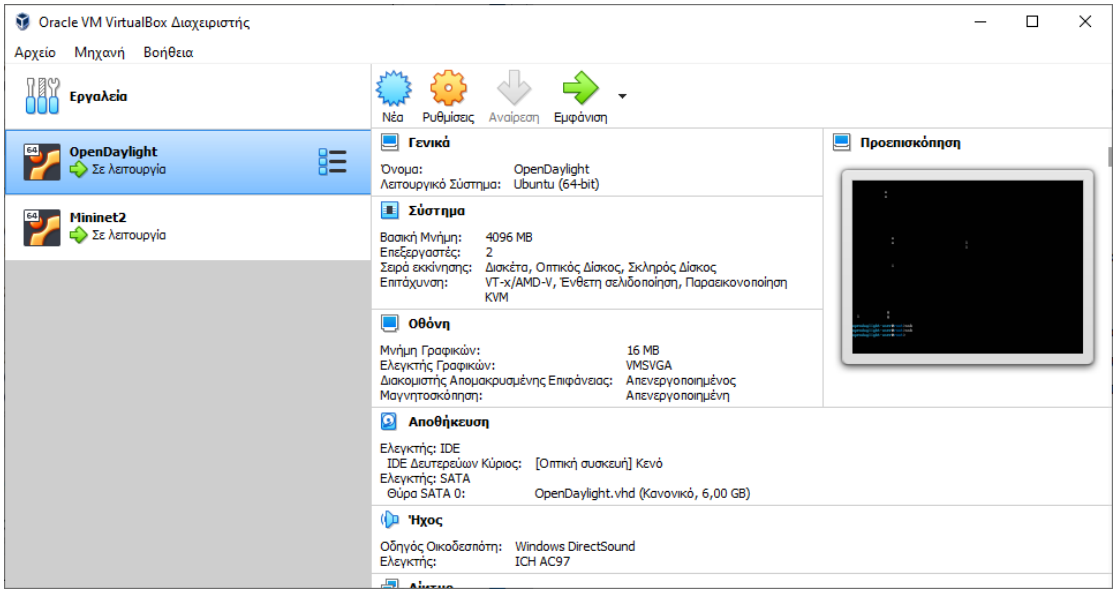
1. Είναι γρήγορο και γι αυτό η δημιουργία ενός απλού δικτύου χρειάζεται δευτερόλεπτα. Άρα ένας ερευνητής μπορεί να εκτελέσει τον βρόχο εκτέλεσης-αναδιαμόρφωσης πολύ γρήγορα.
2. Επιτρέπει την δημιουργία πολλών διαφορετικών τοπολογιών από έναν απλό μεταγωγέα με τερματικό έως διαδικτυακές σχεδόν όπως το δίκτυο τουStanford, το δίκτυο ενός υπολογιστικού κέντρου κ.α.
3. Μπορεί να τροποποιήσει τη μέθοδο προώθησης πακέτων: Οι μεταγωγείς του Mininet είναι προγραμματιζόμενοι μέσω του πρωτοκόλλου OpenFlow. Τα σχέδια δικτύων SDN που τρέχουν στο Mininet μπορούν εύκολα να μεταφερθούν στο υλικό με χρήση OpenFlow συμβατών μεταγωγέων και να επιτευχθούν ρυθμοί μετάδοσης πλησίον των θεωρητικών.
4. Στο Mininet μπορούν να εκτελεστούν πραγματικά προγράμματα, από οτιδήποτε τρέχει σε Linux έως και διακομιστές Διαδικτύου, το Wireshark και προγράμματα παρακολούθησης του πρωτοκόλλου TCP.
5. Μπορεί να εκτελεστεί σε φορητό υπολογιστή, σε διακομιστή, σε εικονική μηχανή, σε μηχανή με ενσωματωμένο Linux, ακόμα και στο Νέφος.
6. Δίνει την δυνατότητα διαμοίρασης και αναπαραγωγής των αποτελεσμάτων των εξομοιώσεων. Ο οποιοσδήποτε μπορεί να εκτελέσει τον κώδικα άλλων χρηστών.
7. Είναι εύκολο στη χρήση: Τα πειράματα στο Mininet χρειάζονται μια απλή ή περίπλοκη περιγραφή σε γλώσσα Python.
8. Το Mininet είναι έργο ανοικτού κώδικα που μπορεί να βρει ο οποιοσδήποτε στο https://github.com/mininet ώστε να τον τροποποιήσει, να διορθώσει προβλήματα, να καταχωρήσει προβλήματα και τις διορθώσεις σε αυτά καθώς και να αιτηθεί νέες δυνατότητες ή να τις ανεβάσει ο ίδιος.
9. Το Mininet είναι έργο σε συνεχή ανάπτυξη με την υποστήριξη μιας ιδιαιτέρως δραστήριας κοινότητας η οποία ενεργά στηρίζει τους χρήστες.

4.2.2 Μειονεκτήματα του Mininet

1. Εξαρτάται από την επεξεργαστική ισχύ του μηχανήματος –οικοδεσπότη. Αν για παράδειγμα η Κεντρική Μονάδα Επεξεργασίας μπορεί στο σύνολο να αποδώσει 10Gbps εξομοιωμένου ρυθμού μετάδοσης, αυτός θα πρέπει να μοιραστεί στις δικτυακές συσκευές. Συνεπώς το πλήθος των συσκευών τις τοπολογίας και το συνολικό μέγεθος αυτής περιορίζεται από την ισχύ του επεξεργαστή.
2. Το Mininet χρησιμοποιεί έναν πυρήνα Linux για όλα τα εικονικά τερματικά οπότε δεν δύναται να τρέξει λογισμικό Windows, BSD Unix ή άλλων λειτουργικών συστημάτων. Αυτό είναι ίσως και το μεγαλύτερο μειονέκτημα αφού η εξομοίωση IoT συσκευών είναι σήμερα εξαιρετικά σημαντική. Είναι δυνατό άλλες συσκευές να εξομοιωθούν σε εικονικές μηχανές που συνδέονται με το Mininet. Προφανώς μια τέτοια λύση για μερικές δεκάδες άλλα λειτουργικά συστήματα με το καθένα σε δική του εικονική μηχανή απαιτεί υπερυπολογιστή.
3. Το Mininet δεν τρέχει άλλους OpenFlow ελεγκτές και για αυτό οι χρήστες πρέπει να γράψουν τον δικό τους. Στην εργασία αυτή το πρόβλημα λύθηκε με χρήση άλλης εικονικής μηχανής που φιλοξενούσε τον OpenDaylight Beryllium.
4. Το δίκτυο του Mininet δεν επικοινωνεί με το τοπικό δίκτυο ή το Διαδίκτυο εκτός αν χρησιμοποιηθεί NAT (Network Address Tranaslation). Μπορεί να προσκολληθεί πραγματικό ή εικονικοποιημένο δικτυακό υλικό στο δίκτυο του Mininet.
5. Όλα τα Mininet τερματικά μοιράζονται το ίδιο σύστημα αρχείων και τους ίδιους αριθμούς διεργασιών (PID) με το σύστημα οικοδεσπότη. Γι αυτό χρειάζεται προσοχή όταν εκτελούνται daemons που απαιτούν παραμετροποίηση στον φάκελο /etc καθώς και να μην τερματίζονται οι λάθος διεργασίες (που ο χρήστης θεωρεί ότι ανήκουν σε κόμβο Mininet αλλά στην πραγματικότητα ανήκουν στο μηχάνημα –οικοδεσπότη)
6. Σε αντίθεση με άλλους εξομοιωτές, στο Mininet δεν υφίσταται εικονικός χρόνος. Άρα όλες οι μετρήσεις χρονισμών βασίζονται σε πραγματικό χρόνο και δεν μπορούν να εξομοιωθούν σενάρια πολύ υψηλών ρυθμών μεταγωγής όπως για παράδειγμα σε δίκτυο των 100Gbps.

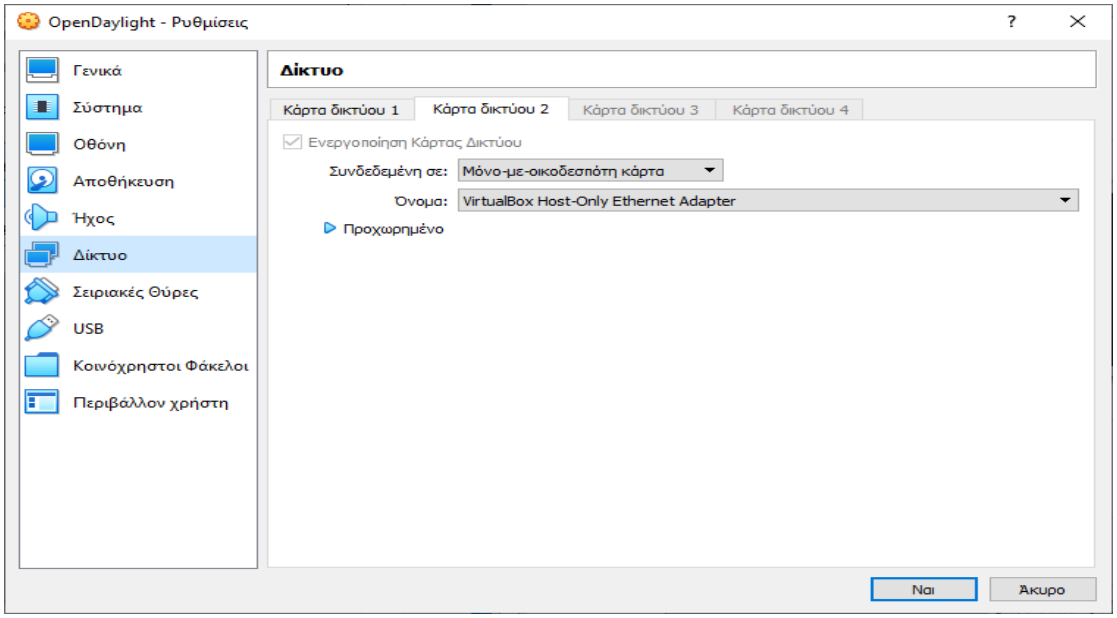
4.3 Βήμα 1ο: Εγκατάσταση Ελεγκτή OpenDaylight σε Εικονική Μηχανή Linux Server

Πρώτα θα γίνει εγκατάσταση του Linux Server v16.04.6 (64-bit) σε εικονική μηχανή του VirtualBox. Για το σκοπό αυτό πέρα από μια .iso εικόνα του λειτουργικού συστήματος ορίζεται στο VirtualBox περιβάλλον με 2 K.M.E, 2GB από κύρια μνήμη και 6GB εικονικός δίσκος (.vhd) ως κύριο μέσο αποθήκευσης και εγκατάστασης του λειτουργικού. Οι επιλογές φαίνονται και στην Εικόνα 27:



Εικόνα 27: Οι ρυθμίσεις για το VM του Ubuntu Server

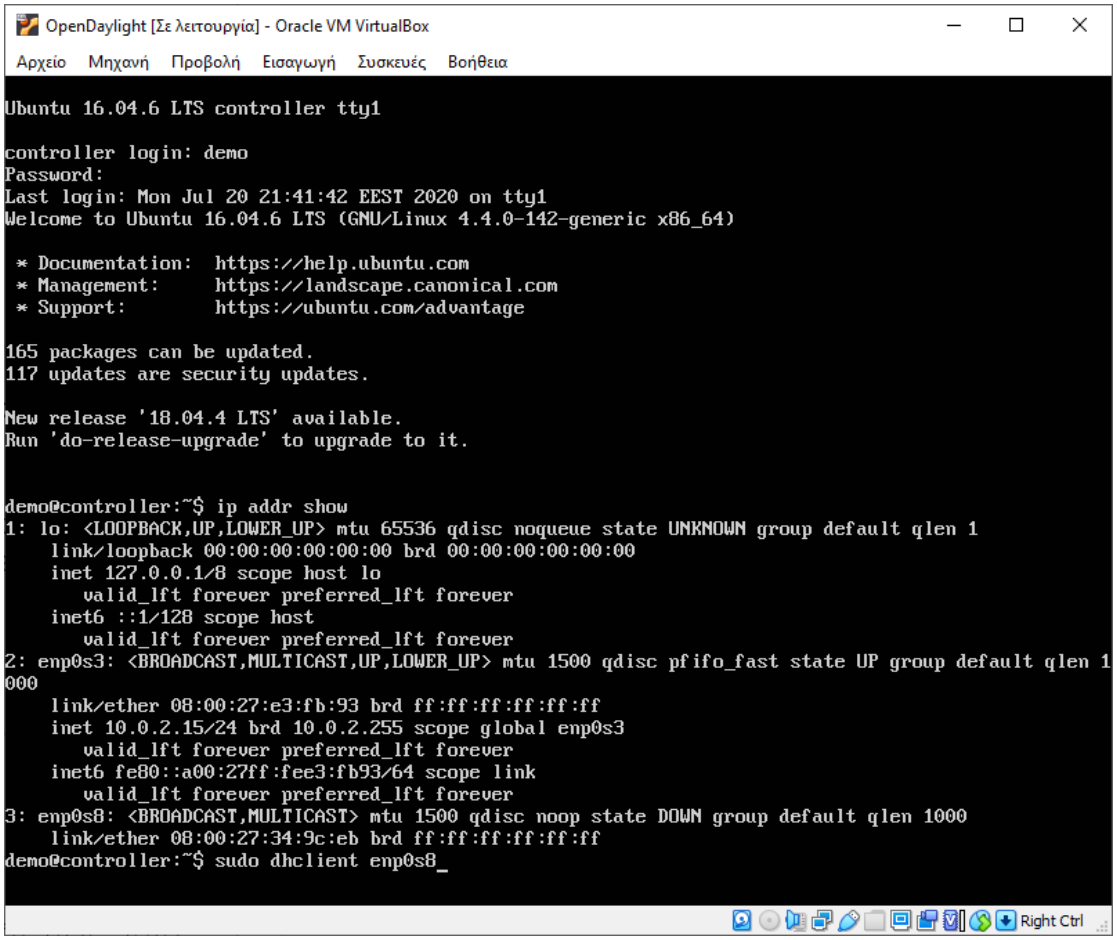
Στις δικτυακές ρυθμίσεις της εικονικής μηχανής υπάρχει μια ενεργή κάρτα δικτύου που επικοινωνεί μέσω NAT οπότε για το εικονικό περιβάλλον επικοινωνίας με την δεύτερη εικονική μηχανή πρέπει να ενεργοποιηθεί και δεύτερη κάρτα δικτύου ως host-only δίκτυο (Εικόνα 28) η οποία αφού εγκατασταθεί και εκκινήσει το Linux, θα παραμετροποιηθεί μέσω DHCP όπου διακομιστής IP είναι το VirtualBox.



Εικόνα 28: Ενεργοποίηση και δεύτερης κάρτας δικτύου στο Host-Only δίκτυο

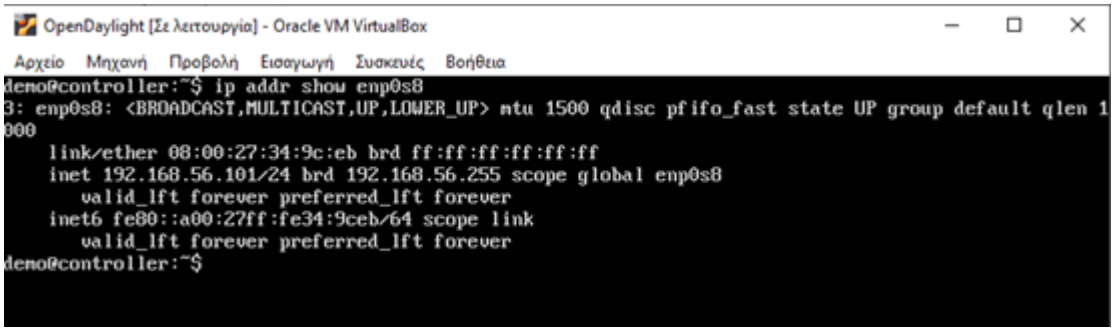
Κατόπιν της διαδικασίας εγκατάστασης του Linux δίνονται οι εντολές:

ip addr show ώστε να βρεθούν οι κάρτες δικτύου με την ονομασία τους από το λειτουργικό (Εικόνα 29)
και αφού βρεθεί ότι η δεύτερη κάρτα δικτύου ονόματι enp0s8 δεν έχει λάβει IP,
sudo dhclient enp0s8 για να αποδοθεί IP από τον DHCP διακομιστή του VirtualBox



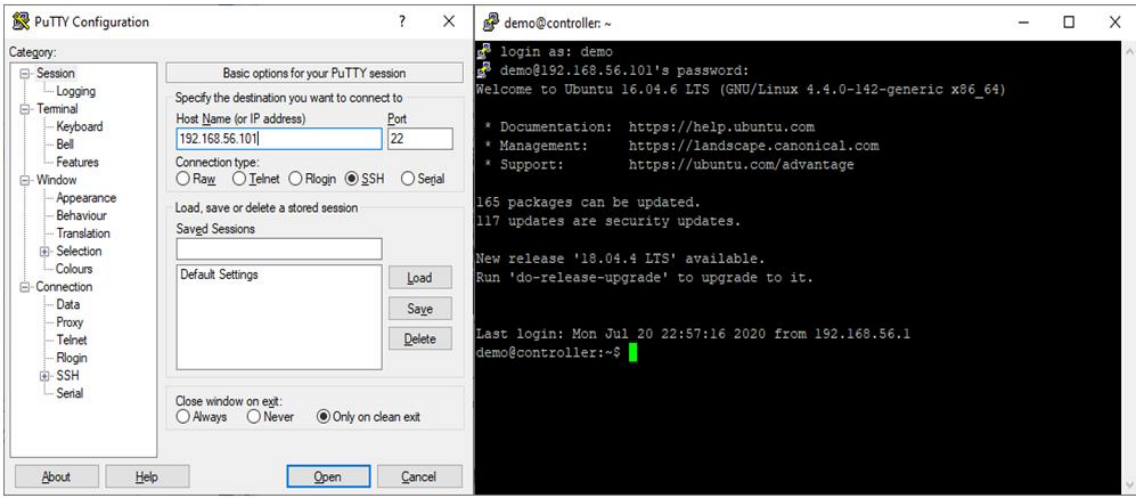
Εικόνα 29: Το αποτέλεσμα της ip addr show

Η IP που λαμβάνει η κάρτα δικτύου κατόπιν εντολής *ip addr show* είναι η 192.168.56.101 (Εικόνα 30)



Εικόνα 30: Η ip που έχει εφεξής ο Controller

Η επικοινωνία του μηχανήματος οικοδεσπότη και της εικονικής μηχανής που θα φιλοξενήσει το OpenDaylight διαπιστώνεται με ping στο 192.168.56.101 και εν τέλει με SSH από PuTTY όπου θα ζητηθεί το όνομα και ο κωδικός που ορίστηκαν κατά την εγκατάσταση. (Εικόνα 31)



Εικόνα 31: Επικοινωνία με PuTTY και SSH με τον διακομιστή

Ακολουθεί η εγκατάσταση Java αφού είναι το προγραμματιστικό περιβάλλον στο οποίο δημιουργήθηκε ο ελεγκτής OpenDaylight και είναι απαραίτητο για τη λειτουργία του.

Δίνονται οι εντολές:

sudo apt-get update

sudo apt-get install default-jre-headless

Για να οριστεί η JAVA_HOME ως **καθολική** μεταβλητή περιβάλλοντος πρέπει να υποστεί επεξεργασία το αρχείο bashrc:

nano ~/ .bashrc

export JAVA_HOME=/usr/lib/jvm/default-java

Το αρχείο πρέπει να ξαναεκτελεστεί για να ενεργοποιηθούν οι αλλαγές:

source ~/.bashrc

Ολοκληρώνοντας με την εικονική μηχανή του ελεγκτή, για την εγκατάσταση του OpenDaylight, πρώτα πρέπει να καταφορτωθούν τα αρχεία εγκατάστασης:

wget https://nexus.opendaylight.org/content/groups/public/org/opendaylight/integration/distribution-karaf/0.4.0-Beryllium/distribution-karaf-0.4.0-Beryllium.tar.gz

Όλες οι εκδόσεις του OpenDaylight περιέχονται μαζί με τα χαρακτηριστικά τους σε container Karaf[1]. Το ίδιο συμβαίνει και με τον ONOS, το δεύτερο σε χρήση ελεγκτή SDN.

Η αποσυμπίεση θα λάβει χώρα στον φάκελο *distribution-karaf-0.4.0-Beryllium.tar.gz* με την εντολή:

tar -xvf distribution-karaf-0.4.0-Beryllium.tar.gz

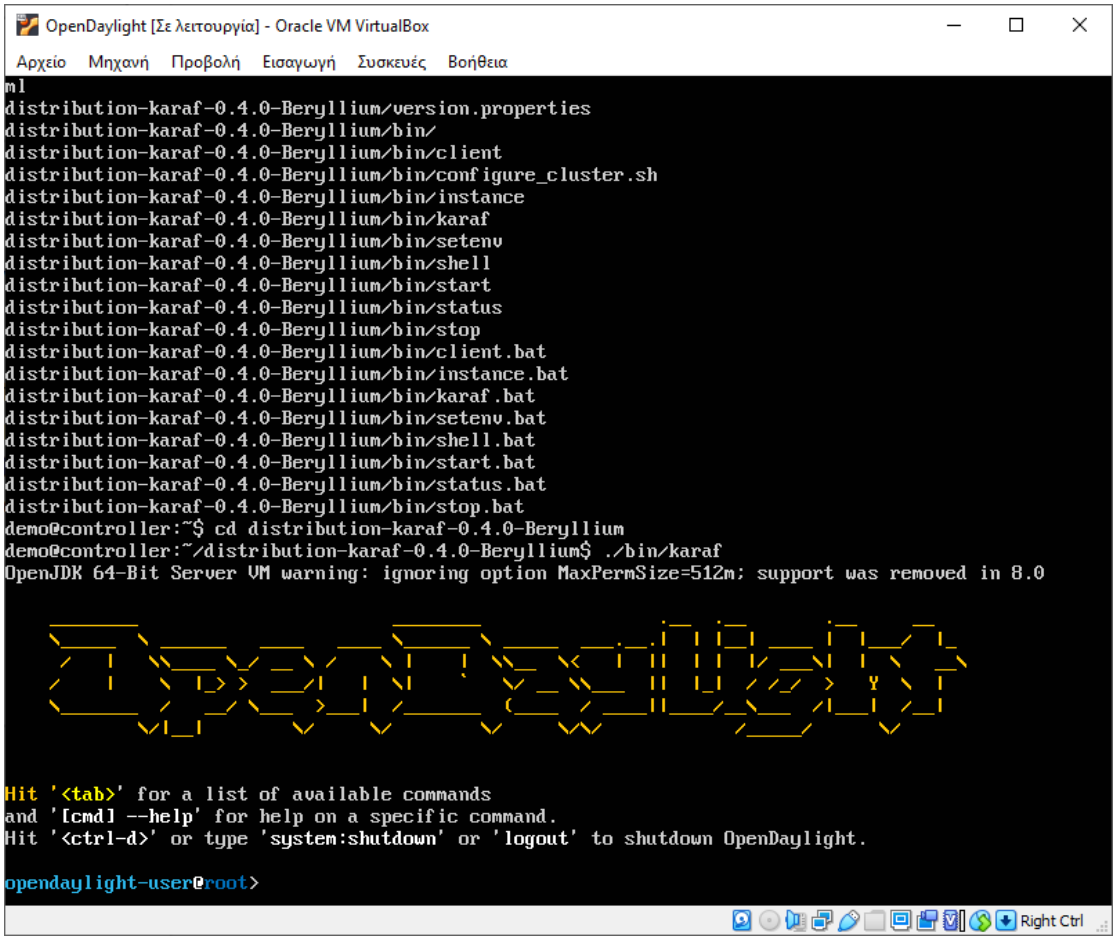
εν συνεχεία, κατόπιν περιήγησης στον φάκελο εγκατάστασης, θα κληθεί η container να εγκαταστήσει τα απαραίτητα αρχεία:

cd distribution-karaf-0.4.0-Beryllium

./bin/karaf

Ο karaf container θα εγκαταστήσει όλα τα απαραίτητα αρχεία και θα ξεκινήσει τον ελεγκτή OpenDaylight:

[1] Το συγκεκριμένο λογισμικό είναι ανοικτού κώδικα και με μακρινές καταβολές στον Apache



Εικόνα 32 Λειτουργία OpenDaylight χωρίς GUI

Το όνομα χρήστη έχει αλλάξει σε *opendaylight-user* και απουσιάζει γραφικό περιβάλλον όπως φαίνεται στην Εικόνα 32. Με την εγκατάσταση των επιπλέων χαρακτηριστικών θα λυθεί το πρόβλημα αυτό και θα αποκτήσει μεγαλύτερη λειτουργικότητα ο ελεγκτής.

feature:install odl-restconf odl-l2switch-switch odl-mdsal-apidocs odl-dlux-all

Τα χαρακτηριστικά που εγκαθίστανται θα ξεκινούν εφεξής με τον ελεγκτή και παραμένουν μόνιμα ενσωματωμένα σε αυτόν.

Όλα τα πιθανά χαρακτηριστικά που περιλαμβάνει ο karaf container δίνονται από την εντολή:

opendaylight-user@root> feature:list

Για να διαπιστωθεί ποια επιπλέον χαρακτηριστικά είναι εγκατεστημένα και ενεργά δίνεται η εντολή:

feature:list –installed

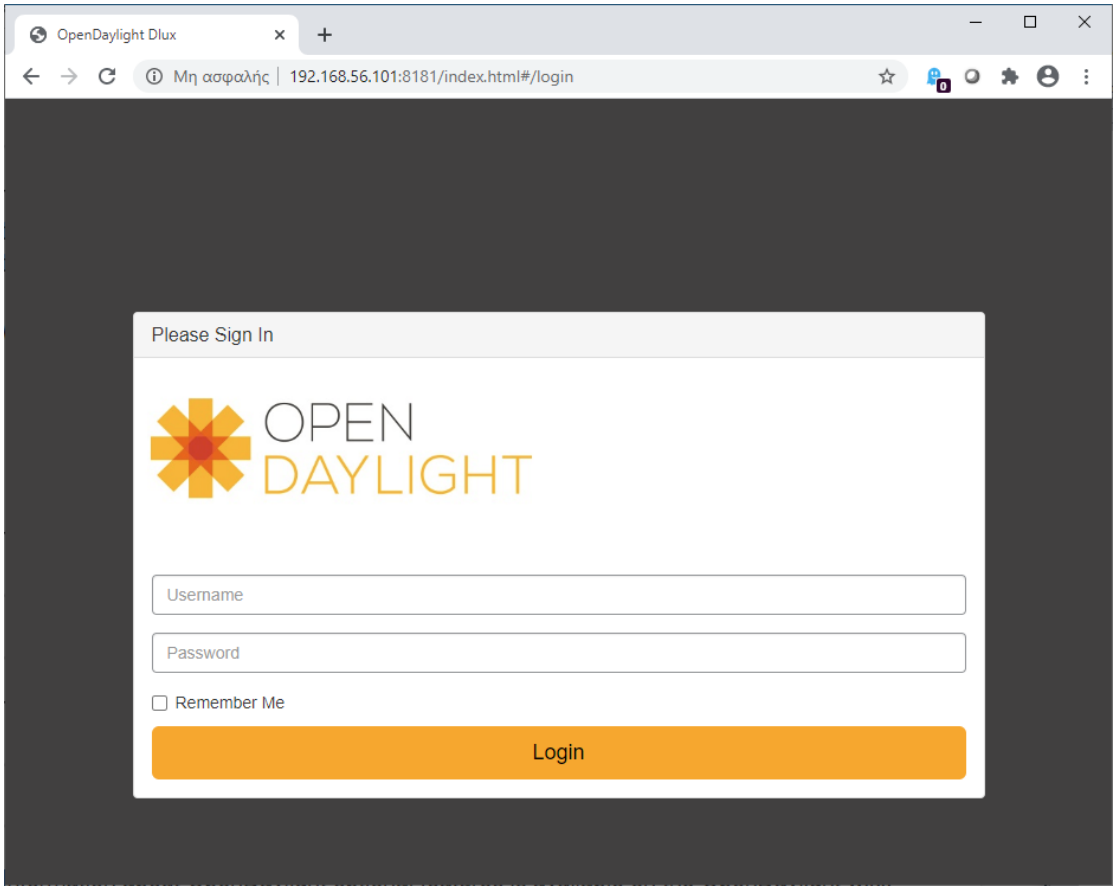
Τα χαρακτηριστικά που εγκαταστάθηκαν και η ωφελιμότητα τους αναλύονται συνοπτικά:

- **odl-restconf:** ενεργοποιεί το RESTCONF API. Σύμφωνα με το RFC 8040 (RESTCONF Protocol), η IETF περιγράφει το RESTCONF ως *«ένα πρωτόκολλο βασιζόμενο στο HTTP που παρέχει προγραμματιστική διεπαφή για την πρόσβαση σε δεδομένα που περιγράφονται σε YANG και χρησιμοποιεί τις έννοιες αποθήκευσης δεδομένων που καθορίζονται από το Network Configuration Protocol (NETCONF)»* Το RESTCONF δίνει τη δυνατότητα στον χειριστή να θέσει αιτήματα (query) και να επιτελέσει λειτουργίες στην κατάσταση διαμόρφωσης (configuration state) ή στην λειτουργική κατάσταση (operation state) μιας μηχανής ή προγράμματος χωρίζοντας την αποθήκη δεδομένων σε config και operational. Και οι δυο είναι προσβάσιμες από τα URI τους:

/restconf/config
/restconf/operational
Συγκρίνοντας με το NETCONF, η στοίβα πρωτοκόλλων του RESTCONF είναι μακράν απλούστερη. Αναλύοντας τα επίπεδα:

- Content (Περιεχόμενο) –Σε αντίθεση με το NETCONF που χρησιμοποιεί κυρίως XML, το RESTCONF επιτρέπει τη χρήση JSON (Javascript Object Notation) ή XML.
- Operations (Λειτουργίες) –Κάθε μια από τις λειτουργίες συμμορφώνεται με τι διάφορες μεθόδους HTTP παρέχοντας την απαιτούμενη συλλογή από CRUD (Create, Replace, Update and Delete) *λειτουργίες*.
- Transport (Μεταφορά) –Το πρωτόκολλο μεταφοράς είναι το HTTP, επιτρέποντας στους χρήστες το HTTPS το οποίο προσφέρει τα πλεονεκτήματα ασφάλειας του TLS.

- **odl-dlux-all:** Ενεργοποιεί το γραφικό περιβάλλον χρήστη. Μέσω ενός φυλλομετρητή η πρόσβαση γίνεται από την σελίδα: http://192.168.56.101:8181



Εικόνα 33: Το Web Interface του ODL

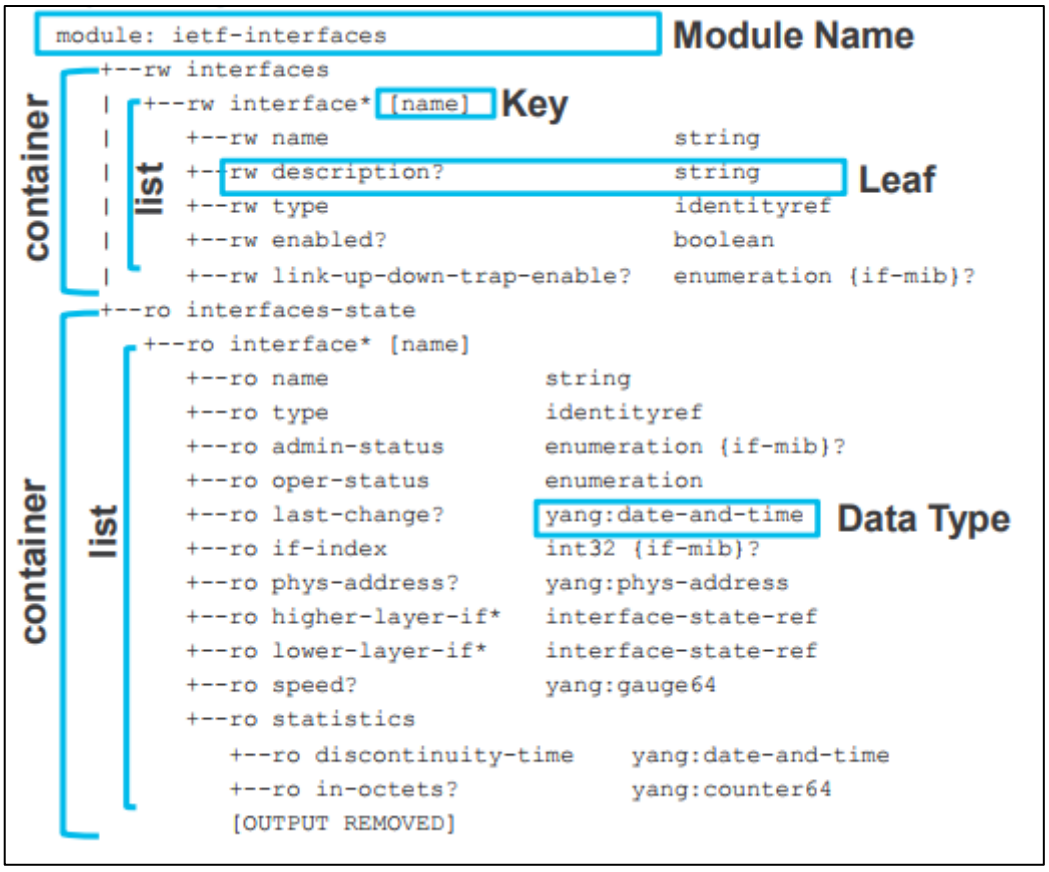
- αν και το πρωτόκολλο διαχείρισης δεν είναι ασφαλές, τουλάχιστον έχει επιλεχθεί άλλη πόρτα (TCP 8181) από την συνήθη 8080
- **odl-l2switch-switch:** Παρέχει δικτυακές λειτουργίες παρόμοιες με έναν Ethernet μεταγωγέα
- **odl-mdsal-apidocs:** Επιτρέπει την πρόσβαση στο YANG API
  Η YANG (Yet Another Next Generation) , είναι γλώσσα μοντελοποίησης δεδομένων που παρέχει έναν τυποποιημένο τρόπο μοντελοποίησης των λειτουργικών δεδομένων και των παραμέτρων διαμόρφωσης μιας δικτυακής συσκευής. Η YANG ως γλώσσα

είναι ανεξάρτητη από το πρωτόκολλο και μπορεί να μετατραπεί σε οποιαδήποτε άλλη γλώσσα περιγραφής δεδομένων όπως XML ή JSON.

- OPEN/NATIVE ΜΟΝΤΕΛΑ
  Τα μοντέλα δεδομένων κατηγοριοποιούνται σε OPEN και NATIVE ανάλογα με τις ομάδες που εργάζονται πάνω σε αυτά.
  - **Μοντέλα OPEN** –Σχεδιάστηκαν ώστε να είναι ανεξάρτητα της υποκείμενης πλατφόρμας και να κανονικοποιούν τις διαφορετικές ανά κατασκευαστή διαμορφώσεις των συσκευών. Τα OPEN YANG μοντέλα αναπτύσσονται από σώματα κατασκευαστών δικτυακού εξοπλισμού και Ομάδων Προτυποποίησης όπως οι IETF, ITU, OpenConfig κ.α.
  - **Μοντέλα Native** –Αναπτύχθηκαν από τους κατασκευαστές δικτυακού εξοπλισμού. Σχεδιάστηκαν ώστε να ενσωματώνουν χαρακτηριστικά και παραμέτρους που σχετίζονται με την εκάστοτε πλατφόρμα.

Συστατικά Μοντέλου YANG

Ένα μοντέλο YANG απαρτίζεται από αρκετά συστατικά όπως φαίνεται στην εικόνα:



Εικόνα 34 Ανάλυση μοντέλου YANG

- **Container** –Πρόκειται για συλλογή λογικά ομαδοποιημένων πληροφοριών. Συνήθως υπάρχει ένα container για διαμόρφωση και ένα για την λειτουργική κατάσταση.
- **List** –Ένα container περιλαμβάνει μια ή περισσότερες λίστες όπως π.χ. μια λίστα από τις θύρες.
- **Key** –Σε κάθε αντικείμενο της λίστας γίνεται αναφορά μέσω ενός κλειδιού

- **Leaf** –Κάθε λίστα περιέχει leafs (φύλλα) τα οποία περιέχουν την πληροφορία
- **Data Type** –Κάθε φύλλο ανήκει σε συγκεκριμένο τύπο δεδομένων

Βήμα 2ο Εικονική Μηχανή Mininet

Η επίσημη ιστοσελίδα του Mininet διαθέτει έτοιμες εικόνες λειτουργικού συστήματος Linux με προεγκατεστημένο και ήδη διαμορφωμένο το Mininet. Επειδή όμως οι εκδόσεις του Linux που έχουν χρησιμοποιηθεί είναι αρκετά και κάποιες από τις εφαρμογές εμφανίζουν ασυμβατότητες, προτιμήθηκε η εγκατάσταση του Mininet σε καθαρή εγκατάσταση Linux Server v 16.04.6 (64 bit) όπως ακριβώς και με την εικονική μηχανή του ελεγκτή. Και σε αυτήν την εικονική μηχανή πρέπει να ενεργοποιηθεί δεύτερη κάρτα δικτύου της οποίας αφού βρεθεί η ονομασία (enp0s8), διαμορφώνεται ώστε να λάβει IP διεύθυνση επίσης μέσω DHCP -τελικά λαμβάνει την 192.168.56.103

Πρώτα από όλα πρέπει να καταφορτωθεί ο πηγαίος κώδικας από το github:

git clone git://github.com/mininet/mininet

Αφού ολοκληρωθεί η λήψη των αρχείων στον φάκελο mininet, πρέπει να επιλεχθεί η κατάλληλη έκδοση:

cd mininet

git tag #εμφανίζει όλες τις διαθέσιμες εκδόσεις

git checkout –b 2.2.2 2.2.2 #προτιμήθηκε από την 2.2.1 και από την νεώτερη 2.3.2

cd ..

Αφού έχει δημιουργηθεί το δέντρο με τα πηγαία αρχεία δίνεται:

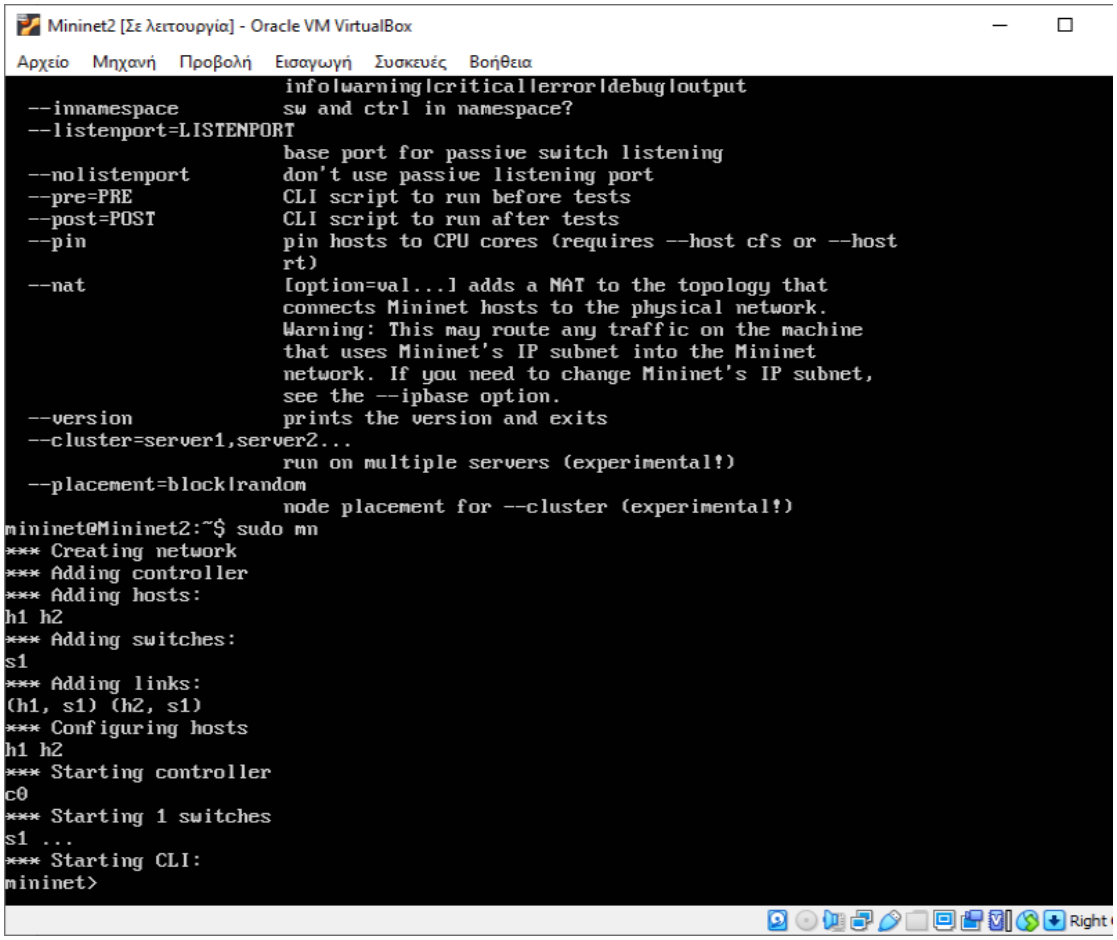
mininet/util/install.sh –a

Με την επιλογή *–a* εγκαθίστανται όλα τα στοιχεία της εικονικής μηχανής του Mininet. Μεταξύ αυτών είναι το Open vSwitch, το OpenFlow Wireshark Dissector και ο γραμμένος σε Python ελεγκτής SDN, POX. Κατά κανόνα αυτά τα εργαλεία εγκαθίστανται σε ξεχωριστούς φακέλους υπό τον κεντρικό φάκελο εγκατάστασης του Mininet.

Εφόσον δεν υπάρξει πρόβλημα κατά την εγκατάσταση του Mininet ή κάποιων από τα πρόσθετα του, εκτελείται το Mininet:

sudo mn

Το Mininet εξαρχής δημιουργεί ένα απλό δικτύωμα με δυο τερματικά (h1 και h2), έναν μεταγωγέα (S1), και έναν ελεγκτή. Φαίνονται στην Εικόνα 35:



Εικόνα 35: Επιτυχής εκκίνηση του Mininet με δίκτυο ενός μεταγωγέα και δυο τερματικών

Στη γραμμή εντολών του Mininet δίνεται η εντολή *–pingall* ώστε να διαπιστωθεί η σωστή λειτουργία του.

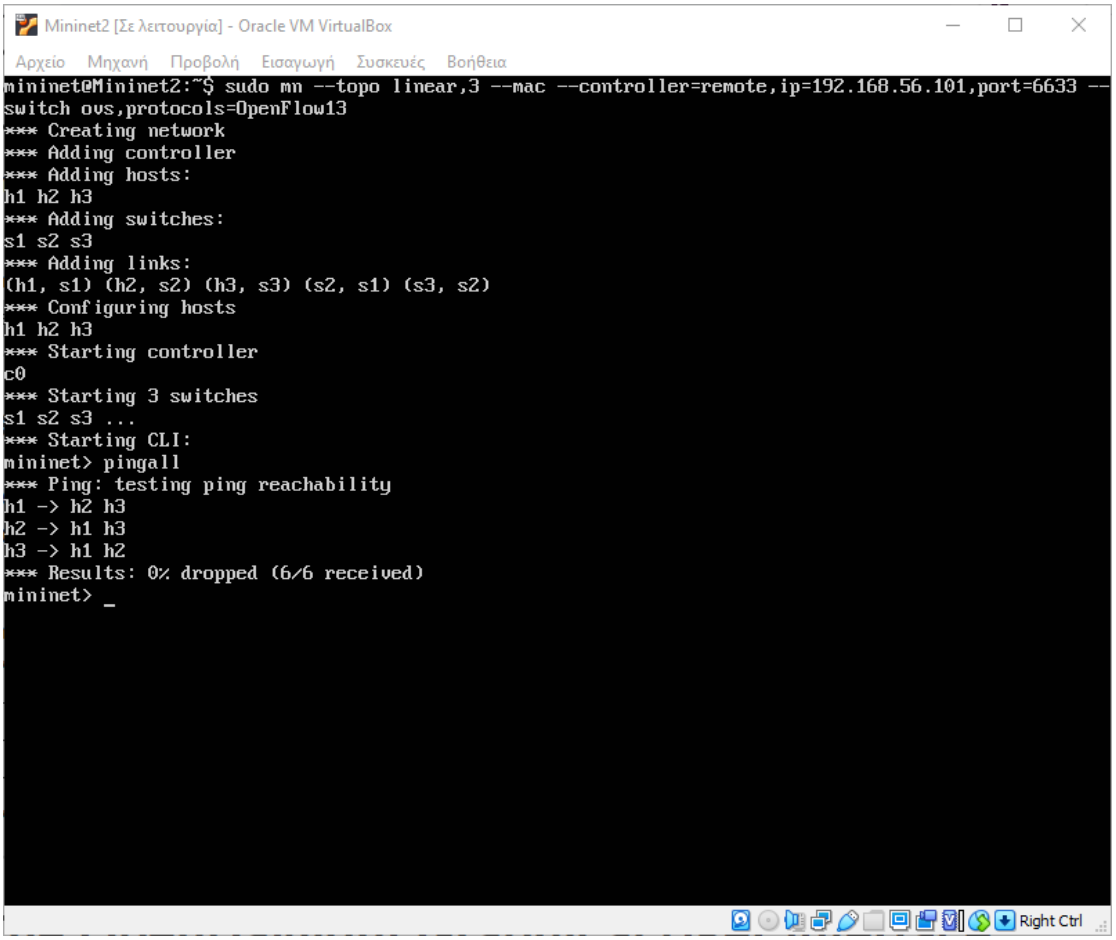
Για τον σκοπό της παρούσας εργασίας δημιουργείται στο Mininet ένα απλό δικτύωμα με τα εξής χαρακτηριστικά:

- Τρεις μεταγωγείς σε γραμμική τοπολογία
- Σε κάθε μεταγωγέα συνδέεται ένα τερματικό
- Η MAC διεύθυνση κάθε μεταγωγέα θα είναι ένα απλός αύξων αριθμός στο δεκαεξαδικό σύστημα
- Η διεύθυνση του απομακρυσμένου ελεγκτή είναι η 192.168.56.101 και το πρωτόκολλο επικοινωνεί στη θύρα 6633 (ενίοτε στην 6653).
- Χρησιμοποιείται το πρωτόκολλο OpenFlow 1.3 που είναι από τις πιο κοινά χρησιμοποιημένες και σταθερότερες εκδόσεις.

Η τοπολογία δημιουργείται με την παρακάτω εντολή:

sudo mn --topo linear,3 --mac --controller=remote,ip=192.168.56.101,port=6633 --switch ovs,protocols=OpenFlow13

Το αποτέλεσμα της εντολής και ο έλεγχος μέσω της εντολής *–pingall* φαίνονται στην Εικόνα 36:

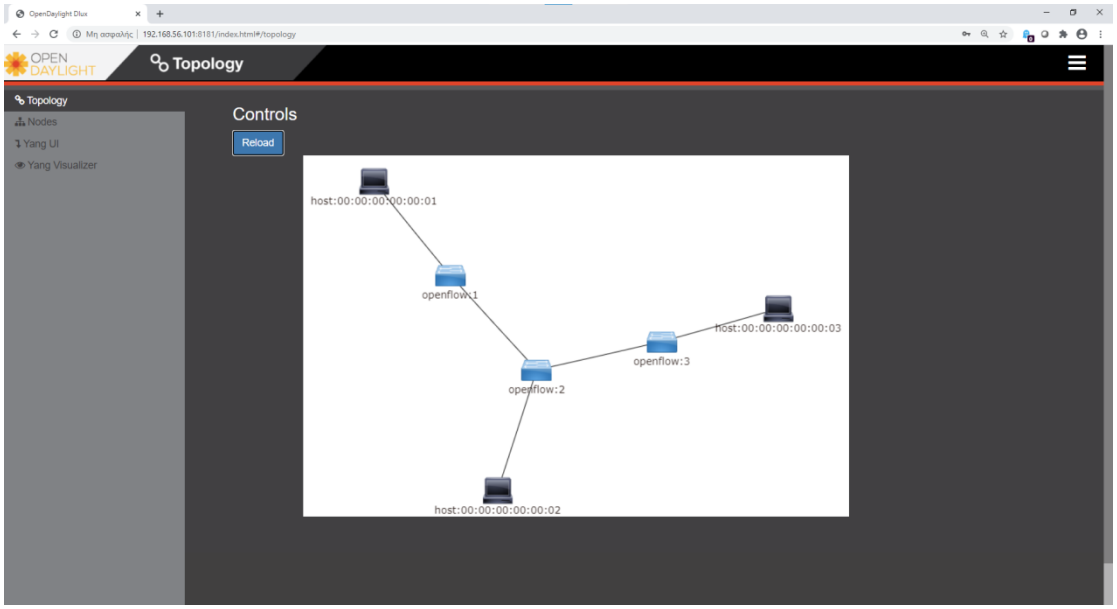


Εικόνα 36: Δημιουργία και έλεγχος της τοπολογίας του σεναρίου

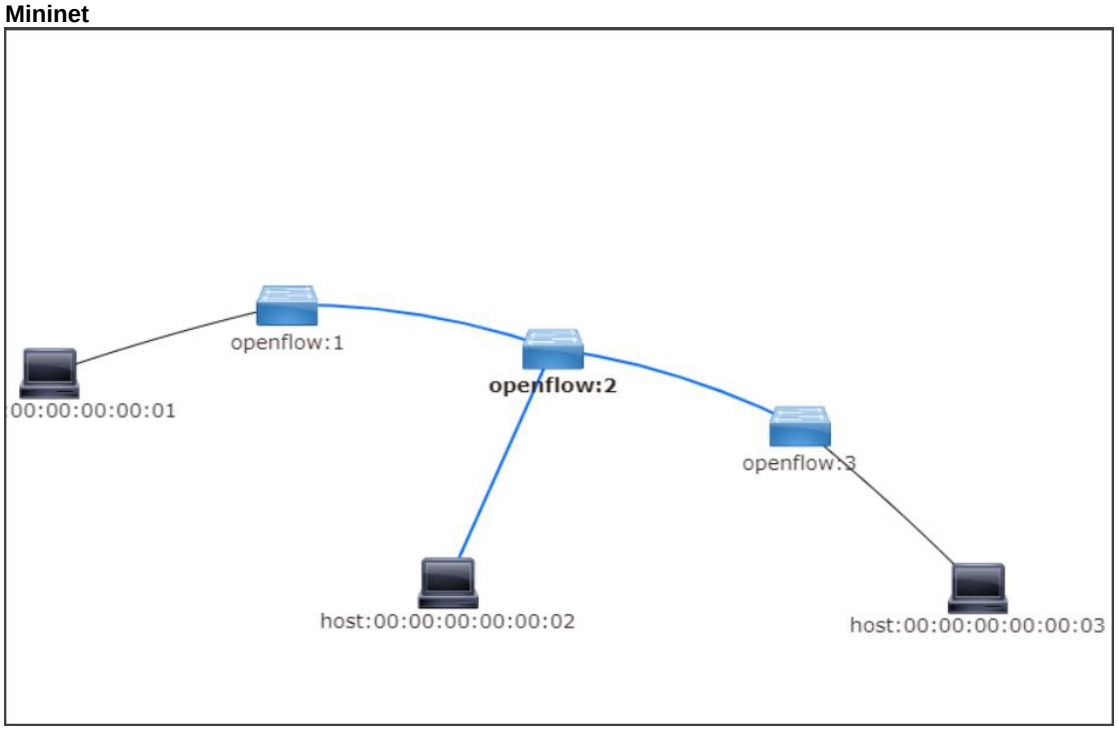
4.4 Εξέταση του δικτύου

Αφού γίνει η καταχώρηση του προεπιλεγμένου ονόματος χρήστη και κωδικού στην αντίστοιχη καρτέλα που εμφανίζεται στην Εικόνα 17 ο διαχειριστής αντικρίζει μια αναπαράσταση της γραμμικής δικτυακής τοπολογία με τους τρεις μεταγωγείς και τα τρία τερματικά. Αξίζει να σημειωθεί ότι η εικόνα είναι «δυναμική», δηλαδή τα δικτυακά στοιχεία που αναπαρίστανται μπορούν να επανατοποθετηθούν με τη βοήθεια του ποντικιού. Σε αυτό το σημείο το Mininet φαίνεται πως ακολουθεί άλλα προγράμματα όπως Packet Tracer της Cisco και GNS3, αλλά αυτή η λειτουργία έχει να κάνει με την ίδια τη μηχανή του Mininet και τον τρόπο που αντιλαμβάνεται τις οδηγίες στη γραμμή εντολών: η γραφική ερμηνεία των εντολών μπορεί να διαφέρει ή και να απέχει από την σκοπούμενη τοπολογία, ακόμα και αν οι διασυνδέσεις είναι όλες σωστές.

Αυτό που λείπει από τη γραφική αναπαράσταση της Εικόνας 37 είναι φυσικά ο ίδιος ο ελεγκτής μέσω του οποίου γίνεται η γραφική απεικόνιση και η φυσική σύνδεση των μεταγωγέων με αυτόν.



Εικόνα 37: Η εικόνα αποδεικνύει τη σωστή επικοινωνία ελεγκτή και εικονικής τοπολογίας του Mininet

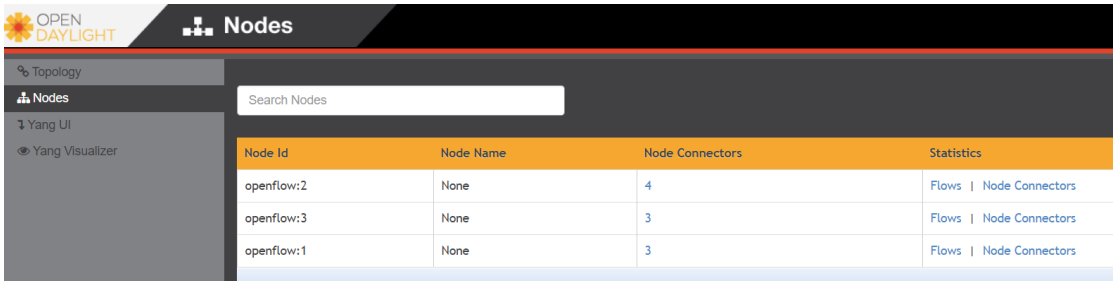


Εικόνα 38: Η γραμμικότητα της τοπολογίας

Με λίγη προσπάθεια αναδεικνύεται η γραμμικότητα της τοπολογίας στην Εικόνα 38. Οι συνδέσεις μεταξύ των μεταγωγέων μπορούν να διακοπούν ώστε να εξεταστεί η συμπεριφορά του δικτύου κατόπιν βλάβης.

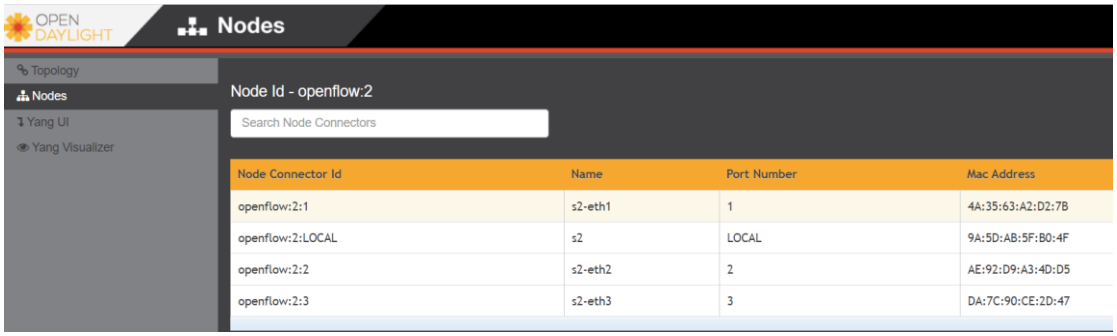
Από την επιλογή “Nodes” στην αριστερή καρτέλα (Εικόνα 39), εμφανίζονται όλοι οι μεταγωγείς που συμμετέχουν στο δίκτυο με τις ταυτότητες που τους έχουν δοθεί από το Mininet (openflow:1, openflow:2 και openflow:3), το πλήθος των συνδέσεων προς άλλες δικτυακές συσκευές, οι πίνακες ροών τους και πλήθος πακέτων ανά σύνδεση και κατεύθυνση.(Node Connectors)

4.1 Η αρχική καταγραφή των μεταγωγέων



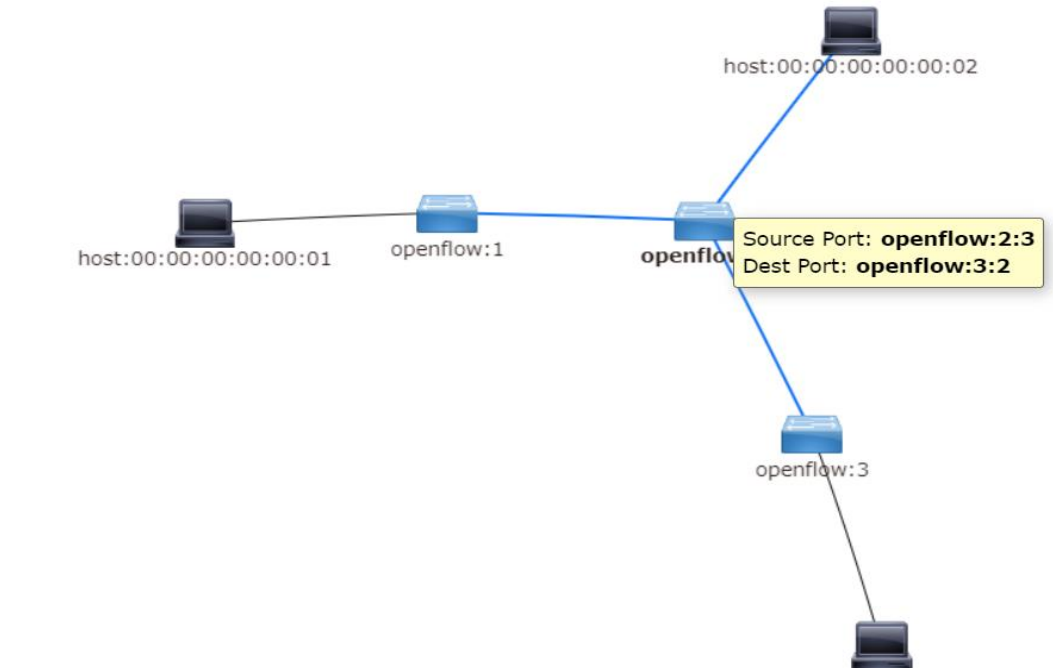
Εικόνα 39: Η καρτέλα "Nodes"

Η αρχική καταγραφή των μεταγωγέων όπου φαίνεται το πλήθος των συνδέσεων του καθενός (ο openflow:2 για παράδειγμα έχει τέσσερις συνδέσεις όπως στην Εικόνα 40)

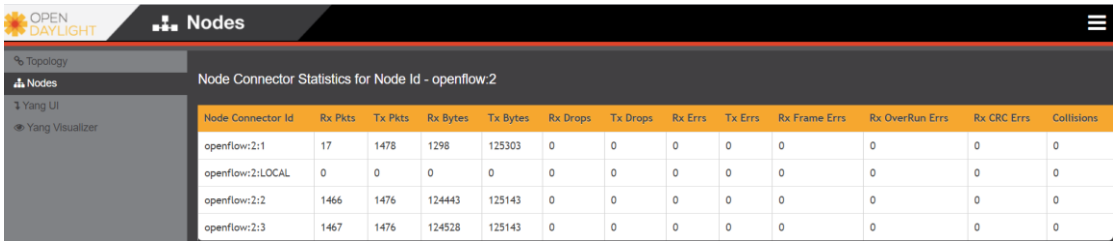


Εικόνα 40 Αναλυτικά οι συνδέσεις του openflow:2 μεταγωγέα

Επιλέγοντας από τη στήλη "Node Connectors" τον πρώτο μεταγωγέα, φαίνονται οι συνδέσεις του προς τους άλλους δυο μεταγωγείς, η σύνδεση προς το τερματικό και μια εσωτερική σύνδεση προς τον εαυτό του που εξυπηρετεί την διαβίβαση μηνυμάτων OpenFlow. Στην Εικόνα 41 φαίνονται οι συνδέσεις.



Εικόνα 41: Επεξηγηματικές λεζάντες συνδέσεων



Εικόνα 42: Τα περιεχόμενα της στήλης "Node Connector" για τον μεταγωγέα openflow:2

Τα περιεχόμενα της στήλης "Node Connector" για τον μεταγωγέα openflow:2 (Εικόνα 42). Αν και το δικτύωμα δεν μεταφέρει δεδομένα, η σηματοδοσία από το OpenFlow και άλλα κοινά δικτυακά πρωτόκολλα (STP-spanning tree) που υποστηρίζονται από το Mininet, έχει αποδώσει μέσα σε διάστημα λίγων ορών πολλές χιλιάδες πακέτα.

Επεξηγηματικά:

RxPkts –πακέτα που ελήφθησαν από τη θύρα

TxPkts –πακέτα που αποστάλθηκαν από τη θύρα

Rx Bytes –ληφθέντα byte ανά θύρα

Tx bytes –απεσταλμένα byte ανά θύρα

Εν συντομία: Drops->απορριφθέντα πακέτα, Errs->πακέτα με σφάλματα, Frame Errs-> πλαίσιο (Επίπεδο 2) με σφάλματα, OverRun Errs->σφάλματα λόγω υπερχείλισης, CRC Errs->Σφάλματα Επιπέδου 2, Collisions-> Συγκρούσεις

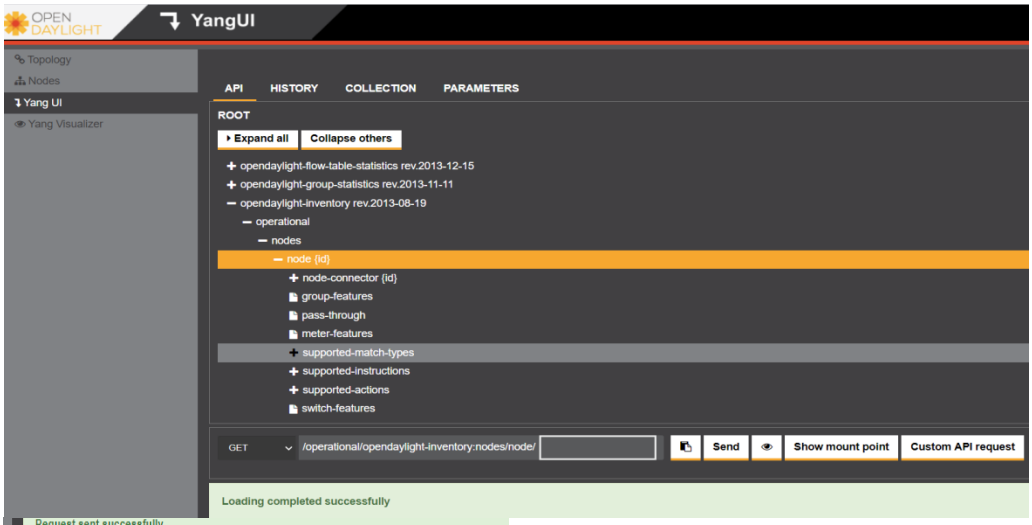
Άρα το SDN και ο ελεγκτής OpenDaylight μπορεί ξεκάθαρα να βοηθήσει στη Διαχείριση του δικτύου και συγκεκριμένα στη διαχείριση σφαλμάτων[2], αφού οι αναφορές αυτές προέρχονται συνήθως από πρωτόκολλα όπως το SNMP και το Syslog.

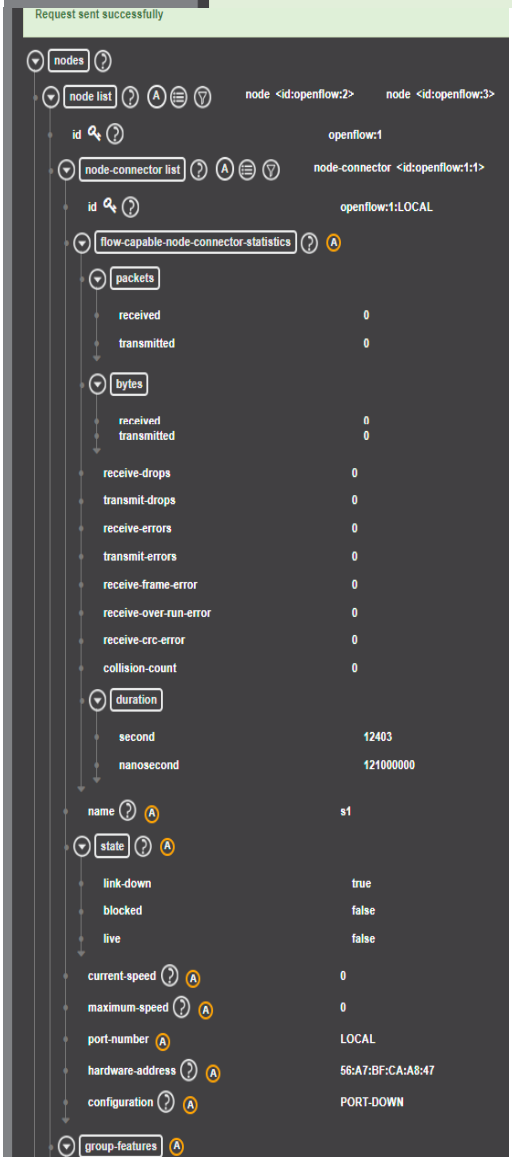
[2] Η διαχείριση σφαλμάτων είναι ένα από τα πέντε είδη διαχείρισης. Τα άλλα τέσσερα είναι: η διαχείριση διαμόρφωσης (ή παραμέτρων), η διαχείριση ασφάλειας, η διαχείριση επιδόσεων και η διαχείριση κόστους

Η καρτέλα Yang UI του OpenDaylight είναι ένας γραφικός πελάτης της REST με τον οποίο δημιουργούνται και αποστέλλονται τα αιτήματα στην αποθήκη δεδομένων του OpenDaylight. Με το Yang UI ανασύρονται πληροφορίες από την αποθήκη δεδομένων ή να δημιουργηθούν REST εντολές που θα αλλάξουν τις πληροφορίες στην αποθήκη δεδομένων και συνεπώς τις δικτυακές παραμέτρους

Επιλέγοντας την καρτέλα Yang UI και εν συνεχεία την επιλογή “Expand All”, εμφανίζονται όλα τα διαθέσιμα API. Δεν λειτουργούν όλα γιατί δεν έγινε πλήρης εγκατάσταση του OpenDaylight αλλά βασικό στοιχείο είναι η επιλογή Inventory η οποία μπορεί να επιστρέψει δεδομένα αφού η τοπολογία στο Mininet διαθέτει τρεις μεταγωγείς.

Κατόπιν επέκτασης της επιλογής Inventory->operational->nodes, επιλέγεται “SEND” ώστε να αποσταλεί το GET API στον ελεγκτή.





Εικόνα 43 Οι ατελείωτες πληροφορίες που δίνει το Yang UI

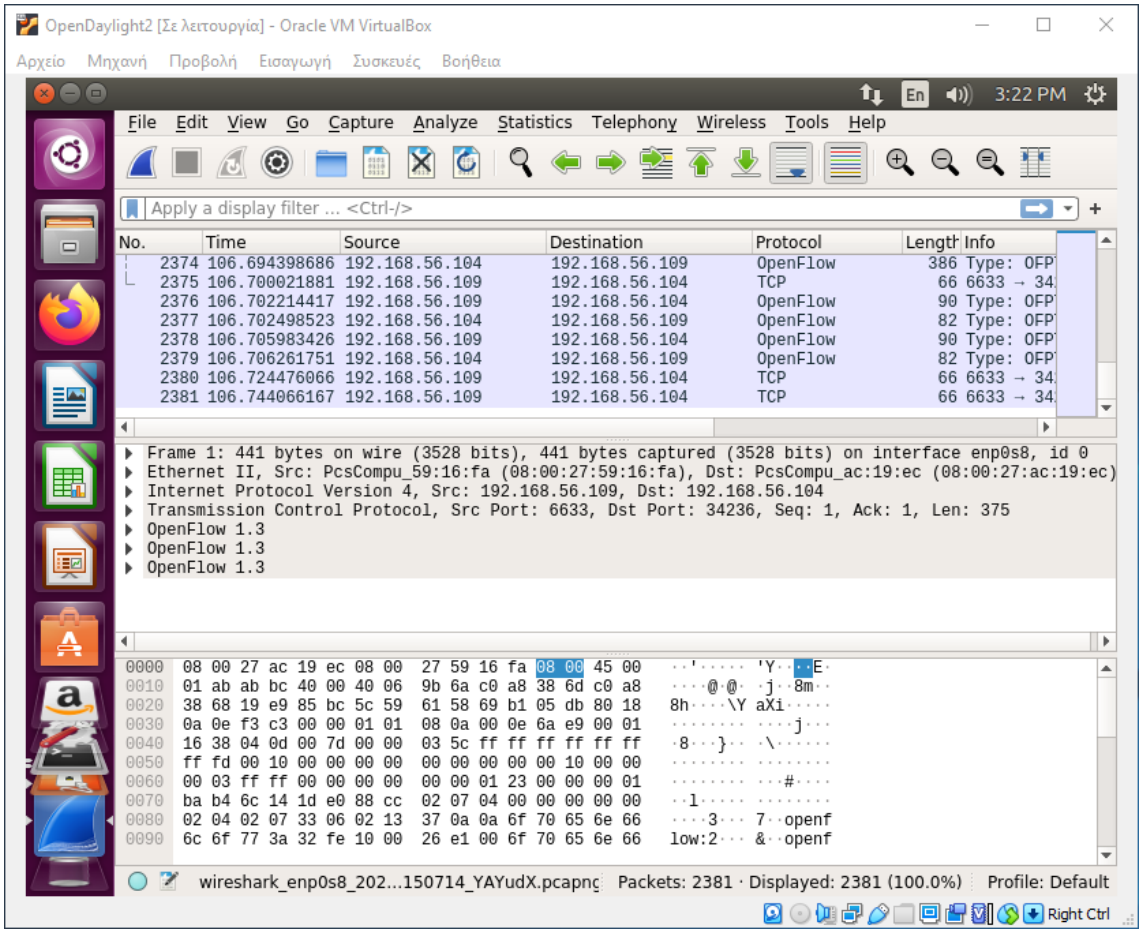
Μικρό μέρος (περίπου ¼) της απάντησης του ελεγκτή, περιλαμβάνει για αυτό το δίκτυο όλες τις πληροφορίες σχετικά με τους κόμβους, τις θύρες, στατιστικά και φυσικά τους πίνακες ροών και τους κανόνες τους (Εικόνα 43).

4.5 Wireshark και OpenFlow

Για να μελετηθούν πακέτα μέσω του εργαλείου ανάλυσης πρωτοκόλλων Wireshark δημιουργήθηκε μια παρόμοια πειραματική τοπολογία με χρήση Ubuntu Server 20.04 (64 bit) ώστε να εκτελεστεί η τελευταία σταθερή έκδοση του Wireshark που μπορεί να συγκρατήσει και πακέτα του πρωτικόλλου OpenFlow. Για λόγους συμβατότητας προτιμήθηκε η εγκατάσταση του Wireshark στον διακομιστή που φιλοξενεί το OpenDaylight και ο οποίος είναι εφοδιασμένος με γραφικό περιβάλλον (διαφορετικά θα έπρεπε να χρησιμοποιηθεί το T-Shark ή να παραμετροποιηθεί περαιτέρω ο διακομιστής ώστε να υποστηρίξει γραφικά)

Επειδή δεν υπήρχε λόγος να καταργηθούν οι αρχικές εικονικές μηχανές, οι νέοι διακομιστές θα έχουν διαφορετικές IP αλλά από το ίδιο δίκτυο /24 του VirtualBox.

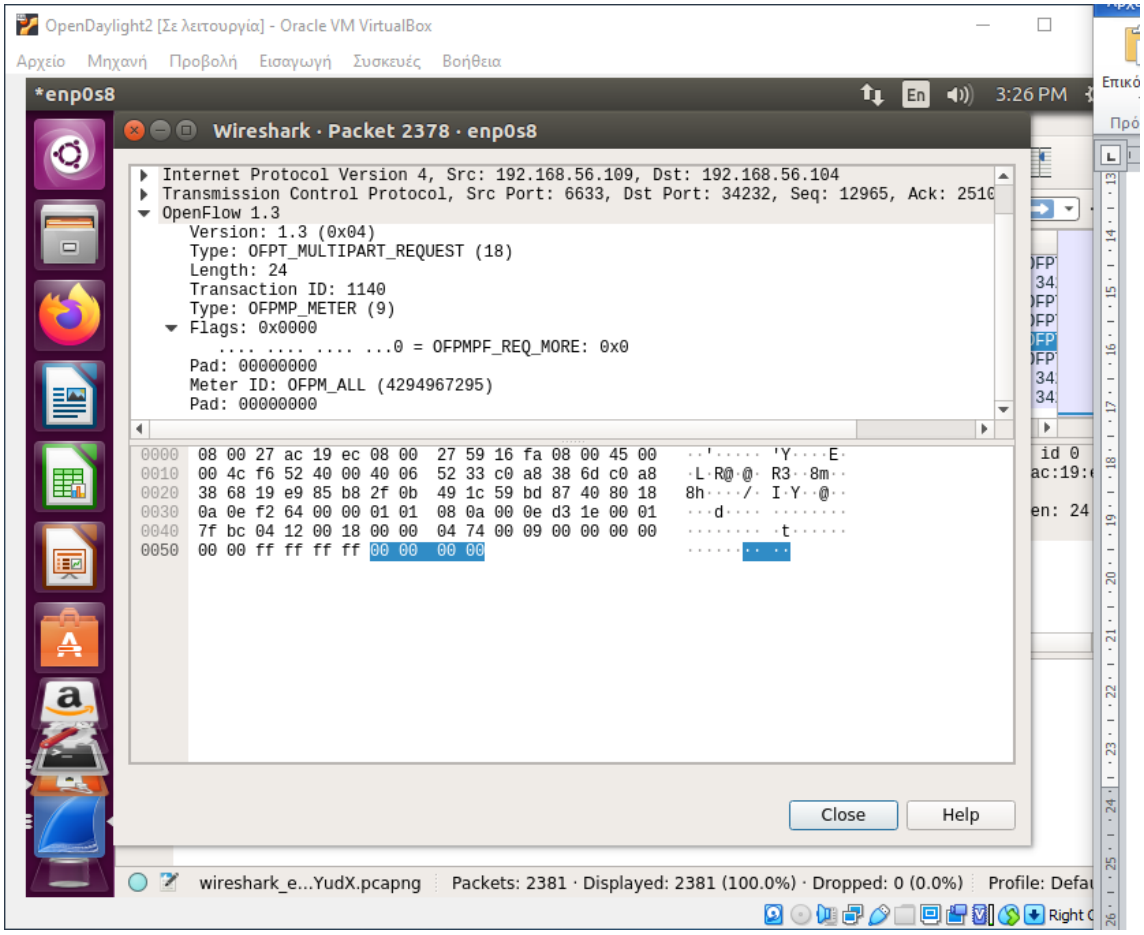
OpenDaylight2: 192.168.56.109 (TCP θύρα 6633 για OpenFlow και 8181 για διαχείριση με



Εικόνα 44: Το Wireshark συγκρατεί επιτυχώς τα πακέτα σηματοδοσία του OpenFlow

γραφικό περιβάλλον)Mininet2: 192.168.56.104

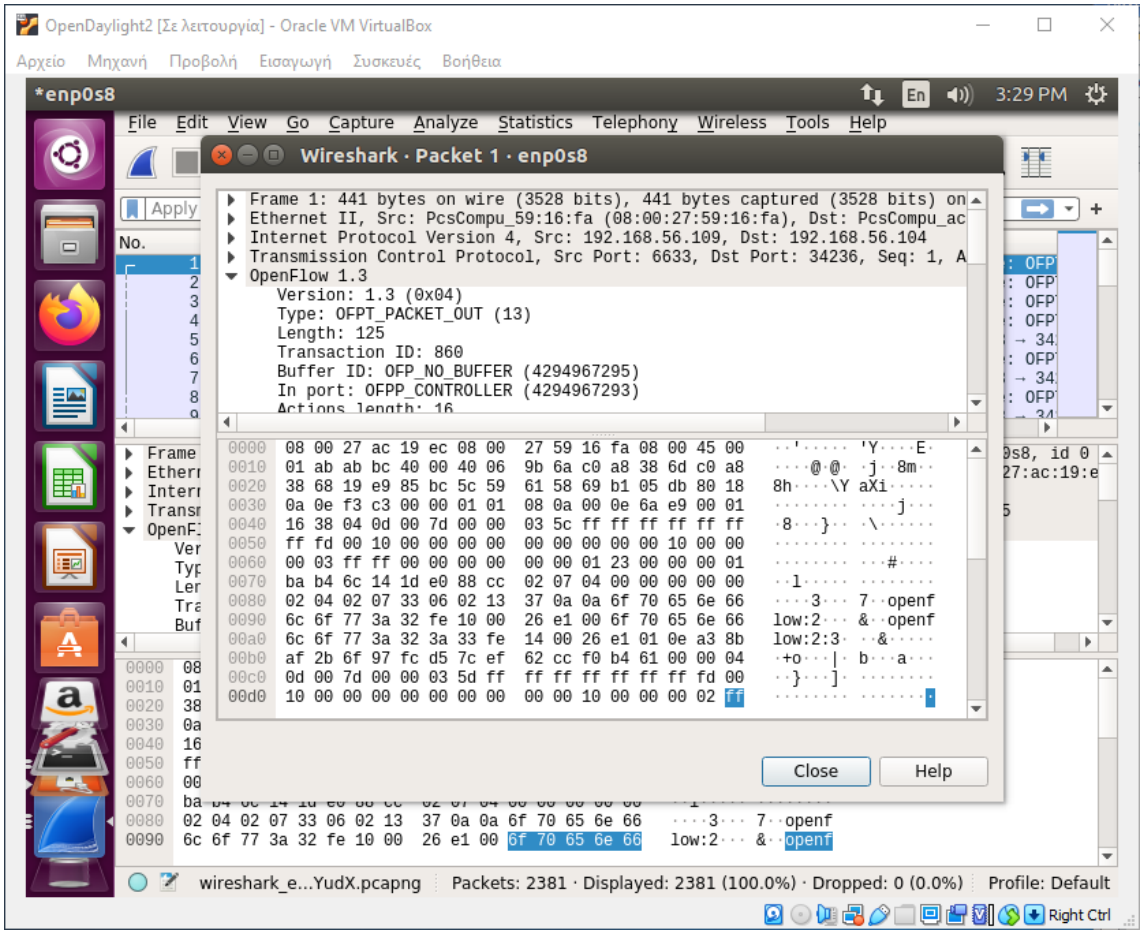
Με την πρώτη δοκιμή το Wireshark στο πρώτο VM καταφέρνει να συλλάβει πακέτα που κυκλοφορούν και στις δύο κατευθύνσεις.



Εικόνα 45 Σε ανάπτυξη ένα από τα πακέτα OpenFlow που συγκράτησε το Wireshark

Επιλέγεται ένα πακέτο που κατευθύνεται από τον ελεγκτή (192.168.56.109) στο δικτύωμα (192.168.56.104) και βρίσκεται ότι είναι OFPT_MULTIPART_REQUEST (Εικόνα 45)

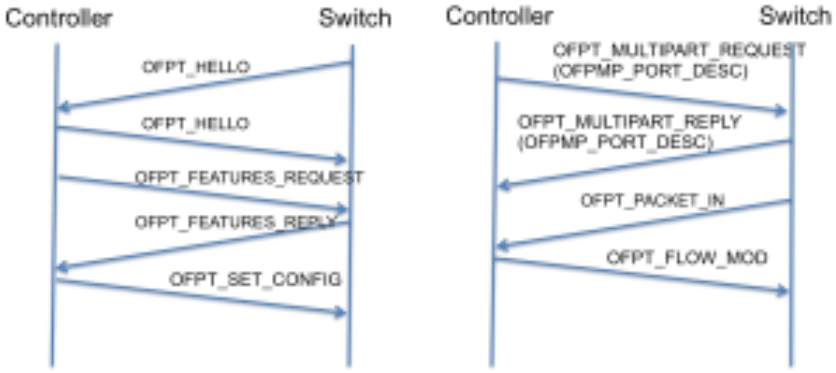
Το δεύτερο πακέτο που συλλαμβάνεται (Εικόνα 46), είναι ένα OFPT_PACKET_OUT.



Εικόνα 46: Το δεύτερο πακέτο είναι ένα OFPT_PACKET_OUT

4.6 Κατανόηση των OpenFlow μηνυμάτων

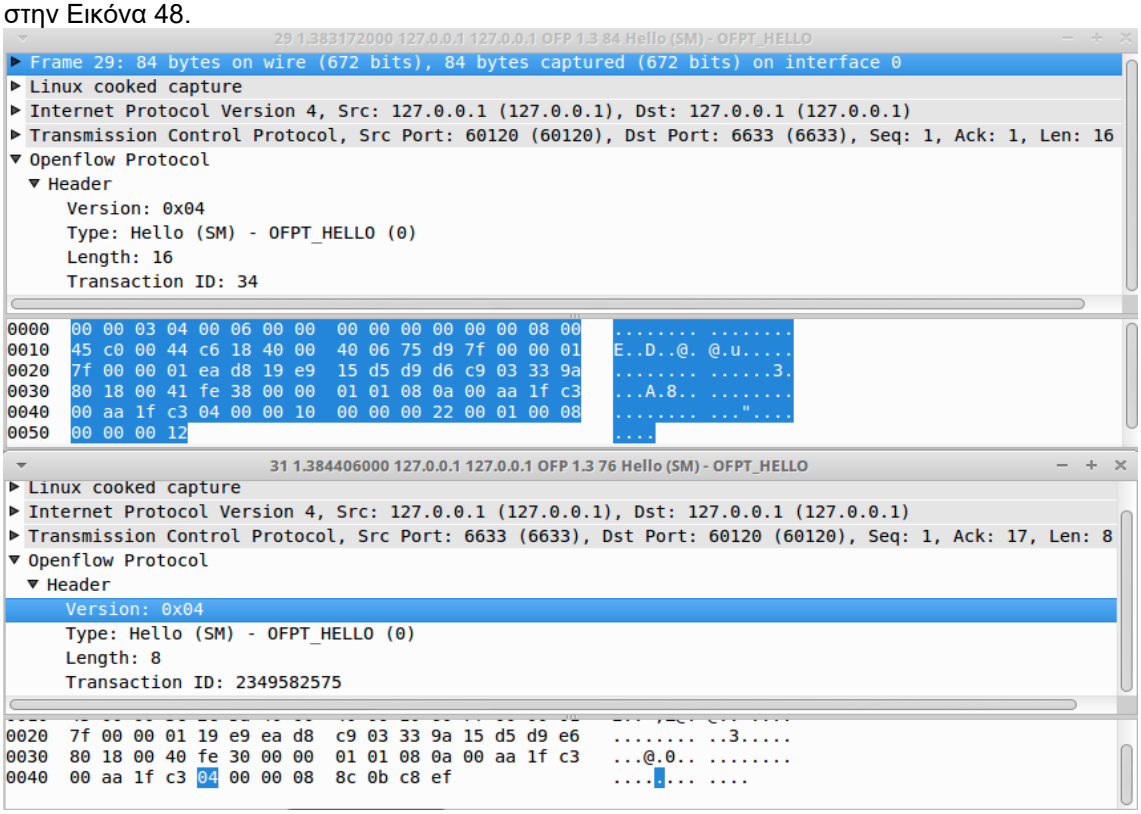
Αφού η πειραματική τοπολογία έχει τρέχει και αποκρίνεται στον διαχειριστή, θα αναλυθούν περαιτέρω τα μηνύματα που ανταλάσσονται μεταξύ ελεγκτή και μεταγωγέων ώστε να είναι δυνατή η ερμηνεία κάθε πακέτου που καταγράφεται στο Wireshark. Το σύνολο των πακέτων φαίνεται στην Εικόνα 47.



Εικόνα 47: Η σηματοδοσία πρίν την εγκατάσταση του OpenFlow

4.6.1 Έναρξη της σύνδεσης

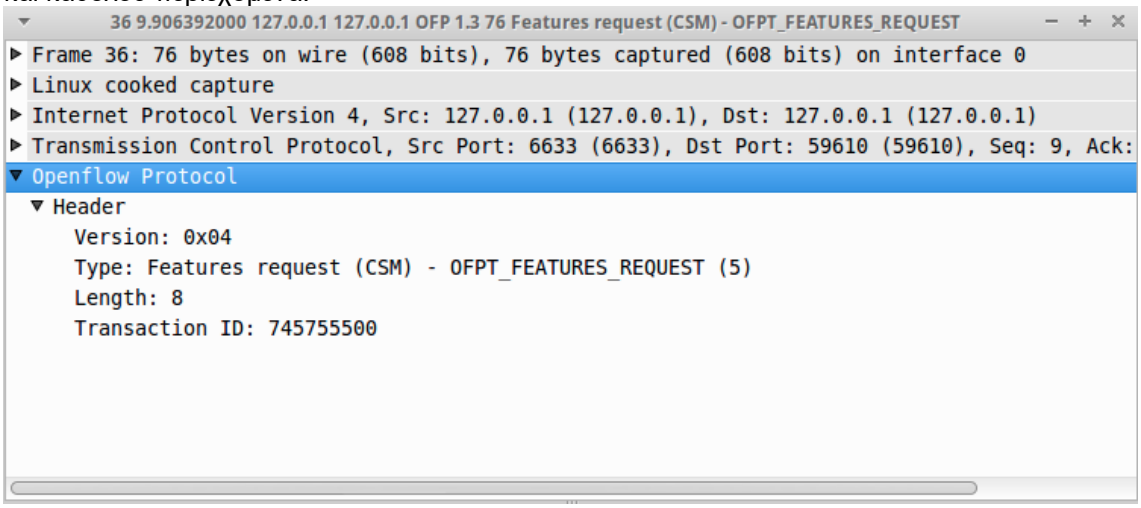
Ο μεταγωγέας εκκινεί μια τυπική TCP (ή TLS) σύνδεση με τον ελεγκτή. Όταν εγκατασταθεί η σύνδεση, κάθε οντότητα πρέπει να στείλει μήνυμα **OFPT_HELLO** με ορισμένη version πρωτοκόλλου την υψηλότερη που υποστηρίζεται από τον αποστολέα. Ακολουθεί παράδειγμα στην Εικόνα 48.



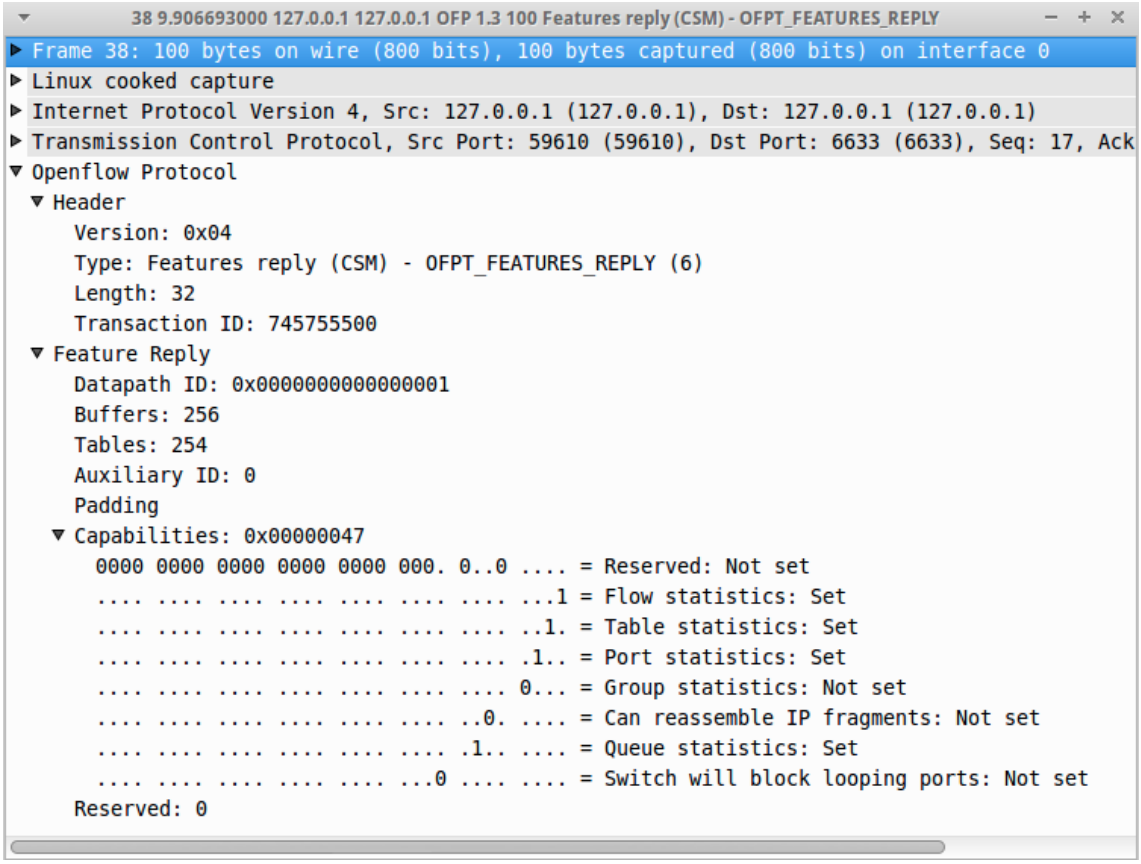
Εικόνα 48: OFPT_HELLO

4.6.2 Αίτημα χαρακτηριστικών – Απάντηση

Αφού εγκατασταθεί επιτυχώς η σύνδεση, ο ελεγκτής θα στείλει ένα μήνυμα **OFPT_FEATURES_REQUEST** (Εικόνα 49) που περιλαμβάνει μόνο μια επικεφαλίδα OpenFlow και καθόλου περιεχόμενα.

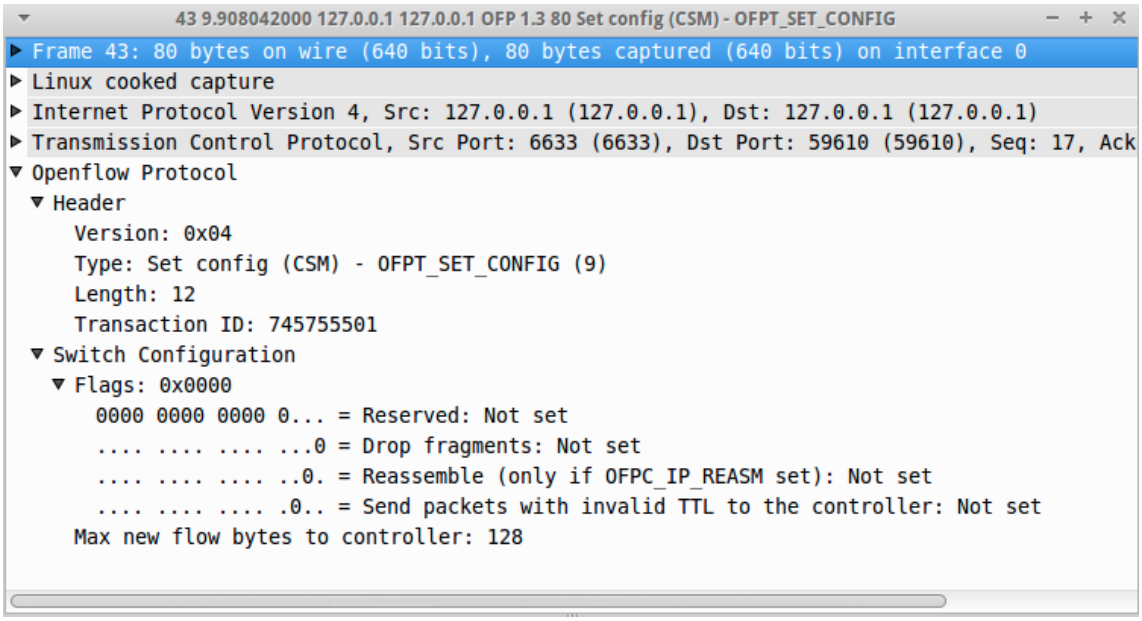


Εικόνα 49: OFPT_FEATURES_REQUEST



Εικόνα 50: OFPT_FEATURES_REPLY

Ο μεταγωγέας απαντά με μήνυμα **OFPT_FEATURES_REPLY** (Εικόνα 50) όπου περιλαμβάνεται το η ταυτότητα της διαδρομής δεδομένων (Datapath ID) και οι ικανότητες του μεταγωγέα.

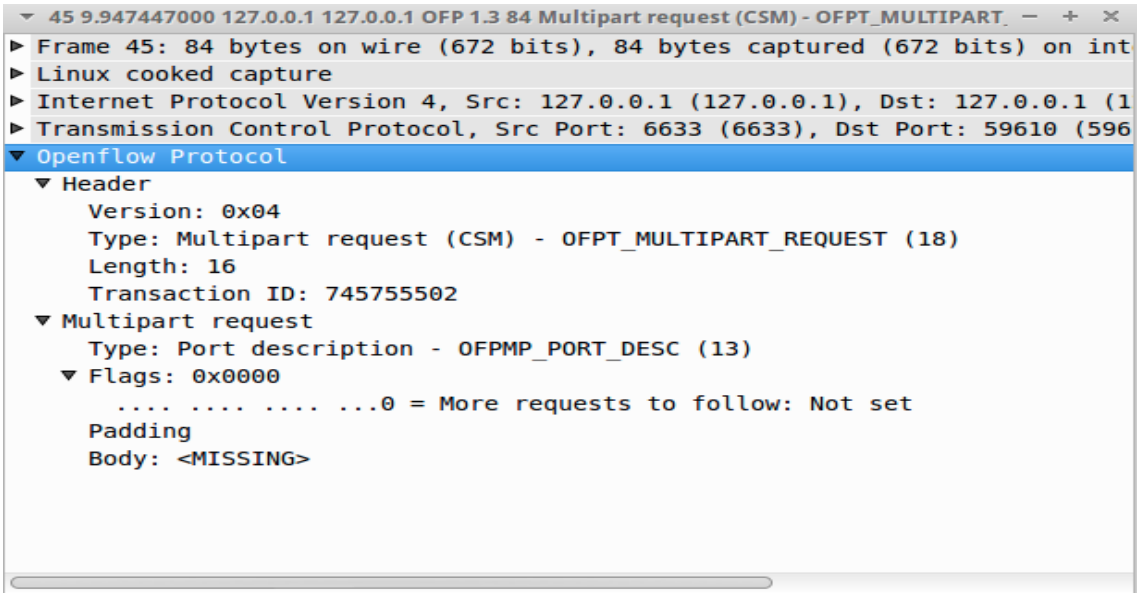


Εικόνα 51: OFPT_SET_CONFIG

Τελικά ο ελεγκτής στέλνει ένα μήνυμα **OFPT_SET_CONFIG** (Εικόνα 51)στον μεταγωγέα. Το μήνυμα αυτό περιλαμβάνει μια σειρά από flag bits και το μέγιστο πλήθος από bytes που μπορούν να σταλούν στον ελεγκτή μέσω του datapath.

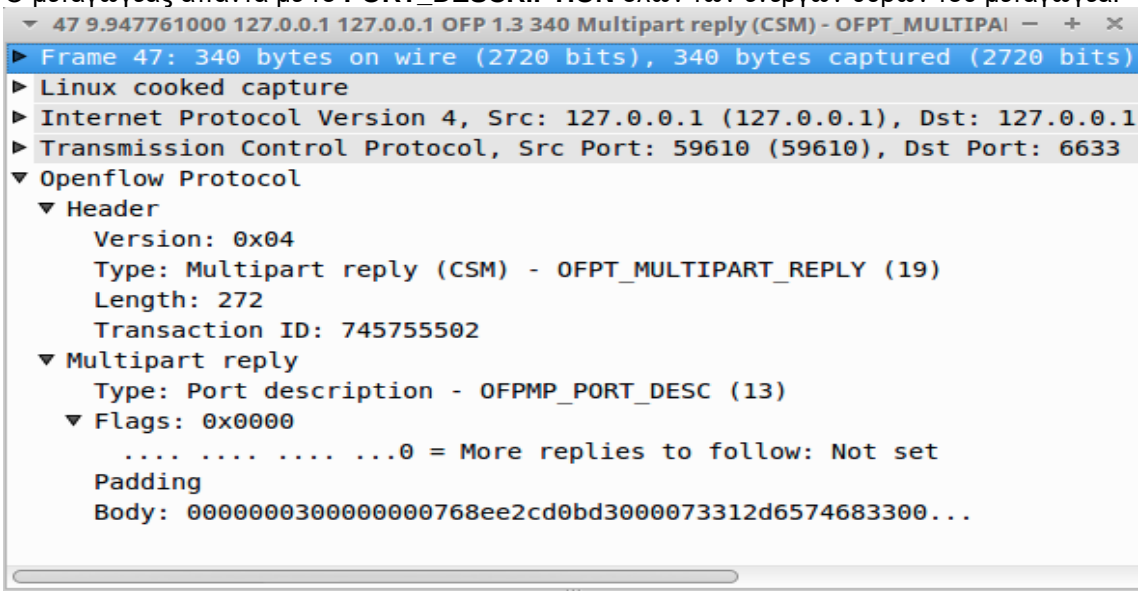
Multipart Request – Reply

Ο ελεγκτής μπορεί να ζητήσει πληροφορίες κατάστασης από το datapath με ένα **OFPT_MULTIPART _REQUEST.** Τα είδη μηνυμάτων που υπάγονται σε αυτή τηκατηγορία περιλαμβάνουν ποικίλα χαρακτηριστικά (FLOW/TABLE/PORT/QUEUE/METER κλπ) ή περιγραφές χαρακτηριστικών (METER_CONFIG.TABLE_FEATURES/PORT_DESC κλπ). Ακολουθεί υπόδειγμα μέσω της Εικόνας 52 και της Εικόνας 53:



Εικόνα 52: OFPT_MULTIPART_REQUEST

Ο μεταγωγέας απαντά με το **PORT_DESCRIPTION** όλων των ενεργών θυρών του μεταγωγέα.

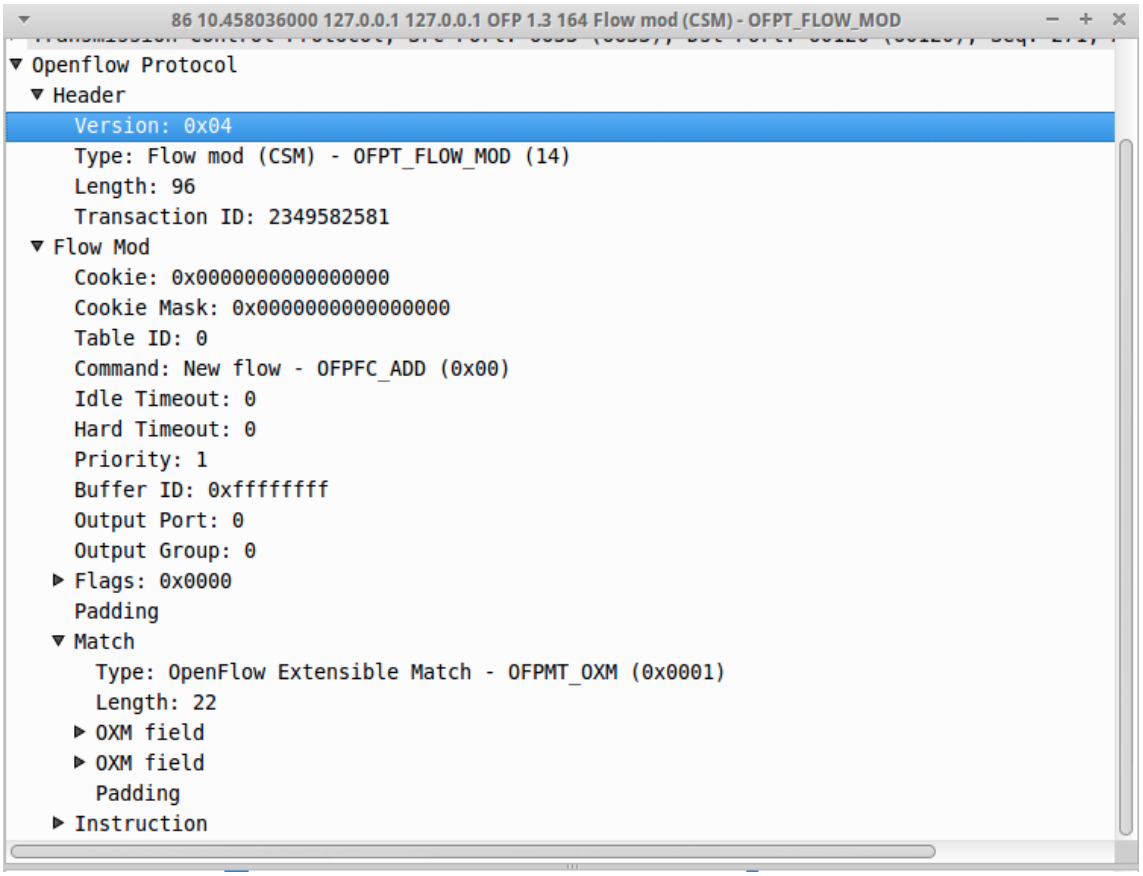


Εικόνα 53 OFPT_MULTIPART_REPLY

4.6.3 Flow Mod

Οι ροές μπορεί να αποστέλλονται από τον ελεγκτή προληπτικά (proactively) ή αντιδραστικά reactively). Τα μηνύματα τροποποίησς ροών ανήκουν στα εξής είδη: OFPFC_ADD, OFPFC_DELETE, OFPFC_DELETE_STRICT, OFPFC_MODIFY, OFPFC_MODIFY_STRICT

Στην Εικόνα 54, φαίνεται ο διακομιστής να εγκαθιστά μια νέα ροή που δείχνει ότι πέρα από το σύνολο παραμέτρων OpenFlow 1.0, υπάρχουν και παράμετροι όπως priority, idle_timeout κλπ των οποίων η σύνταξη και ο τρόπος εξέτασης μοιάζουν με τις αντίστοιχες του πρωτοκόλλου OpenFlow 1.3

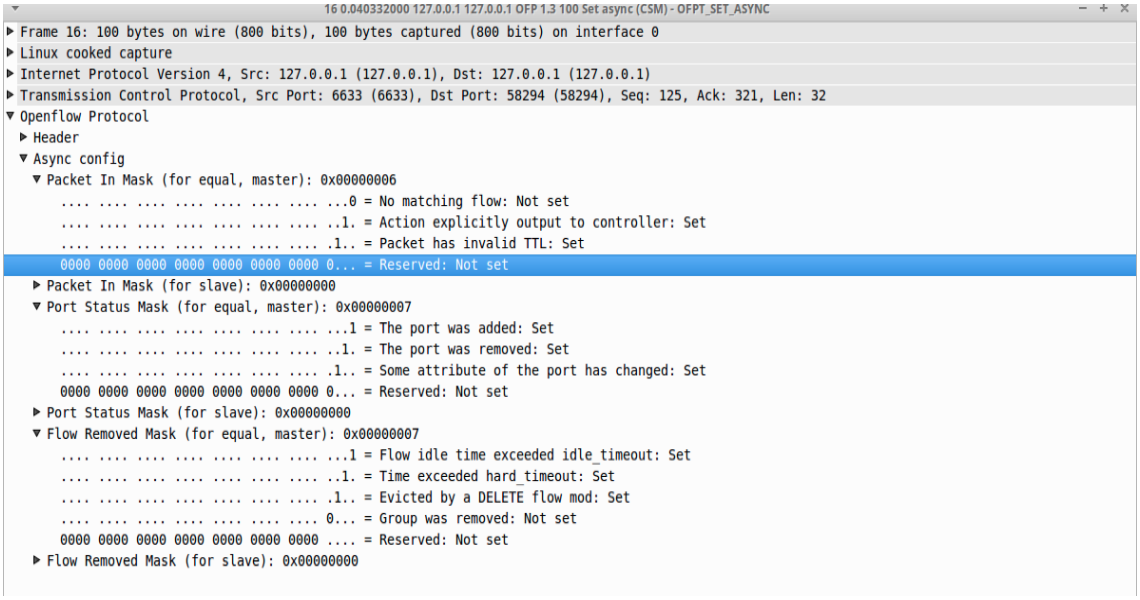


Εικόνα 54: OFPT_FLOW_MOD

Πρέπει να σημειωθεί ότι ο μεταγωγέας δεν επιβεβαιώνει τη λήψη των μηνυμάτων FLOW_MOD. Αν όμως υπάρξει σφάλμα στη λήψη, τότε το μήνυμα FLOW_MOD απαντάται με OFPET_FLOW_MOD_FAILED.

4.6.4 Μήνυμα Ασύγχρονης Διαμόρφωσης

Τα ασύγχρονα μηνύματα αποστέλλονται από ένα μεταγωγέα στον ελεγκτή. Το σύνολο των μηνυμάτων που υποστηρίζονται από το πρωτόκολλο OpenFlow περιλαμβάνει τα μηνύματα Packet-Ins, Flow-Removed, Port-Status ή Error. Όταν ο μεταγωγέας συνδέεται στον ελεγκτή, ο δεύτερος μπορεί να ορίσει το σύνολο των μηνυμάτων που μπορεί να λάβει μέσω του OpenFlow καναλιού.



Εικόνα 55: OFPT_ASYNC_CONFIG

Η Εικόνα 55 δείχνει ένα async config μήνυμα που αποστέλει ο ελεγκτής. Ανάλογα με το είδος των flag bits ο μεταγωγέας δύναται να λάβει ποικίλα async μηνύματα.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Το SDN δεν χρειάζεται διαφήμιση, ούτε και κάποια ιδιαίτερη ενίσχυση. Από ότι φαίνεται οι κατασκευαστές δικτυακού εξοπλισμού από απλούς οικιακούς δρομολογητές έως whiteboxes, SD-WAN συσκευές αλλά και οι μεγαλύτεροι πάροχοι τηλεπικοινωνιακών υπηρεσιών το έχουν υιοθετήσει με τη μια ή την άλλη μορφή. Αυτό που το έκανε αγαπητό είναι η δυνατότητα που δίνει στους αρχιτέκτονες και μηχανικούς δικτύων να κατασκευάζουν εργαλεία για τις πιο απλές έως και τις πιο υψηλές λειτουργίες των δικτυών. Για να εκπαιδευτεί μια καινούργια γενιά μηχανικών σε αυτό πρέπει να εντοπιστεί το σύνολο των προαπαιτούμενων εργαλείων όπως η άψογη γνώση λειτουργικών συστημάτων και θεμελιωδών εννοιών τους, ο καλός χειρισμός του Linux και της γραμμής εντολών του καθώς και οι στοιχειώδεις γνώσεις δικτύων και εννοιών όπως μεταγωγή, δρομολόγηση κλπ. Ο προγραμματισμός ίσως και να είναι το απλούστερο κομμάτι αφού χρησιμοποιούνται σύγχρονες γλώσσες στη γραφή κώδικα και στα μοντέλα δεδομένων.

Στην αναζήτηση εργαλείων για την εκμάθηση SDN προτιμήθηκε το Mininet που ακολουθεί κατά πόδας το SDN από τη γέννηση του και έχει δημιουργηθεί για την εξομοίωση τοπολογιών SDN καθώς και για την βοήθεια στην εκμάθηση του. Υποστηρίζει τις περισσότερες εκδόσεις του πρωτοκόλλου OpenFlow και επιτρέπει την ανάπτυξη μοντέλων για την εξομοίωση λοιπών συσκευών σε αυτό.

Βασίζεται σε ανοιχτό κώδικα και όπως όλα τα παρόμοια προγράμματα σχετίζεται με το GitHub και την κοινότητα του Apache, έστω και έμμεσα. Άρα είναι το καταλληλότερο για χρήση σε εκπαίδευση; Μάλλον όχι, κατά την ενασχόληση μου με το παρόν έργο διαπίστωσα ότι καταρχάς ο εκπαιδευόμενος πρέπει ήδη να κατέχει άψογα το λειτουργικό σύστημα Linux και όλες τις ιδιομορφίες του. Πρέπει να γνωρίζει άψογα τις τεχνολογίες εικονικοποίησης και δικτύων αλλά και να διαθέσει άπλετο χρόνο ώστε να αναζητά σε φόρουμ και το GitHub λύσεις στα προβλήματα που ανακύπτουν συνεχώς αφού τα δεκάδες δομικά στοιχεία αναβαθμίζονται ανεξάρτητα προκαλώντας ασυμβατότητες και δυσλειτουργίες.

Συνεπώς δεν απευθύνεται σε άτομα που δεν έχουν κάποια τριτοβάθμια εκπαίδευση πάνω στην πληροφορική και συγκεκριμένα σε υψηλές έννοιες της επιστήμης υπολογιστών.

Από την άλλη αποδεικνύει την ολότητα της επιστήμης υπολογιστών αφού θα χρειαστούν και γνώσεις προγραμματισμού για να επιτύχει κάποιος σημαντική πρόοδο στην εκμάθηση των σύγχρονων δικτύων.

Το Mininet περιστοιχίζεται από μια εξαιρετική κοινότητα μηχανικών δικτύων οι οποίοι φροντίζουν να αναπτύσσουν συνέχεια τα δομικά του στοιχεία και να προσθέτουν νέα χαρακτηριστικά. Εδώ εντοπίζεται και ένα από τα μεγαλύτερα προβλήματα του αφού η τεκμηρίωση του δεν ακολουθεί τις εξελίξεις και τις βελτιώσεις αφήνοντας τους νέους ερευνητές με ένα τεράστιο έργο αναζήτησης σε πολλούς διαφορετικούς ιστόχωρους μέχρι να καταφέρουν να δημιουργήσουν την πιο απλή δικτυακή τοπολογία.

Η «θυσία» αυτή δεν είναι χωρίς αντίκρισμα, ο χρήστης – εκπαιδευόμενος αρχίζει σε πολύ μικρό διάστημα να οικειοποιείται πολύπλοκα και περιζήτητα εργαλεία της πληροφορικής όπως η εικονικοποίηση, οι containers, το GitHub, το scripting και το CLI (Command Line Interface) ώστε να μπορεί να ανταποκριθεί στις σημερινές και μελλοντικές απαιτήσεις των εταιρειών που εμπλέκονται στα δίκτυα, τις τηλεπικοινωνίες, τις τεχνολογίες Νέφους και το IT γενικότερα.

ΕΠΙΛΟΓΟΣ

Δεν υπήρξε σύγκριση του Mininet με άλλα προγράμματα εξομοίωσης και εικονικοποίησης δικτύων επειδή είναι πρωτίστως εξομοιωτής προγραμματζομένων δικτύων (SDN) και μάλιστα δημιουργήθηκε από το Πανεπιστήμιο του Stanford με σκοπό την εκπαίδευση. Το Packet Tracer της Cisco Systems δεν διαθέτει στην τελευταία έκδοση του (version 7.3.x) κάποιο χαρακτηριστικό SDN, αφήνοντας μοναδικό ανταγωνιστή το GNS3 (Graphical Newtwork Simulator v3) που διαθέτει ιδιαιτέρως πλούσια χαρακτηριστικά αλλά είναι επεξεργαστικά πιο απαιτητικό και δημιουργήθηκε για να εξομοιώσει πιο «παραδοσιακά» δίκτυα. Παρά τις δυσκολίες στην επιτυχή υλοποίηση του απλού σεναρίου που παρουσιάζεται στην εργασία αυτή, ο γραφών σίγουρα βγαίνει εμπειρότερος και την ικανοποίηση ότι οι θεωρητικές γνώσεις θα λύνουν πάντα τα δυσκολότερα τεχνικά προβλήματα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

Coker, O. & Azodolmolky, S. (2017). Software-Defined Networking with OpenFlow. *2nd* ed. Birmingham: Packt Publishing.

Comer, D. (2004), ΔΙΚΤΥΑ ΚΑΙ ΔΙΑΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ: εφαρμογές τους στο Internet. Αθήνα: εκδ. Κλειδάριθμος.

Douligeris, C. & Serpanos, D. (2007). Network security: current status and future directions. John Wiley & Sons.

Edelman, et al. (2015), Network Programmability and Automation: SKILLS FOR THE NEXT-GENERATION ENGINEER. Sebastopol: O' Reilly Media.

Kurose, J. & Ross, K. (2013). Computer Networking: A Top-Down Approach Featuring the Internet. New Jersey: *6th Ed*. Pearson.

Lemay, et al. (2017). OpenDaylight Cookbook. Birmingham: Packt Publishing.

Mishra, V.(2019). Software Defined Networks. New York: MOMENTUM PRESS.

Noble, S. (2017). Building Modern Networks. Birmingham: Packt Publishing.

Toghraee, R. (2017). Learning OpenDaylight. Birmingham: Packt Publishing.

Walrand, J. (2003). ΔΙΚΤΥΑ ΕΠΙΚΟΙΝΩΝΙΩΝ: ΕΝΑ ΠΡΩΤΟ ΜΑΘΗΜΑ, Αθήνα: εκδ. ΕΘΝΙΚΟΥ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟΥ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΑΘΗΝΩΝ.

White, R. & Donohue, D.(2014). The Art of Network Architecture Business Driven Design. Indianapolis: Cisco Press

Δουληγέρης Χρ. (2005) Τηλεπικοινωνιακά και Δικτυακά Πρωτόκολλα. Μοσχάτο: εκδ. ΝΗΡΗΙΔΕΣ.

OPEN NETWORKING FOUNDATION (2012). *Software*-defined Networking: The New Norm for Networks, April

Cisco Systems (2013). *Software-defined Networking: Why We Like It and How We Are Building On It.*

Metaswitch (*2019)*. *A Guide to NFV and SDN.*

Heavy Reading.(2013), Practical Implementation of SDN & NFV IN THE WAN.

OPTICAL INTERNETWORKING FORUM & OPEN NETWORKING FOUNDATION (2017), SDN Transport API Interoperability Demonstration,

Braun, W. & Menth, M. (2014). Software-Defined Networking Using Openflow: Protocols, Applications and Architectural Design Choices..