ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ - NETWORK MANAGEMENT

Εισαγωγή - Introduction

Πρότυπο τριών Διαστάσεων Λειτουργίας - Network Operation Planes

Μοντέλο Διαχείρισης FCAPS - ISO Telecommunications Management Model

Το Δίκτυο του Ε.Μ.Π. - NTUA LAN

Περιβάλλον Εργαστηριακών Ασκήσεων - Laboratory Setup

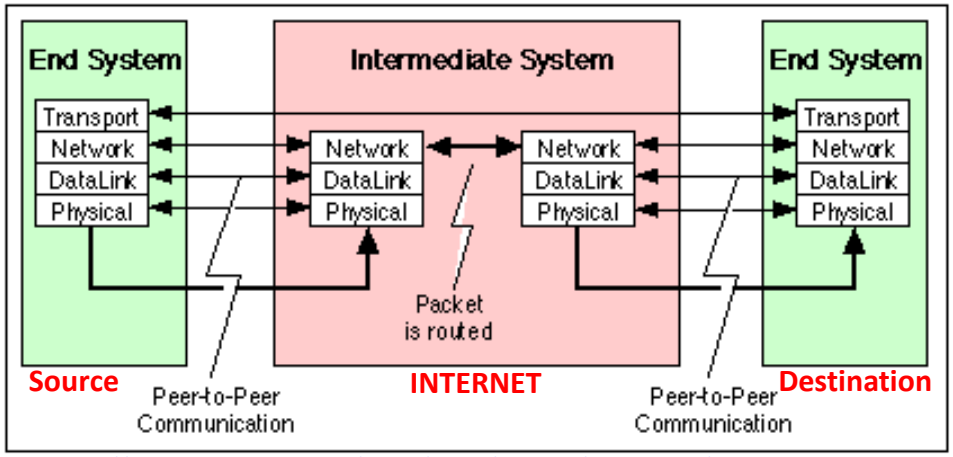
Β. Μάγκλαρης

maglaris@netmode.ntua.gr

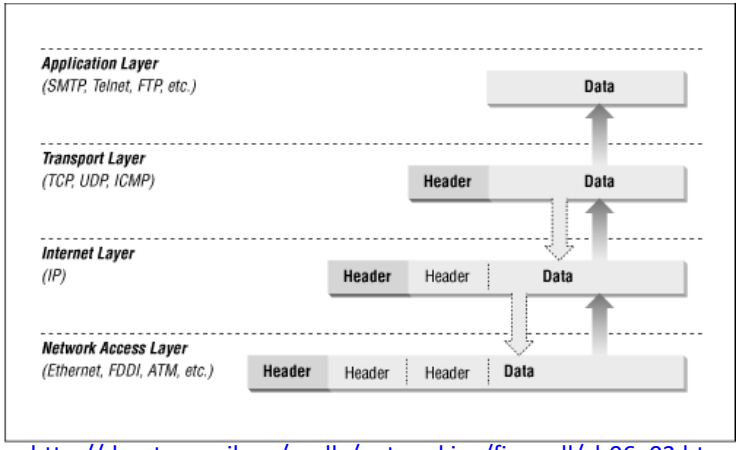
www.netmode.ntua.gr

11/10/2021

ΣΤΟΙΒΑ ΠΡΩΤΟΚΟΛΛΩΝ TCP/IP ΣΤΟ INTERNET



http://www.erg.abdn.ac.uk/users/gorry/eg3567/inet-pages/transport.html

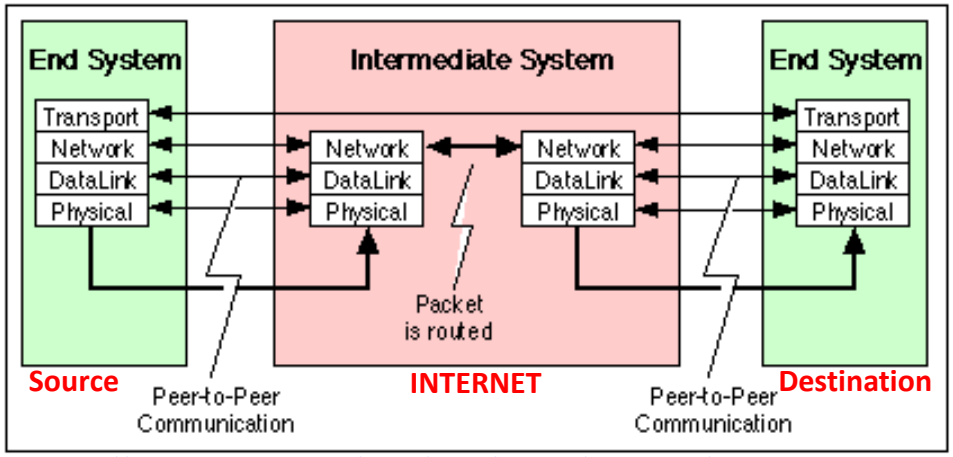


http://docstore.mik.ua/orelly/networking/firewall/ch06_03.htm

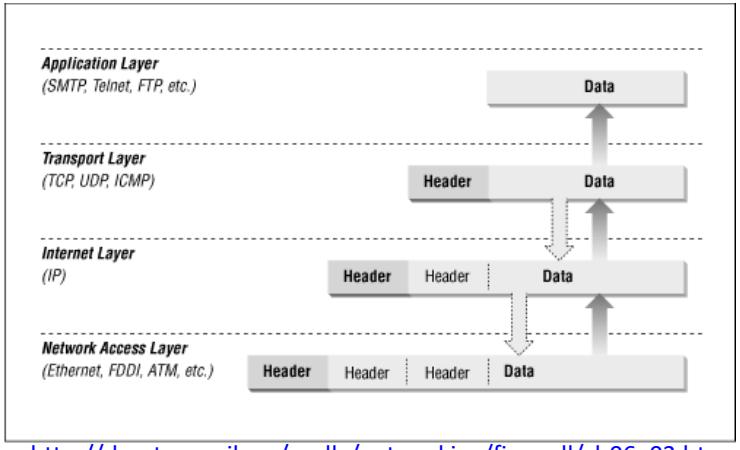
Σε ένα δίκτυο υπολογιστών αρχιτεκτονικής ***Internet***:

- Τα δύο άκρα (source - destination) υλοποιούν εφαρμογές (applications) με συνεργατικό τρόπο (π.χ. *Simple Mail Transfer Protocol - SMTP* για e-mail) μέσω ανταλλαγής κωδικοποιημένων ψηφιακών μηνυμάτων, τεμαχισμένα σε **πακέτα** που προωθούνται αυτόνομα στο Internet
- Για την διάφανη και αξιόπιστη υλοποίηση της επικοινωνίας, τα δύο άκρα υλοποιούν διαδικασίες **πρωτοκόλλων peer-to-peer** σε πολλαπλά στρώματα (layers) που καθιστούν συμβατές τις επιμέρους εφαρμογές, ανεξάρτητα από λειτουργικά συστήματα, κατασκευαστή και λεπτομέρειες υλοποίησης (π.χ. *Transport Layer, TCP/UDP/ICMP*)
- Η υλοποίηση γίνεται με την διαδοχική ενθυλάκωση των **πακέτων** σε φακέλους (onion skin model) με επικεφαλίδες που επιτρέπουν την συμβατή προώθηση στα δίκτυα επικοινωνιών, χωρίς γνώση του περιεχόμενού τους (π.χ. *Internet Layer*, αλγόριθμος δρομολόγησης - routing με βάση τις διευθύνσεις *IP* των δυο άκρων)
- Στα χαμηλότερα στρώματα γίνεται η αξιόπιστη και αποδοτική πρόσβαση στο φυσικό μέσο (*PHY*) των ενδιαμέσων δικτύων, συμπεριλαμβανόμενης της διαμόρφωσης του ψηφιακού μηνύματος σε σήματα (ηλεκτρικά, οπτικά, ηλεκτρομαγνητικά) ανάλογα με τα χαρακτηριστικά του μέσου (π.χ. *Network Access Layer = Data Link & Physical Layers*: Αλγόριθμοι πρόσβασης Ethernet, *διαμόρφωση - modulation*, *πολυπλεξία – multiplexing)*
- Από τα επίπεδα πρωτοκόλλων τα τρία πρώτα (***Physical, Data Link & Network***) αφορούν στις ενδιάμεσες δικτυακές υποδομές (switches, routers) που μπορεί να τροποποιούν τις επικεφαλίδες ανάλογα με τις προδιαγραφές των δικτύων. Οι επικεφαλίδες ***Transport*** (TCP/UDP/ICMP) και το αρχικό περιεχόμενο των πακέτων (***payload***) αφορούν μόνο τις τελικές εφαρμογές και διαπερνούν διαφανώς τις ενδιάμεσες δικτυακές διασυνδέσεις

ΣΤΟΙΒΑ ΠΡΩΤΟΚΟΛΛΩΝ TCP/IP ΣΤΟ INTERNET



http://www.erg.abdn.ac.uk/users/gorry/eg3567/inet-pages/transport.html



http://docstore.mik.ua/orelly/networking/firewall/ch06_03.htm

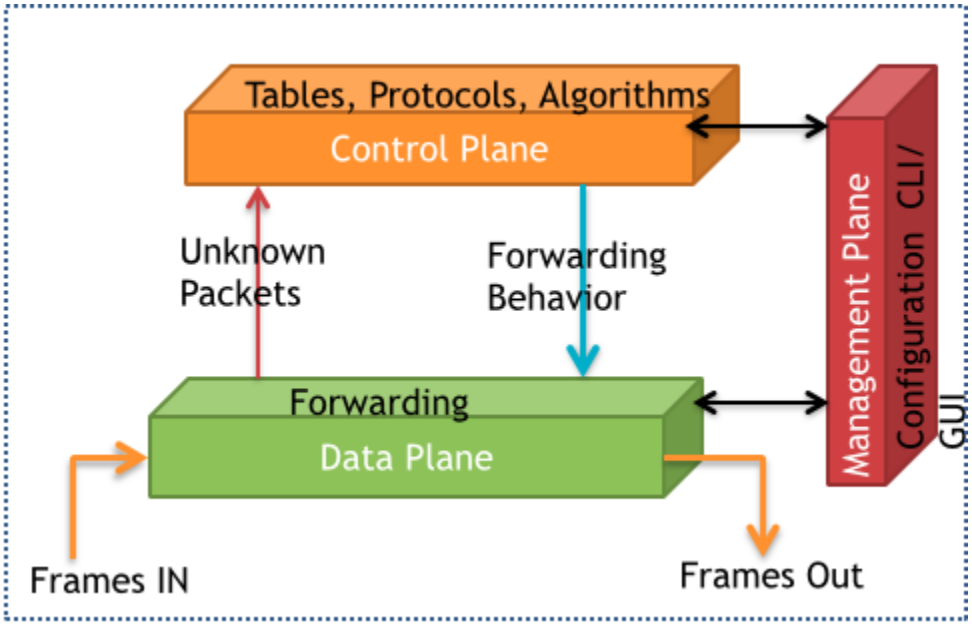
Σε ένα δίκτυο υπολογιστών αρχιτεκτονικής ***Internet***:

- Τα δύο άκρα (source - destination) υλοποιούν εφαρμογές (applications) με συνεργατικό τρόπο (π.χ. *Simple Mail Transfer Protocol - SMTP* για e-mail) μέσω ανταλλαγής κωδικοποιημένων ψηφιακών μηνυμάτων, τεμαχισμένα σε **πακέτα** που προωθούνται αυτόνομα στο Internet
- Για την διάφανη και αξιόπιστη υλοποίηση της επικοινωνίας, τα δύο άκρα υλοποιούν διαδικασίες **πρωτοκόλλων peer-to-peer** σε πολλαπλά στρώματα (layers) που καθιστούν συμβατές τις επιμέρους εφαρμογές, ανεξάρτητα από λειτουργικά συστήματα, κατασκευαστή και λεπτομέρειες υλοποίησης (π.χ. *Transport Layer, TCP/UDP/ICMP*)
- Η υλοποίηση γίνεται με την διαδοχική ενθυλάκωση των **πακέτων** σε φακέλους (onion skin model) με επικεφαλίδες που επιτρέπουν την συμβατή προώθηση στα δίκτυα επικοινωνιών, χωρίς γνώση του περιεχόμενού τους (π.χ. *Internet Layer*, αλγόριθμος δρομολόγησης - routing με βάση τις διευθύνσεις *IP* των δυο άκρων)
- Στα χαμηλότερα στρώματα γίνεται η αξιόπιστη και αποδοτική πρόσβαση στο φυσικό μέσο (*PHY*) των ενδιαμέσων δικτύων, συμπεριλαμβανόμενης της διαμόρφωσης του ψηφιακού μηνύματος σε σήματα (ηλεκτρικά, οπτικά, ηλεκτρομαγνητικά) ανάλογα με τα χαρακτηριστικά του μέσου (π.χ. *Network Access Layer = Data Link & Physical Layers*: Αλγόριθμοι πρόσβασης Ethernet, *διαμόρφωση - modulation*, *πολυπλεξία – multiplexing)*
- Από τα επίπεδα πρωτοκόλλων τα τρία πρώτα (***Physical, Data Link & Network***) αφορούν στις ενδιάμεσες δικτυακές υποδομές (switches, routers) που μπορεί να τροποποιούν τις επικεφαλίδες ανάλογα με τις προδιαγραφές των δικτύων. Οι επικεφαλίδες ***Transport*** (TCP/UDP/ICMP) και το αρχικό περιεχόμενο των πακέτων (***payload***) αφορούν μόνο τις τελικές εφαρμογές και διαπερνούν διαφανώς τις ενδιάμεσες δικτυακές διασυνδέσεις

Αναλογία με πρωτόκολλα συνεννόησης μεταξύ δυο στελεχών ενός οργανισμού, τοποθετημένων σε απομακρυσμένες εγκαταστάσεις:

- Στο υψηλότερο επίπεδο τα στελέχη ενδιαφέρονται για το περιεχόμενο του μηνύματος και όχι τη μορφοποίηση ή τη διαδικασία μεταφοράς του
- Το μήνυμα κωδικοποιείται από τη γραμματεία σε μορφή συμβατή με το πρωτόκολλο του οργανισμού
- Η υπηρεσία διακίνησης εγγράφων το τοποθετεί σε σφραγισμένο φάκελο με τη διεύθυνση προορισμού
- Στο χαμηλότερο (φυσικό) επίπεδο το μήνυμα διαβιβάζεται μέσω του δικτύου ταχυδρομικών υπηρεσιών

ΣΧΗΜΑΤΙΚΗ ΠΑΡΑΣΤΑΣΗ ΤΡΙΣΔΙΑΣΤΑΤΩΝ ΛΕΙΤΟΥΡΓΙΩΝ ΔΙΚΤΥΟΥ



https://thenewstack.io/defining-software-defined-networking-part-1/

Data Plane: Μετάδοση - Προώθηση Δεδομένων σε Πλαίσια/Frames ή Πακέτα
Control Plane: Έλεγχος - Σηματοδοσία Ροής Πακέτων Δεδομένων
Management Plane: Διαχειριστικές Λειτουργίες Δικτύου

ΠΡΟΤΥΠΟ ΤΡΙΩΝ ΔΙΑΣΤΑΣΕΩΝ (1/3)

Διάσταση Μετάδοσης Δεδομένων - Data (forwarding) Plane

- Πολυπλεξία στο φυσικό επίπεδο:
  - Διαμόρφωση πλαισίων TDM: ITU-T SDH/GFP framing (από STM-1=155 Mbps → STM-*n*, εφεδρεία ring protection, virtual concatenation (150 Mbps VC-4, 1 Gbps VC-4-7v = 7 x VC-4)
  - Optical Digital Wrapper (ITU-T G.709: 2.5, 10, 40, 100 Gbps, Forward Error Correction - FEC)
- Κωδικοποίηση σε πακέτα Ethernet, WiFi (IEEE 802.11), MPLS, IP
- Προώθηση (forwarding) δεδομένων σε μεταγωγείς (switches) & δρομολογητές (routers)
- Προς αρχιτεκτονικές Programmable Data-Plane: Ευφυής πολύ-επίπεδη επεξεργασία πακέτων εντός του Δικτύου Μετάδοσης Δεδομένων (in-network processing) για μετρήσεις (***monitoring***, ***in-network telemetry - INT***) και προώθηση (***forwarding***)
  - Προτεινόμενη Γλώσσα Προγραμματισμού Ειδικού Σκοπού (Domain Specific Language - ***DSL***): ***P4*** (***P***rogramming ***P***rotocol-Independent ***P***acket ***P***rocessors) σε συμβατούς μεταγωγείς ή software emulated routers ή με χρήση προγραμματιζόμενου hardware – FPGA boards
  - Προτεινόμενη Γλώσσα σε Διεπαφές (Smart Network Interface Cards - NIC): ***XDP*** (e***X***press ***D***ata ***P***ath) για Linux servers (restricted C, δημοφιλής σε μεγάλα Data Centers)

ΠΡΟΤΥΠΟ ΤΡΙΩΝ ΔΙΑΣΤΑΣΕΩΝ (2/3)

Διάσταση Ελέγχου - Control Plane

- ***In-band Signaling***: Σηματοδοσία ενσωματωμένη σε επικεφαλίδες πακέτων: IP headers, MPLS labels, VLAN tags
  - Ξεχωριστά μηνύματα / πακέτα ελέγχου για σύνταξη πινάκων δρομολόγησης (Interior Gateway Protocol – IGP, Exterior/Border Gateway Protocol – EGP/BGP)
  - Πακέτα ελέγχου «υγείας» του δικτύου – ICMP/ping/traceroute
  - Μηνύματα σηματοδοσίας για αποκατάσταση μονοπατιού – path (RSVP, LDP) & αντιστοίχηση επικεφαλίδων (*labels*) σε γραμμές MPLS
  - Σηματοδοσία αντιστοίχησης time slots (ή χρώματος) σε γραμμές SDH (ή WDM)
  - Πρωτόκολλα ARP & DNS, αντιστοίχηση VLAN tags….

- ***Out-of band Signaling***: Εξαγωγή των λειτουργιών ελέγχου εκτός μηχανισμών μετάδοσης, εξωτερικές βάσεις δεδομένων και εφαρμογές ***ευφυούς δικτύου***:
  - Ψηφιακή τηλεφωνία: Σηματοδοσία Common Channel Signalling CCS7, ***Intelligent Networks***
  - Προγραμματιζόμενα ευφυή δίκτυα νέας γενιάς (user programmable networks): ***Software Defined Networks - SDN***
  - Πρωτόκολλο ***OpenFlow*** σηματοδοσίας μεταγωγέα (***switch***) και ελεγκτή (***controller***) → ***Programmable Data-Planes***, ***P4***

ΠΡΟΤΥΠΟ ΤΡΙΩΝ ΔΙΑΣΤΑΣΕΩΝ (3/3)

Διάσταση Διαχείρισης - Management Plane

- Υλοποίηση πολιτικών διαχείρισης: Οδηγίες προς Data Plane μέσω σηματοδοσίας Control Plane
- Παραδοσιακό Μοντέλο Διαχειριστικών Λειτουργιών ISO/OSI: ***FCAPS*** (***F***ault, ***C***onfiguration, ***A***ccounting, ***P***erformance, ***S***ecurity)
- Δραματικά αυξανόμενη πολυπλοκότητα διαχείρισης υποδομών:
  - Τοπικά Δίκτυα (***LAN***), Μητροπολιτικά Δίκτυα (***MAN***), Δίκτυα Κορμού Ευρείας Περιοχής (***WAN***), Sensor Networks - Internet of Things (***IoT***), Data Centers, Clouds, Content Delivery Networks (***CDN***)
  - Σταθερής (Fixed Optical/Copper/Microwave) και κινητής τοπολογίας (4G, 5G Mobile Networks)
  - Ανάγκη ενοποιημένων και ευέλικτων πλατφορμών διαχείρισης, φιλικών προς το Διαχειριστή
- Ανάγκη μετάβασης προς ευφυές περιβάλλον ***NetDevOps***:
  - Αναφορά σε ***Data Models*** (***YANG***…), χρήση κατάλληλων εργαλείων διαχείρισης βάσεων δεδομένων (NoSQL, Elasticsearch Logstash Kibana – ***ELK***…)
  - Από εργαλεία Command-Line Interface (***CLI***) → Application Programming Interfaces (***API***) σε εξυπηρετητές ***Linux***
  - Από SNMP/SMI → ***NETCONF/YANG***
  - Automation - Templates (***Ansible***…)
  - Vendor Independence (Network Function Virtualization - ***NFV***)
  - Network Programmability (Network Operating Systems, Software Defined Networks - ***SDN***)
  - Χρήση αλγορίθμων Μηχανικής Μάθησης (***Machine Learning***) και συνεργατικών πολιτικών για αντιμετώπιση κυβερνο-επιθέσεων (sharing attack datasets, συνεργαζόμενα συστήματα intrusion detection/mitigation με περιορισμούς λόγω privacy…)

Τυποποίηση διάρθρωσης εξοπλισμού και λειτουργιών μέσω εξειδίκευσης data models

ΔΙΑΧΕΙΡΙΣΤΙΚΟ ΜΟΝΤΕΛΟ ΑΝΑΦΟΡΑΣ FCAPS (ISO – OSI)

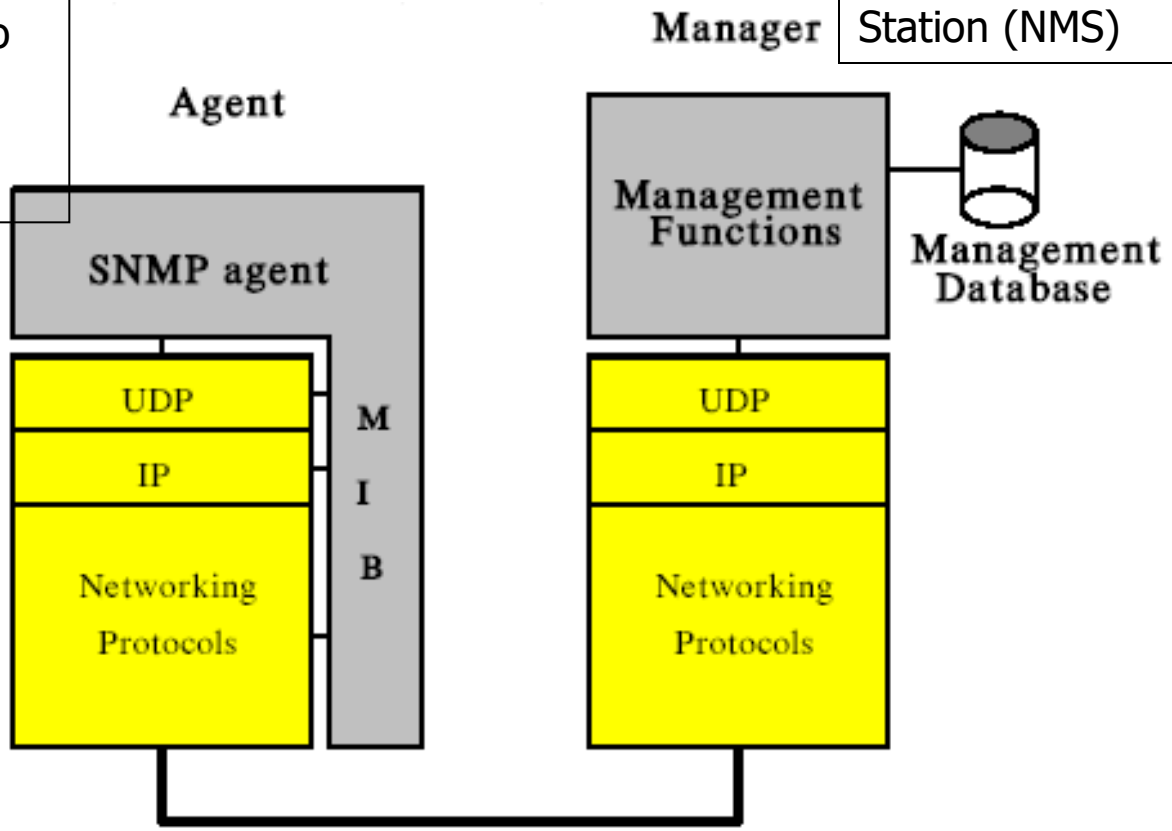
- **F**ault Management (Διαχείριση Βλαβών)
- **C**onfiguration Management (Διαχείριση Διάρθρωσης)
- **A**ccounting Management (Λογιστική Διαχείριση)
- **P**erformance Management (Διαχείριση Επιδόσεων)
- **S**ecurity Management (Διαχείριση Ασφαλείας)

ΠΑΡΑΔΟΣΙΑΚΗ ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΔΙΑΧΕΙΡΙΣΗΣ SNMP

(Simple Network Management Protocol)

Σύστημα συνδεμένο στο δίκτυο που μπορεί να εκτελεί οποιαδήποτε εργασία

Network Management Station (NMS)



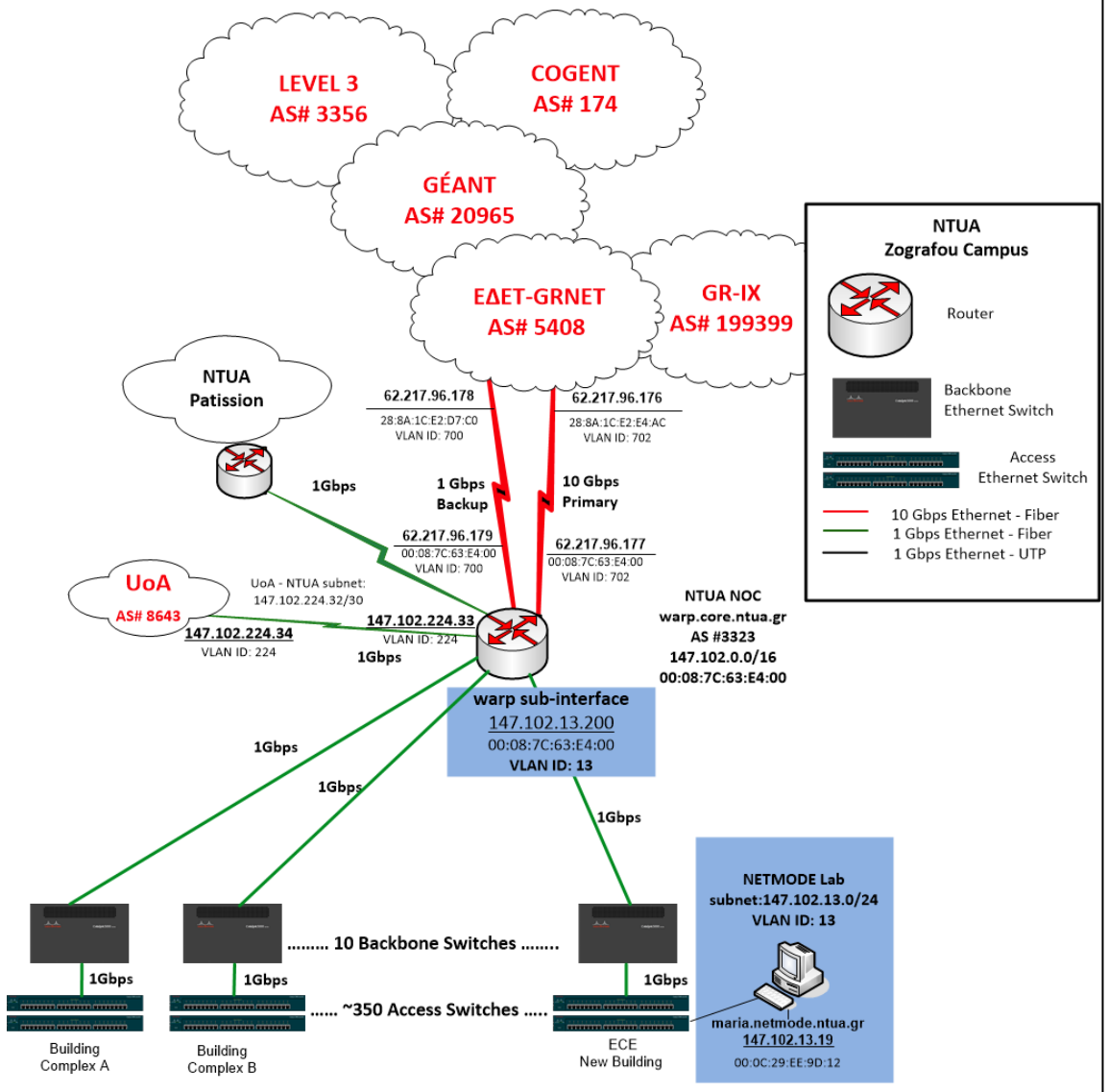
Κλήση SNMP (CLI)

Απάντηση στην ερώτηση

Ασύγχρονο μήνυμα (Trap) προς το manager

ΤΟ ΔΙΚΤΥΟ ΤΟΥ Ε.Μ.Π. (2016 – Collapsed Backbone)

ntua.gr (147.102.0.0/16, 2001:648:2000::/48, AS# 3323)



- **Αρχική Στάδιο (1994)**: Distributed Topology με 50+ IP Routers, κοντά στα υποδίκτυα. Η εσωτερική και εξωτερική δρομολόγηση γινόταν σε επίπεδο 3 (IP). Γειτονικοί τελικοί χρήστες του ιδίου υποδικτύου Ethernet μπορούσαν να επικοινωνήσουν σε επίπεδο 2 (Medium Access Control - MAC)
- **Ενδιάμεσο Στάδιο**: Collapsed Backbone Topology, αστέρας με δενδρική διασύνδεση τελικών υποδικτύων μέσω ενδιάμεσων διαφανών μεταγωγέων (Ethernet Switches) και δρομολόγηση εντός υποδικτύου σε επίπεδο 2 σαν Virtual LANs (VLAN), χωρίς περιορισμούς φυσικής γειτνίασης. Έχουν διαμορφωθεί από το Κέντρο Διαχείρισης (ΚΕΔ) – Network Operation Center (NOC) πάνω από 200 VLANs. Η δρομολόγηση σε επίπεδο 3 (IP) γίνεται στο κεντρικό σύστημα για κίνηση μεταξύ VLANs και με το Internet
- **Σύγχρονη Τάση**: Τεχνολογία Data Center με Extended VLANs (VXLAN) επιπέδου 2 διαμορφωμένα σαν Ethernet VPNs (EVPN) overlays πάνω από εικονικά υποδίκτυα IP (IP Virtual Private Network – VPN)

ΕΡΓΑΣΤΗΡΙΑΚΟ ΠΕΡΙΒΑΛΛΟΝ ΜΑΘΗΜΑΤΟΣ (2016)