ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ

Ευφυή Προγραμματιζόμενα Δίκτυα

Προγραμματιζόμενες Δικτυακές Υποδομές

Κίνητρα για Software Defined Networking – SDN

Το Πρωτόκολλο OpenFlow

Εφαρμογές σε Κατανεμημένες Υπολογιστικές Υποδομές

Β. Μάγκλαρης

maglaris@netmode.ntua.gr

www.netmode.ntua.gr

7/1/2019

ΕΥΦΥΪΑ & ΠΟΛΙΤΙΚΕΣ ΠΡΟΩΘΗΣΗΣ ΠΑΚΕΤΩΝ
Οι επιλογές της Κοινότητας του Internet

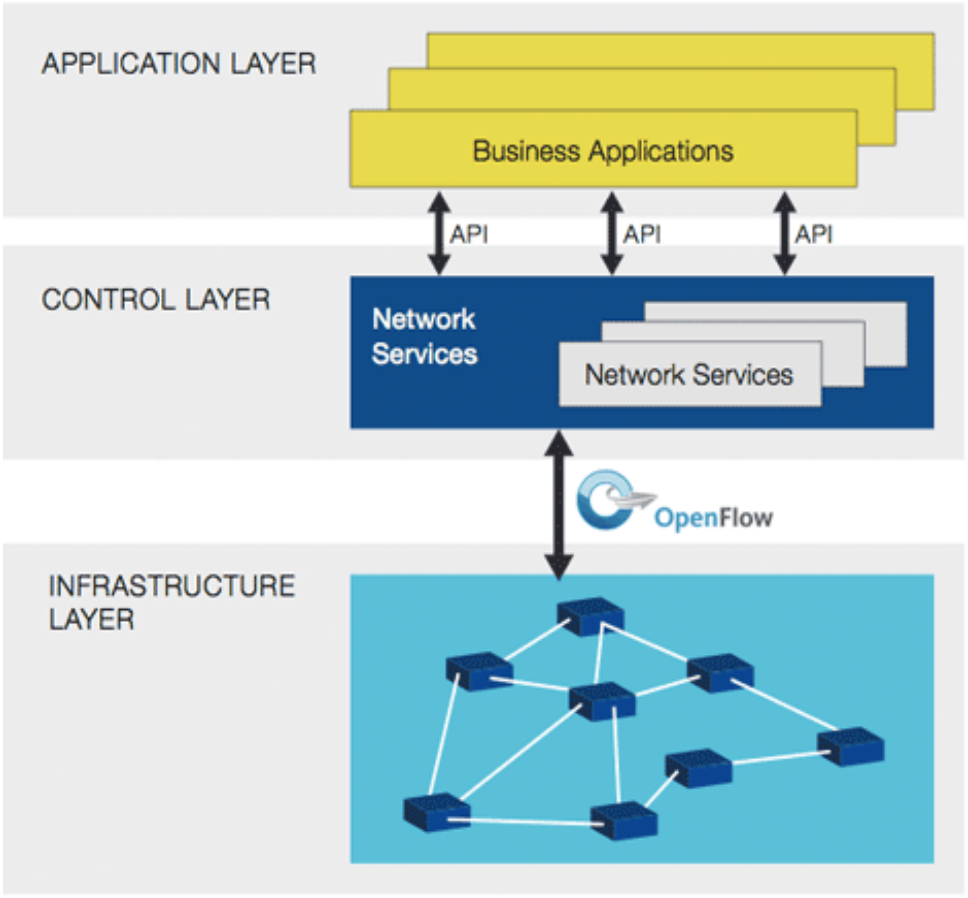
- Τοπικά Δίκτυα:
  - **Επίπεδο 2:** Μεταγωγή (Ethernet Switching), VLANs
  - **Επίπεδο 3:** Δρομολόγηση IP (destination based, OSPF, iBGP)
  - **Επίπεδα 2-4:** Ευφυή Προγραμματιζόμενα Δίκτυα ανά Εφαρμογή (flow)
    - Software Defined Networks SDN, OpenFlow
    - Εικονικά Περιβάλλοντα – Virtrualized Data-Centers

- Δίκτυα Μεγάλης Απόστασης – Μεγάλης Συγκέντρωσης (Wide Area Networks, WANs - Backbone Networks)
  - **Επίπεδο 2:** Layer 2 VPNs μέσω end-to-end tunnels, **VPLS**, Virtual Extensible LAN (**VXLAN**), MAC-in-MAC, Q-in-Q, Provider Backbone Bridges
  - **Επίπεδο 2.5:** *Single domain* MPLS (Multi-Protocol Label Switching), Traffic Engineering
  - **Επίπεδο 3:** Δρομολόγηση IP (destination based)
    - *Single Domain* IGP (OSPF, RIP, Intermediate System to Intermediate System IS-IS, iBGP)
    - *Multiple Domain* EGP (eBGP)
  - **Επίπεδα 2-4:** *Single domain* SDN, OpenFlow

OpenFlow (OF) CONTROL στο INTERNET του ΜΕΛΛΟΝΤΟΣ

Software Defined Networks (SDN) – OpenFlow Protocol

https://www.opennetworking.org



Source: Open Networking Foundation (ONF)

Διαχειριστικές Εφαρμογές – Network Programmability

- Πολιτικές δρομολόγησης
- Monitoring, security…

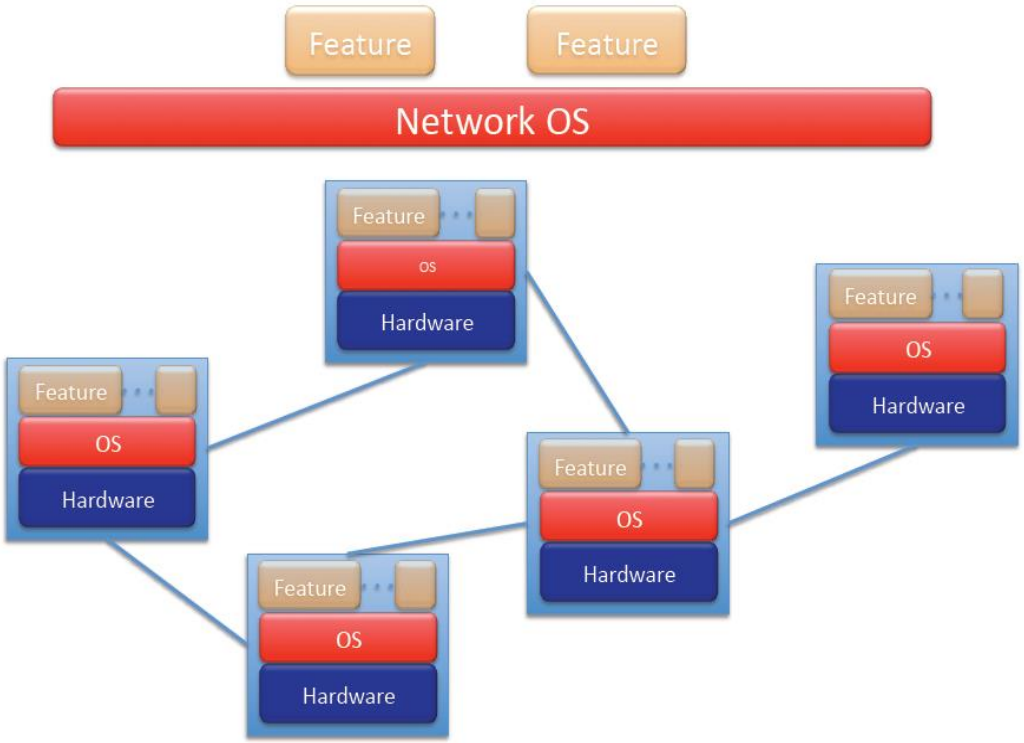
Separate Control Plane - OpenFlow Controller

- Κανόνες δρομολόγησης ανά ροή (flow)
- Συντήρηση Πινάκων Ροών (Flow Table – επίπεδα 2, 3, 4)
- Διεπαφή (Northbound API): Rest

Data Forwarding - OpenFlow Switch

- Δρομολόγηση πλαισίων 2ου επιπέδου (**L2 MAC**) ανάλογα με **ροή (flow)** επιπέδων **L2, L3, L4**
- Έλεγχος από εξωτερικό OF Controller
- Διεπαφή (Northbound API): Πρωτόκολλο OF

ΓΙΑΤΙ ΧΡΕΙΑΖΟΜΑΣΤΕ ΠΡΟΓΡΑΜΜΑΤΙΖΟΜΕΝΑ ΔΙΚΤΥΑ; (1/2)



Κάθε δικτυακός κόμβος έχει δικό του:

1. **Λειτουργικό Σύστημα (OS)**
2. **Επίπεδο προώθησης δεδομένων (forwarding plane)**
3. **Επίπεδο ελέγχου (control plane)**

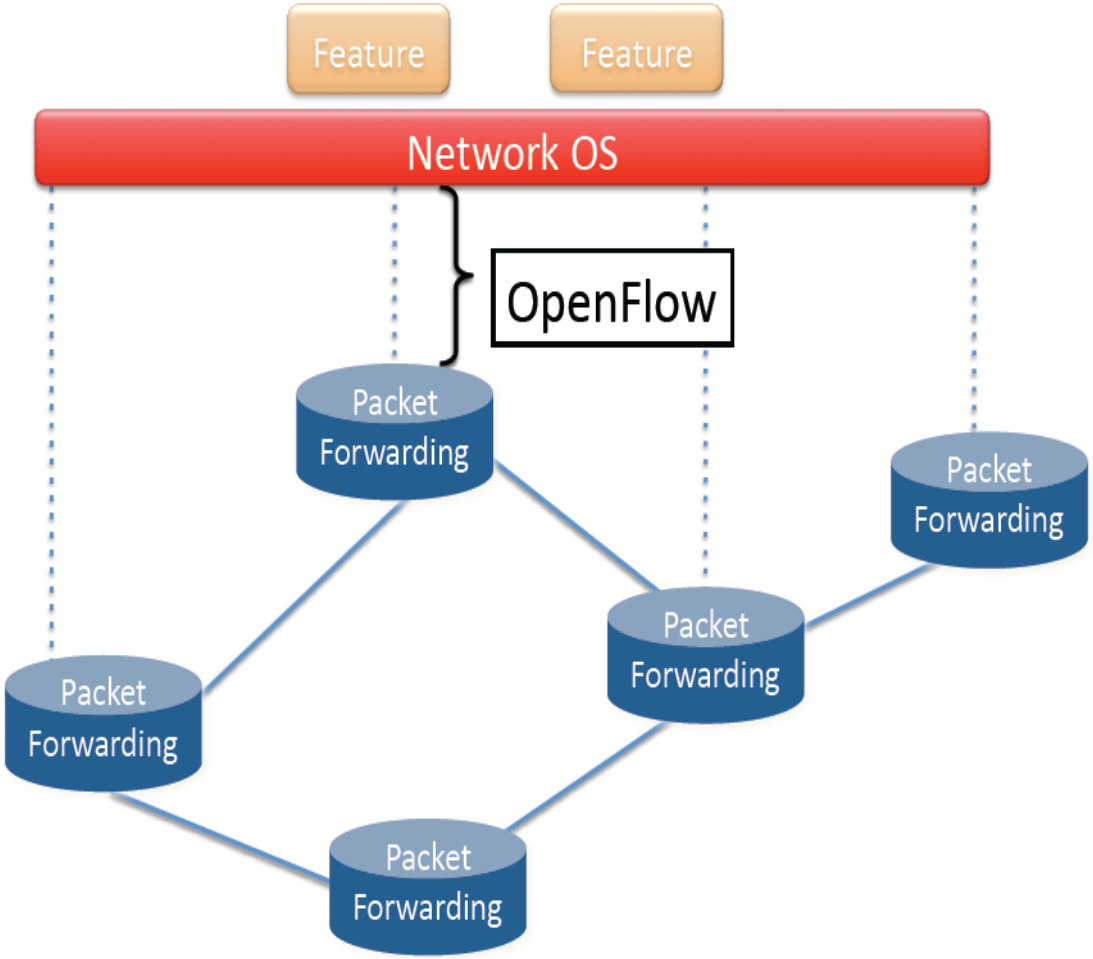
αλλά

1. **Οι αποφάσεις πρέπει να λαμβάνονται συνεργατικά**
2. **Οποιαδήποτε ειδική μεταχείριση πακέτων θα πρέπει να γίνεται ανά κόμβο (ACLs)**

+ Υψηλή Ανθεκτικότητα

- Υψηλό διαχειριστικό κόστος
- Εξάρτηση από κατασκ/στές
- Δυσκολία εφαρμογής κεντρικής πολιτικής

ΓΙΑΤΙ ΧΡΕΙΑΖΟΜΑΣΤΕ ΠΡΟΓΡΑΜΜΑΤΙΖΟΜΕΝΑ ΔΙΚΤΥΑ; (2/2)



Κάθε δικτυακός κόμβος έχει δικό του:

1. **Επίπεδο προώθησης δεδομένων (forwarding plane)**

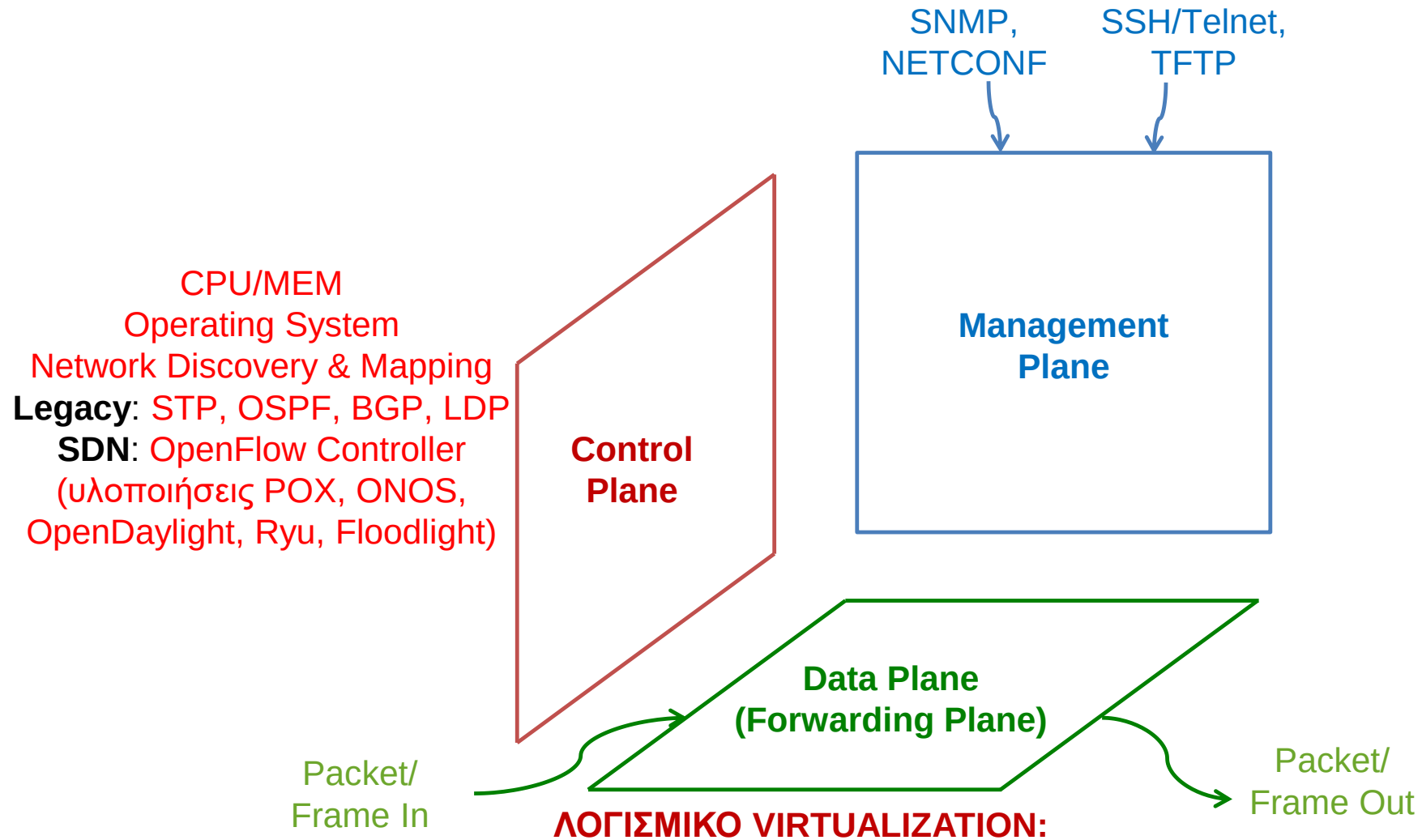
Το OS του δικτύου υλοποιεί:

1. **Κεντρικοποιημένο επίπεδο ελέγχου (control plane)**
2. **Οποιαδήποτε πολιτική ειδικής μεταχείρισης πακέτων**

- **Μειωμένη Ανθεκτικότητα**

+ Χαμηλό διαχειριστικό κόστος
+ Πολλαπλοί κατασκευαστές
+ Ευκολία εφαρμογής κεντρικής πολιτικής

ΕΠΙΠΕΔΑ ΛΕΙΤΟΥΡΓΙΑΣ ΣΕ ΠΕΡΙΒΑΛΛΟΝ OpenFlow



ΛΟΓΙΣΜΙΚΟ VIRTUALIZATION:

Network Hypervisors, Cloud Middleware (OpenStack)

Πλαίσιο Network Function Virtualization – NFV

Υλοποιήσεις Εικονικών Δικτυακών Λειτουργιών (Virtual Network Functions – VNFs)

https://en.wikipedia.org/wiki/Network_function_virtualization

http://packetpushers.net/sdn-network-virtualization-hypervisors/

ΕΥΦΥΗ – ΠΡΟΓΡΑΜΜΑΤΙΖΟΜΕΝΑ ΔΙΚΤΥΑ

Software Defined Networks (SDN) – OpenFlow Protocol

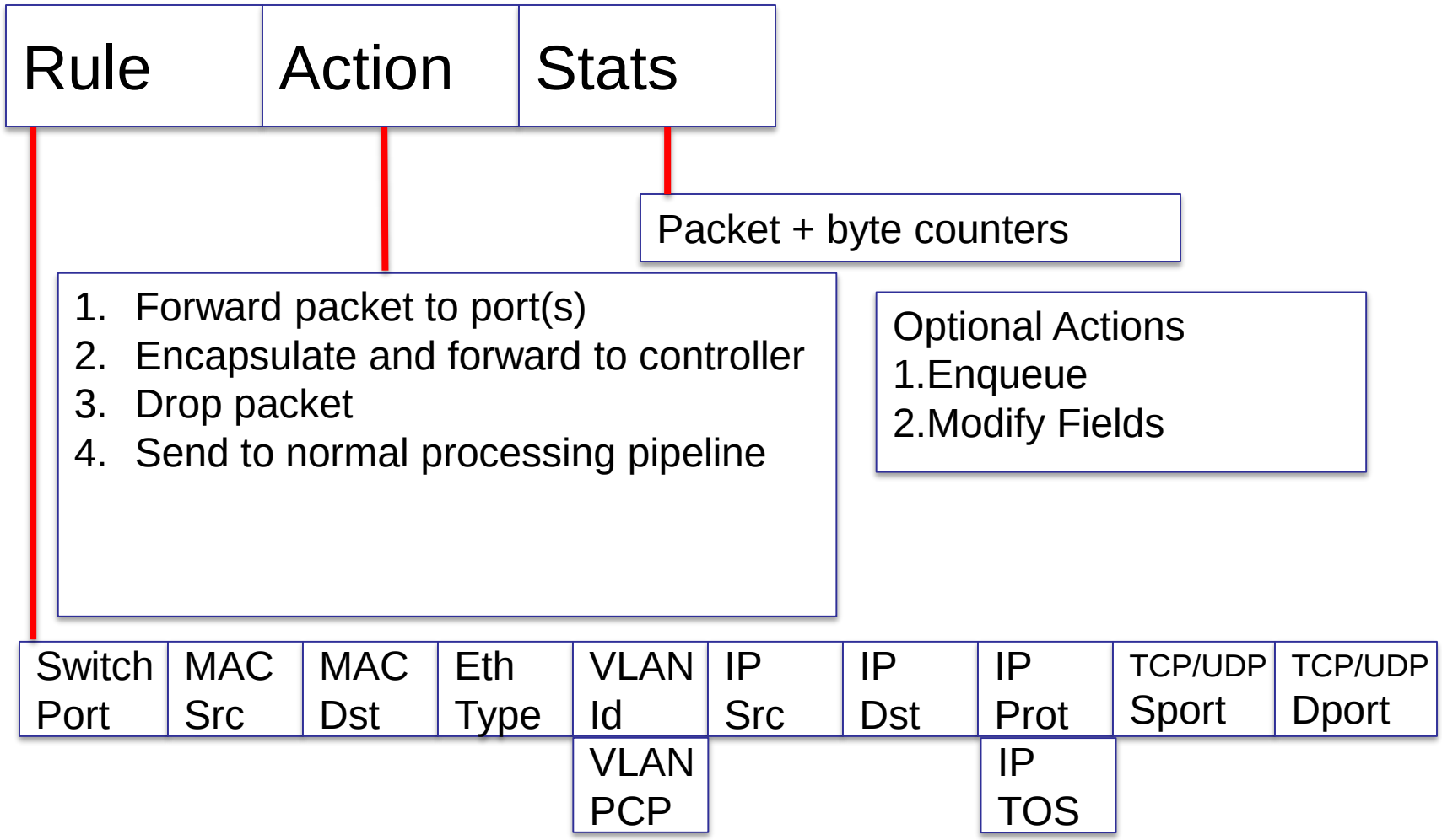
https://www.opennetworking.org

Cross-Layer Forwarding
OpenFlow 1.0 tuple

Layer 2 – Layer 4 flow rules: Cross-Layer Forwarding & Monitoring

In Port	MAC src	MAC dst	Ether type	VLAN PCP	VLAN ID	IP src	IP dst	IP Proto	IP ToS	TCP/ UDP Src	TCP/ UDP dst	Action	Count
1	26:46: 9f:12: 6a:91	f6:02: 84:d2: e4:99	0x0800	0x1	0xFFF	10.0. 0.2	10.0. 0.1	1 (ICMP)	0x00	0	0	port 3	235
*	*	*	*	*	*	5.6.7. 8	18.2. 4.9	*	*	*	80	port 1	1000
*	*	f6:02: 84:d2: e4:99	*	*	*	*	17.2. 4.9	*	*	*	22	port 2	300
4	*	*	0x0800	*	*	*	*	6 (TCP)	*	*	25	drop	892
3	00:0c: 9f:ba: 6a:91	*	0x0806	*	*	*	*	*	*	*	*	local	120
*	*	*	*	*	*	*	*	*	*	*	*	controller	11

OpenFlow v1.0



OPEN DAYLIGHT

First Code Release "Hydrogen"

VTN: Virtual Tenant Network
DOVE: Distributed Overlay Virtual Ethernet
DDoS: Distributed Denial Of Service
LISP: Locator/Identifier Separation Protocol
OVSDB: Open vSwitch DataBase protocol
BGP: Border Gateway Protocol
PCEP: Path Computation Element Communication Protocol
SNMP: Simple Network Management Protocol

Management GUI/CLI

VTN Coordinator

OpenStack Neutron

DDoS Protection

Network Applications Orchestrations & Services

OpenDaylight APIs (REST)

Base Network Service Functions

Topology Manager

Stats Manager

Switch Manager

Host Tracker

Shortest Path Forwarding

DOVE Manager

Affinity Service

Traffic Redirection

LISP Service

VTN Manager

Service Abstraction Layer (SAL)
(Plugin Manager, Capability Abstractions, Flow Programming, Inventory, etc.)

Controller Platform

OpenFlow 1.0 1.3

OVSDB

NETCONF

LISP

BGP

PCEP

SNMP

Southbound Interfaces & Protocol Plugins

OpenFlow Enabled Devices

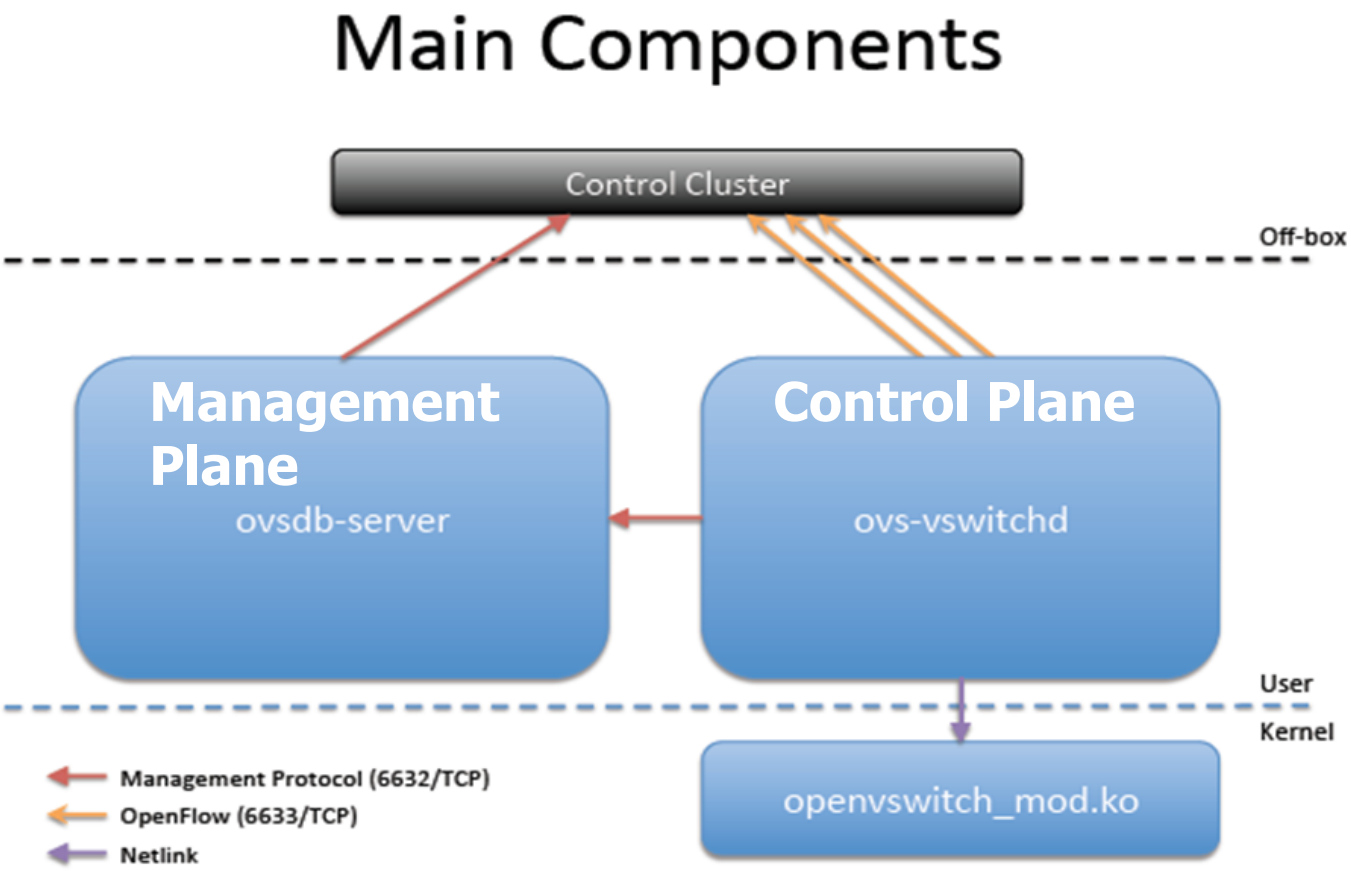
Open vSwitches

Additional Virtual & Physical Devices

Data Plane Elements (Virtual Switches, Physical Device Interfaces)

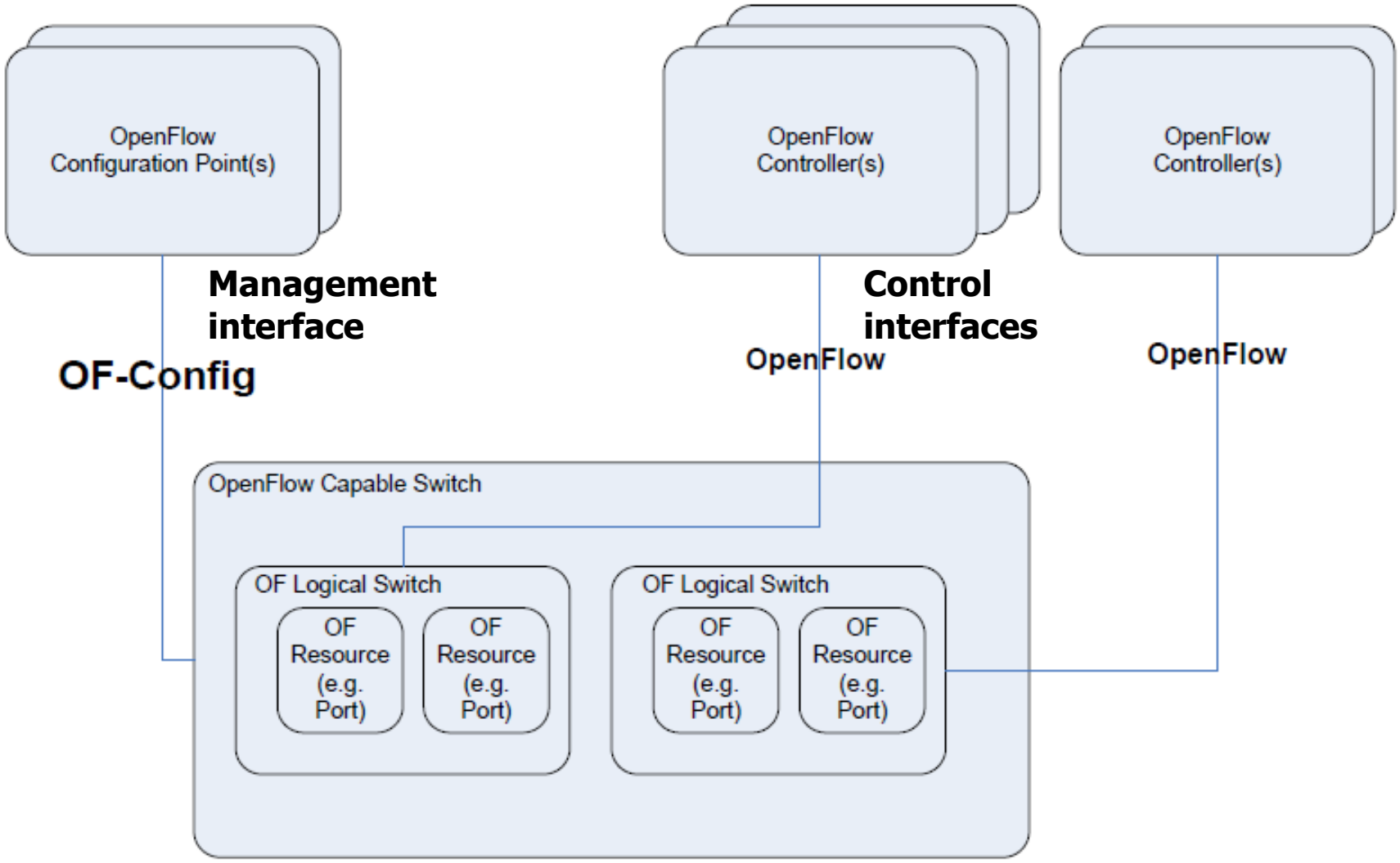
ΠΡΟΓΡΑΜΜΑΤΙΖΟΜΕΝΟΣ ΜΕΤΑΓΩΓΕΑΣ ΛΟΓΙΣΜΙΚΟΥ

Open vSwitch



ΔΙΕΠΑΦΕΣ ΕΛΕΓΧΟΥ & ΔΙΑΧΕΙΡΙΣΗΣ

Control & Management interfaces (as defined from ONF)



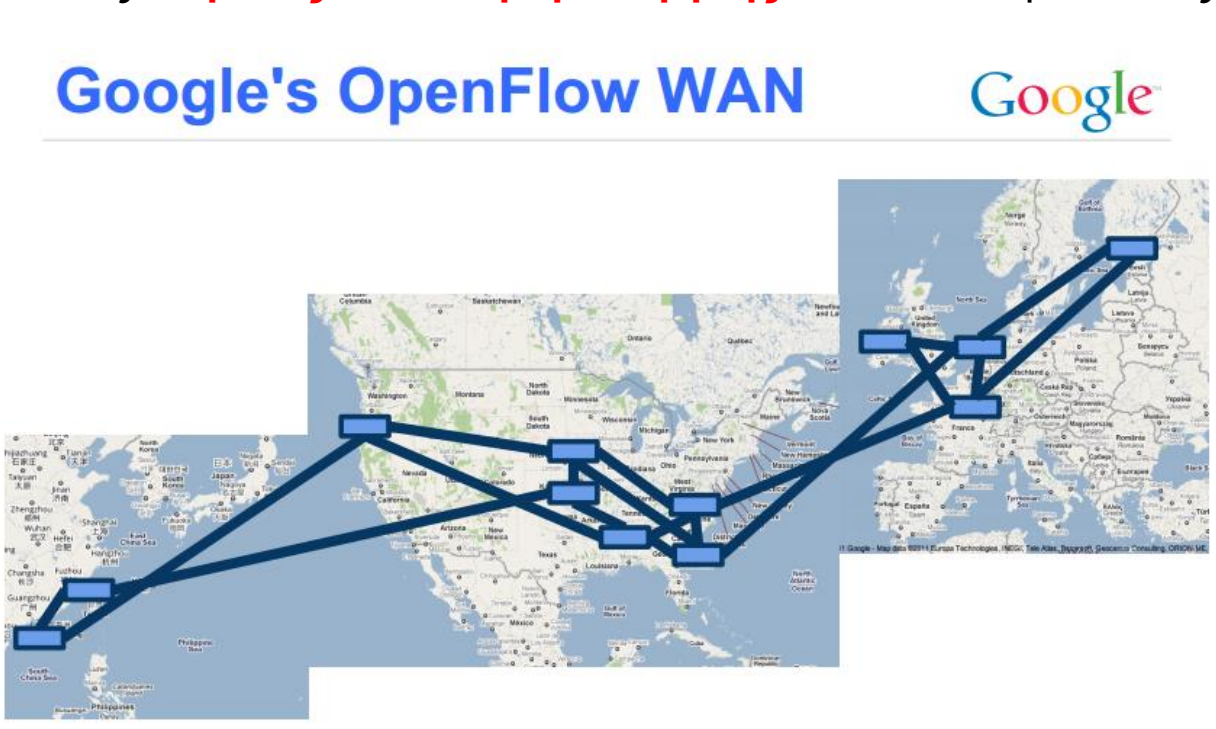
1ο ΠΑΡΑΔΕΙΓΜΑ WAN SDN:

B4 Google's OpenFLow WAN

http://www.opennetsummit.org/archives/apr12/hoelzle-tue-openflow.pdf

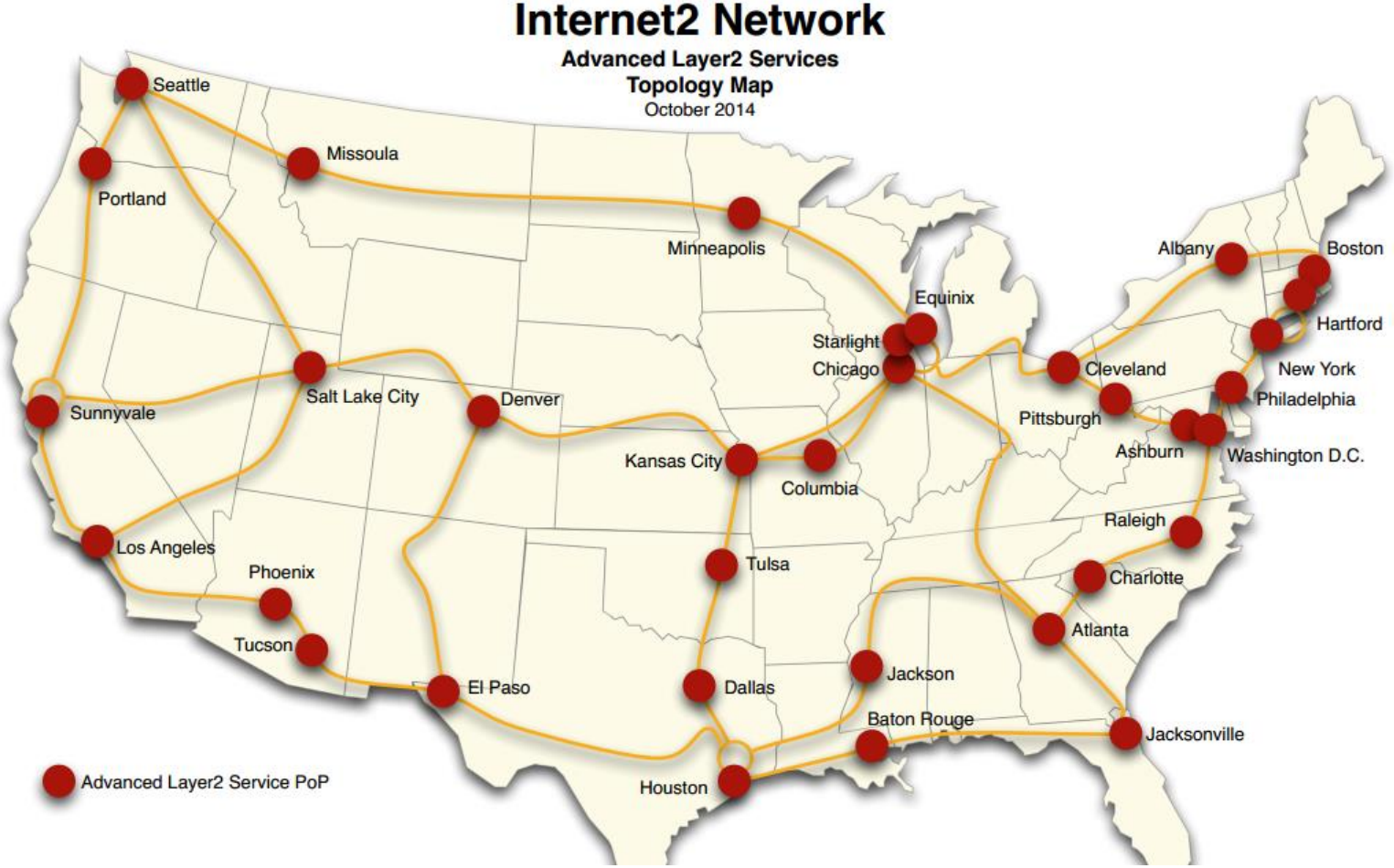
http://cseweb.ucsd.edu/~vahdat/papers/b4-sigcomm13.pdf

- **B4:** Οπτικό ιδιωτικό δίκτυο της Google μεταξύ Data Centers
- Πρόσβαση τελικών χρηστών υπηρεσιών της Google (Search Engine, Analytics, YouTube): **Μέσω ISPs & Internet Exchanges**
- Κεντρικός Έλεγχος του **B4** & Data Centers: Σαν **Single domain OpenFlow SDN**
- **OF Controllers με custom H/W**, διαλειτουργικότητα μέχρι τον τελικό κόμβο (VM)
- Αποδοτική διαχείριση δικτυακών πόρων μέσω **Centralized Traffic Engineering - TE**
- Αξιοπιστία: Πολιτικές **Ευφυούς Επαναδρομολόγησης Ροών** σε περιπτώσεις βλαβών



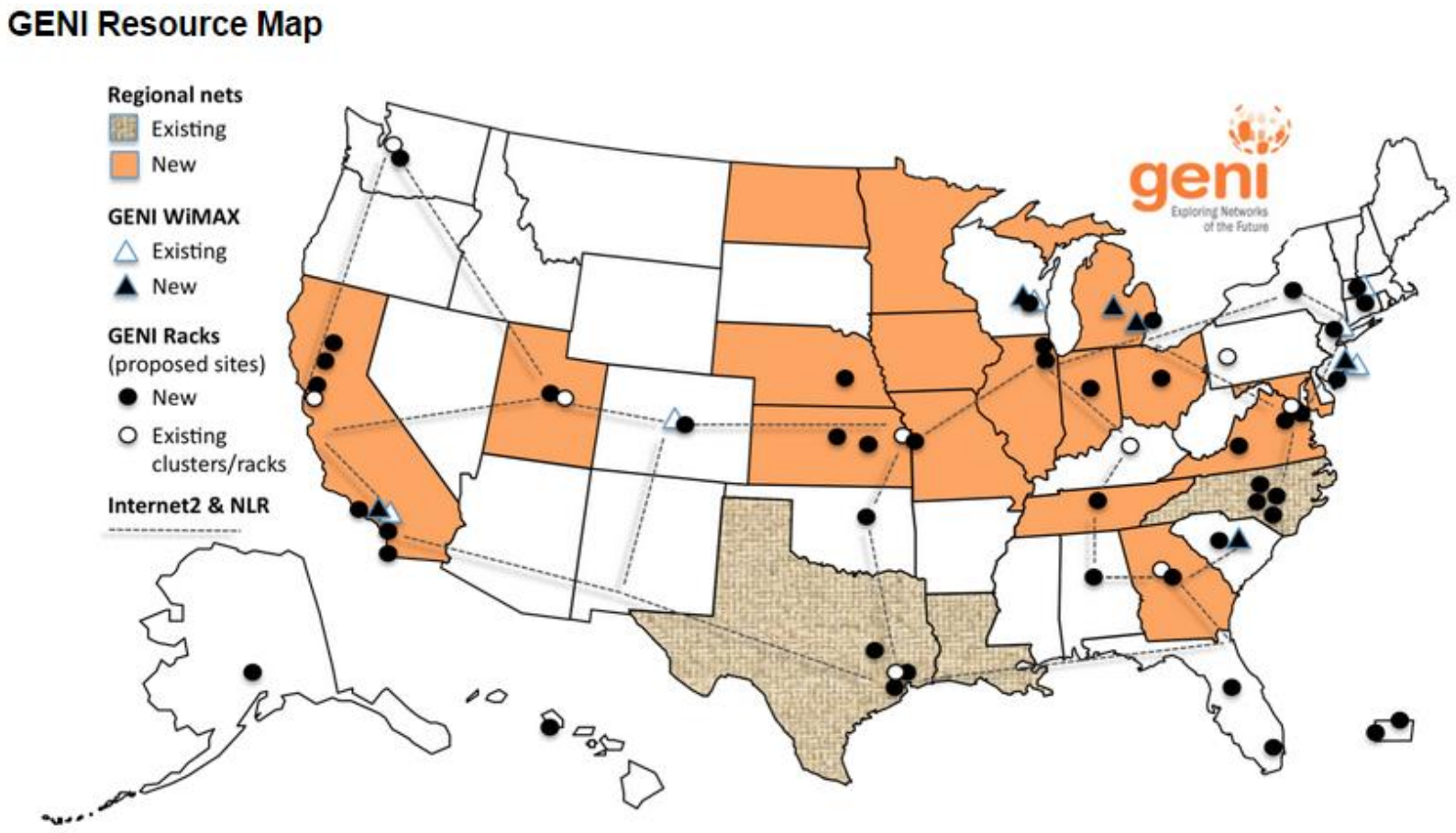
2ο ΠΑΡΑΔΕΙΓΜΑ WAN SDN:
Internet2 Advanced Layer 2 Services (AL2S)

https://noc.net.internet2.edu/i2network/advanced-layer-2-service.html



Το **Internet2** πρόσφατα απενεργοποίησε το **OpenFlow** και επανέφερε το **MPLS/TE** για παροχή κυκλωμάτων κάτω από το **IP**

3ο ΠΑΡΑΔΕΙΓΜΑ WAN SDN:
U.S. National Science Foundation (NSF)
GENI Testbeds
Global Environment for Networking Innovations
http://www.geni.net/



ΤΟ ΠΕΡΙΒΑΛΛΟΝ ΕΞΟΜΟΙΩΣΗΣ GENI
Disruptive Experiments on Future Internet Architectures (FIA)

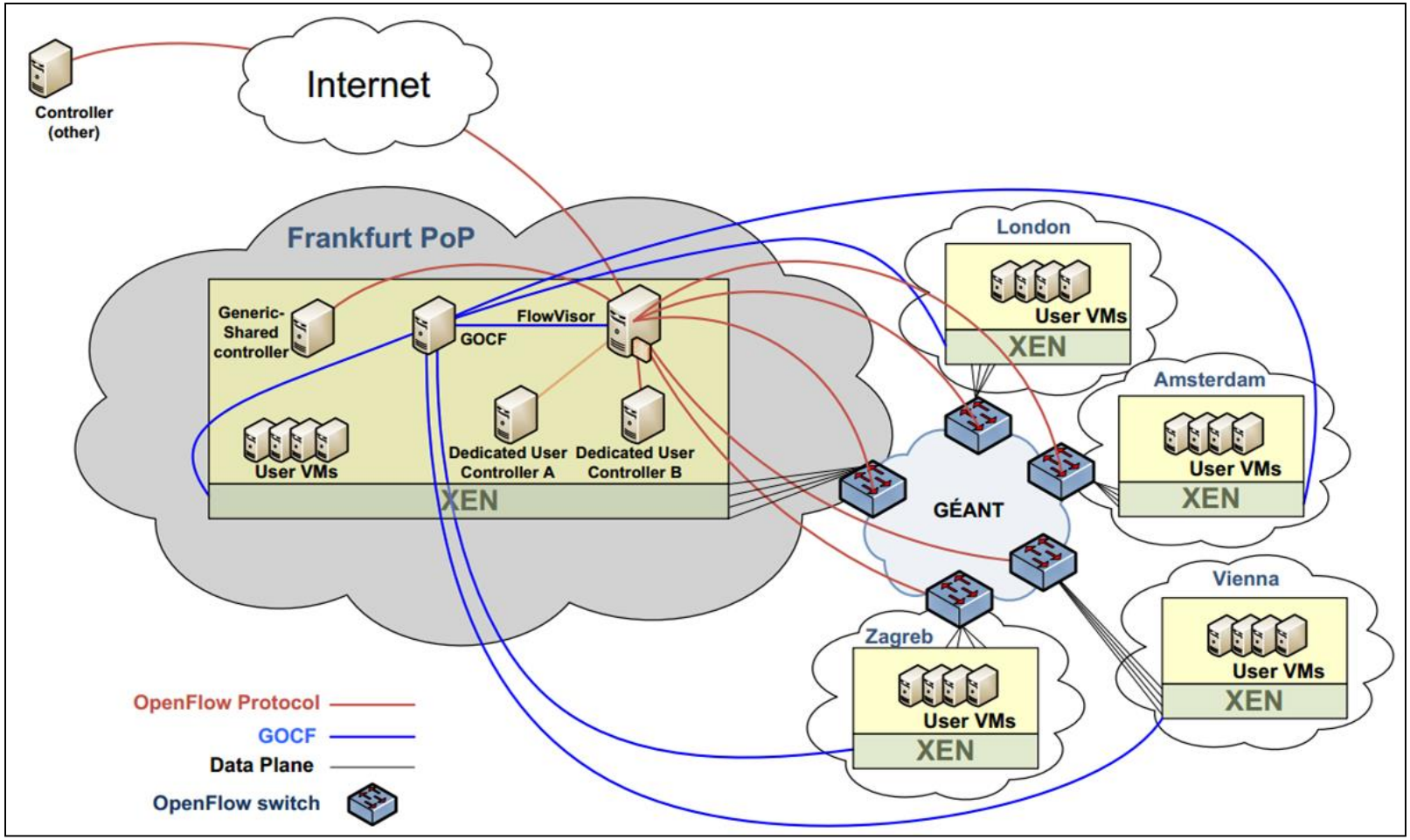
- Πρόγραμμα της US National Science Foundation (NSF) για Αρχιτεκτονικές & Πρωτόκολλα του Internet του Μέλλοντος
- Παρέχει πόρους και υπηρεσίες στην Ερευνητική Κοινότητα για εξομοίωση disruptive προτάσεων π.χ. κοινότητες εικονικών υποδομών βασισμένων σε *OpenFlow* και Ασύρματα Δίκτυα 4ης Γενιάς (*WiMax* σε licensed συχνότητες 2.5 GHz αφιερωμένες σε Educational Broadband Service – EBS, LTE;)
- Βασίζεται σε ομοσπονδία αυτόνομων εικονικών κοινοτήτων (*Aggregates*) διαχειριστικής ευθύνης Πανεπιστημίων – Ερευνητικών Κέντρων των ΗΠΑ, διασυνδεόμενων σε επίπεδο 2 (VLANs) μέσω του Internet*2 AL2S* (Advanced Layer 2 Service)
- *Υποστήριξη εκπαιδευτικών πειραματικών αναγκών σε Παγκόσμιο επίπεδο*
- *Το Ε.Μ.Π. από τα πρώτα ΑΕΙ εκτός ΗΠΑ που εγκαινίασε την υπερατλαντική χρήση εικονικών υποδομών του GENI το 2014*
- *Συμφωνία για Single-Sign-On Authentication χρηστών του LDAP* ***user@ntua.gr*** *με την Αμερικάνικη Εκπαιδευτική Ομοσπονδία EDUCAUSE*

ΕΥΧΑΡΙΣΤΙΕΣ
Credits

- ***Vicrag Thomas*** < 2018 GENI Project Office – BBN, Cambridge, Mass, USA
- ***Niky Riga (Νίκη Ρήγα)*** FaceBook Inc. San Francisco Bay, USA (<2016 GENI Project Office)
- ***Θανάσης Δουίτσης*** Κέντρο Δικτύων Ε.Μ.Π.

GÉANT OpenFlow Facility (GOF)

Υποστήριξη από GRNET/ΕΔΕΤ & NETMODE



Παράδειγμα Πειραματικής Διάταξης στο NETMODE @ NTUA Tetsbed:

Scalable DDoS Attack – Mitigation