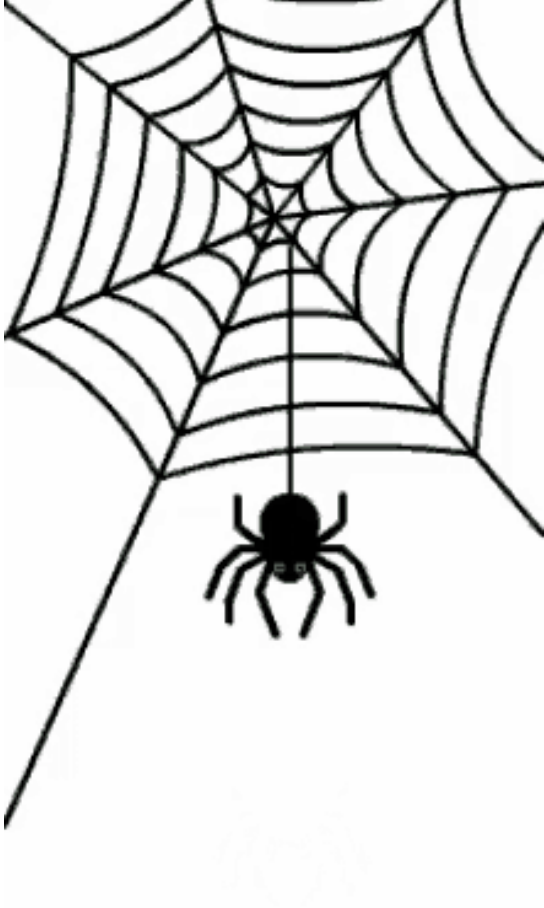
N e t w o r k s

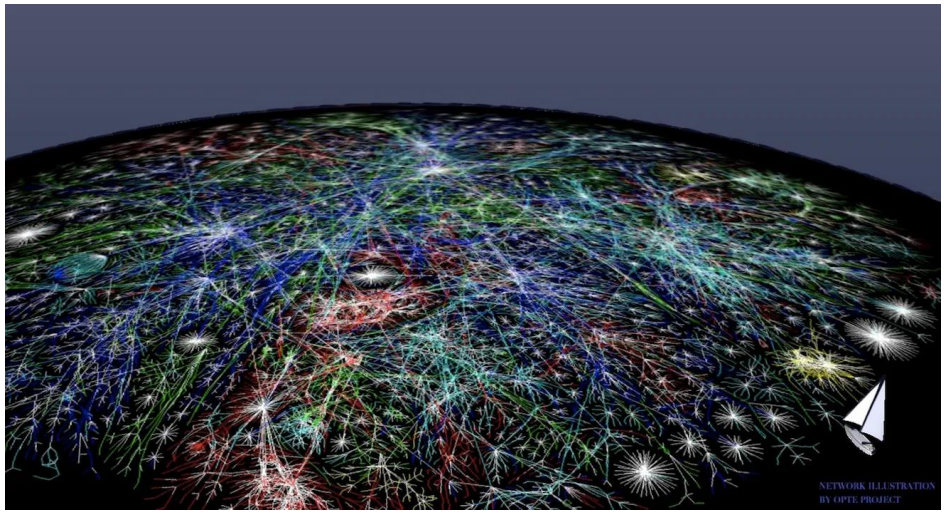
IEEE Ethical Hacking Team

2023-2024



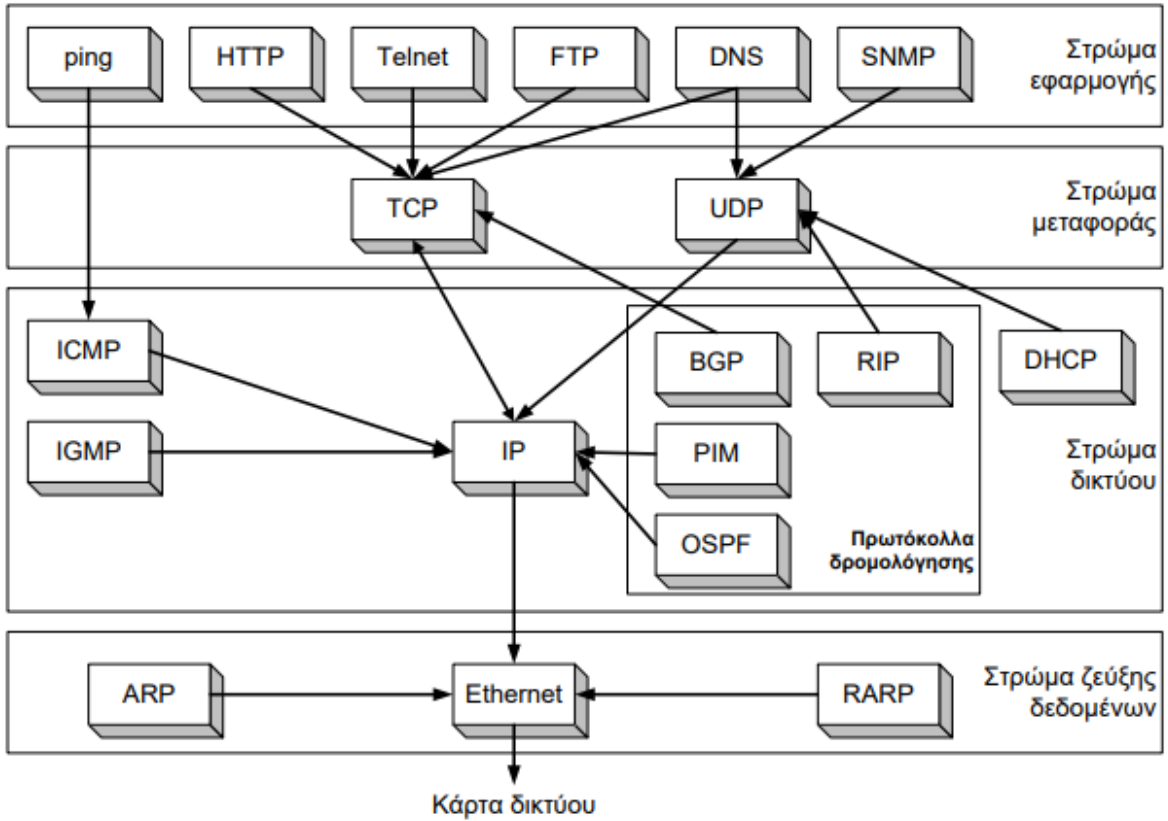
Τι είναι τα δίκτυα;

- Μία συλλογή από υπολογιστές, δρομολογητές και άλλες συσκευές που συνδέονται με σκοπό την μεταφορά και την ανταλλαγή δεδομένων.
- Πολλά δίκτυα μαζί ενώνονται σε ένα παγκόσμιο δίκτυο, το διαδίκτυο.



TCP/IP model

Για την καλύτερη οργάνωση των διαφόρων λειτουργιών, τα πρωτόκολλα οργανώνονται σε στρώματα με βάση το μοντέλο TCP/IP.



Στρώμα ζεύξης

MAC Address(Media Access Control address)

Η διαφοροποίηση των συσκευών γίνεται μέσω των διευθύνσεων MAC (Media Access Control address).

Στο ethernet κάθε κάρτα δικτύου έχει μια μοναδική φυσική διεύθυνση που αντιστοιχεί στο υπόστρωμα MAC. Αυτή η διεύθυνση MAC χρησιμεύει ώστε να ταυτοποιηθεί μοναδικά μια συσκευή σε ένα τοπικό δίκτυο (LAN).

Μία διεύθυνση MAC αποτελείται από 48 bits (6 bytes). Ορισμένα από αυτά καθορίζονται από τον κατασκευαστή της κάρτας (vendor specific).

Στρώμα δικτύου

IP address (Internet Protocol address)

- Είναι κάτι σαν τη διεύθυνση του σπιτιού μας.
- Χρησιμοποιείται κατά τη δρομολόγηση.
- Είναι μια μοναδική διεύθυνση που ταυτοποιεί μία συσκευή στο διαδίκτυο ή σε ένα τοπικό δίκτυο και χωρίς αυτή δε θα μπορούσαν να επικοινωνήσουν με τη συσκευή μας.
- Δύο συσκευές επικοινωνούν μεταξύ τους μέσω των IP (όχι πάντα!).

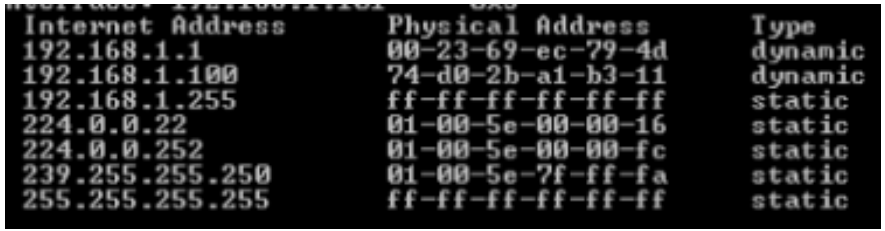
MAC VS IP

Οι MAC δεν αλλάζουν ποτέ μόνες τους, σε αντίθεση με τις IP που είναι δυναμικές και πολλές από αυτές μπορούν να αλλάζουν περιοδικά ανάλογα με τον χρόνο ή τις λεπτομέρειες της σύνδεσης (βλ. DHCP).

Συνδέονται στενά μεταξύ τους μέσω του πρωτοκόλλου ARP (Address Resolution Protocol), το οποίο λειτουργεί μεταξύ των στρωμάτων ζεύξης και δικτύου.

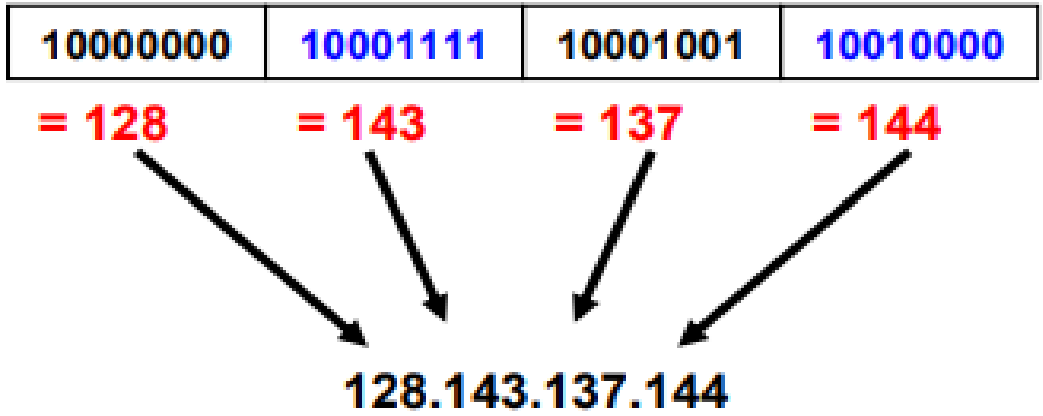
ARP

- Απαραίτητο για την επικοινωνία εντός ενός τοπικού δικτύου.
- Αντιστοιχίζει διευθύνσεις IP σε MAC. Η πληροφορία αυτή βρίσκεται αποθηκευμένη εντός του πίνακα Arp.
- Κάθε υπολογιστής που συμμετέχει στο LAN διαθέτει έναν arp table. Μπορείτε να δείτε τον δικό σας εκτελώντας **arp -a** σε ένα τερματικό.
- Το ARP δε σχεδιάστηκε για να παρέχει ασφάλεια (δεν παρέχει authentication). Ως εκ τούτου, είναι ευάλωτο σε επιθέσεις MitM (Man in the Middle) και DoS (Denial of Service).



IPv4

Οι διευθύνσεις IPv4 έχουν μήκος 4 bytes.
Είναι μια ακολουθία από τέσσερις (8-bit) αριθμούς που χωρίζονται μεταξύ τους με τελείες.
Το εύρος κάθε αριθμού είναι από 0 μέχρι 255. Δηλαδή, το εύρος των IP διευθύνσεων είναι από 0.0.0.0 μέχρι 255.255.255.255.
Τα τελευταία χρόνια έχει αρχίσει σταδιακά η μετάβαση στο IPv6 (έλλειψη σε IPv4 διευθύνσεις).

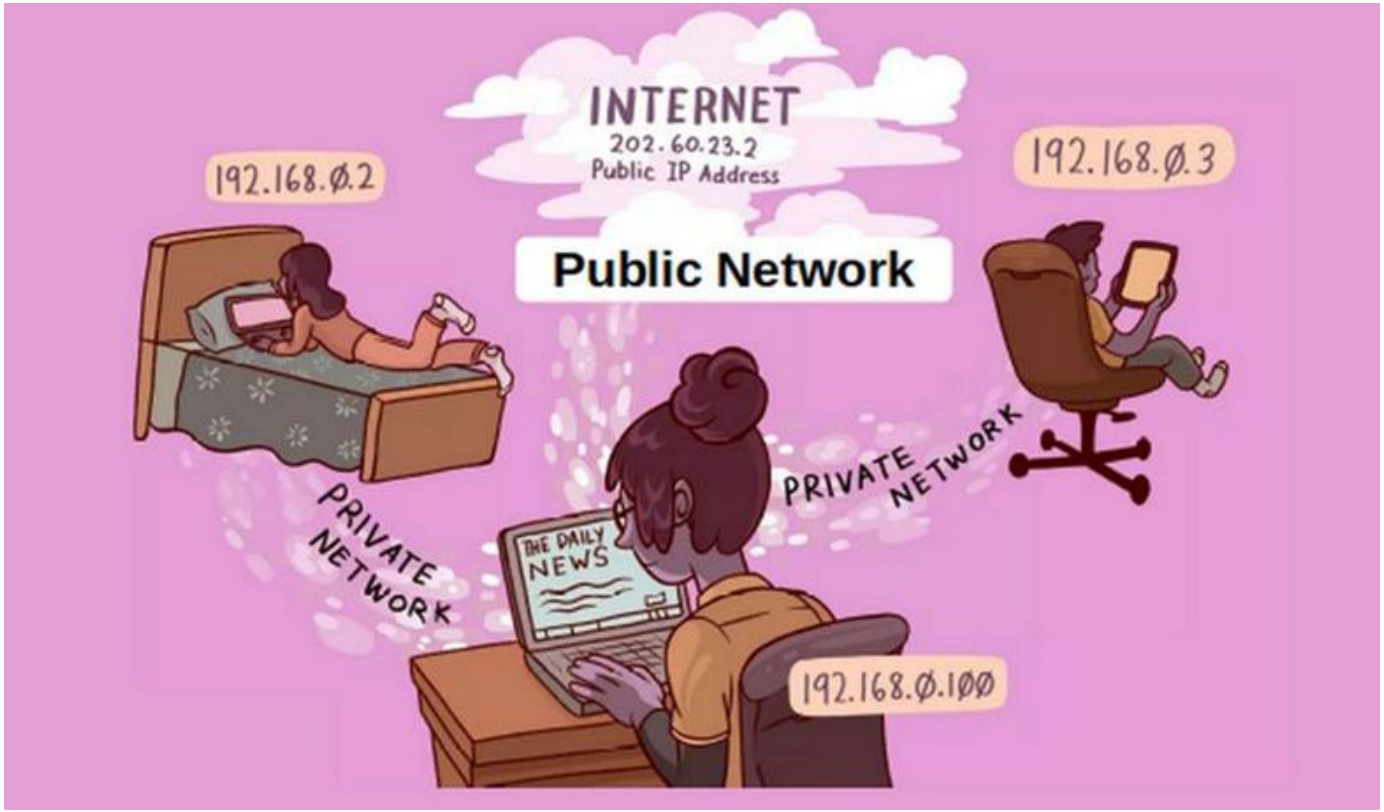


Private και Public IP

- *Private/local addresses:* για την επικοινωνία **εντός** ενός ιδιωτικού δικτύου κάθε συσκευή έχει μια μοναδική private IP address, την οποία της αποδίδει ο router. Private addresses είναι οι **10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/24**. Οι ιδιωτικές διευθύνσεις δε δρομολογούνται.

- *Public address:* είναι η διεύθυνση που βλέπουν όλες οι υπόλοιπες συσκευές που είναι συνδεδεμένες στο διαδίκτυο. Ένα οικιακό δίκτυο συνήθως έχει μια public address η οποία είναι κοινή για όλες τις συσκευές που συνδέονται στο ίδιο router (NAT).

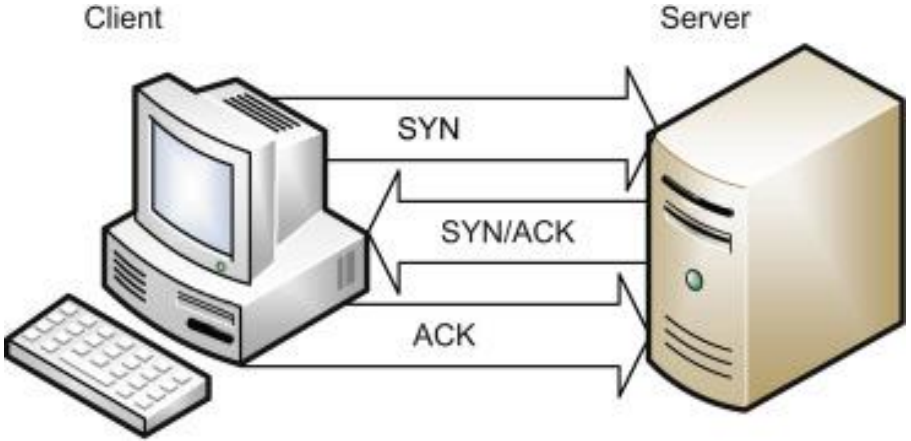
Private VS Public IP



Στρώμα μεταφοράς

TCP(Transmission Control Protocol)

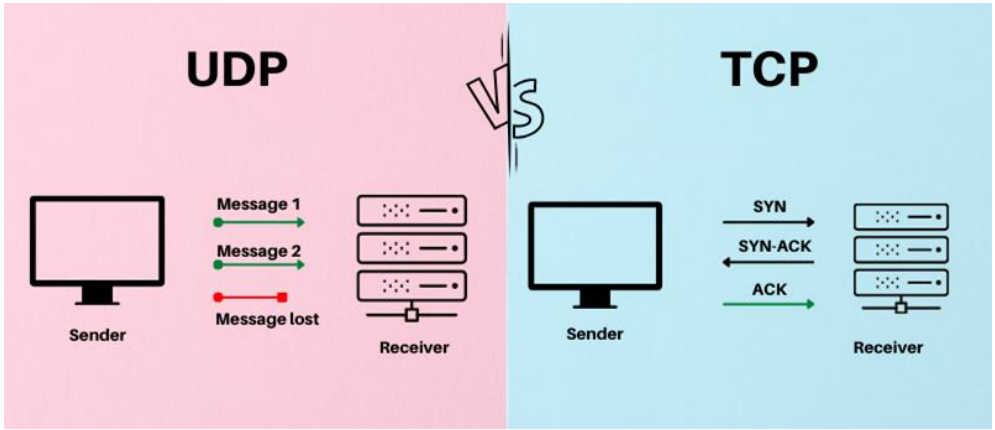
- Συνδεσμοστρεφές (μέσω τριπλής χειραψίας)
- Αξιόπιστο
- Παρέχει διόρθωση λαθών
- Χρησιμοποιείται για την αποστολή emails, αρχείων και γενικά σε εφαρμογές όπου είναι αναγκαία η ακέραια αποστολή δεδομένων



Στρώμα μεταφοράς

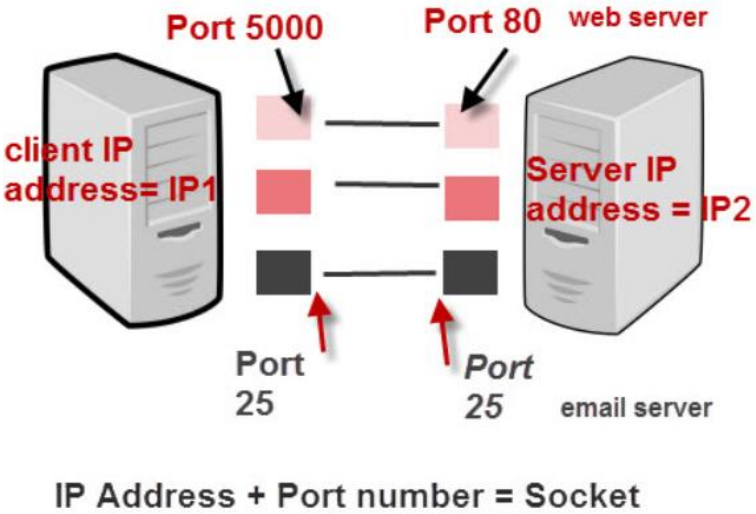
UDP (User Datagram Protocol)

- **Δε** δημιουργεί συνδέσεις μεταξύ των hosts
- **Δεν** εγγυάται παράδοση των πακέτων
- **Ούτε** τη σωστή σειρά παράδοσης τους
- Χρησιμοποιείται σε time-sensitive εφαρμογές όπου προτιμάμε άμεση παρά ακέραια παράδοση(πχ. VoIP, streaming)



Θύρες - Ports

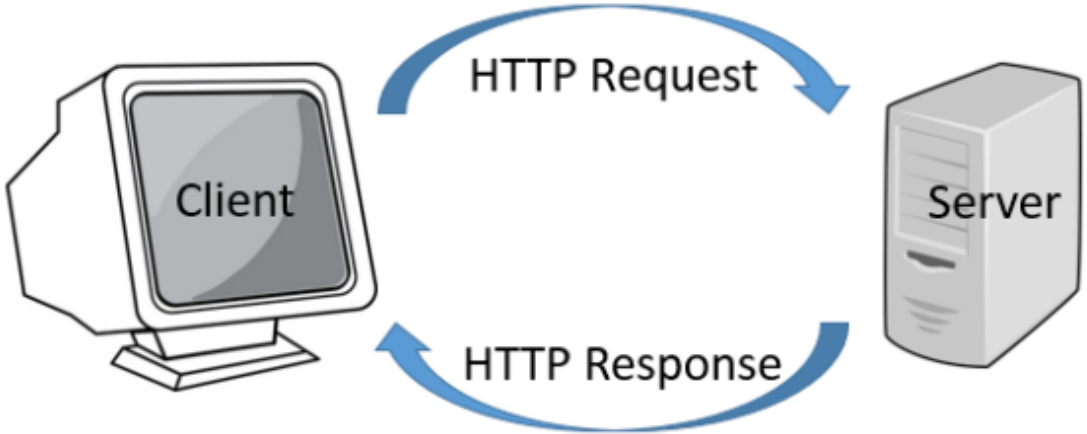
- Η επικοινωνία στο επίπεδο μεταφοράς γίνεται μέσω αριθμημένων θυρών(0-65535).
- Αυτό είναι χρήσιμο για να διαφοροποιούνται οι υπηρεσίες που λαμβάνουν χώρα. Οι πιο συχνές υπηρεσίες έχουν συγκεκριμένες θύρες στις οποίες στέλνονται (πάντα) τα πακέτα τους. Γενικά, οι θύρες 0-1023 θεωρούνται well-known.
- πχ. για το HTTP χρησιμοποιείται η θύρα 80, για το DNS η θύρα 53 ενώ για το SSH η θύρα 22



Στρώμα εφαρμογής

HTTP

- Χρησιμοποιείται για τη μεταφορά web content
- Η μεταφορα γίνεται με TCP καθώς μας ενδιαφέρει η αξιοπιστία όταν θέλουμε να επισκεφτούμε μια ιστοσελίδα
- Χρησιμοποιεί τη θύρα 80
- Υπάρχει η ασφαλής επέκταση του HTTPS (στη θύρα 443)

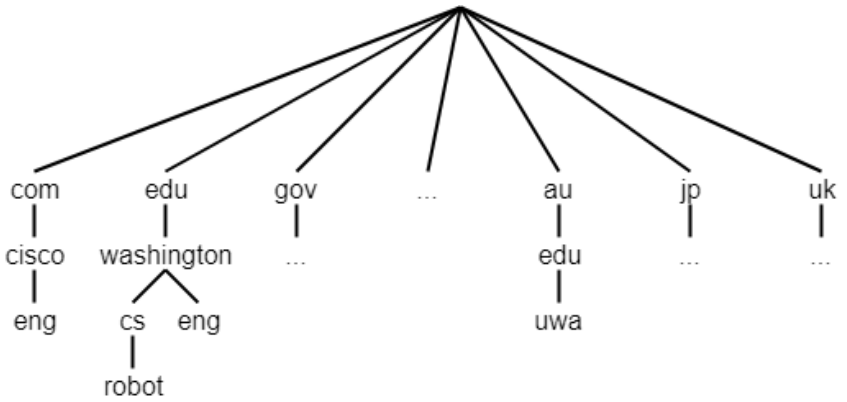


DNS

- Για να κατεβάσουμε και να δούμε μια ιστοσελίδα στον υπολογιστή μας χρειάζεται να συνδεθούμε με τον server που την περιέχει μέσω της IP του.
- Όμως εμείς δεν ξέρουμε την IP των περισσότερων ιστοσελίδων. Πώς ξέρει ο browser μας με ποιον server να συνδεθεί;
- Τη λύση δίνει το πρωτόκολλο DNS που “μεταφράζει” το όνομα της ιστοσελίδας (πχ. ieee.ntua.gr) στη σωστή IP(147.102.3.69). Αυτό γίνεται μέσω ενός DNS query σε έναν DNS server.
- Χρησιμοποιεί τη θύρα 53.

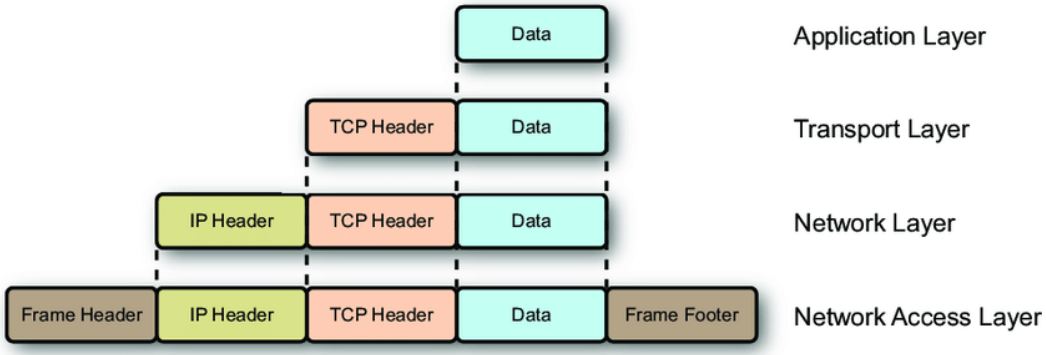
DNS

- Στο DNS έχουμε έναν νοητό διαχωρισμό του διαδικτύου.
- Χωρίζεται σε εκατοντάδες διαφορετικές περιοχές ονομάτων (domain names) υψηλού επιπέδου όπως για παράδειγμα com, org, gr οι οποίες αντίστοιχα χωρίζονται σε άλλες υποπεριοχές (subdomains) κοκ.



Ενθυλάκωση (encapsulation)

- Μια διαδικασία κατά την οποία ένα πρωτόκολλο κατώτερου επιπέδου λαμβάνει δεδομένα από πρωτόκολλο ανώτερου επιπέδου και τα τοποθετεί στο πεδίο δεδομένων που του αναλογεί.
- Σημασία: εξασφαλίζει καλύτερη και αποδοτικότερη διαχείριση των δεδομένων από τους κόμβους του δικτύου.



Εντολή ping

- Ελέγχουμε αν είναι δυνατή η σύνδεση σε μια απομακρυσμένη πηγή.
- Η πηγή μπορεί να είναι είτε μια ιστοσελίδα στο διαδίκτυο είτε ένας υπολογιστής στο οικιακό δίκτυο.
- Χρησιμοποιεί το πρωτόκολλο ICMP.
- Σύνταξη: ping <target>
- Επιστρέφει την IP address για τον server του target στον οποίο συνδέθηκε και όχι το URL που ζητήθηκε.

```
C:\WINDOWS\system32>ping google.com

Pinging google.com [142.250.184.78] with 32 bytes of data:
Reply from 142.250.184.78: bytes=32 time=31ms TTL=119
Reply from 142.250.184.78: bytes=32 time=28ms TTL=119
Reply from 142.250.184.78: bytes=32 time=28ms TTL=119
Reply from 142.250.184.78: bytes=32 time=32ms TTL=119

Ping statistics for 142.250.184.78:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 28ms, Maximum = 32ms, Average = 29ms
```

Εντολή traceroute/tracert

- Δείχνει όλο το μονοπάτι-βήματα που ακολουθεί το request του υπολογιστή μας για να φτάσει στον προορισμό του, δηλαδή στην μηχανή-στόχο.
- Γενικά, για να φτάσουμε εκεί που θέλουμε πρέπει να περάσουμε από διάφορους ενδιάμεσους κόμβους-δρομολογητές. Οπότε, το traceroute μας επιτρέπει να δούμε όλες αυτές τις ενδιάμεσες συνδέσεις (διεπαφές) μέχρι τον στόχο.
- Σύνταξη: tracert <destination>

```
C:\WINDOWS\system32>tracert google.com

Tracing route to google.com [142.250.184.78]
over a maximum of 30 hops:

  1     4 ms     4 ms     3 ms  147.102.236.200
  2     8 ms     4 ms     3 ms  ntua-zogr-3-gw.eier.access-link.grnet.gr [62.217.96.168]
  3     3 ms     8 ms    10 ms  grnet-ias-geant-gw.mx2.ath.gr.geant.net [83.97.88.69]
  4    64 ms    30 ms    58 ms  ae2.mx1.mil2.it.geant.net [62.40.98.150]
  5    29 ms    28 ms    28 ms  72.14.203.32
  6    42 ms    32 ms    30 ms  74.125.245.225
  7    37 ms    30 ms    32 ms  142.251.50.139
  8    29 ms    38 ms    31 ms  mil41s03-in-f14.1e100.net [142.250.184.78]

Trace complete.
```