ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

ΕΙΣΑΓΩΓΗ ΣΤΗΝ ΕΠΙΣΤΗΜΗ ΤΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

http://eclass.aueb.gr/courses/INF511/

Δικτύωση και Διαδίκτυο (ΚΕΦΑΛΑΙΟ 4)

Αλκμήνη Σγουρίτσα

Κοδριγκτώνος 12, 2ος όροφος

E-mail: alkmini@aueb.gr

Κεφάλαιο 4: Δικτύωση και Διαδίκτυο

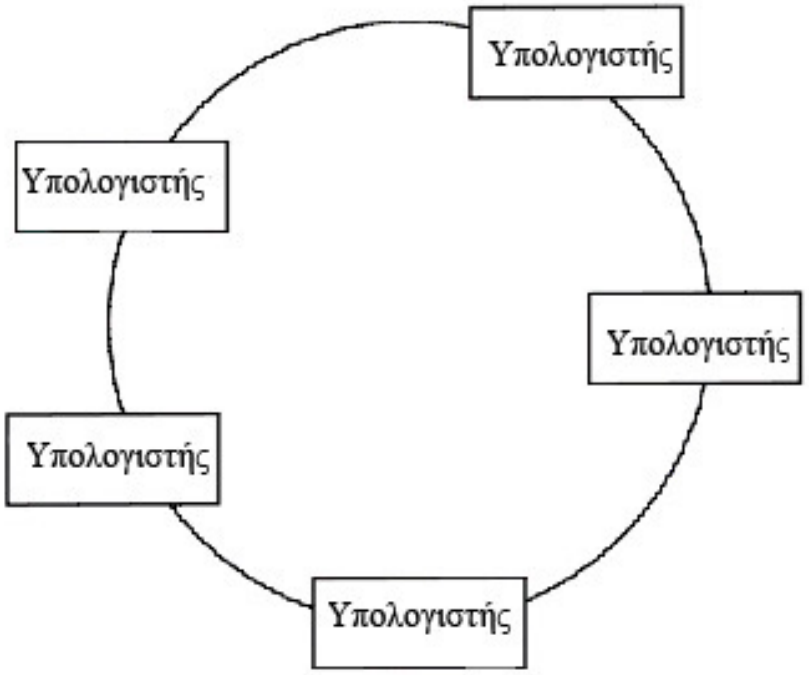
- Τοπολογίες δικτύων
- Πρωτόκολλα πολλαπλής πρόσβασης
  - Ethernet (CSMA/CD)
  - WiFi (CSMA/CA)
- Δομή Διαδικτύου
- Διευθυνσιοδότηση και Domain Name System (DNS)
- Εφαρμογές διαδικτύου: Email, FTP
- Διαστρωμάτωση και διαδικτυακά πρωτόκολλα
  - Πρωτόκολλα δρομολόγησης
  - Πρωτόκολλα μεταφοράς TCP και UDP
  - Έλεγχος ροής και έλεγχος συμφόρησης στο TCP
- Βασικά στοιχεία ασφάλειας και κρυπτογραφίας
  - Κρυπτογράφηση δημοσίου κλειδιού

Κατηγορίες Δικτύων

- Δίκτυα = διασυνδεδεμένα συστήματα υπολογιστών
- Εμβέλεια:
  - Τοπικά δίκτυα (Local Area Networks, LANs): κλίμακα κτιρίου
  - Μητροπολιτικά δίκτυα (Metropolitan Area Networks, MANs): κλίμακα κοινότητας (γειτονιάς)
  - Δίκτυα ευρείας περιοχής (Wide Area Networks, WANs), κλίμακα πόλης και μεγαλύτερα
- Ιδιοκτησία:
  - Κλειστά ή ιδιόκτητα (closed, proprietary), ανοιχτά (open)
- Τοπολογία (διευθέτηση) κόμβων:
  - Διαύλου (bus): π.χ. Ethernet
  - Αστέρα (star): π.χ. ασύρματα δίκτυα με κεντρικό σημείο πρόσβασης
  - Δακτυλίου
  - Άτακτη τοπολογία

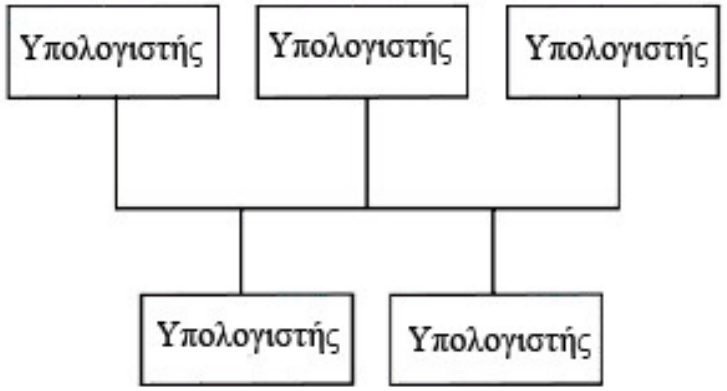
Τοπολογίες δικτύων (1)

α. Δακτύλιος



β. Δίαυλος

Ethernet

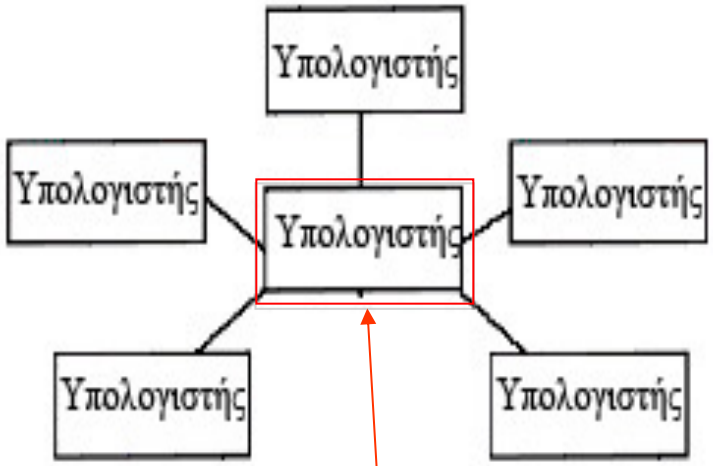


Τοπολογίες δικτύων (2)

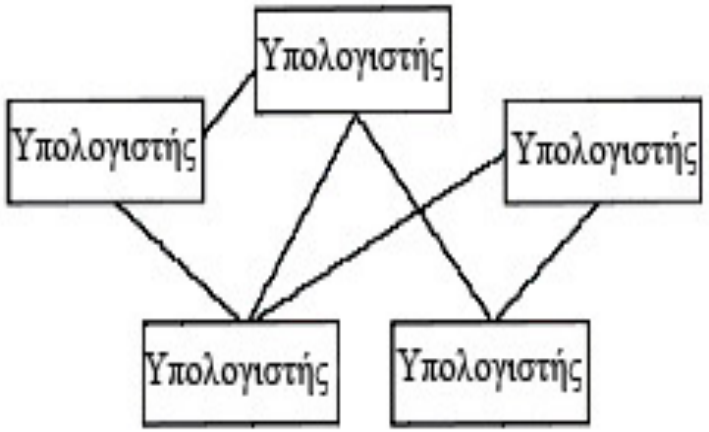
Wireless mesh or ad-hoc networks
Ασύρματα αδόμητα δίκτυα

γ. Αστέρας

Ethernet, WiFi



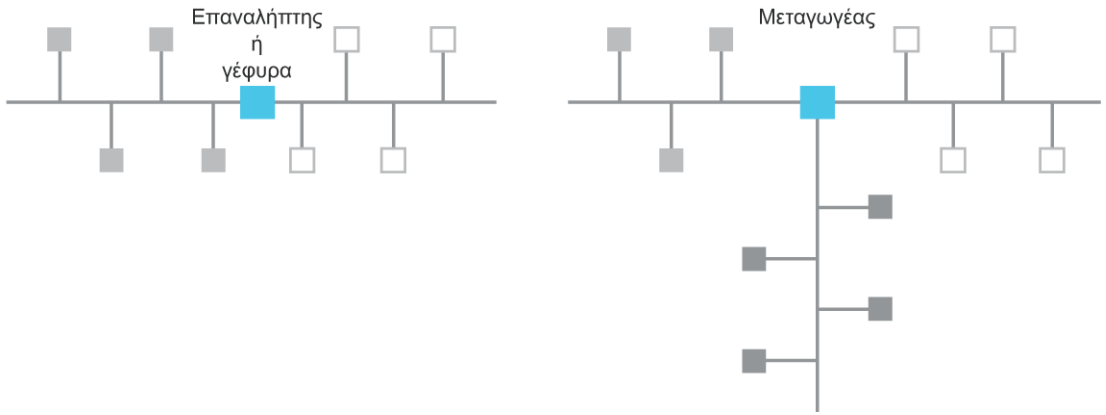
δ. Ατακτη τοπολογία



όχι απλός υπολογιστής αλλά δικτυακός κόμβος
(εξειδικευμένη δικτυακή συσκευή)

Διασύνδεση Δικτύων (1)

- **Επαναλήπτης* (repeater) ή γέφυρα* (bridge):** Επεκτείνει ένα δίκτυο και συνδέει δύο συμβατά δίκτυα
- **Μεταγωγέας (switch):** Συνδέει πολλά συμβατά δίκτυα
  - Π.χ. πολλά ενσύρματα ή πολλά ασύρματα



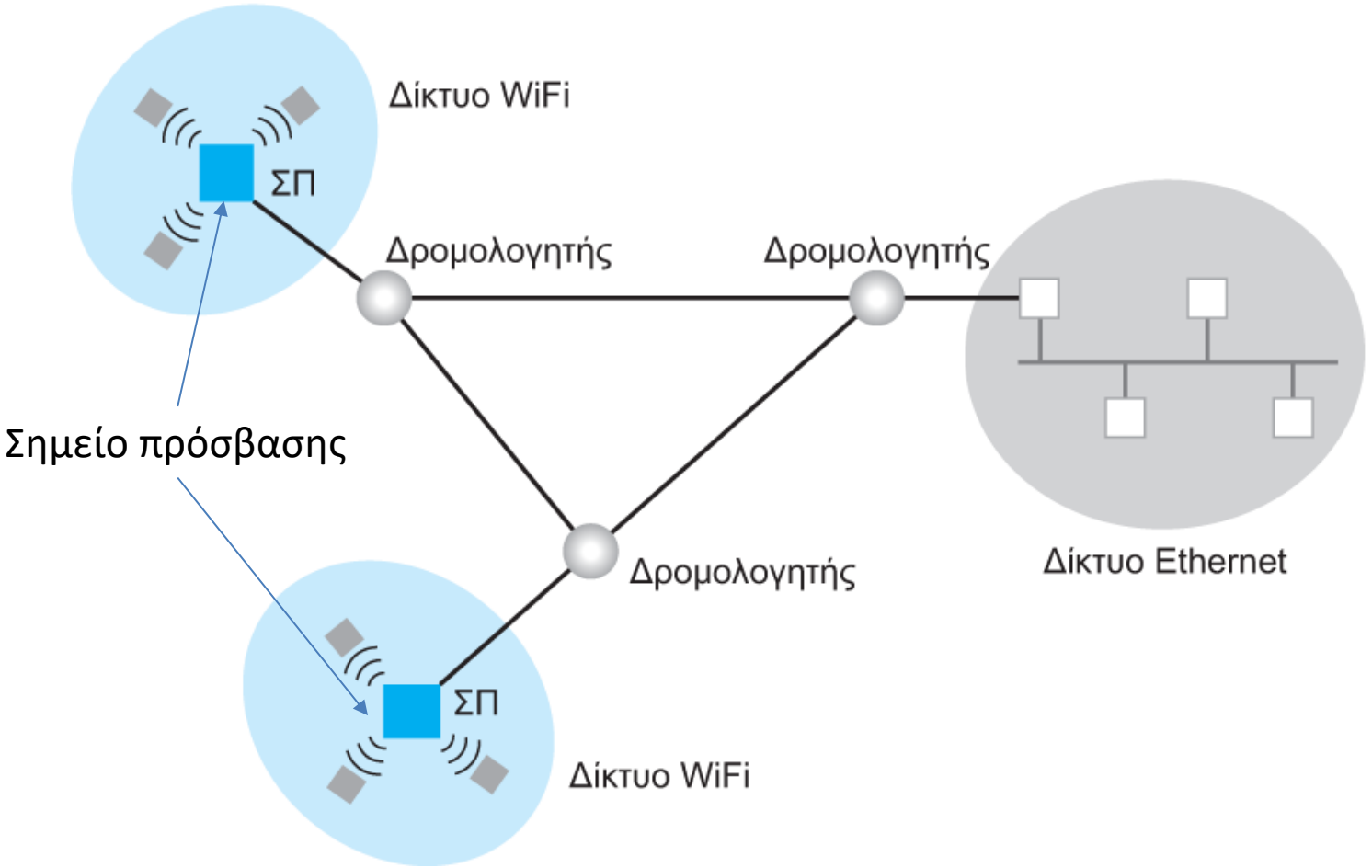
α. Επαναλήπτης ή γέφυρα που συνδέει δύο διαύλους

β. Μεταγωγέας που συνδέει πολλούς διαύλους

***Επαναλήπτης**: απλά αναπαράγει το λαμβανόμενο σήμα
***Γέφυρα**: δρα ως φίλτρο, περνάει μόνο τα πακέτα για τα οποία ο αποστολέας και ο παραλήπτης βρίσκονται σε διαφορετικά κομμάτια του δικτύου

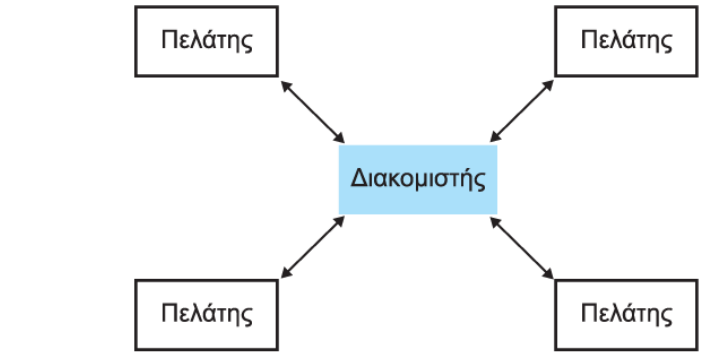
Διασύνδεση Δικτύων (2)

- **Δρομολογητής (router):** Συνδέει δύο ή περισσότερα ασύμβατα (διαφορετικού είδους) δίκτυα, δημιουργώντας ένα δίκτυο δικτύων που ονομάζεται **διαδίκτυο**

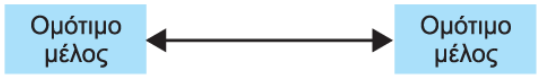


Μοντέλα Επικοινωνίας Υπολογιστών

- Μοντέλο πελάτη-Διακομιστή (client-server)
  - Ένας διακομιστής (server), πολλοί πελάτες
  - Ο πελάτης κάνει αιτήσεις για εργασίες, ο διακομιστής (εξυπηρετητής) τις ικανοποιεί
- Παραδείγματα:
  - Πελάτες ζητούν πρόσβαση σε αρχεία που υπάρχουν σε έναν διακομιστή
- Μοντέλο ομοτίμων (peer-to-peer, P2P)
  - κάθε υπολογιστής παίζει το ρόλο πελάτη και εξυπηρετητή (δηλ. ταυτόχρονα παράγει αιτήσεις προς άλλους Η/Υ και ικανοποιεί αιτήσεις άλλων)
- Παραδείγματα:
  - Ανταλλαγή αρχείων με συστήματα peer-to-peer
  - Αλληλο-δραστικά παιχνίδια (interactive games)



α. Ο διακομιστής πρέπει να είναι προετοιμασμένος να εξυπηρετήσει πολλούς πελάτες οποιαδήποτε στιγμή.

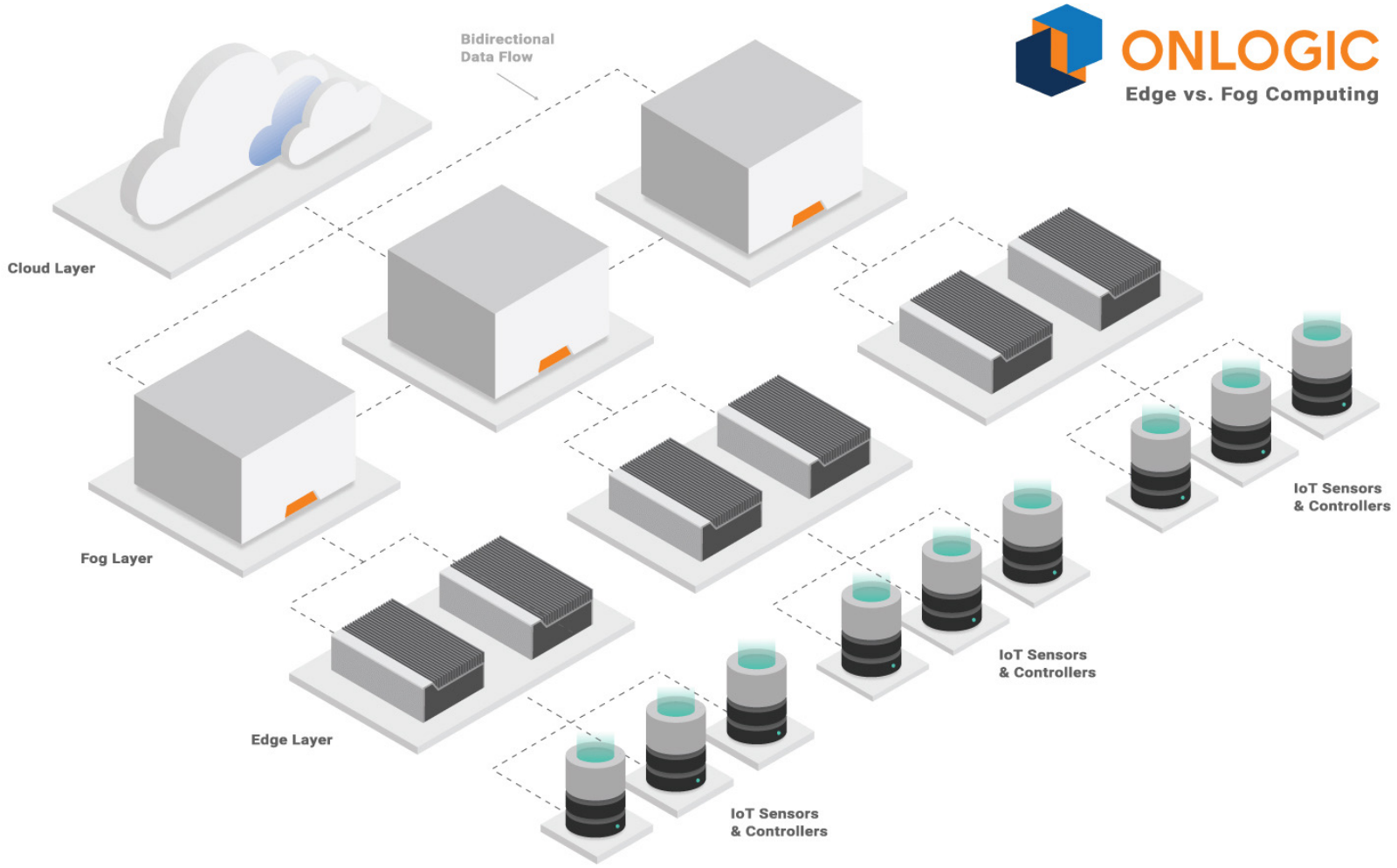


β. Τα ομότιμα μέλη επικοινωνούν ως ισότιμα σε μια βάση ένας προς ένας.

Εξέλιξη Συστημάτων Υπολογιστών

- Υπολογιστική Συστάδας (Cluster Computing), 1990s
  - Πολλοί ανεξάρτητοι Η/Υ εργάζονται από κοινού για εργασίες υπολογισμού σαν να ήταν μια μεγάλη μηχανή
- Υπολογιστική Πλέγματος (Grid Computing), 2000s
  - Μηχανές σε διαφορετικά μέρη συνεισφέρουν την υπολογιστική τους ισχύ (αν αυτή δεν χρησιμοποιείται) για εκτέλεση περίπλοκων εργασιών
  - π.χ. επεξεργασία ιατρικών/επιστημονικών πειραματικών δεδομένων κ.α.
- Υπολογιστική Νέφους (Cloud Computing), 2010s
  - Ίδια λογική, μεγαλύτερη κλιμάκωση
  - Π.χ. Amazon Elastic Cloud, Apple iCloud, Google GoogleDocs
  - Εκτέλεση υπολογιστικών εργασιών ή αποθήκευση δεδομένων (ο χρήστης δεν μαθαίνει ποτέ σε ποιον συγκεκριμένο υπολογιστή γίνεται η εργασία ή η αποθήκευση δεδομένων)
- Υπολογιστική Ομίχλης ή Άκρου (Fog/Edge Computing), 2015-
  - Οι συσκευές κοντά στον χρήστη (wearables, κινητά, αισθητήρες κλπ.) εκτελούν τους υπολογισμούς

Εξέλιξη Συστημάτων Υπολογιστών



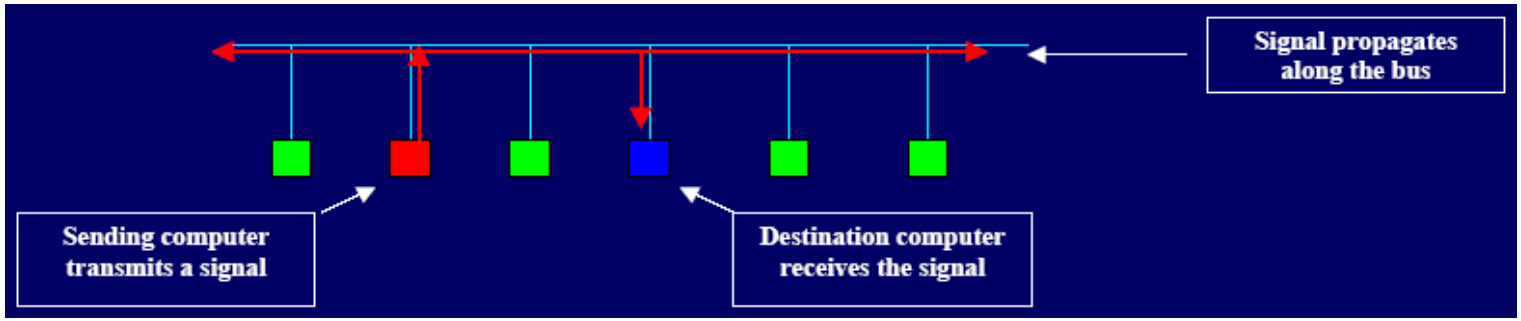
Πρωτόκολλα δικτύων

- Δίκτυο = κατανεμημένο σύστημα
  - Όχι κεντρικός έλεγχος
  - Χρειάζονται κανόνες σύμφωνα με τους οποίους θα λειτουργεί το δίκτυο
  - Π.χ. κανόνας που λέει πότε θα μεταδίδει ένας κόμβος, σε ποιον θα μεταδίδει ένας κόμβος ή με τι ρυθμό (bits/sec)
- Πρωτόκολλο: Σύνολο από κανόνες που πρέπει να ακολουθούν οι συσκευές για να λειτουργούν ως σύστημα
  - Πως ερμηνεύουν εισερχόμενα μηνύματα
  - Πως αντιδρούν σε αυτά
  - Τι μηνύματα να στείλουν στους γείτονες
- Πακέτο: ομάδα από bits πληροφορίας που μεταδίδονται όλα μαζί
  - π.χ. 1 πακέτο = 1500 bytes στο WiFi

Δομή DATA πακέτου

- DATA ή Payload: Bits πληροφορίας που κουβαλάει το πακέτο
- Transmitter ID: διεύθυνση αποστολέα
- Receiver ID: διεύθυνση παραλήπτη

Πρωτόκολλα Πολλαπλής Πρόσβασης (Multiple Access Protocols)

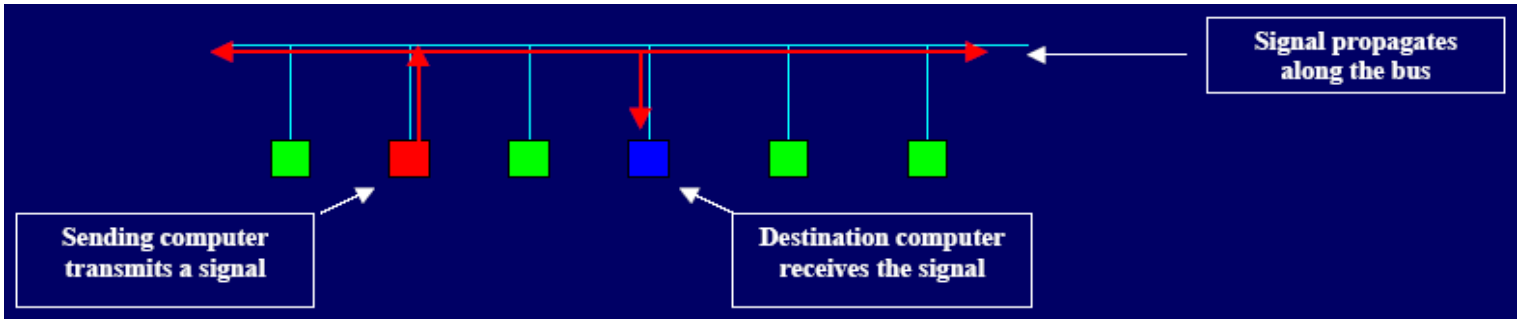


- Έστω ένα τερματικό θέλει να στείλει πακέτο σε ένα άλλο
- Κάθε τερματικό έχει την δική του διεύθυνση
- Η επικοινωνία γίνεται στο ίδιο "κανάλι" δηλ. το μέσο διάδοσης
- Όλα τα τερματικά ακούνε και στέλνουνε πακέτα στο ίδιο κανάλι
- Τυχαία πολλαπλή πρόσβαση (Random multiple access): όχι κεντρικός έλεγχος
- Κεντρικός έλεγχος θα υπήρχε αν ανέθετε χρονο-θυρίδες (time slots) για το πότε να μεταδώσει ο κάθε κόμβος (TDMA)

Συγκρούσεις σε πρωτόκολλα Πολλαπλής Πρόσβασης

- Αντιμετώπιση συγκρούσεων (ταυτόχρονων μεταδόσεων):
  - Τις καταλαβαίνω εγκαίρως: σταματάω να εκπέμπω και ξαναστέλνω μετά από τυχαίο χρόνο
    - Collision detection, CD
    - περίπτωση ενσύρματου δικτύου: στέλνω και ακούω ταυτόχρονα, άρα καταλαβαίνω αμέσως τη σύγκρουση
  - Δεν μπορώ να τις καταλάβω εγκαίρως ή και καθόλου: προσπαθώ με έξυπνο τρόπο να τις **αποφύγω** όσο γίνεται εκ των προτέρων → Ζητώ επιβεβαίωση από τον παραλήπτη
    - Collision avoidance, CA
    - περίπτωση ασύρματου δικτύου (WiFi): δεν μπορώ να ακούω το κανάλι ταυτόχρονα ενώ μεταδίδω

Ενσύρματο Ethernet

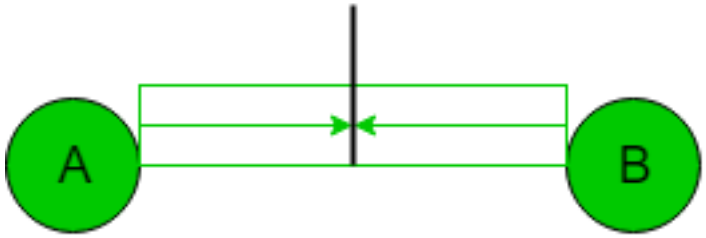


Πρωτόκολλο CSMA/CD Πολλαπλή προσπέλαση με ανίχνευση φέροντος(Carrier Sense Multiple Access) και ανίχνευση σύγκρουσης (Collision Detection)

- Κάθε κόμβος Α ακούει συνέχεια το κανάλι
- Μόλις αυτό είναι ελεύθερο (δηλ. κανείς άλλος δε μεταδίδει), ο Α μεταδίδει (αν έχει κάτι να στείλει)
- Αν κάποιος κόμβος Β αρχίσει μετάδοση **ενώ μεταδίδει ο Α**, και οι δυο σταματούν να μεταδίδουν
- Ο καθένας προσπαθεί και πάλι να μεταδώσει μετά από ένα τυχαίο χρονικό διάστημα (back-off interval)
- Back-off: διαλέγει ένα τυχαίο χρόνο Τ να περιμένει, και ξαναστέλνει
- Βασική προϋπόθεση: κάθε συσκευή μπορεί να ακούει και να μεταδίδει ταυτόχρονα → ανιχνεύει έγκαιρα τυχόν σύγκρουση **ενώ μεταδίδει**

Ενσύρματο Ethernet

At t = 0 , both A and B start transmission

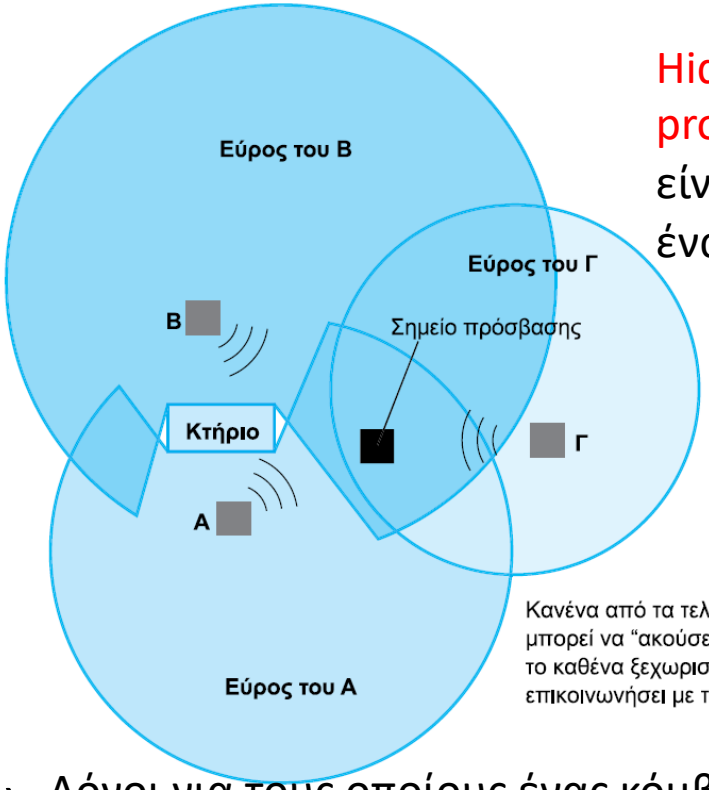


Packets of both A and B collide

Both stations A and B detect collision

Ασύρματο Δίκτυο (WiFi) (1)

- Τερματικά Α, Β, Γ επικοινωνούν ασύρματα με ένα σταθμό βάσης
- Carrier Sense Multiple Access Collision Avoidance (CSMA/CA)
  - Χρησιμοποιείται στο WiFi (ασύρματο δίκτυο)
  - Εμβέλεια (range) μετάδοσης ενός κόμβου Α: απόσταση γύρω από τον κόμβο όπου μπορεί να φτάσει το πακέτο που μεταδίδει ο Α



Hidden terminal problem, π.χ. Α, Β είναι κρυμμένα το ένα για το άλλο

Λόγοι για τους οποίους ένας κόμβος (Α) δεν μπορεί να ανιχνεύσει σύγκρουση (με τον Β)

- Ο Α δεν μπορεί να λαμβάνει και να μεταδίδει ταυτόχρονα (λόγω περιορισμών στο hardware της ασύρματης κάρτας)
- Ο Α βρίσκεται εκτός εμβέλειας του Β, και ο Α δεν τον ακούει
- Το σήμα του Β είναι αρκετά ασθενές

Ασύρματο Δίκτυο (WiFi) (2)

- **1ο Πρόβλημα**: Η ασύρματη κάρτα ΔΕΝ μπορεί να ακούει όταν στέλνει
  - Δεν μπορεί να ανιχνεύσει σύγκρουση
- **Λύση**: πρωτόκολλο CSMA/CA (Collision Avoidance) χωρίς RTS/CTS
  - Λογική: εξ' αρχής προσπάθησε να αποφύγεις τις συγκρούσεις

    WiFi χωρίς RTS/CTS: Back off -> DATA -> ACK …

  - Πριν μεταδώσεις ξεκίνησε ένα τυχαίο μετρητή με χρόνο t που μετράει αντίστροφα όσο το κανάλι είναι ελεύθερο (το t επιλέγεται τυχαία από το σύνολο τιμών {0,1,..,T-1} = {0,1,…, 2^W-1} ($T=2^W$)
  - Όταν μηδενιστεί ο μετρητής, μετέδωσε το 1ο DATA πακέτο
  - Περίμενε επιβεβαίωση (ACK) από τον δέκτη
  - Εάν δε λάβεις επιβεβαίωση (σημαίνει είτε ότι υπήρξε σύγκρουση είτε ότι δεν έφτασε το πακέτο στον δέκτη), επανέλαβε το ίδιο με μετρητή t που επιλέγεται τυχαία από το σύνολο τιμών {0,1,..,2T-1} = {0,1,…2^{W+1}-1} (binary exponential backoff)
  - Αν λάβεις επιβεβαίωση επανέλαβε τα βήματα από την αρχή για το επόμενο πακέτο

Ασύρματο Δίκτυο (WiFi) (3)

- **2ο Πρόβλημα**: Πρόβλημα κρυμμένου τερματικού
- **Λύση :** πρωτόκολλο CSMA/CA (Collision Avoidance) με RTS/CTS

  Εκδοχή 2: WiFi με RTS/CTS:

  Backoff -> RTS-> CTS -> DATA -> ACK …

  - Ξεκίνησε έναν μετρητή με χρόνο t που μετράει αντίστροφα όσο το κανάλι είναι ελεύθερο (το t επιλέγεται τυχαία από το σύνολο {0,1,..T-1} = {0,1,…, 2^W-1}
  - Όταν λήξει, στείλε το μικρό πακέτο Request to Send, RTS (άδεια για μετάδοση)
  - Περίμενε πακέτο Clear to Send, CTS από τον παραλήπτη
    - Τα RTS, CTS ουσιαστικά λένε σε όλους τους άλλους κόμβους στην εμβέλεια των A,B (πλην των A,B) να μην μεταδώσουν (δηλ. κάνουν «κράτηση» του χώρου)
  - Εάν έγινε σύγκρουση (CTS δεν ελήφθη), ξεκίνα πάλι τον μετρητή με χρόνο t που επιλέγεται τυχαία στο σύνολο τιμών {0,1,…2^{W+1}-1}
    - Οι συγκρούσεις είναι πιθανές πάλι, αλλά δεν έχουν μεγάλο κόστος (το μήκος του πακέτου RTS είναι πολύ μικρό)
  - Αν ο πομπός λάβει το CTS, στέλνει το πακέτο DATA, περιμένει ACK, κ.ο.κ.

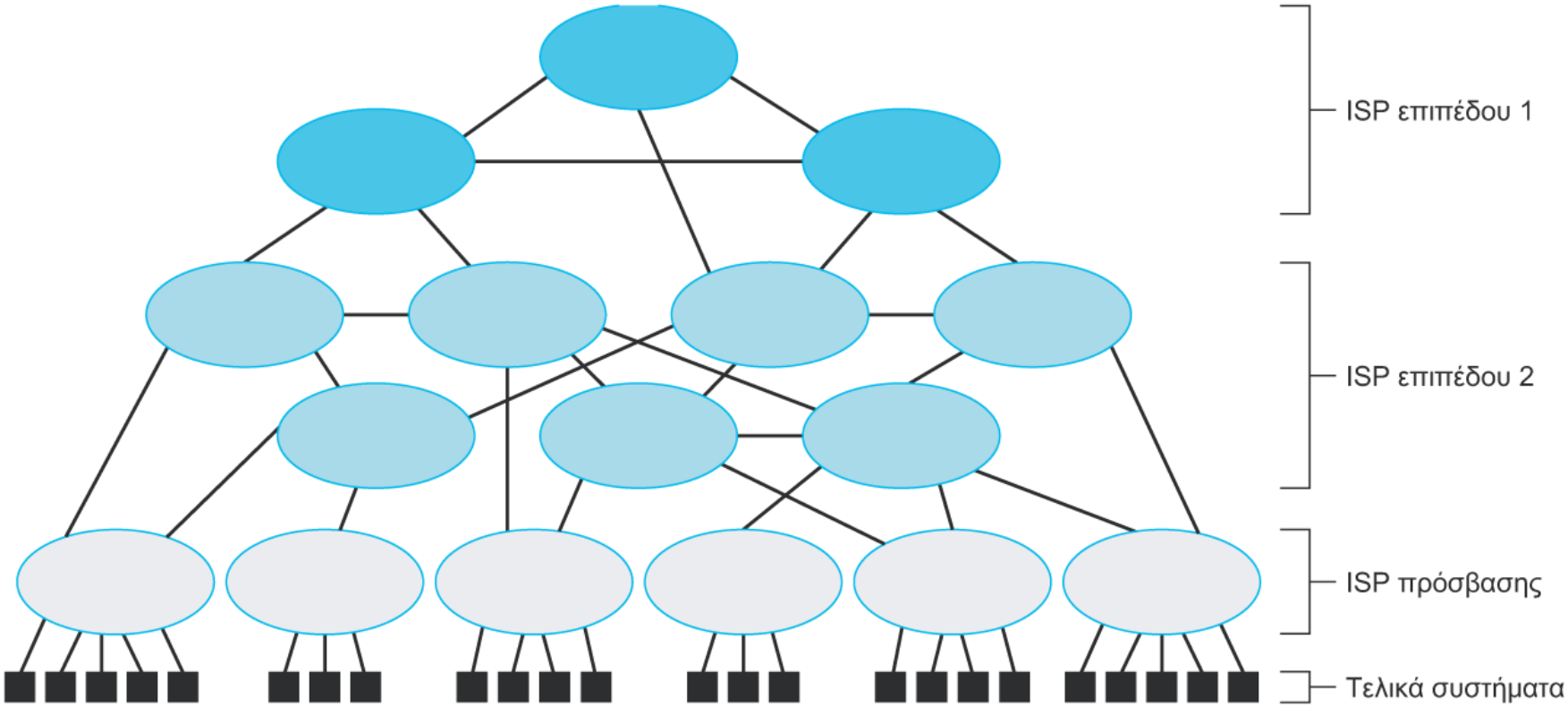
Το Διαδίκτυο

- Το Διαδίκτυο: Ένα διαδίκτυο που εκτείνεται σε όλο τον κόσμο
  - Αρχικός στόχος ήταν η σύνδεση κόμβων σε ένα δίκτυο που δεν θα επηρεαζόταν από τοπικές καταστροφές
  - Ξεκίνησε από την Αμερική (DARPA, Defense Advanced Research Projects Agency), the 1970s, με το δίκτυο ARPAnet
  - Σήμερα έχει μετατραπεί από ακαδημαϊκό ερευνητικό πείραμα σε παγκόσμιο μέσο διασύνδεσης

Αρχιτεκτονική Διαδικτύου

- Πάροχος Υπηρεσιών Διαδικτύου (Internet Service Provider, ISP)
  - Επιπέδου (tier) 1: πολύ υψηλής ταχύτητας
  - Επιπέδου (tier) 2: περισσότερο τοπικοί
  - Πυρήνας του διαδικτύου
- ISP πρόσβασης (access ISP): Παρέχει συνδεσιμότητα (πρόσβαση) στο Διαδίκτυο, π.χ. OTENET, AOL, Forthnet, Vodafone, κλπ
- Πρόσβαση στο διαδίκτυο μέσω:
  - Ethernet
  - Ασύρματης σύνδεσης (Σημεία Πρόσβασης - Access Points / APs)
    - Η περιοχή εμβέλειας ενός AP λέγεται hotspot
- Τερματικά συστήματα (end-systems) ή hosts
  - Κινητά τηλέφωνα, laptops, tablets, Η/Υ,…

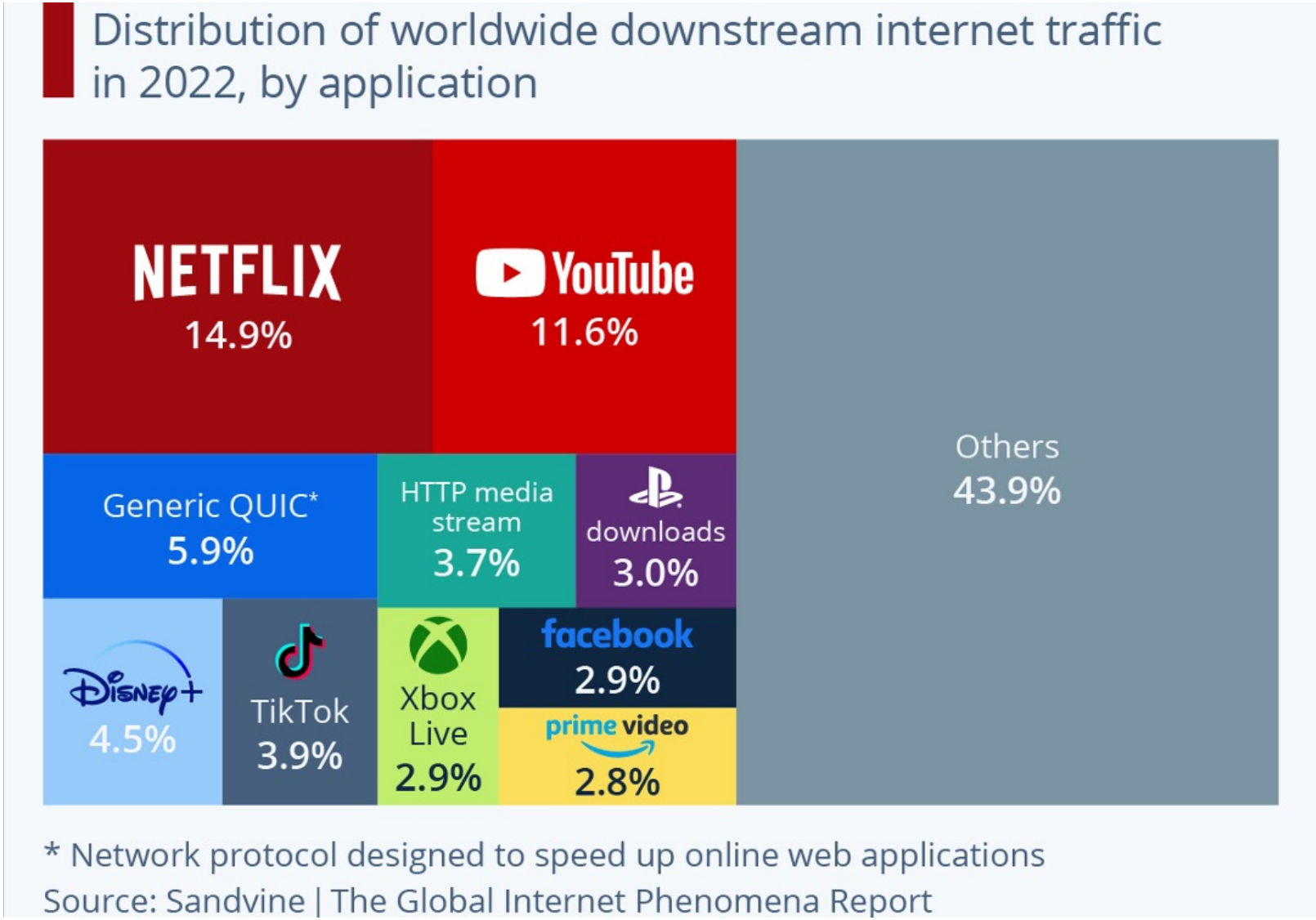
Ιεραρχία Διαδικτύου



Παραδείγματα ISPs:

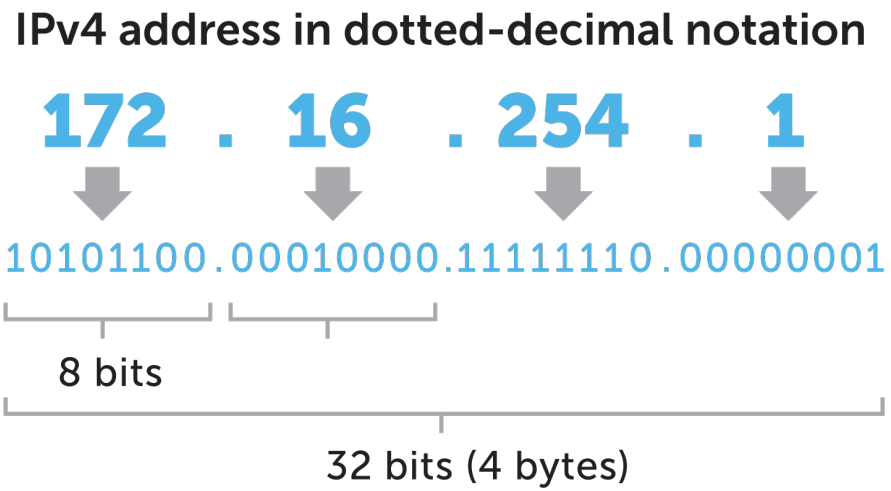
- Tier 1: Sprint, AT&T (ΗΠΑ), Deutsche Telekom (Γερμανία), Telia-Sonera (Σκανδιναβία), NTT (Ιαπωνία), KPN (Ολλανδία) Orange (Γαλλία), British Telecom (Ην. Βασίλειο)
- Tier 2: Τοπικοί, μικρότερης εμβέλειας ISPs. Αγοράζουν πρόσβαση από τους Tier 1

Τηλεπικοινωνιακή κίνηση στο Διαδίκτυο



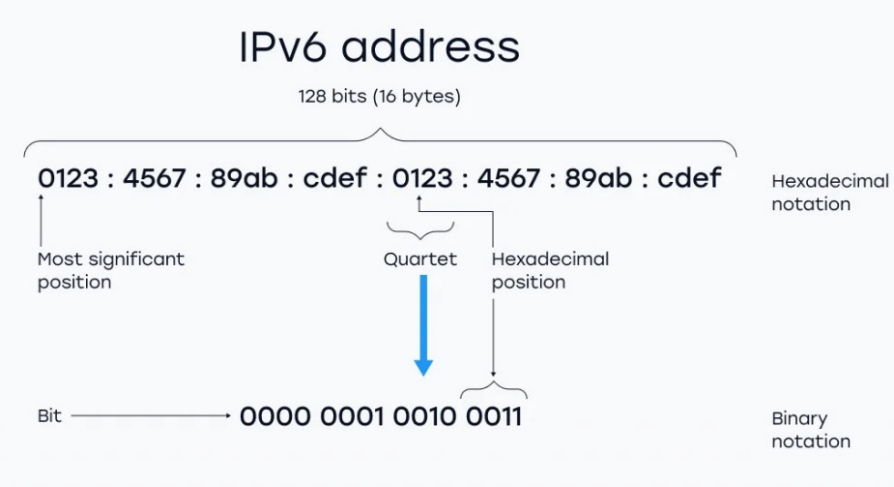
Διευθυνσιοδότηση στο Διαδίκτυο: διευθύνσεις IP

- **Διεύθυνση IP (IP address)**: σχήμα 4 bytes που χρησιμοποιείται για τον προσδιορισμό της **φυσικής διεύθυνσης** μιας **μοναδικής** μηχανής στο Διαδίκτυο (όπως ο τηλεφωνικός αριθμός +30 210 8203933 προσδιορίζει μια μοναδική τηλεφωνική σύνδεση)
- Οι **τελείες δεκαδικού συμβολισμού** αποτελούν το πρότυπο γραφής μίας IP διεύθυνσης και χωρίζουν τα 4 bytes της διεύθυνσης (πχ: 192.207.177.133): Το κάθε byte παίρνει τιμές από 0 ως 255



Διευθυνσιοδότηση στο Διαδίκτυο: διευθύνσεις IP

- **Διεύθυνση δικτύου Α**: 192.207.177.1xx
  - Περιλαμβάνει όλες τις μηχανές που έχουν IP address που αρχίζει με 192.207.177.1 (πχ 192.207.177.145,…)
- **ICANN**: Διαδικτυακός Οργανισμός για Εκχώρηση Ονομάτων και Αριθμών (Internet Corporation for Assigned Names and Numbers)
  - Εκχωρεί συνεχόμενες διευθύνσεις IP στους ISPs, που κατόπιν εκχωρούν αυτές τις διευθύνσεις μέσα στις περιοχές τους.
- Διεύθυνση IP: σχήματα των 32 ή 128 bit
  - 32 bit: IPv4
  - 128 bit: IPv6



Δείτε: https://en.wikipedia.org/wiki/IPv6

Μνημονικά ονόματα

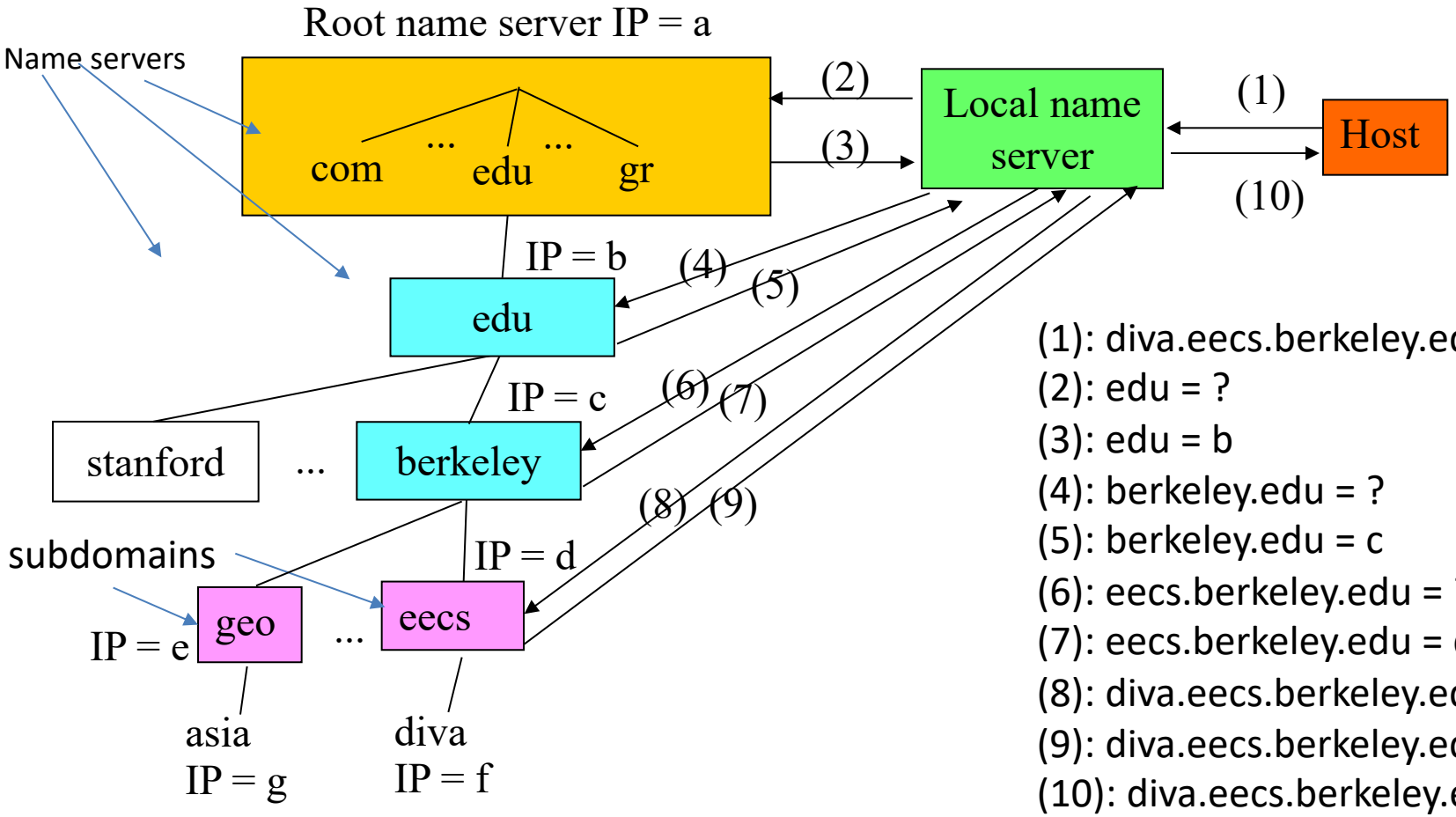
- Το **όνομα** ενός υπολογιστή (host name) (ή της υπηρεσίας που προσφέρει) είναι ένα μνημονικό όνομα, ακολουθούμενο από μια ιεραρχία από περιοχές (domains)
  - Όνομα υπολογιστή = υπηρεσία ή "παρατσούκλι" υπολογιστή.όνομα περιοχής (π.χ. dias.cs.aueb.gr, ftp.aueb.gr, www.in.gr)
  - **Υπηρεσία**: ftp, www, smtp, imap, pop3, telnet,…
- Το **όνομα περιοχής** (domain name) χαρακτηρίζει μια οντότητα, όχι απαραίτητα γεωγραφικά ενιαία (εταιρία, ISP, πανεπιστήμιο, δημόσιο οργανισμό,...)
  - Ιεραρχικό: www.aueb.gr, www.cs.aueb.gr
  - Η κατάληξη (**περιοχή ανώτατου επιπέδου - top-level domain**) κατηγοριοποιεί:
    - Κατά κατηγορία χρήσης – π.χ. .com = εμπορική περιοχή, .edu = πανεπιστήμιο, .gov = κυβερνητικός οργανισμός, …
    - Κατά χώρα – π.χ. .gr = περιοχή Ελλάδας

Domain Name System (DNS) – Σύστημα ονομάτων περιοχών

- Βασικό θέμα: πως βρίσκει ένα πρωτόκολλο την αντιστοιχία μνημονικό όνομα ←→ δικτυακή διεύθυνση (IP address)
  - Το μνημονικό όνομα της μηχανής χρησιμεύει στη διεπαφή με τον χρήστη
- **Domain Name System (DNS)**: κατάλογος ονομάτων περιοχών
  - Κάθε domain διατηρεί ένα **διακομιστή ονομάτων** (name server)
  - Ένας name server ενός domain γνωρίζει:
    - Τις IP διευθύνσεις των υπολογιστών εντός του domain που παρέχουν υπηρεσίες (ftp, smtp, www,…), ή έχουν κάποιο παρατσούκλι
    - Τις IP διευθύνσεις των name servers των sub-domains του (π.χ ο name server του aueb.gr γνωρίζει την IP address του name server του cs.aueb.gr – αλλά **όχι** τις IP διευθύνσεις των υπολογιστών εντός του cs.aueb.gr)

Λειτουργία του DNS

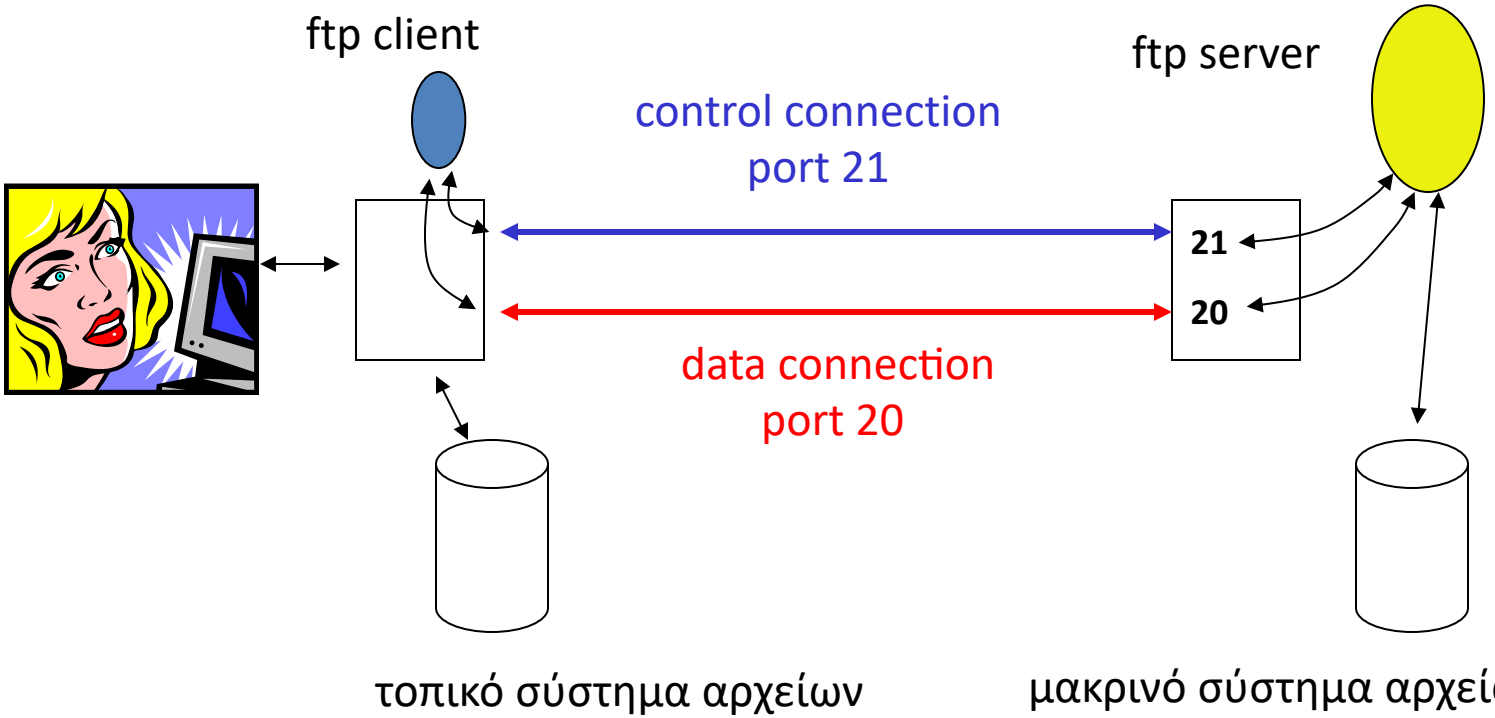
Παράδειγμα: Εύρεση του IP address για diva.eecs.berkeley.edu



(1): diva.eecs.berkeley.edu = ?
(2): edu = ?
(3): edu = b
(4): berkeley.edu = ?
(5): berkeley.edu = c
(6): eecs.berkeley.edu = ?
(7): eecs.berkeley.edu = d
(8): diva.eecs.berkeley.edu = ?
(9): diva.eecs.berkeley.edu = f
(10): diva.eecs.berkeley.edu = f

Οργάνωση name servers σε δεντρική δομή

Διαδικτυακές εφαρμογές: File Transfer Protocol



Control: user id, list, chdir, put, get, ...

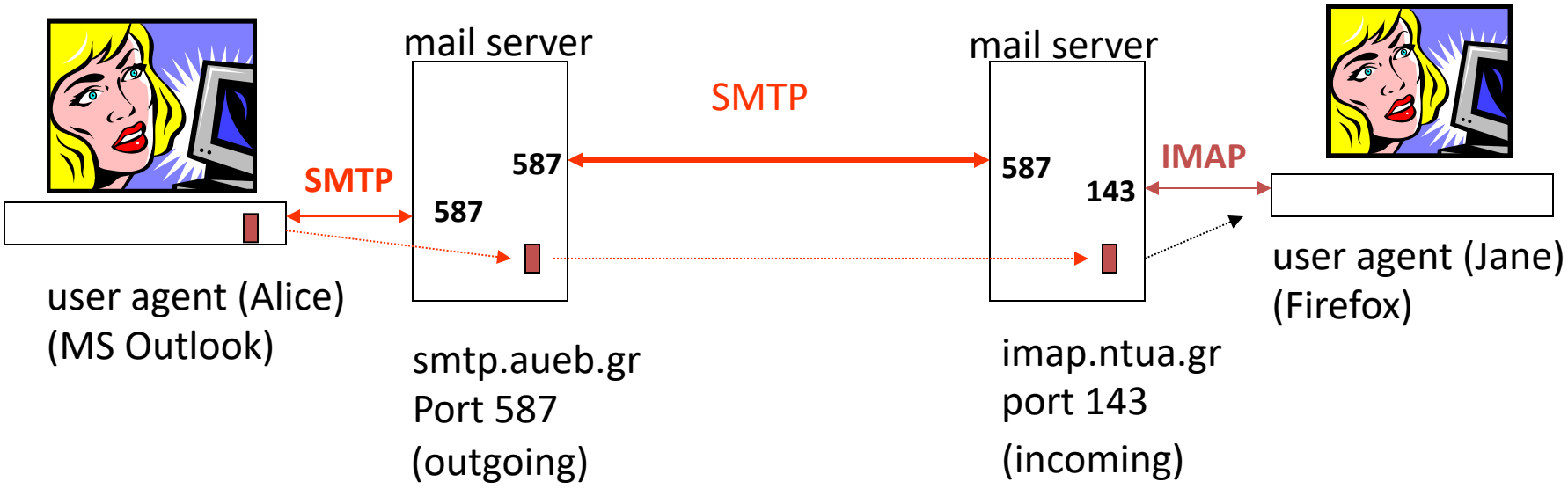
- Θύρα (port): κατασκευή λογισμικού, φροντίζει για την αναχώρηση ή άφιξη πακέτων για μια εφαρμογή
- Η θύρα του αποστολέα συνδέεται με την θύρα του παραλήπτη για να μεταδοθούν πακέτα για την εφαρμογή
- Ξεχωριστή θύρα για κάθε εφαρμογή

Ηλεκτρονικό Ταχυδρομείο (1)

- Ηλεκτρονική αλληλογραφία (email)
  - Ο διακομιστής αλληλογραφίας (mail server) συλλέγει και παραδίδει την εισερχόμενη αλληλογραφία και μεταδίδει την εξερχόμενη αλληλογραφία
- Μεταφορά μηνυμάτων μεταξύ mail servers: πρωτόκολλο SMTP (Simple Mail Transfer Protocol)
- Παραδίδει εισερχόμενη αλληλογραφία στους πελάτες μέσω των πρωτοκόλλων POP3 (Post Office Protocol 3) ή IMAP (Internet Mail Access Protocol)
  - POP3: τα μηνύματα κατεβάζονται και σώζονται τοπικά, στον υπολογιστή του χρήστη
    - Μπορεί να σώζονται και στον server ή όχι
    - Δεν υπάρχει πρόσβαση στα ίδια μηνύματα από διαφορετικούς clients
  - IMAP: τα μηνύματα σώζονται στον mail server
    - Πρόσβαση στα ίδια μηνύματα από πολλές διεπαφές: web, clients, webmail, από κινητό κλπ

Ηλεκτρονικό Ταχυδρομείο (2)

Αποστολή email από alice@aueb.gr σε jane@ntua.gr



Αποστολή e-mail:
Simple Mail Transfer Protocol (SMTP): port 587

Λήψη email:
POP3: port 110
IMAP: port 143

Link: https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

Ο Παγκόσμιος Ιστός – Ορολογία (1)

- **Παγκόσμιος Ιστός** (World Wide Web): ένα διαδίκτυο (δίκτυο υπολογιστών) που περιέχει έγγραφα **υπερκειμένου (hypertext)** (ή **υπερμέσα, hypermedia**)
  - Έγγραφα υπερκειμένου: ιστοσελίδες (web pages)
  - Οι ιστοσελίδες συνδέονται μεταξύ τους με υπερ-συνδέσμους (hyper-links)
  - **Τοποθεσία Ιστού** (Web site): συλλογή στενά συσχετισμένων ιστοσελίδων
    - Web site example: Amazon.com
    - Web pages of Amazon.com: registration page, contact page, about page…
  - **HTML**: γλώσσα σήμανσης εγγράφων υπερκειμένου

Ο Παγκόσμιος Ιστός – Ορολογία (2)

- **HTML**: γλώσσα σήμανσης εγγράφων υπερκειμένου (Hypertext Markup Language)
  - Κωδικοποιείται ως έγγραφο κειμένου
  - Περιέχει ετικέτες επικοινωνίας με το φυλλομετρητή
    - Πληροφορίες που χρειάζεται ο φυλλομετρητής για να εμφανίσει σωστά την σελίδα στον χρήστη
    - Εμφάνιση, π.χ.
      - <h1> για ξεκίνημα επικεφαλίδας επιπέδου 1
      - <p> για ξεκίνημα νέας παραγράφου
    - Σύνδεση με άλλα έγγραφα και περιεχόμενο
      - <a href = . . . >
    - Εισαγωγή εικόνων
      - <img src = . . . >

Μια απλή ιστοσελίδα

α. Η σελίδα κωδικοποιημένη με τη χρήση HTML.

Ετικέτα που προσδιορίζει την αρχή του εγγράφου

Αρχικές πληροφορίες

Τμήμα της σελίδας που θα εμφανίζεται στους φυλλομετρητές

Ετικέτα που προσδιορίζει το τέλος του εγγράφου

```
<html>
<head>
<title>σελίδα επίδειξης</title>
</head>
<body>
<h1>Η ιστοσελίδα μου</h1>
<p>Πατήστε εδώ για άλλη σελίδα.</p>
</body>
</html>
```

β. Η σελίδα όπως θα εμφανιζόταν στην οθόνη του υπολογιστή.

Μια βελτιωμένη ιστοσελίδα

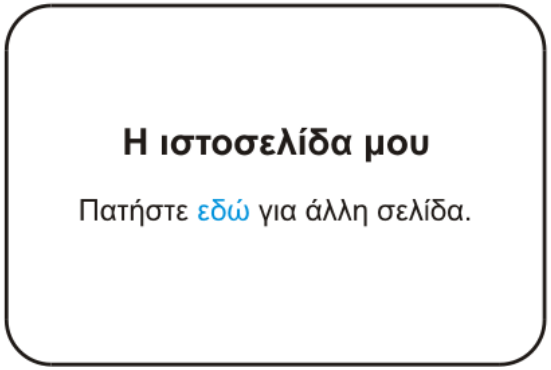
α. Η σελίδα κωδικοποιημένη με τη χρήση HTML.

```
<html>
<head>
<title>σελίδα επίδειξης</title>
</head>
<body>
<h1>Η ιστοσελίδα μου</h1>
<p>Πατήστε
   <a href="http://crafty.com/demo.html">
   εδώ
   </a>
   για άλλη σελίδα.</p>
</body>
</html>
```

Ετικέτα αγκύρωσης που περιέχει παράμετρο

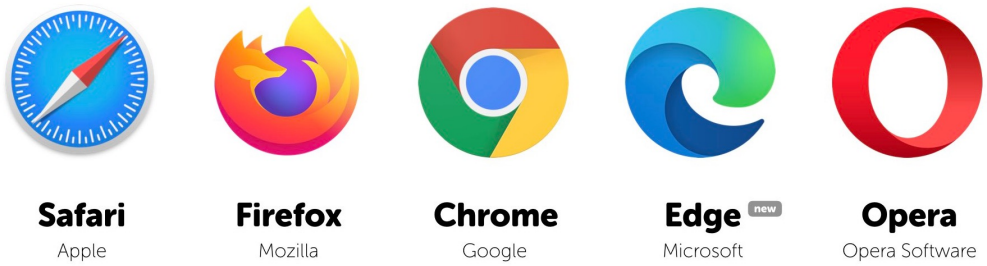
Κλείσιμο της ετικέτας αγκύρωσης

β. Η σελίδα όπως θα εμφανιζόταν στην οθόνη του υπολογιστή.

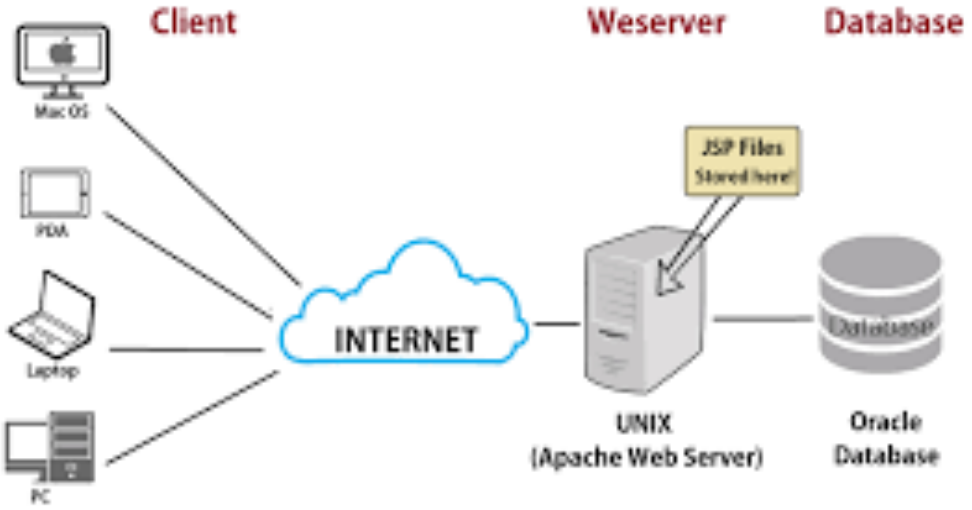


Ο Παγκόσμιος Ιστός – Ορολογία (3)

- **Φυλλομετρητής** (browser): πρόσβαση χρηστών στις ιστοσελίδες

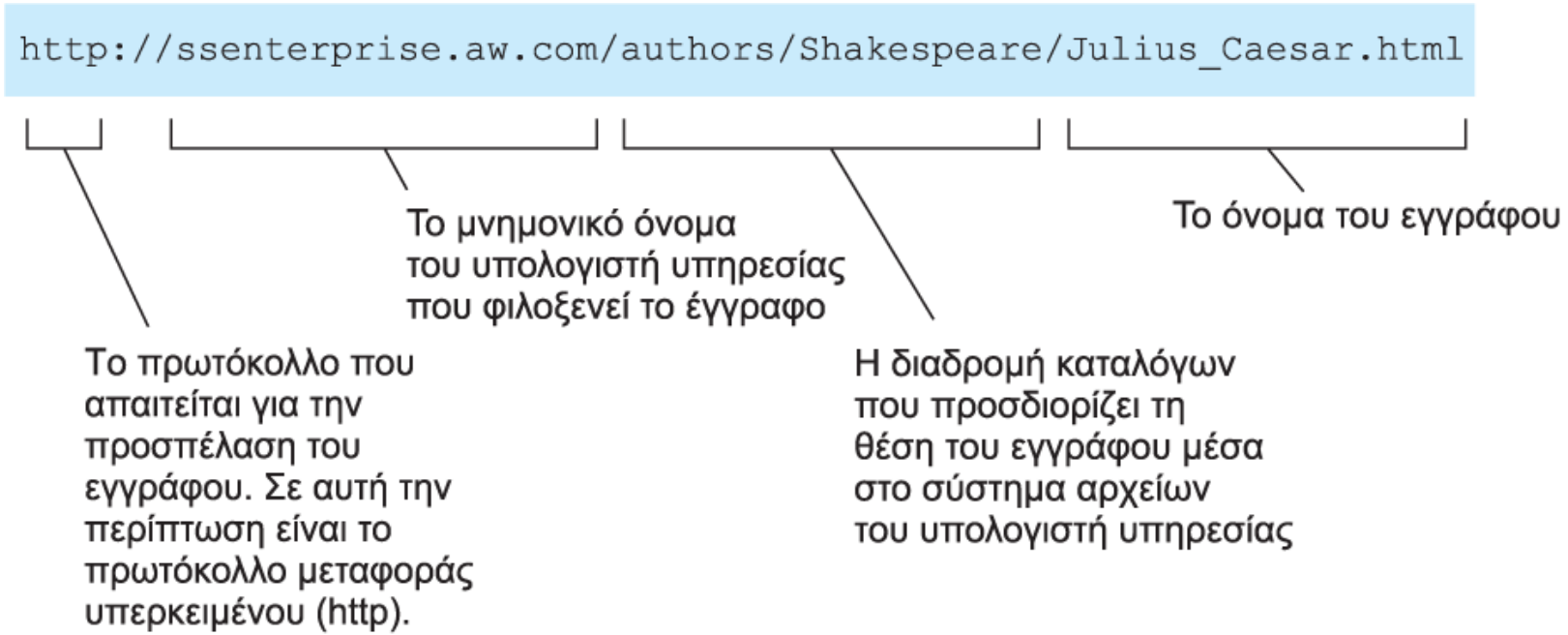


- **Διακομιστής Ιστού** (Web server): παρέχει πρόσβαση στα έγγραφά του σύμφωνα με τις αιτήσεις των πελατών/χρηστών



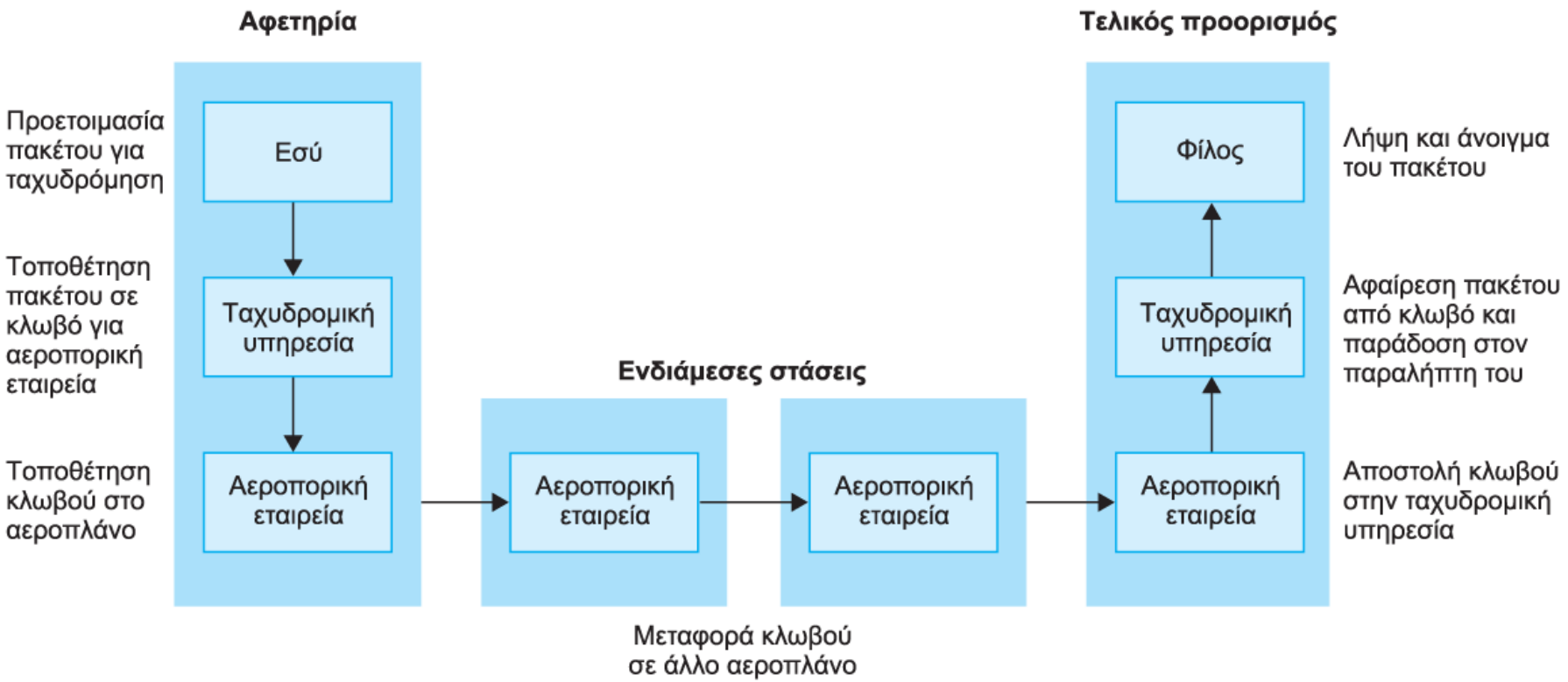
Ο Παγκόσμιος Ιστός – Ορολογία (4)

- **Πρωτόκολλο Μεταφοράς Υπερκειμένου** (Hyper-Text Transfer Protocol, HTTP): πρωτόκολλο που μεταφέρει έγγραφα υπερκειμένου μεταξύ φυλλομετρητή (browser) και διακομιστή Ιστού (web server)
- **Ενιαίος εντοπιστής πόρων** (Uniform Resource Locator, URL): η μοναδική διεύθυνση ενός εγγράφου στο δίκτυο



Ο browser του χρήστη επικοινωνεί με τον web server του υπολογιστή με όνομα ssenterprise.aw.com

Πρωτόκολλα Διαδικτύου: Παραλληλισμός με την ταχυδρόμηση πακέτου



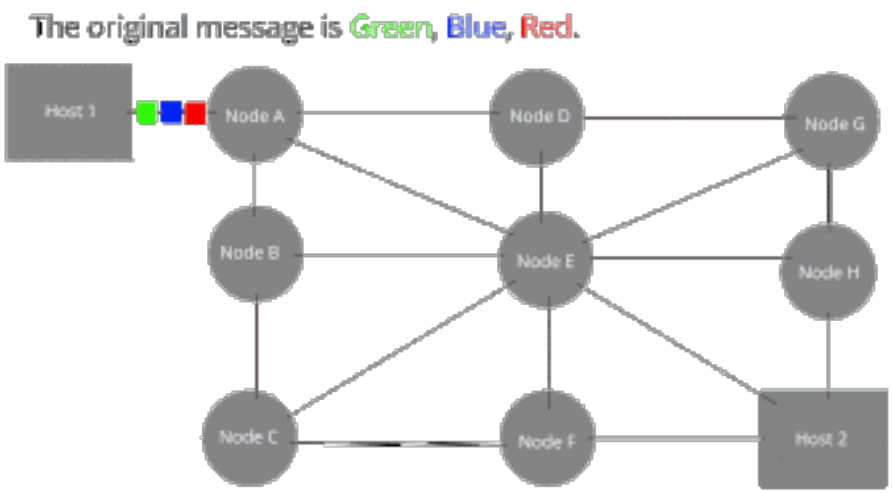
Πρωτόκολλο Διαδικτύου: προσδιορίζει πως μεταφέρεται η πληροφορία από μια μηχανή σε μια άλλη στο Διαδίκτυο

Επίπεδα διαδικτύου (Internet Layers)

- **Επίπεδο Εφαρμογής (Application Layer):** Κατασκευάζει το μήνυμα με διεύθυνση του παραλήπτη (π.χ. βίντεο).
- **Επίπεδο Μεταφοράς (Transport Layer):** Τεμαχίζει το μήνυμα σε πακέτα.
- **Επίπεδο Δικτύου (Network Layer):** Χειρίζεται τη δρομολόγηση μέσω του Διαδικτύου, προς τα που θα κατευθυνθούν τα πακέτα.
- **Επίπεδο Συνδέσμου (Link Layer):** Χειρίζεται τη μετάδοση των πακέτων μεταξύ 2 κόμβων.
- Κάτω από το επίπεδο συνδέσμου, υπάρχει το **Φυσικό Επίπεδο (Physical Layer)** όπου η πληροφορία είναι bits.

Επίπεδα Μεταφοράς και Δικτύου

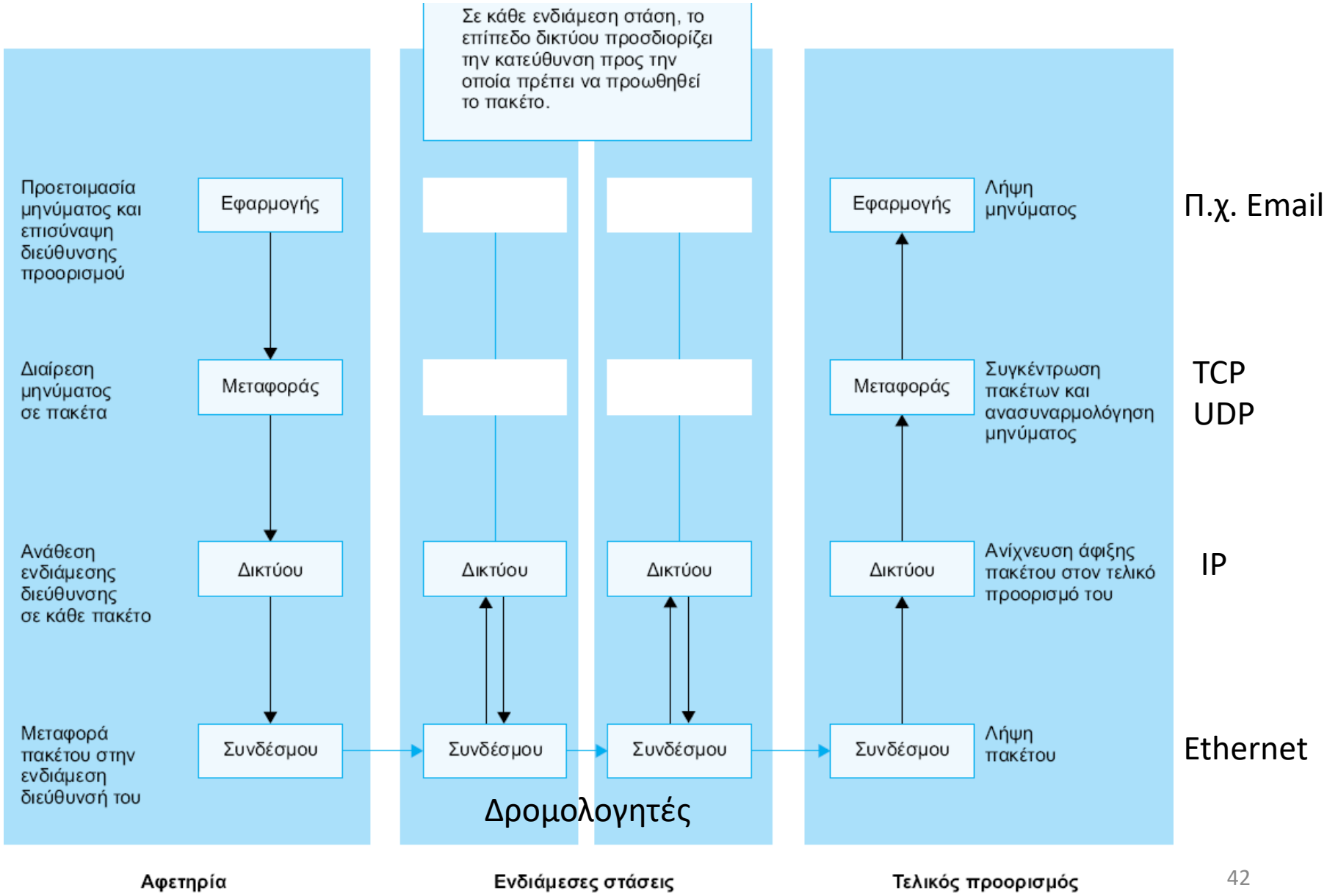
- Επίπεδο Μεταφοράς: χωρίζει την πληροφορία σε πακέτα και τη δίνει στο επίπεδο δικτύου
  - Το κάθε πακέτο από εδώ και πέρα ταξιδεύει ανεξάρτητα από τα άλλα
  - Πακέτα που έχουν τον ίδιο παραλήπτη μπορεί να ακολουθήσουν διαφορετικές διαδρομές προς αυτόν
- Επίπεδο Δικτύου: Δρομολόγηση (routing)
  - Κάθε δρομολογητής έχει έναν πίνακα (πίνακας προώθησης) με διευθύνσεις άλλων δρομολογητών
  - Μπορεί να έχει και άλλες πληροφορίες, π.χ. πόση καθυστέρηση υπάρχει από αυτόν προς έναν άλλον δρομολογητή
  - Προωθεί τα πακέτα και τελικά καθορίζει το μονοπάτι που αυτά θα ακολουθήσουν στο διαδίκτυο



Επίπεδο Συνδέσμου (Link Layer)

- Επίπεδο Δικτύου: προσδιορίζει τη μετάδοση προς τον επόμενο κόμβο
- Επίπεδο Συνδέσμου: έχει την ευθύνη για την μετάδοση του πακέτου στον αμέσως επόμενο κόμβο (δεν ενδιαφέρεται που θα πάει τελικά το πακέτο)
- Πρωτόκολλα σε επίπεδο συνδέσμου: π.χ. CSMA/CA, CSMA/CD
- Το επίπεδο Συνδέσμου στον δέκτη ελέγχει αν το πακέτο έχει ληφθεί σωστά
  - Με κώδικες ανίχνευσης λαθών
  - Αν μπορεί, διορθώνει τα λάθη (σε συνεργασία με το φυσικό επίπεδο) με κώδικες διόρθωσης λαθών
  - Αν όχι, ζητά επαναμετάδοση από τον πομπό

Διαστρωμάτωση και Διαδικτυακά πρωτόκολλα

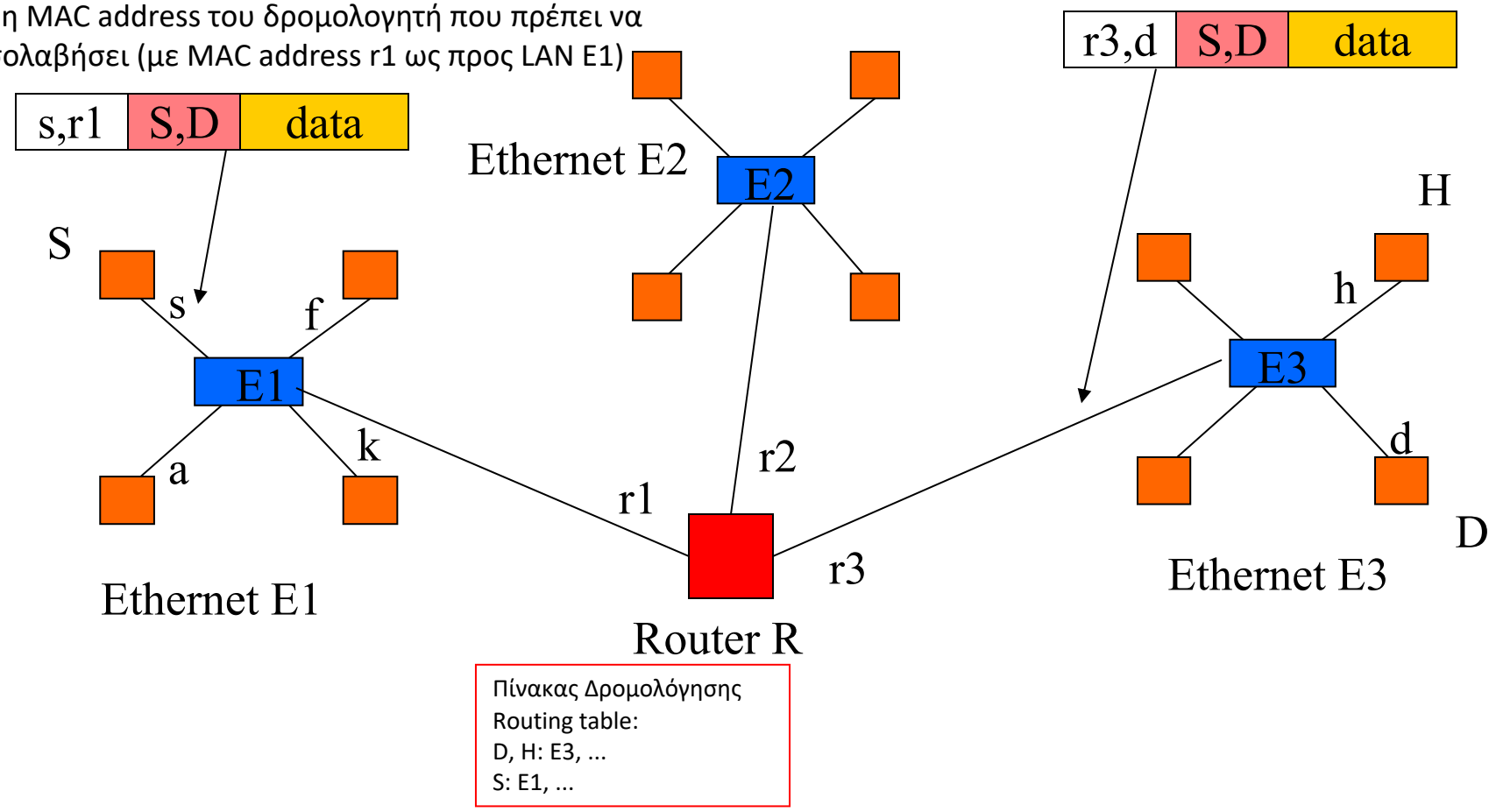


Πρωτοκόλλο Δρομολόγησης IP

- Κάθε φορά που μια πηγή στέλνει ένα πακέτο, βάζει σε αυτό:
  - Διευθύνσεις (IP) αποστολέα και προορισμού
  - Δεδομένα (Data)
  - Μετρητής αλμάτων (hop count) ή χρόνος ζωής (Time to Live, TTL) πακέτου
    - Είναι ο μέγιστος αριθμός φορών που μπορεί να προωθηθεί ένα πακέτο πριν φτάσει στον προορισμό του
    - Περιορίζει την άσκοπη διαρκή κυκλοφορία πακέτων στο δίκτυο
- Δρομολόγηση: Μπορεί να αλλάζει το μονοπάτι (route) από την πηγή προς τον προορισμό σε περίπτωση ανάγκης (π.χ. αν το μονοπάτι κοπεί για κάποιο λόγο, αν έρθει ένας νέος κόμβος, κ.α.)
- Internet Protocol (IP), IPv4 και IPv6
  - IPv4: διευθύνσεις 32-bit: 4 ομάδες της δεκαδικής αναπαράστασης ενός byte
    - Π.χ. 192.0.5.255
  - IPv6: διευθύνσεις 128-bit: 8 ομάδες των 4 δεκαεξαδικών ψηφίων χωρισμένες με “:”
    - Π.χ. 2001:0db8:85a3:0042:1000:8a2e:0370:7334.

Παράδειγμα Δρομολόγησης (1)

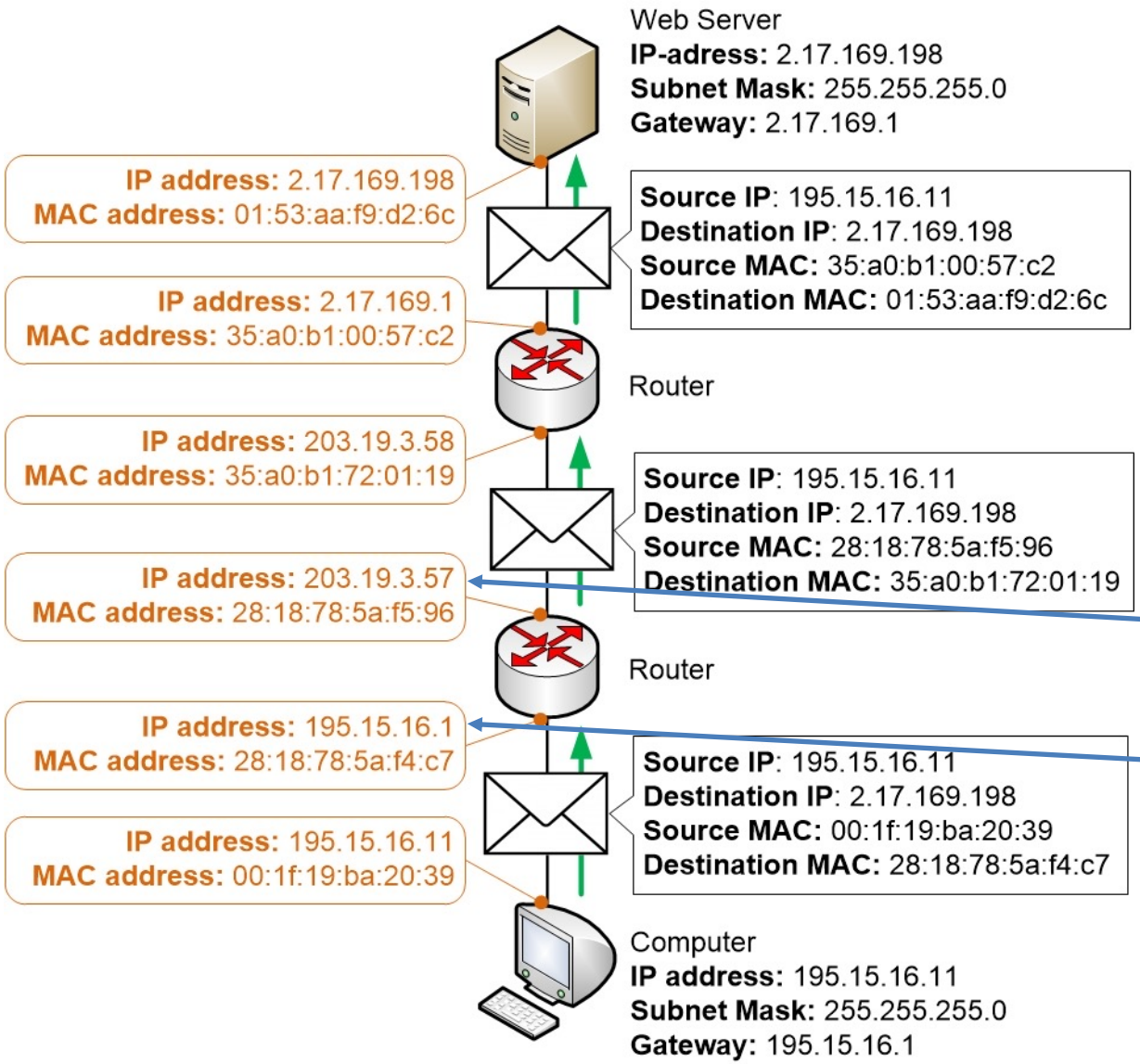
Πακέτο από κόμβο με δ/νση S προς κόμβο με δ/νση D.
Στο έξω μέρος μπαίνει η MAC address (s) της πηγής,
και η MAC address του δρομολογητή που πρέπει να
μεσολαβήσει (με MAC address r1 ως προς LAN E1)



Πίνακας Δρομολόγησης
Routing table:
D, H: E3, ...
S: E1, ...

Ο δρομολογητής με network address R **έχει mac address r1 ως προς LAN E1 Και r3 ως προς LAN E3**. Προωθεί το πακέτο που προορίζεται για D στο LAN E3. Βγάζει το έξω μέρος του πακέτου και βάζει το δικό του mac (r3), και την mac address προορισμού (d). Το E3 προωθεί στον D.

Παράδειγμα Δρομολόγησης (2)



Κάθε συσκευή έχει διαφορετική MAC address για κάθε δίκτυο στο οποίο συνδέεται.

WAN (public) IP address to connect to the Internet

LAN (private) IP address

IP address vs MAC address

Difference between IP Address vs MAC Address

IP Address	MAC Address
1. IP stands for Internet Protocol.	1. MAC stands for Media Access Control.
2. It is a Logical Address.	2. It is a Physical Address.
3. It is provided by the Internet Service Provider(ISP)	3. It is provided by Comp. Manufacturer.
4. It can be changed by changing ISP.	4. MAC Address is fixed Address for a particular device.
5. It has various classes like A,B,C,D,E.	5. It has no class concept.
6. It is applicable on Network Layer of OSI Model	6.It is applicable on Data link Layer of OSI Model.
7. The Length of IPv4 is 32 bits. The Length of IPv6 is 128 bits.	7. The length of MAC Address is 48 bits.

Παράδειγμα IP address (in IPv4)
150.60.122.98

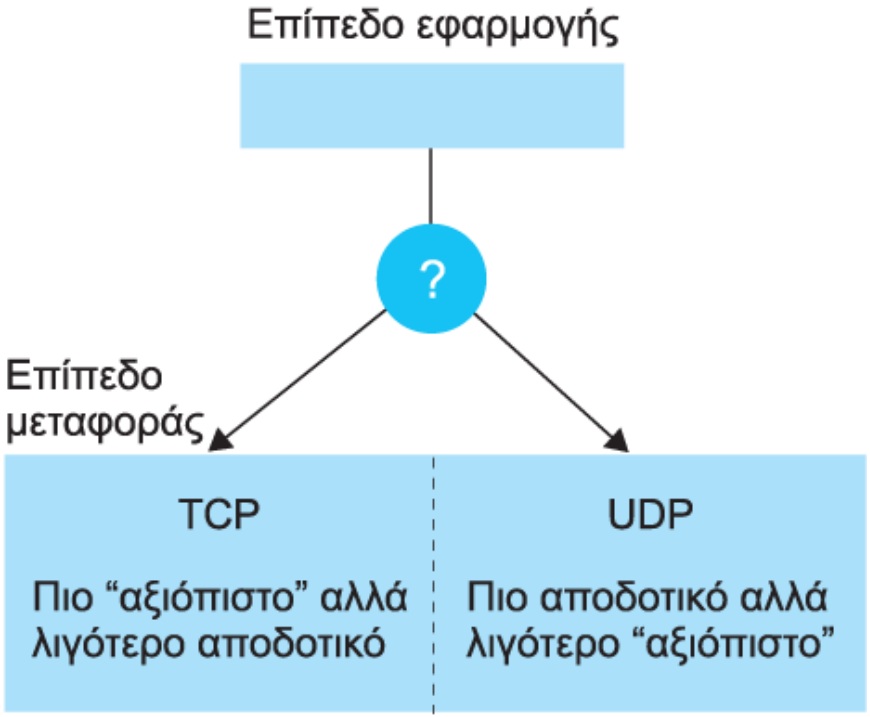
Παράδειγμα MAC address
00:0C:F5:09:56:E8

Η MAC address είναι σαν το όνομά σου ή ο αριθμός ταυτότητας, δεν αλλάζει. Αν κάποιος θέλει να επικοινωνήσει μαζί σου χρειάζεται το τηλέφωνό σου στο χώρο που βρίσκεσαι. Η IP address είναι σαν το νούμερο του τηλεφώνου.

Πρωτόκολλα για επίπεδο μεταφοράς

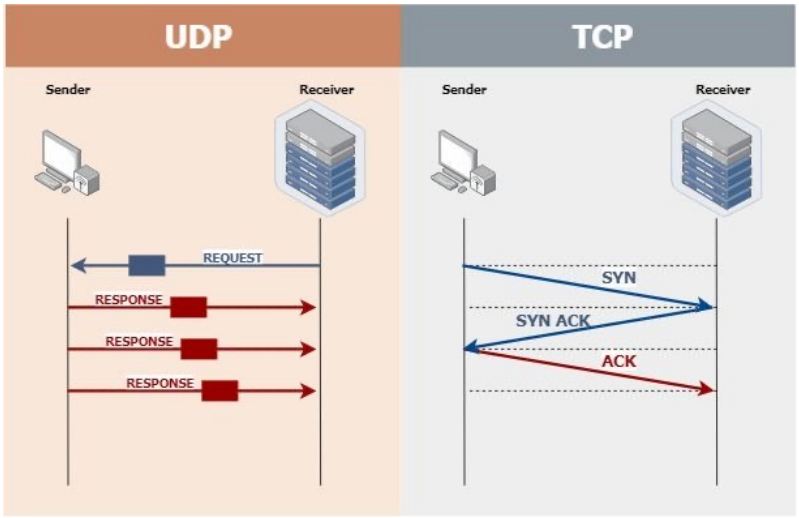
Πρωτόκολλα για Επίπεδο μεταφοράς

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)
- Αναλογία με το είδος ταχυδρομικής υπηρεσίας συστημένο ή express



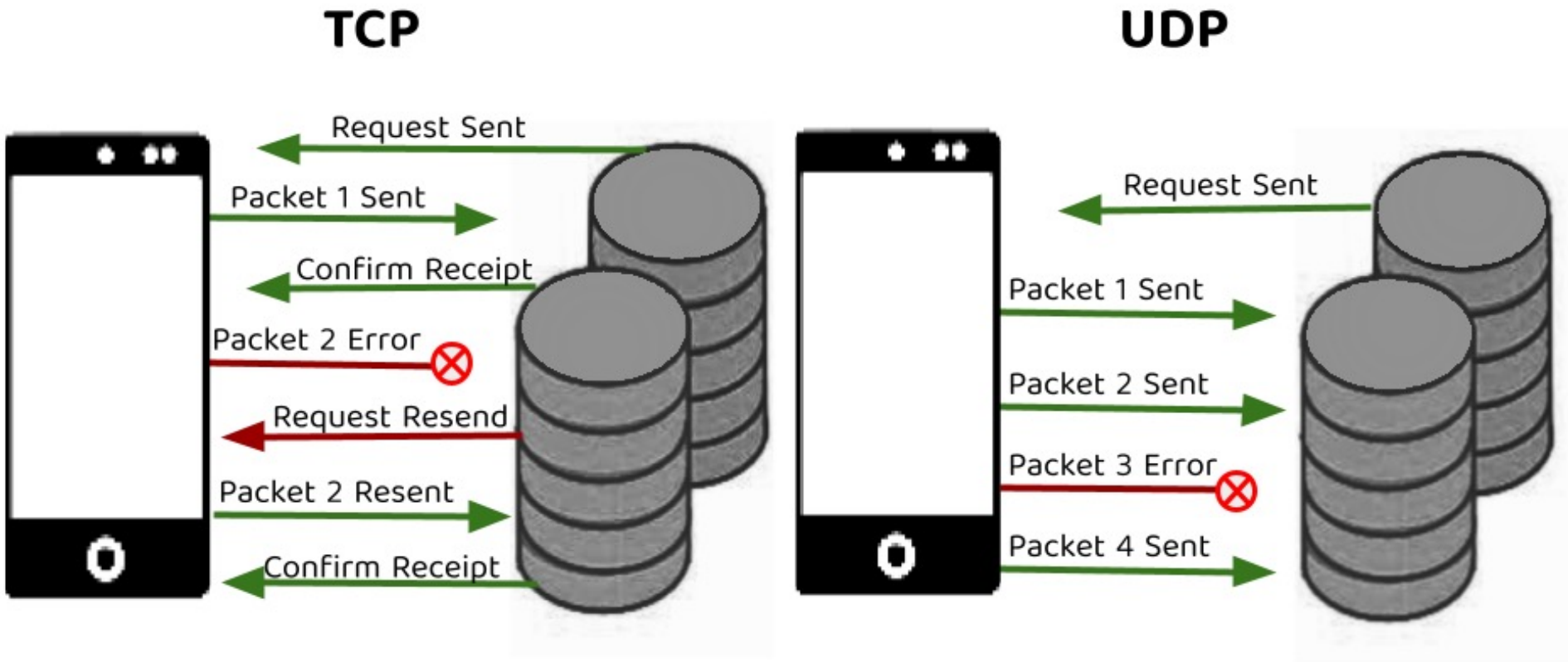
Διαφορές TCP και UDP (1)

- 1. Αποκατάσταση και προετοιμασία σύνδεσης πριν την μετάδοση
  - TCP: πριν τη μετάδοση, το επίπεδο μεταφοράς της πηγής αποστέλλει μήνυμα προς το επίπεδο μεταφοράς του προορισμού και περιμένει επιβεβαίωση (acknowledgment, ACK)
  - UDP: πρωτόκολλο χωρίς σύνδεση, απλά μεταδίδει



- 2. Έλεγχος λήψης στον προορισμό
  - TCP: πακέτα επιβεβαίωσης (ACK) από τον προορισμό. Αν ένα πακέτο δεν έχει επιβεβαιωθεί, επαναμετάδοση (retransmission) από την πηγή
  - UDP: δεν κάνει επαναμεταδόσεις (όχι αξιόπιστο πρωτόκολλο)

Πρωτόκολλα για επίπεδο μεταφοράς



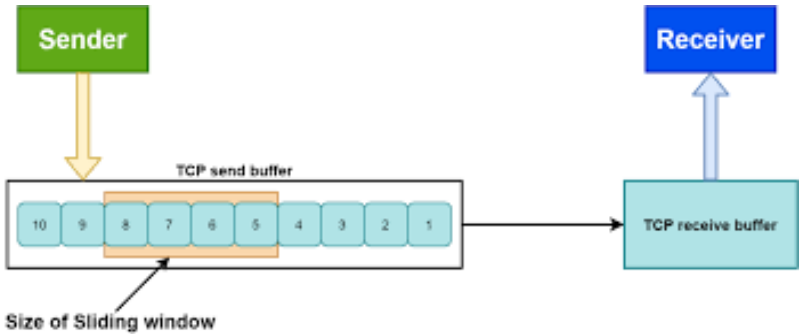
Source: Medium.com

Πότε χρησιμοποιείται το TCP και πότε το UDP?

- UDP: Αν η εφαρμογή είναι ευαίσθητη σε χρόνο (time-sensitive), δηλ. χρειάζεται να διεκπεραιωθεί γρήγορα, π.χ. gaming, streaming, αναζήτηση DNS
- TCP: Αν είναι πιο σημαντική η ασφαλής μετάδοση και όχι ο χρόνος, π.χ. emails, chatting, browsing

Θέματα στο Επίπεδο Μεταφοράς

- Στην πορεία των πακέτων καθ' οδόν προς τον προορισμό μπορεί να υπάρξουν προβλήματα
- **Στον προορισμό:**
  - Ο προορισμός έχει έναν buffer
  - Το επίπεδο εφαρμογής στον προορισμό μπορεί να αργεί να «διαβάσει» πακέτα από τον buffer
  - Στόχος: να **ταιριάξει** ο ρυθμός εκπομπής από την πηγή στον ρυθμό απορρόφησης από τον προορισμό
- **Μέσα στο δίκτυο:** συμβαίνουν απώλειες πακέτων
  - λόγω του ότι μπορεί να γεμίσει ο buffer **κάποιου κόμβου** στη διαδρομή (buffer overflow), απορρίπτοντας τα επιπλέον πακέτα
    - Αυτά τα πακέτα δεν επιβεβαιώνονται από τον προορισμό
    - Επαναμεταδίδονται από την πηγή
    - Η πηγή θα ελαττώσει το ρυθμό μετάδοσης
  - Μεγάλες καθυστερήσεις (αναμονή στις ουρές των buffers στους δρομολογητές)



Ελέγχου Συμφόρησης από-άκρο-σε-άκρο

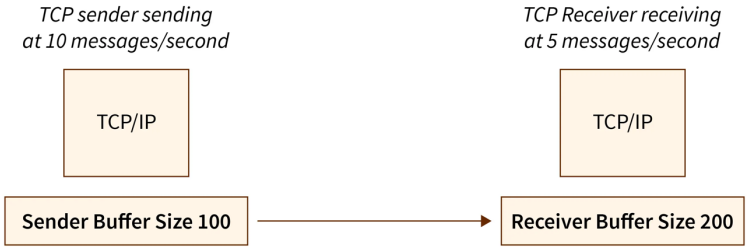
End-end congestion control

- Δεν χρησιμοποιεί πληροφορίες από το δίκτυο ως ανατροφοδότηση
- Προβλέπει/συμπεραίνει την συμφόρηση από μετρήσεις που κάνει η συσκευή του χρήστη (end-system) από τις καθυστερήσεις ή τις απώλειες πακέτων
- Αυτή η προσέγγιση ακολουθείται από το TCP
- Αυτό χρησιμοποιείται τώρα στο Διαδίκτυο

Η Έννοια του Ελέγχου Ροής

Γρήγορος αποστολέας, αργός δέκτης

- Ο **παραλήπτης** λαμβάνει πακέτα που αποστέλλονται από τον αποστολέα με ρυθμό 5 πακέτα/sec.
- Ο **αποστολέας** στέλνει πακέτα με ρυθμό 10 πακέτα/sec.
- Όταν ο αποστολέας στέλνει το πακέτο στον δέκτη, αυτό μπαίνει στην ουρά/buffer του παραλήπτη.
- Με τι ρυθμό γεμίζει ο **buffer** του παραλήπτη; 10-5=5 πακέτα/sec.
- Αν το **μέγεθος buffer** του παραλήπτη μπορεί να φιλοξενήσει 200 πακέτα, σε πόσο χρόνο θα γεμίσει ο buffer; Σε 40 sec
- Έτσι, **μετά από 40 δευτερόλεπτα**, τα πακέτα θα χάνονται καθώς δεν θα υπάρχει χώρος για τα εισερχόμενα πακέτα.

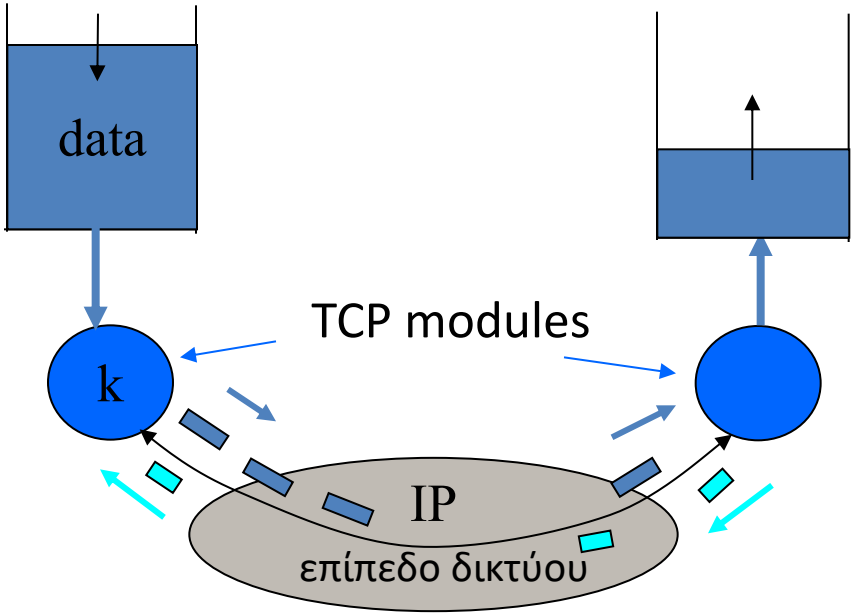


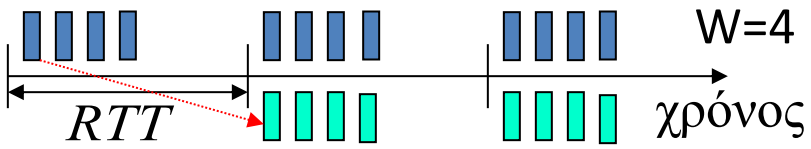
Link: https://www.scaler.com/topics/computer-network/tcp-flow-control/

Έλεγχος ροής TCP (1)

Αλγόριθμος (input: W: παράθυρο TCP)
Μέτρα το k : αριθμός μη επιβεβαιωμένων πακέτων

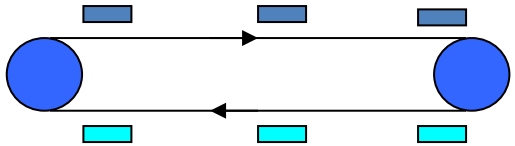
- Στέλνε πακέτα όσο k ≤ W
- Μην στέλνεις εάν k > W
- Ξαναστείλε τα χαμένα πακέτα
- Διάλεγε συνέχεια το σωστό W





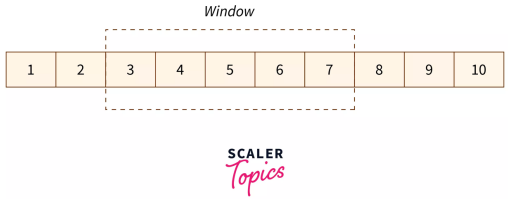
= πακέτα δεδομένων

= επιβεβαιώσεις (acknowledgements, ACKs)



RTT (round-trip time): χρόνος μέχρι να πάει ένα πακέτο στον προορισμό και να επιστρέψει στην πηγή πακέτο επιβεβαίωσης (ack) από αυτόν στην πηγή

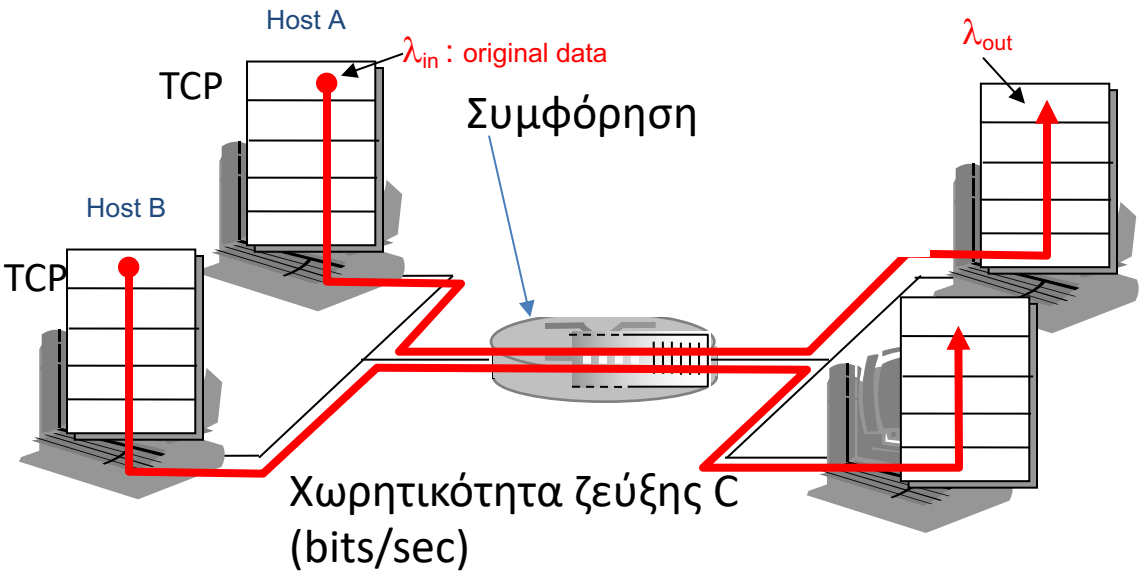
Έλεγχος ροής TCP (2)

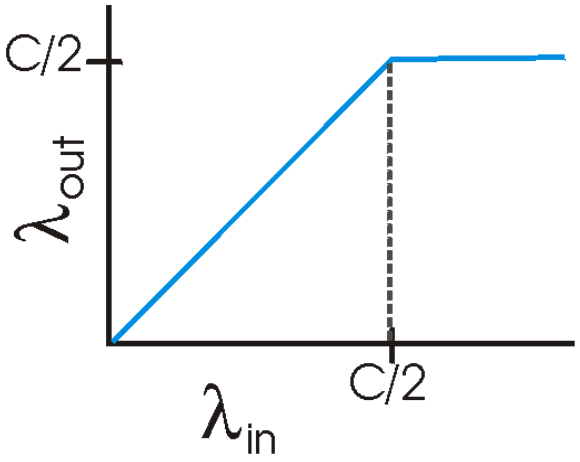


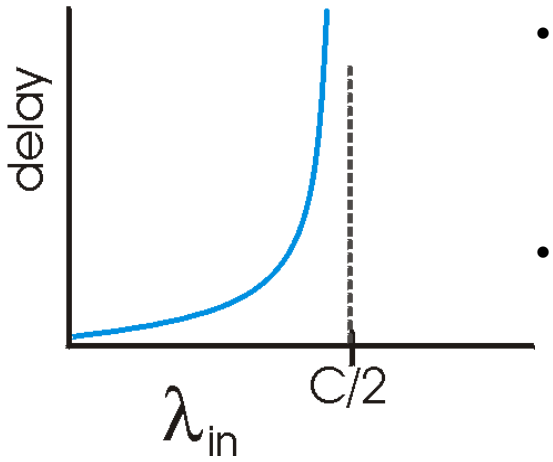
- Παράθυρο TCP (TCP window) W:
  αριθμός των πακέτων που μεταδίδονται
  - Έστω τα πακέτα αριθμούνται 0,1,2,...
  - k = (Αριθμός τελευταίου πακέτου που στάλθηκε) – (Αριθμός τελευταίου πακέτου που επιβεβαιώθηκε)
  - Στέλνε όσο k ≤ W, μη στέλνεις αν k > W (και ξαναστείλε τα μη επιβεβαιωμένα πακέτα)
- Αλλάζοντας το W, **αυξομειώνω** το ρυθμό μετάδοσης πακέτων
  - W μικρό: Σημαίνει ότι σταματώ την μετάδοση πιο συχνά (για να ξαναστέλνω τα μη επιβεβαιωμένα πακέτα)
    - άρα δε μεταδίδω νέα πακέτα συχνά
  - W μεγάλο: σημαίνει ότι σταματώ τη μετάδοση λιγότερο συχνά (για να ξαναστέλνω τα μη επιβεβαιωμένα πακέτα)
- Μέγιστος ρυθμός μετάδοσης πακέτων:
  - R = W / (RTT) (πακέτα/sec)
  - αριθμός μεταδιδόμενων πακέτων ανά μονάδα χρόνου

Έλεγχος συμφόρησης (Congestion Control)

- 2 πηγές, 2 προορισμοί
- 1 δρομολογητής, μεγάλο μέγεθος buffer
- Μέγιστο ποσό bits/sec που μπορεί να σταλεί σε μια ζεύξη ανά μονάδα χρόνου → χωρητικότητα ζεύξης (link capacity)







- C/2: Μέγιστη δυνατή ρυθμοαπόδοση (throughput) ανά πηγή (bits/sec)
- **Καθυστέρηση στην λήψη πακέτων** στον προορισμό λόγω συμφόρησης στη ζεύξη αν $\lambda_A+\lambda_B > C$

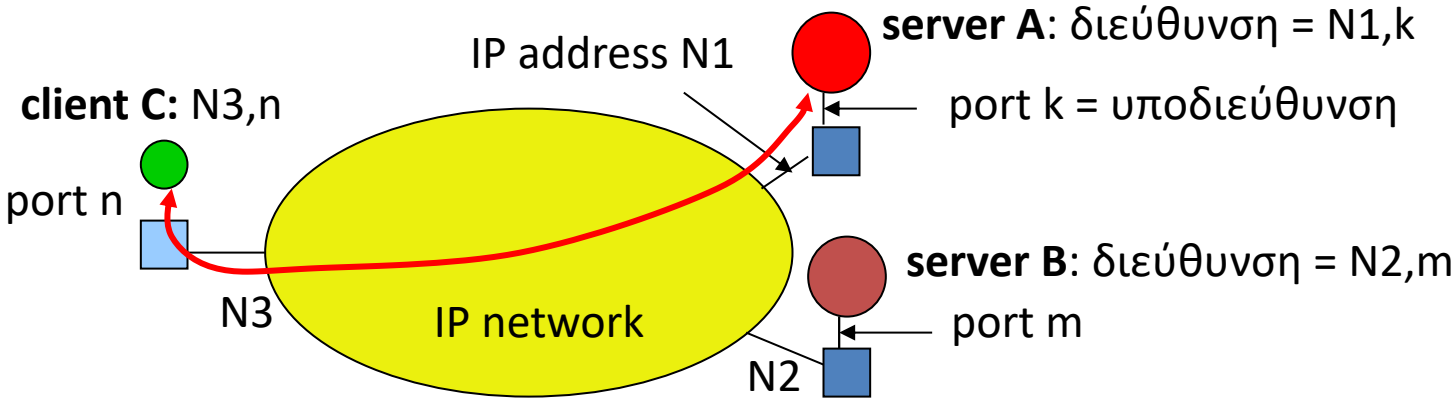
Σήμα από τον buffer μεταδίδεται πίσω στην πηγή (congestion notification signal)

Διαφορές TCP και UDP (2)

- 3. Έλεγχος Ροής (flow control)
  - TCP: αυξομείωση ρυθμού μετάδοσης πακέτων από την πηγή
  - Αν π.χ. ο προορισμός δεν επιβεβαιώνει πακέτα, η πηγή μειώνει το ρυθμό μετάδοσης πακέτων
  - UDP: δεν παρέχει έλεγχο ροής
- 4. Έλεγχος συμφόρησης (congestion control)
  - TCP: αυξομείωση ρυθμού μετάδοσης πακέτων από την πηγή για αντιμετώπιση συμφόρησης κίνησης σε κάποιο ενδιάμεσο σημείο μεταξύ πηγής-προορισμού
  - Σήμα ειδοποίησης για συμφόρηση (congestion notification signal)
  - Αν π.χ. ένας κόμβος στείλει τέτοιο μήνυμα, ή αν η μετρούμενη καθυστέρηση λήψης είναι μεγάλη, η πηγή μειώνει το ρυθμό μετάδοσης πακέτων
  - UDP: δεν παρέχει έλεγχο συμφόρησης

Επίπεδο Εφαρμογής: Σύνδεση εφαρμογών σε θύρες (ports)

Πλήρης διεύθυνση διαδικασίας = [IP address , port #]



- Θύρα (port) "εσωτερικά γραμματοκιβώτια": κατασκευή λογισμικού, συγκεκριμένη για μια εφαρμογή ή διεργασία
- Χρησιμεύει ως αναγνωριστικό για την εκτέλεση της εφαρμογής

- **Servers**: ακούν σε γνωστές θύρες
- **Clients**: συνδέονται στους servers, **παίρνουν** πληροφορία, την παρουσιάζουν στους χρήστες

- Αφού ληφθεί το μήνυμα στο επίπεδο μεταφοράς στον προορισμό, αυτό το προωθεί στην κατάλληλη θύρα στο επίπεδο εφαρμογής (π.χ. Θύρα 80 για HTTP)

Επιθέσεις και Ασφάλεια Υπολογιστών

- Κακόβουλο λογισμικό:
  - **Ιός (virus):** εισέρχεται σε προγράμματα, προκαλεί διάφορες δυσλειτουργίες
  - **Σκουλήκι (worm):** ταξιδεύει στο δίκτυο, εγκαθίσταται στον Η/Υ και προωθεί αντίγραφά του σε άλλους Η/Υ
  - **Δούρειος ίππος (Trojan horse):** εισέρχεται στον Η/Υ μεταμφιεσμένο σε κάποιο επιθυμητό λογισμικό
  - **Λογισμικό υποκλοπής (spyware/sniffing software):** συλλέγει πληροφορίες για την δραστηριότητα
- Ψάρεμα (phishing): απόκτηση πληροφορίας ζητώντας τη ρητά (μέσω δελεαστικών emails)
- Άρνηση υπηρεσίας (Denial of Service): υπερφόρτωση server με (ψεύτικα) αιτήματα
- Ενοχλητική ηλεκτρονική αλληλογραφία (spam)

Προστασία

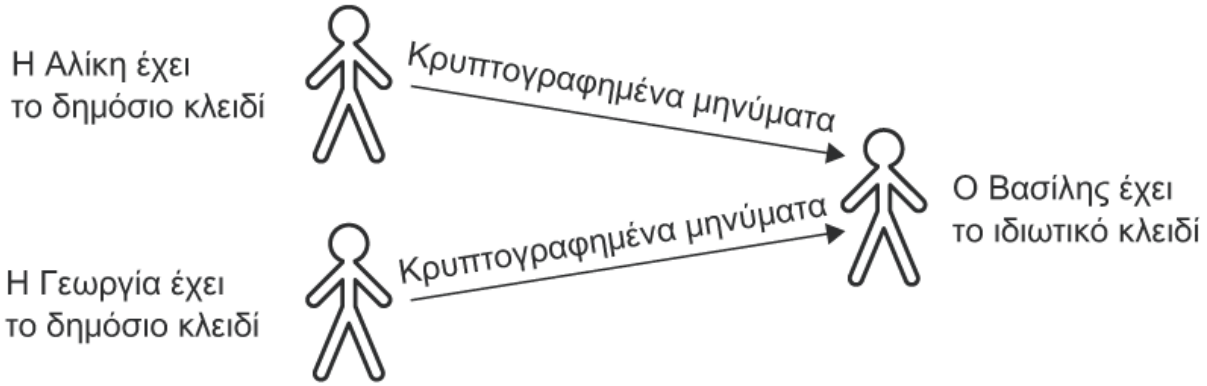
- Τείχη προστασίας (firewalls): φιλτράρισμα πληροφορίας που περνάει μέσα στο τοπικό δίκτυο
- Φίλτρα για ενοχλητική αλληλογραφία (spam filters)
- Λογισμικό προστασίας από ιούς (antivirus): ανιχνεύει και απομακρύνει ιούς

Κρυπτογράφηση (encryption)

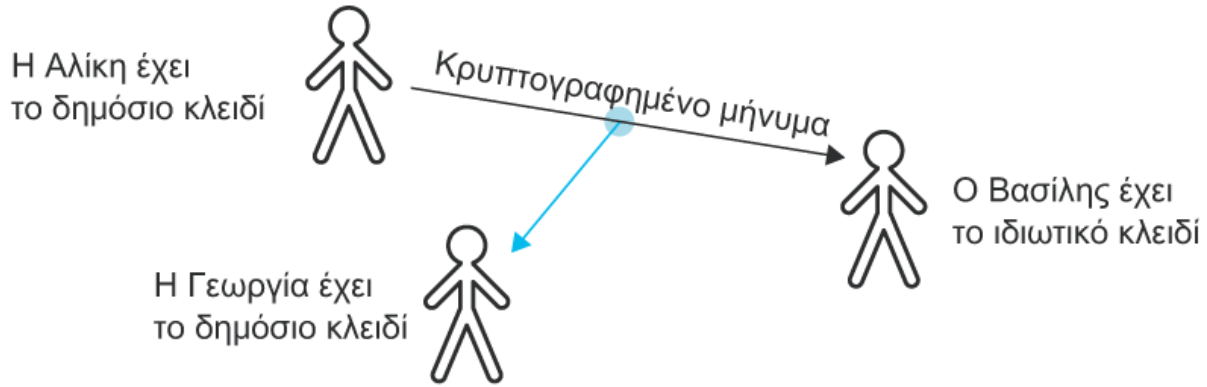
- Κρυπτογράφημένη (κωδικοποιημένη) μετάδοση πληροφορίας για να αποτραπεί η υποκλοπή της
  - Κάθε πακέτο πληροφορίας μετατρέπεται σε ένα κρυπτογραφημένο πακέτο
- Κρυπτογραφία δημόσιου κλειδιού (public-key encryption)
  - Δημόσιο κλειδί: χρησιμοποιείται για κρυπτογράφηση μηνυμάτων που στέλνονται
  - Ιδιωτικό κλειδί: Χρησιμοποιείται για αποκρυπτογράφηση μηνυμάτων από τους δέκτες
  - Η γνώση για το πως κρυπτογραφούνται τα μηνύματα δεν προσφέρει δυνατότητα για αποκρυπτογράφηση

Κλειδί: παράμετρος που καθορίζει το αποτέλεσμα της κρυπτογράφησης δηλ. της απεικόνισης plaintext -> ciphertext

Κρυπτογράφηση δημόσιου κλειδιού

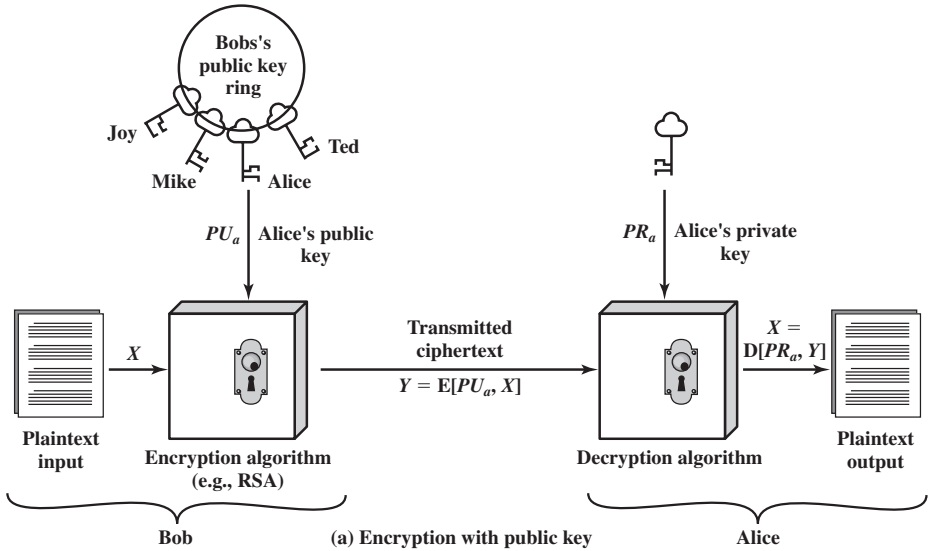


Η Αλίκη και η Γεωργία μπορούν να στέλνουν κρυπτογραφημένα μηνύματα στον Βασίλη



Η Γεωργία δεν μπορεί να αποκρυπτογραφήσει το μήνυμα της Αλίκης, παρόλο που γνωρίζει πώς το κρυπτογράφησε εκείνη.

Κρυπτογράφηση δημόσιου κλειδιού (Public Key Encryption - PKE)



- Κάθε χρήστης **δημιουργεί ένα ζεύγος κλειδιών** που χρησιμοποιούνται για κρυπτογράφηση και αποκρυπτογράφηση μηνυμάτων προς αυτόν
- Τοποθετεί ένα από τα δύο κλειδιά σε δημόσιο μητρώο (registry) ή προσβάσιμο αρχείο
  - Αυτό είναι το δημόσιο κλειδί
  - Το άλλο κλειδί παραμένει ιδιωτικό
- Κάθε χρήστης διατηρεί μια συλλογή δημόσιων κλειδιών που έχουν ληφθεί από άλλους
- Αν ο Bob επιθυμεί να στείλει προσωπικό μήνυμα στην Alice, ο Bob κρυπτογραφεί το μήνυμα χρησιμοποιώντας το δημόσιο κλειδί της Alice
- Όταν η Alice λαμβάνει το μήνυμα, το αποκρυπτογραφεί χρησιμοποιώντας το ιδιωτικό της κλειδί. Κανένας άλλος παραλήπτης δεν μπορεί να αποκρυπτογραφήσει το μήνυμα επειδή μόνο η Alice γνωρίζει το ιδιωτικό κλειδί της.

Για όποιον/α θέλει να το ψάξει περισσότερο

- Περιγράψτε τον αλγόριθμο RSA (Rivest–Shamir–Adleman στην κρυπτογραφία

- Τι είναι τα Distributed Ledger Technologies και το Blockchain και πώς επηρεάζουν την τεχνολογία στις μέρες μας;

Τέλος Κεφαλαίου 4

- Είδαμε δομές δικτύων και διαδικτύου, πρωτόκολλα πολλαπλής πρόσβασης, διευθυνσιοδότηση και πρωτόκολλα δρομολόγησης και μεταφοράς.

- Στο επόμενο κεφάλαιο θα ασχοληθούμε με αλγορίθμους: έννοιες, βασικοί αλγόριθμοι και πολυπλοκότητα.