

ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ - NETWORK MANAGEMENT

**Εξέλιξη & Σύγκλιση Διαδικτυακών Υποδομών -
Evolution of Converged Internet Infrastructures**

**Ενοποιημένες Εικονικές Υποδομές - Virtualization
Ανωνυμία, Πρωτόκολλα Tor - The onion router, Dark Web
Σύγκλιση Επικοινωνιών - Fixed Mobile Convergence
IP Integrated Networks, Internet of Things (IoT)**

B. Μάγκλαρης

maglaris@netmode.ntua.gr

www.netmode.ntua.gr

9/12/2024

ΕΠΙΠΕΔΟ ΕΛΕΓΧΟΥ - Control Plane (1/4) (επανάληψη)

Κατανομή Καναλιού & Δρομολόγηση Circuit Switching

- Σηματοδοσία **Channel Associated Signaling - CAS** (π.χ. ψηφιακή τηλεφωνία + υπηρεσίες call forwarding, caller ID...)
- Σηματοδοσία κοινού καναλιού **Common Channel Signaling - CCS**, ανεξάρτητη από την δρομολόγηση της υπό έλεγχο κλήσης

Ψηφιακή πρόσβαση Integrated Services Digital Network - ISDN

- **Συγχρονισμός** χρονικού πλαισίου (**TDM** frame synchronization): επαναλήψεις κάθε **125 μsec**
- **Πολυπλεξία** καναλιών **B** σύγχρονης μετάδοσης φωνής (PCM @ 64 Kbps FDX) και Καναλιού **D** σηματοδοσίας (FDX) - μπορεί να μεταδίδει και ασύγχρονα πακέτα δεδομένων
- **2B+D, Basic Rate Interface (BRI) @ 144 Kbps FDX**: **2B** κανάλια PCM @ 64 Kbps, **1D** κοινό κανάλι σηματοδοσίας @ 16 Kbps
- **30B+D, Primary Rate Interface (PRI) @ 2 Mbps FDX**: **30B** κανάλια PCM @ 64 Kbps, **1D** κοινό κανάλι σηματοδοσίας @ 64 Kbps

Πρωτόκολλο Signaling System 7 - SS7

- Έλεγχος διασύνδεσης παρόχων ψηφιακής τηλεφωνίας, περιαγωγή λειτουργιών ευφυούς δικτύου (**Intelligent Networks**) μέσω ξεχωριστών υποδικτύων σηματοδοσίας
- **Common Channel Signaling – CCS Networks** (π.χ. διεθνής περιαγωγή – roaming κινητής τηλεφωνίας GSM)

ΕΠΙΠΕΔΟ ΕΛΕΓΧΟΥ - Control Plane (2/4) (επανάληψη)

Σηματοδοσία ελέγχου μεταγωγής - δρομολόγησης - δέσμευσης πόρων ενσωματωμένες σε πακέτα TCP/IP στο data-plane

- Σηματοδοσία με μορφή πεδίων επικεφαλίδων (π.χ. πεδία επικεφαλίδων Ethernet, TCP/IP, MPLS) στα υπό έλεγχο πακέτα δεδομένων (τύπου **associated in-band signaling**)
- Αυτόνομα πακέτα υλοποίησης πρωτοκόλλων (π.χ. DNS, ARP, δρομολόγησης IGP/BGP) διακινούμενα μαζί με πακέτα δεδομένων (**in-band signaling**)
- Σηματοδοσία για video - voice conference over IP: ITU/T H323 (Multi-Conference Unit, MCU), **SIP** (Session Initiation Protocol, IETF RFC 4579...)

Σηματοδοσία για Ευφυή Προγραμματιζόμενα Δίκτυα Νέας Γενιάς (Software Defined Networking - SDN)

- Έλεγχος συνυπαρχόντων σε κοινές δικτυακές υποδομές (substrate) «απομονωμένων» εικονικών δικτύων VPN σε επίπεδα 2 (VLAN), 3 (IP VPN) ή και 4 (εφαρμογές – πόρτες TCP/UDP)
- Σηματοδοσία - έλεγχος - ευφυΐα έξω από το δίκτυο διακίνησης δεδομένων (out-of-band signaling), π.χ. **OpenFlow Controllers** προγραμματιζόμενα ανά **ιδιοκτήτη (tenant)** εικονικού δικτύου, έξω από το δίκτυο δεδομένων αλλά με αμφίδρομη πρόσβαση σε πολιτικές δρομολόγησης εικονικών δικτύων
- Ευφυής Δρομολόγηση σε Δίκτυα Κορμού (**Core, Carrier Networks, Content Delivery Networks - CDN**) με προδιαγραφές επίδοσης (**Traffic Engineering - TE**) για διαχωρισμό ροών μεταξύ υποσυνόλων ζευγών πηγών – προορισμών διασυνδεόμενων δικτύων

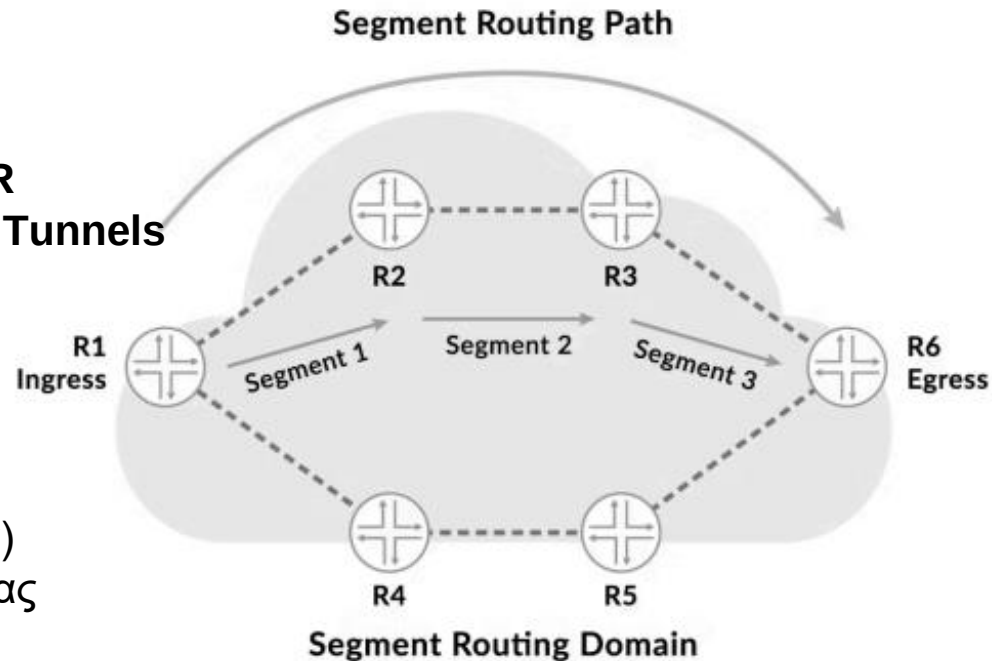
ΕΠΙΠΕΔΟ ΕΛΕΓΧΟΥ - Control Plane (3/4) (επανάληψη)

Ευφυής Δρομολόγηση Ροών Source - Destination

- Παραδοσιακή Δρομολόγηση στο **Internet: Destination-based** (π.χ. **BGP**)
- Προγραμματιζόμενα Δίκτυα Νέας Γενιάς (**Software Defined Networks - SDN**): Παρέχουν δυνατότητες διαχωρισμού δρομολόγησης ροών πακέτων ανάλογα με την αρχική τους πηγή (**Source Routing**)
- Ευφυής Δρομολόγηση σε Δίκτυα Κορμού (**Core, Carrier Networks, Content Delivery Networks - CDN**) με προδιαγραφές επίδοσης (**Traffic Engineering - TE**) ανά ροή μεταξύ ζευγών πηγών – προορισμών (**Source – Destination**)
- Από **MPLS-TE** σε αλγορίθμους **Source Routing & Segment Routing (SR)**:

- MPLS-TE → SR-MPLS
- IPv6 → SRv6

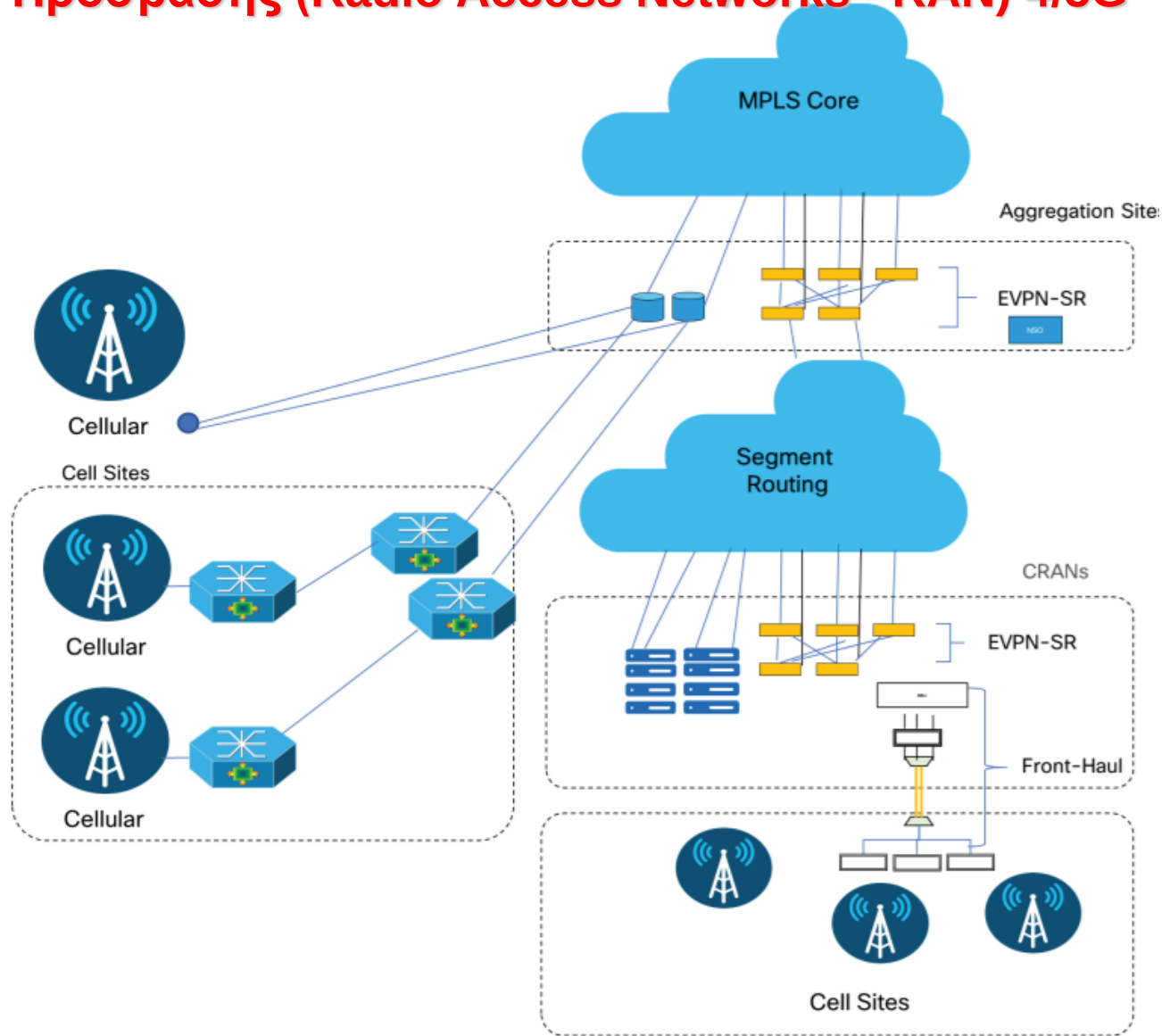
- **Segment Routing (RFC 8402)**
 - Τα πακέτα μιας ροής σε μια περιοχή **SR** δρομολογούνται σε **Ingress → Egress Tunnels** κατά μήκος **Segment Routing Paths**
 - Οι δρομολογητές **Ingress** υπολογίζουν **συνολικές** διαδρομές στη περιοχή συμβατές με **πολιτικές επίδοσης** και με βάση τις δικτυακές καταστάσεις όλων των κόμβων (και των ενδιαμέσων) που ανακοινώνονται μέσω σηματοδότης τύπου **IGP/MPLS** ή **BGP**



<https://www.juniper.net/us/en/research-topics/what-is-segment-routing.html#:~:text=Contact%20Us-,What%20is%20segment%20routing%3F,headers%20at%20an%20ingress%20node>

ΕΠΙΠΕΔΟ ΕΛΕΓΧΟΥ - Control Plane (4/4) (επανάληψη)

Ευφυείς Ευρυζωνικές Ζεύξεις Backhauling Ασύρματων Υποδικτύων Πρόσβασης (Radio Access Networks - RAN) 4/5G



<https://www.cisco.com/c/dam/en/us/solutions/service-provider/industry/telco/assets/pdf/backhaul-use-case.pdf>

ΕΝΟΠΙΗΜΕΝΗ ΑΡΧΙΤΕΚΤΟΝΙΚΗ Software-Defined Network

Programmable SDN Software Stack - *Peterson et.al. Ch. 3 (επανάληψη)*

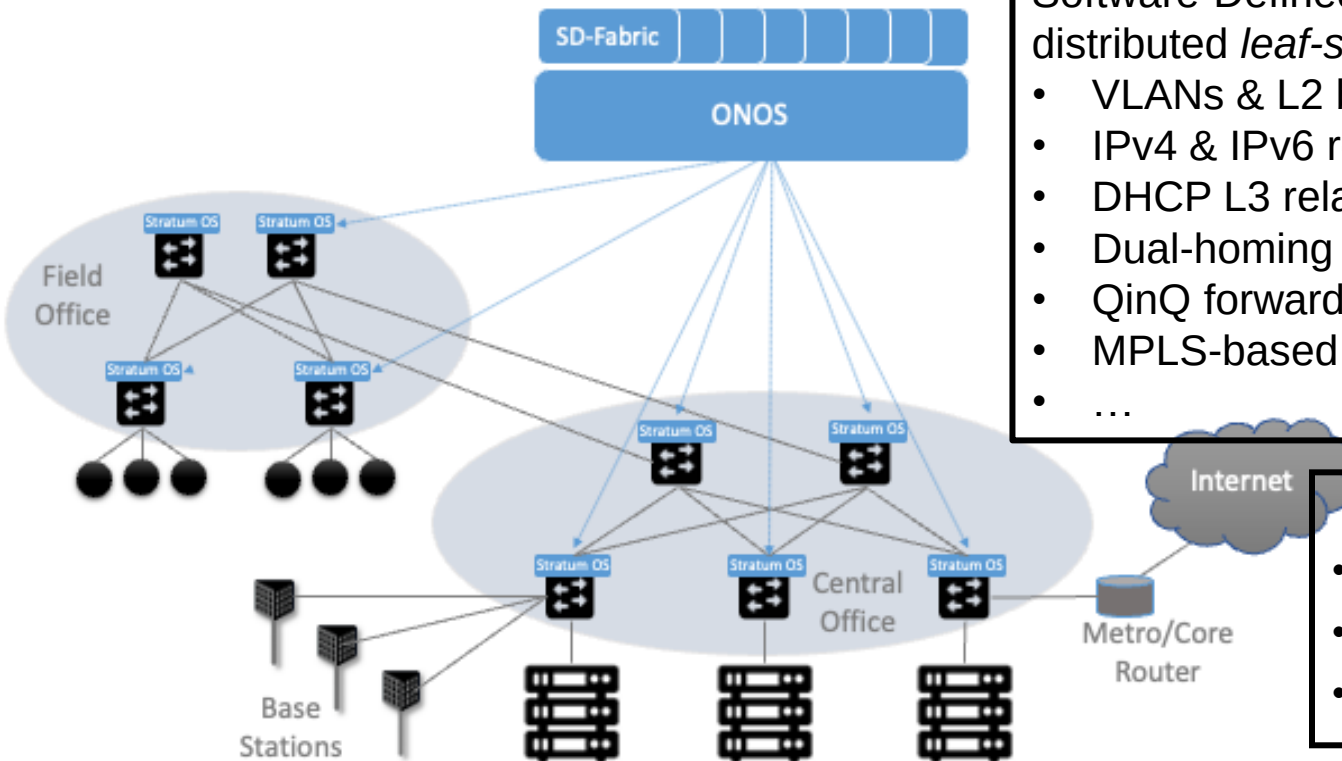
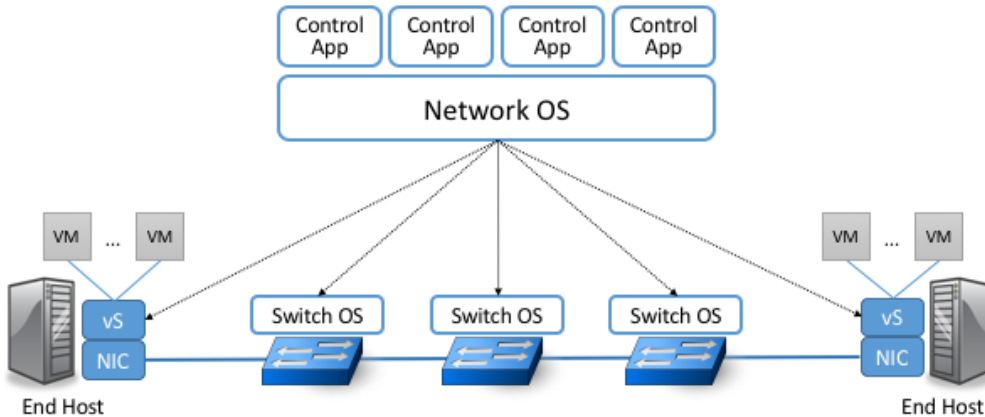
<https://sdn.systemsapproach.org/arch.html>

SDN End-to-End Perspective

end-host/VM → virtual Switch (vS) →
transit Switches → vS → end-host/VM

Configuration & Control Software

- Network OS (e.g. [ONOS](#))
- Switch OS (e.g. [Stratum](#))
- Control App (e.g. [Trellis](#))



Trellis Control Apps

Software-Defined (SD) Fabric suite in distributed *leaf-spine* data-center topologies:

- VLANs & L2 bridging
- IPv4 & IPv6 routing
- DHCP L3 relay
- Dual-homing of Servers/Routers
- QinQ forwarding/termination
- MPLS-based pseudowires
- ...

ONOS Functionality

- Topology Management
- Configuration Management
- Control of Switches

ΕΠΙΠΕΔΟ ΔΙΑΧΕΙΡΙΣΗΣ (επανάληψη)

Management Plane

- Τηλεπικοινωνιακές υποδομές παρόχων δικτυακών υπηρεσιών: Κλειστά διαχειριστικά συστήματα ανάλογα με τον προμηθευτή τηλεπικοινωνιακού εξοπλισμού κέντρων μεταγωγής, εξοπλισμού πολυπλεξίας SDH κλπ.
 - ✓ Μοντέλο **OS/NE** (Operation System / Network Element)
 - ✓ Διαχείριση οπτικών δικτύων **DWDM** (επέκταση κλειστών proprietary συστημάτων διαχείρισης SDH, χρήση scripts, Java - JMX, Web Services, Q3 - TL1 - Corba...)
 - ✓ Ενοποιημένα συστήματα διαχείρισης **TMN** (Telecommunications Management Network)
- Διαχείριση δικτύων TCP/IP (Internet – Intranet – Extranet) μέσω **SNMP**
 - ✓ SNMP transactions using UDP over IP, **SMI** Data Model, **BER** for **MIB** syntax
- Διαχείριση δικτύων TCP/IP μέσω **NETCONF**
 - ✓ **YANG** Data Model, πρωτόκολλα RPC over TCP/TCL, **XML** format, **Datastore** CRUD (Create, Read, Update, Delete) operations
 - ✓ **RESTCONF**: https/REST Web API as a front-end to NETCONF RPCs
- Διαχειριστικές λειτουργίες OSI, **CFAPS** (υλοποίηση σε πλατφόρμα OS ή NMS)
 - ✓ **C**onfiguration (Διαχείριση Διάρθρωσης)
 - ✓ **F**ault (Διαχείριση Βλαβών)
 - ✓ **A**ccounting (Λογιστική Διαχείριση)
 - ✓ **P**erformance (Διαχείριση Απόδοσης)
 - ✓ **S**ecurity (Διαχείριση Ασφαλείας)

ΣΥΝΟΨΗ ΕΡΓΑΛΕΙΩΝ ΔΙΑΧΕΙΡΙΣΗΣ (επανάληψη)

Network Management Tools

- **Diagnostics**
 - ICMP: ping, traceroute
 - tcpdump, Wireshark (Ethereal)
- **net-snmp** (NMS - Agent/MIB, SMI, BER για UDP PDUs)
 - snmp-get
 - snmp-walk
 - snmp-trap
 - snmp-set
- **NETCONF** (NMS - YANG Core Modules, YANG, XML με SSH ή TLS/SOAP/https)
- **Monitoring protocols & tools** (per-flow statistics, sampling)
 - Netflow
 - sFlow
 - Visualization tools (e.g. open source NTOP)
 - MRTG (RRDtool)
- **Transmission** (DWDM, SDH tools): CMIP, TMN, **Proprietary**
 - TL1, Q3, Corba

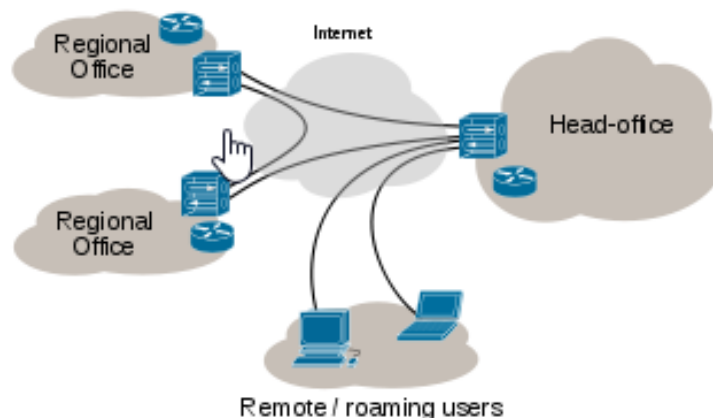
ΟΛΟΚΛΗΡΩΜΕΝΑ ΕΡΓΑΛΕΙΑ ΔΙΑΧΕΙΡΙΣΗΣ (επανάληψη)

Integrated Management Tools

- Αυτοματοποιούν διαδικασίες διαμόρφωσης, Automatic Configuration Templates: Ansible <https://www.ansible.com/overview/it-automation> (Open Source, Linux - based...)
- Ομαδοποιούν λειτουργίες FCAPS
- Open Source
 - Nagios – Service Monitoring <http://www.nagios.org/>
 - OpenNMS – Network Monitoring http://www.opennms.org/index.php/Main_Page
 - Cluster Management
 - Linux Heartbeat <http://www.linux-ha.org/doc/users-guide/users-guide.html>
 - Ganglia <http://ganglia.info/>
 - Big Data, Hadoop Clusters <http://hadoop.apache.org/>
- Commercial
 - HP Openview
 - IBM Tivoli
 - CiscoWorks....

ΕΙΚΟΝΙΚΑ ΙΔΙΩΤΙΚΑ ΔΙΚΤΥΑ (επανάληψη)

Virtual Private Networks – VPNs



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

Με τα **VPNs** χρήστες κοινών κατανεμημένων πόρων δημιουργούν **ιδιωτικές** υποδομές **Overlay Networks** ή εταιρικά δίκτυα **Intranet/Extranet** πάνω από **δημόσια** δίκτυα όπως το **Internet** ή δίκτυο μακράς αποστάσεως (Wide Area Network – WAN) ενός ISP αρχιτεκτονικής **IP/MPLS** ή **Enterprise Local Area Networks - LANs & Data Centers** με πολλαπλές αυτόνομες κοινότητες χρηστών, διασφαλίζοντας:

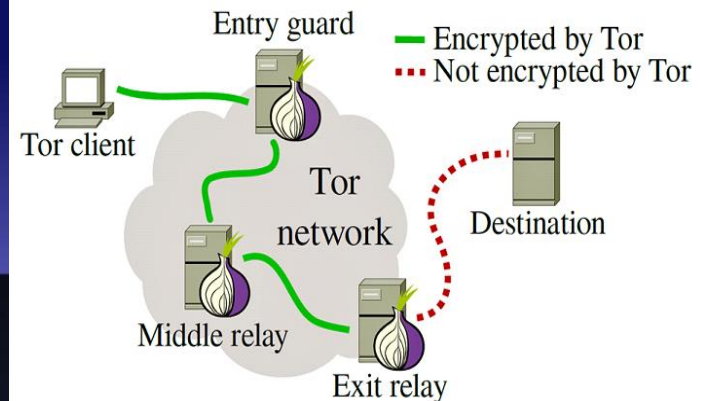
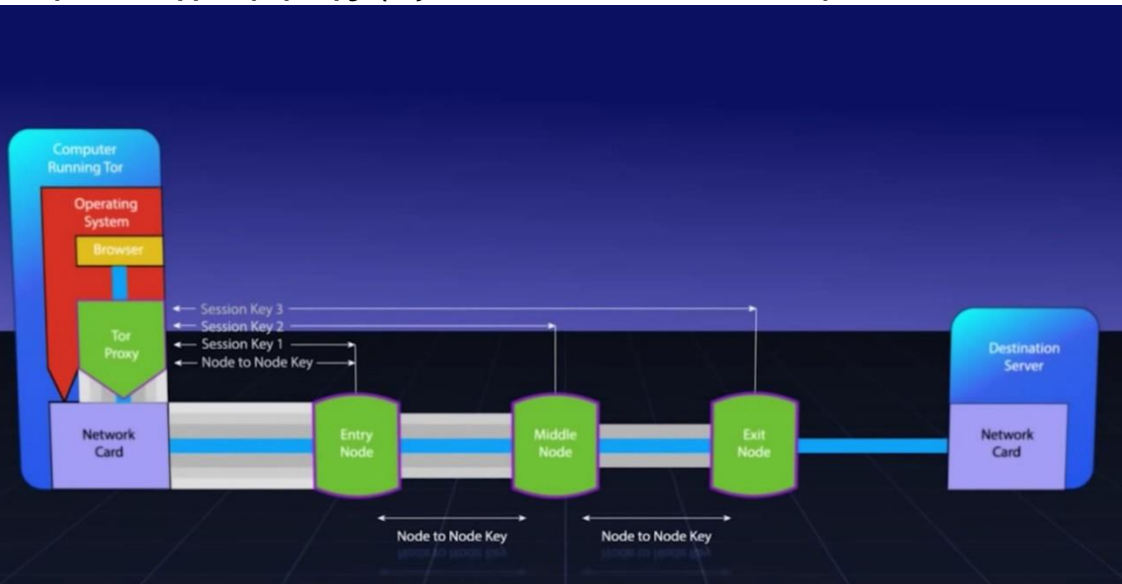
- Απομόνωση από άλλες κοινότητες π.χ. μέσω ενθυλάκωσης πακέτων του VPN (μαζί με τους ιδιωτικούς headers) σε πακέτα συμβατά με πρωτόκολλα Δημοσίου Δικτύου (**tunneling**)
- Διαχείριση δικτυακών πόρων & υπηρεσιών ανά VPN:
 - Επέκταση πεδίου διευθύνσεων **VLAN tags** ή **IP** σε απομακρυσμένες νησίδες ενός VPN
 - Δρομολόγηση με περιορισμούς ασφαλείας και διαμοιρασμού φορτίου – **traffic engineering**
 - Ασφαλής μετάδοση και σηματοδότηση όπως σε αυστηρά ελεγχόμενο τοπικό δίκτυο (LAN)

Anonymity Network - The Onion Router (Tor)

<https://2019.www.torproject.org/about/overview.html.en>

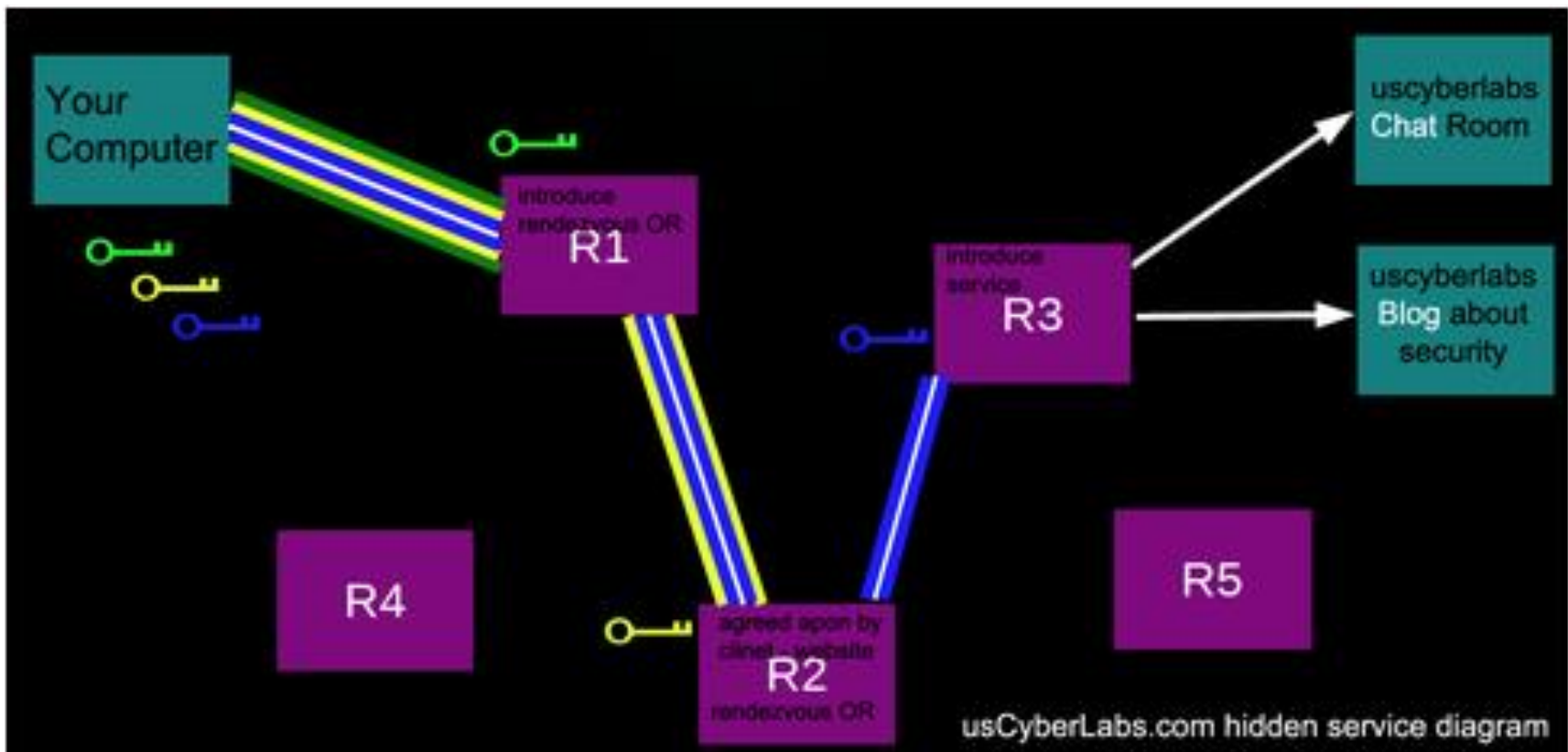
<http://fossbytes.com/everything-tor-tor-tor-works/>

- **Tor Project:** Δεκαετία 1990, κρατική χρηματοδότηση ΗΠΑ (Naval Research Laboratory – NRL)
- Απαιτείται ειδικός browser στον **Tor client**
- Βασίζεται σε υπερκείμενο (overlay) δίκτυο εθελοντικών **Tor relays** (>7000) συνδεδεμένων σε **public Internet routers** με διαδρομές που συρράπτονται από ανεξάρτητες κρυπτογραφημένες συνδέσεις
- Μονοπάτια (e2e routes) δημιουργούνται από συρραφή συνδέσεων μεταξύ των **Tor relays**
- Ο browser του χρήστη ανοίγει **Encrypted TLS** session από τον **Tor client** στον **Entry Node** δημιουργώντας **Session Key 1**
- Το session επεκτείνεται σε **Middle Node** με **Node-to-Node Key** με δημιουργία **Session Key 2**
- Ο **Exit Node** ανοίγει session με τον Server και μεσολαβεί για **Session Key 3** με τον **Tor client** χωρίς να γνωρίζει το IP του χρήστη (anonymity) και τα **Middle Nodes** στο μονοπάτι
- Η ανταλλαγή data μεταξύ **user browser** και **server** περνά από διαδοχικά στρώματα κρυπτογράφησης (εξ' ου και **onion router**)



The Deep & Dark Web

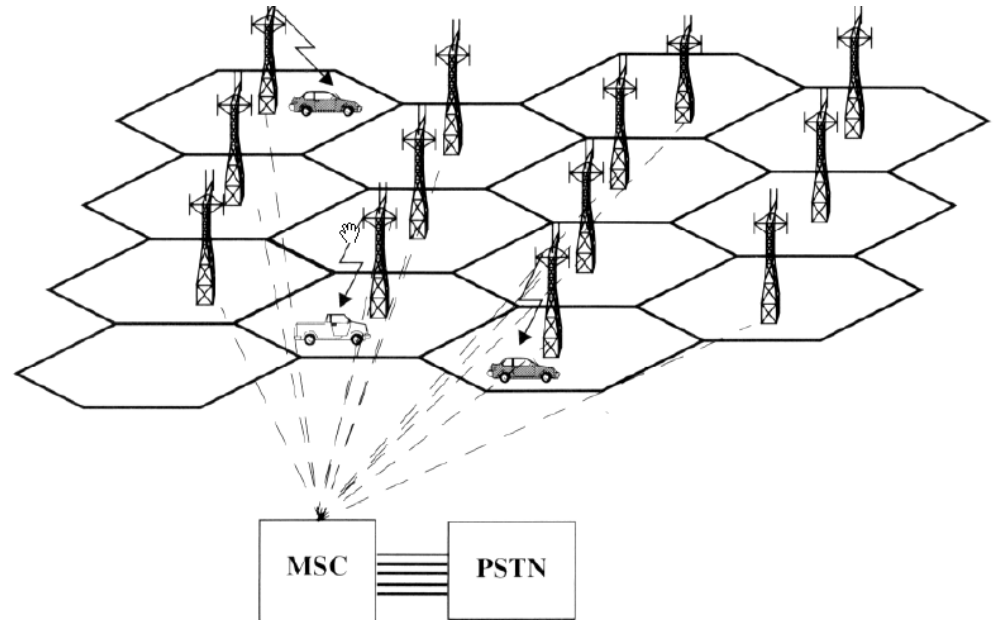
- **Deep Web:** Sites μη ανοικτής πρόσβασης (not indexed by search engines, π.χ. Google) https://en.wikipedia.org/wiki/Deep_web
- **Dark Web:** Υποσύνολο του Deep Web με προστασία ανωνυμίας sites & users π.χ. μέσω Tor https://en.wikipedia.org/wiki/Dark_web



- **Onion Service Protocol** (hidden services over a Tor overlay)
<https://2019.www.torproject.org/docs/onion-services>
<https://medium.jkala.sh/blog/2019/4/24/the-dark-web-everything-you-need-to-know>

ΕΞΕΛΙΞΗ ΚΙΝΗΤΗΣ ΤΗΛΕΦΩΝΙΑΣ

GSM (2G, 1988) - UMTS (3G, 2000) - LTE (4G, 2010)

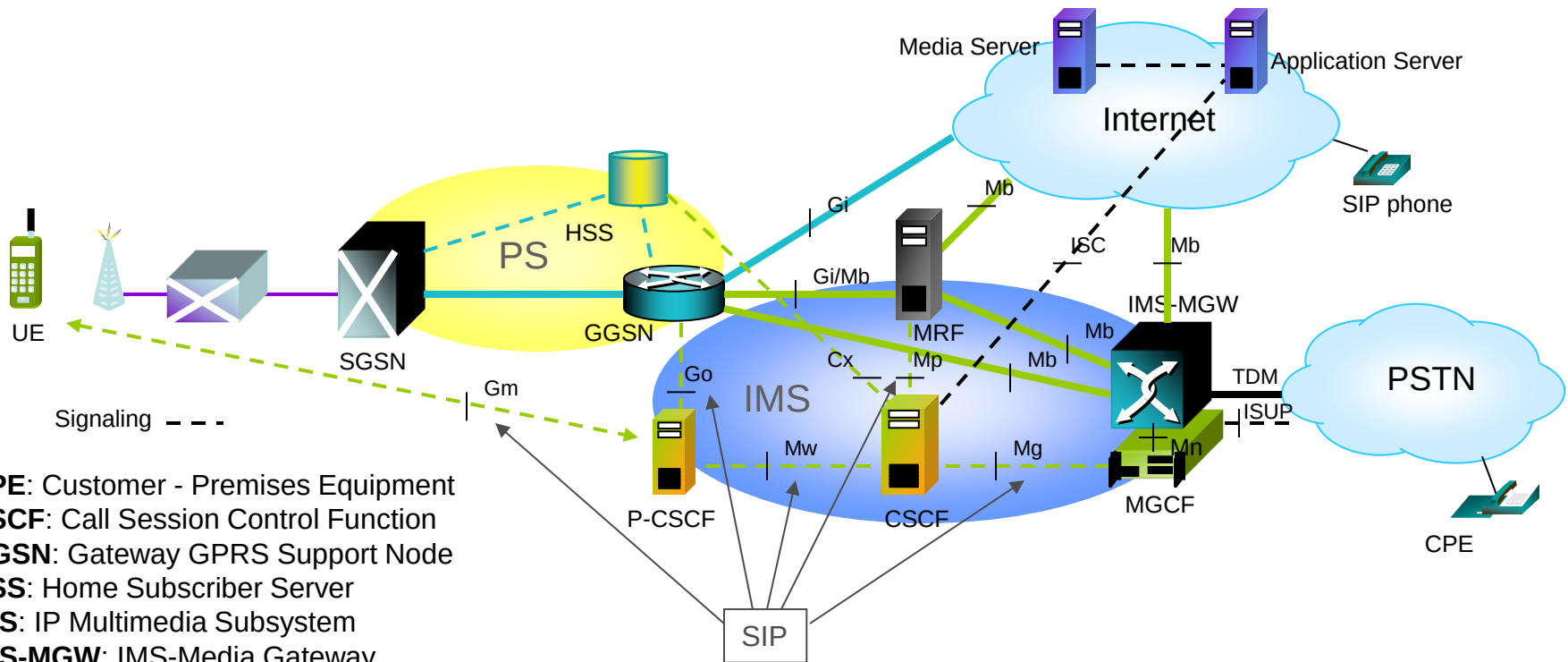


MSC: Mobile Switching Center (Κέντρο Μεταγωγής Κινητής Τηλεφωνίας)

PSTN: Public Switched Telephone Network (Δημόσιο Τηλεφωνικό Δίκτυο)

ΕΝΟΠΟΙΗΜΕΝΗ ΑΡΧΙΤΕΚΤΟΝΙΚΗ IMS (IP Multimedia Subsystem)

Άποψη της ITU-T & Τηλεπικοινωνιακών Παρόχων (TELCO Operators) για Converged Networking



CPE: Customer - Premises Equipment
CSCF: Call Session Control Function
GGSN: Gateway GPRS Support Node
HSS: Home Subscriber Server
IMS: IP Multimedia Subsystem
IMS-MGW: IMS-Media Gateway
ISUP: ISDN (Integrated Services Digital Network) User Part
MGCF: Media Gateway Control Function
MRF: Media Resource Function
P-CSCF: Proxy - Call Session Support Function
PS: Packet Switching domain
PSTN: Public Switched Telephone Network
SIP: Session Initiation Protocol
SGSN: Serving GPRS Support Node
UE: User Equipment

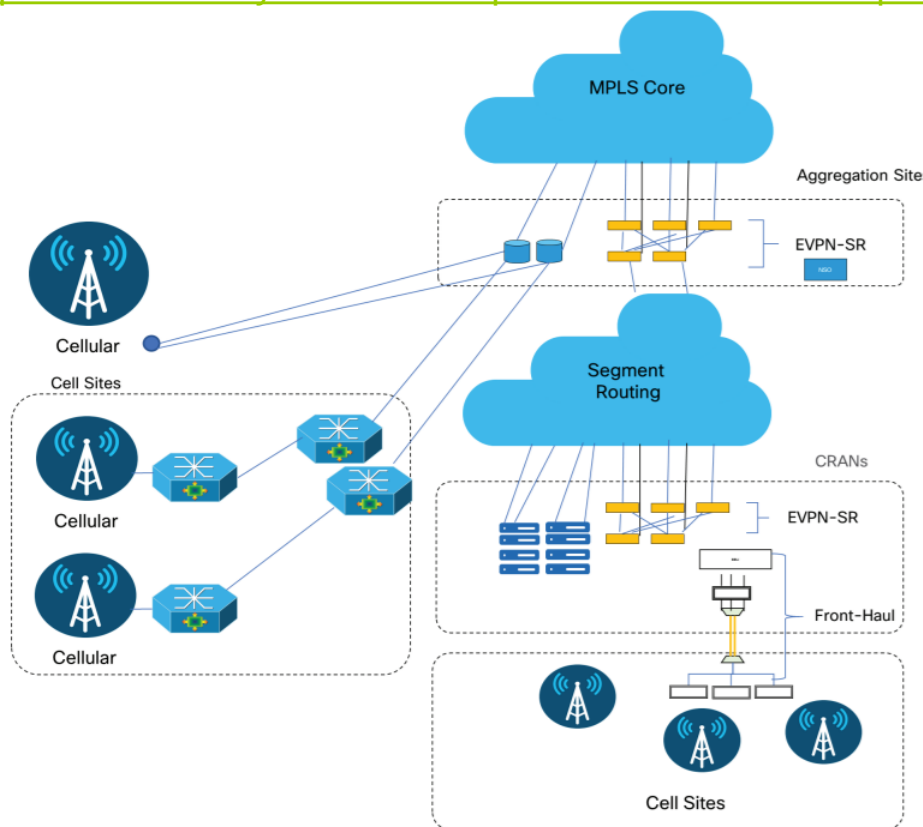


Η 5^η ΓΕΝΙΑ ΚΙΝΗΤΩΝ ΕΠΙΚΟΙΝΩΝΙΩΝ

Σύγκλιση Επικοινωνιών: Fixed-mobile Convergence (FMC) Ενοποιημένο Internet του 2020++

<https://5g-ppp.eu/white-papers/>

<https://www.cisco.com/c/dam/en/us/solutions/service-provider/industry/telco/assets/pdf/backhaul-use-case.pdf>



Προδιαγραφές 3GPP

(3rd Generation Partnership Project)

<https://www.3gpp.org/technologies/5g-system-overview>

Radio Access Fronthaul Network (RAN)

- Hand-held Devices, I/A & Streaming Video
- Antennas (Microcells, Metro Cells, MIMO, Drones)
- Cell antennas → Edge Servers
- Low-Band: 600-850 MHz (30-250 Mbps)
- Mid-Band: 2.5-3.7 GHz (100-900 Mbps)
- High-Band: 25-39 GHz (> 1 Gbps)

Backhaul Network

- Edge Servers → Aggregation Site
- Microwave, VDSL, GPON, p2p Fibers...
- GPRS Tunneling (GTP), MPLS TE...
- Segment Routing - eVPN

Core Network

- Aggregation Site → CDNs, Data Centers...
- MPLS Label Distribution Protocols (LDP), RSVP TE...

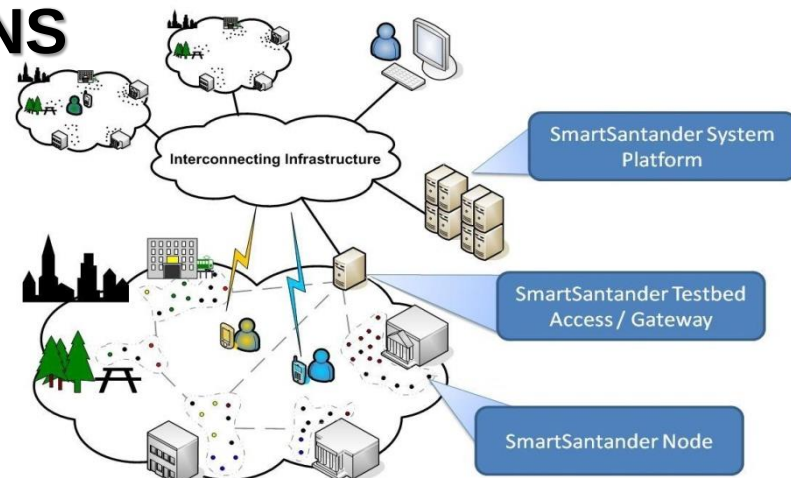
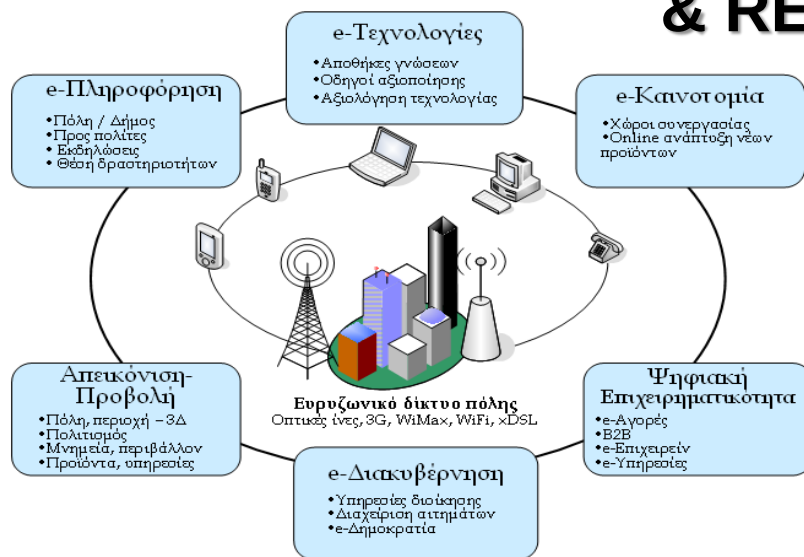
Air Latency

- Goal: 1 - 4 msec (Edge Servers δίπλα σε κεραίες)
- Σημερινές επιδόσεις: 20-30 msec

Εφαρμογές

- Enhanced Mobile Broadband, **eMBB** (Smart Cellphones 4G → 5G, 800-1400 Euros/Συσκευή)
- Ultra-Reliable Low-Latency Communications, **URLLC** (Factory Automation - **Industry 4.0**, Robotics, Transport Security - Autonomous Vehicles, Τηλεϊατρική...)
- Massive Machine-Type Communication, **mMTC** (Μαζικός Αρ. Τερματικών - **Sensor Networks, IoT**)

SENSOR NETWORKS, IoT - Internet of Things, SMART CITIES & REGIONS



Η Ευφυής Πόλη Santander, Β.Δ. Ισπανία

Δίκτυα Πρόσβασης με 12.000 Αισθητήρες (Wireless Sensors)

Καταμεμημένες Εφαρμογές σε Υπολογιστικά Νέφη (Clouds)

<http://www.smartsantander.eu/>

Ευφυείς Πόλεις: Υποδομές & Εφαρμογές

Tsarchopoulos, P. (2006) Evaluating Scenarios for Digital Cities

Η εποχή του Διαδικτύου του Μέλλοντος (Future Internet) έχει ξεκινήσει:

- **Οπτικά & Ασύρματα Δίκτυα Κορμού** σε παγκόσμια κλίμακα, Content Delivery Networks (**CDN**)
- **Ασύρματα Δίκτυα Πρόσβασης Αισθητήρων** (Wireless Sensor Networks), 35 δισεκατομμύρια τελικοί κόμβοι (εκτίμηση για 2020+)
- **Σύγκλιση Δικτυακών Τεχνολογιών**: Ευρωζωνικές οπτικές & δορυφορικές ζεύξεις, ασύρματα δίκτυα (GPRS, GSM, LTE, 5G Radio Access Network - RAN), τοπικά δίκτυα Ethernet & WiFi, επικοινωνίες μικρής εμβέλειας Bluetooth, IR, RFID...
- **Τεχνολογίες Ασύρματων Δικτύων Αισθητήρων** χαμηλής ισχύος & κόστους (Zigbee, Bluetooth, SigFox, **LoRa**, **NB-IoT** / Narrow Band Internet of Things)
- **Πρόσβαση σε Εικονικά Υπολογιστικά Περιβάλλοντα**, private – public clouds ευφυείς ψηφιακές εφαρμογές, υπηρεσίες triple play, αυτόματη οδήγηση, Industry 4.0
- **Smart Data, Control & Management Plane**, Network Softwarization, **Segment Routing** (SR-MPLS, SRv6), Programmable Data Planes (**P4**, **XDP**), Machine Learning

Οι 4 μεγαλύτεροι κατασκευαστές τηλεπικοινωνιακού εξοπλισμού



ΟΛΟΚΛΗΡΩΜΕΝΕΣ ΕΥΦΥΕΙΣ ΥΠΟΔΟΜΕΣ & ΥΠΗΡΕΣΙΕΣ

Converged Programmable Communication Infrastructures & Services

- Υπηρεσίες **Triple-Play** (Internet, Voice, Video) πάνω σε **ενοποιημένα δίκτυα IP**
- **IP Multimedia System (IMS)**: Σχέδιο Σύγκλησης της **3G.IP** (forum κατασκευαστών κινητής τηλεφωνίας, μετέπειτα **3GPP**) από το **1999** που υιοθετήθηκε από τις **TELCO (PNO, Public Network Operators)** και την **ITU-T** (International Telecommunication Union)
- Το μέλλον των Ενοποιημένων Επικοινωνιών: Η σημερινή άποψη της **Fixed-mobile Convergence** με την **Αρχιτεκτονική 5^{ης} Γενιάς (5G)** και το επερχόμενο τσουνάμι των **Sensor Networks → Internet of Things (IoT)**
- Αυτοματοποίηση διαμόρφωσης, ελέγχου και διαχείρισης υποδομών και υπηρεσιών σε ευφυές, προγραμματιζόμενο (software-defined) και **ΑΣΦΑΛΕΣ** οικοσύστημα με εγγυήσεις (;) διασφάλισης προσωπικών δεδομένων - **privacy**
- Διασύνδεση Σηματοδοσίας - Επιπέδων Ελέγχου σε **ομοσπονδιακό περιβάλλον πολλαπλών διαχειριστικών περιοχών (;;;)**

Stitching of CONTROL PLANE PROTOCOLS across Autonomous Domains (Multi-domain Signaling Protocols)

ONLY TWO SUCCESS STORIES

- **SS7 (International Telephony)**
- **BGP (Global Internet)**