Δίκτυα Υπολογιστών

Επίπεδο εφαρμογής

Το Σύστημα Ονομασίας Τομέων DNS

Κ. Βασιλάκης

Μεγάλο μέρος του περιεχομένου, προέρχεται από τις παρουσιάσεις (στα αγγλικά) των συγγραφέων του βιβλίου: Δικτύωση Υπολογιστών, προσέγγιση από πάνω προς τα κάτω, 6η έκδοση, (Computer Networking: A Top Down Approach), Jim Kurose & Keith Ross.

Περίγραμμα – ενότητες που εξετάζονται

- Τι είναι το DNS (Domain Name System)
- Αντιστοίχιση ονομάτων (η κύρια υπηρεσία του DNS)
- Άλλες υπηρεσίες του DNS
- Αρχιτεκτονική
  - Η κατανεμημένη βάση του DNS
  - Εξυπηρετητές ονομάτων ρίζας
  - Εξυπηρετητές τομέων ανώτερου επιπέδου
  - Αυθεντικοί εξυπηρετητές
  - Τοπικοί Εξυπηρετητές Ονομάτων
- Οι εγγραφές στη κατανεμημένη βάση του DNS
- Τα μηνύματα του DNS.

http://blog.etonic.net/

Σύστημα Ονομασίας Τομέων (DNS)

- Οι άνθρωποι έχουν πολλούς τρόπους αναγνώρισης (ταυτότητα, ΑΦΜ, ΑΜΚΑ κλπ).
- Οι κόμβοι του Διαδικτύου αναγνωρίζονται είτε με
  - την *IP-διεύθυνση* (32 bit) του κόμβου – χρησιμοποιείται για διευθυνσιοδότηση στα δεδομενογράμματα (π.χ. 121.7.106.83), είτε με
  - το *ανθρωποκεντρικό όνομα* του κόμβου, π.χ., www.hmu.gr – χρησιμοποιείται από τους ανθρώπους (hostname).
- Οι άνθρωποι χρησιμοποιούν ονόματα και οι υπηρεσίες του Διαδικτύου *IP-διευθύνσεις*, για ν' αναγνωρίσουν τους κόμβους του Δικτύου.
- Όμως τα ανθρωποκεντρικά ονόματα των κόμβων δίνουν λίγες ή καθόλου πληροφορίες για τη θέση τους στο Διαδίκτυο.
- Η αντιστοιχία ανάμεσα στη IP διεύθυνση του κόμβου και το όνομα του στο Διαδίκτυο, γίνεται με τη *υπηρεσία DNS*.

Τι είναι το DNS (Domain Name System)

- Το DNS αποτελείται από:
  - Μια *κατανεμημένη βάση* δεδομένων που υλοποιείται και συντηρείται με μια ιεραρχία πολλών εξυπηρετητών ονομάτων (Domain Name Servers).
  - Ένα *πρωτόκολλο επιπέδου εφαρμογής* που επιτρέπει σε τερματικά συστήματα και σε εξυπηρετητές ονομάτων να υποβάλουν ερωτήματα στη κατανεμημένη βάση για «μετάφραση» των ονομάτων (αντιστοίχηση διεύθυνσης - ονόματος).
- Πρόκειται για μια βασική λειτουργία του Διαδικτύου που υλοποιείται ως πρωτόκολλο επιπέδου εφαρμογής και συνήθως χρησιμοποιείται από άλλα πρωτόκολλα (υπηρεσίες).
- Η όλη διαδικασία της «μετάφρασης» υλοποιείται σε hosts (πολυπλοκότητα στο «άκρο» του δικτύου). Ένα γνωστό τέτοιο λογισμικό είναι το *BIND* των *Unix (Linux)* συστημάτων.

Πριν σταλθεί ένα μήνυμα

- Η εφαρμογή του πελάτη (πχ ένας φυλλομετρητής) θέλει να στείλει ένα μήνυμα σε ένα εξυπηρετητή web.
- Θα πρέπει να γνωρίζει τη *IP διεύθυνση* του εξυπηρετητή.
- Πως γίνεται αυτό;
  - Η εφαρμογή (φυλλομετρητής) δίνει το όνομα του εξυπηρετητή (web-server) στη εφαρμογή DNS που «τρέχει» στον πελάτη.
  - Η εφαρμογή DNS του πελάτη στέλνει ένα ερώτημα (DNS μήνυμα που περιέχει το όνομα) προς έναν εξυπηρετητή DNS (DNS server).
  - Η εφαρμογή DNS του πελάτη δέχεται τελικά ένα μήνυμα που περιλαμβάνει τη IP διεύθυνση του εξυπηρετητή (web-server) και την περνά στη εφαρμογή του πελάτη (φυλλομετρητής).
  - Η εφαρμογή του πελάτη στέλνει το μήνυμα στη IP διεύθυνση.
- Όλα τα μηνύματα του DNS στέλνονται σε δεδομενογράμματα (datagrams) χρησιμοποιώντας το *πρωτόκολλο UDP* στη θύρα 53.
- Η όλη διαδικασία προσθέτει καθυστέρηση στη μετακίνηση (χρησιμοποιούνται τεχνικές *caching* για να μειωθεί η καθυστέρηση).

Άλλες υπηρεσίες του DNS

- Ψευδώνυμα υπολογιστών (*host aliasing*)
  - Τα hosts εκτός από τα κανονικά ονόματα (canonical) μπορούν να έχουν και ψευδώνυμα (alias names) που συνήθως είναι πιο εύκολο να τα θυμηθεί κάποιος. Το DNS μπορεί να επιστρέψει κανονικά ονόματα.
- Ψευδώνυμα εξυπηρετών ταχυδρομείου (*mail server aliasing*)
  - Το DNS μπορεί να κληθεί από μια εφαρμογή ηλεκτρονικού ταχυδρομείου και να επιστρέψει το κανονικό όνομα του εξυπηρετητή, εκτός από την IP διεύθυνση του.
- Κατανομή φορτίου (*load distribution*)
  - Το DNS μπορεί να χρησιμοποιηθεί για να κάνει κατανομή φορτίου ανάμεσα σε εξυπηρετητές – αντίγραφα (replicated servers: πολλές διευθύνσεις IP που αντιστοιχούν σε ένα κανονικό όνομα). Το DNS κατανέμει τη κίνηση περιστρέφοντας τις IP διευθύνσεις. Χρήση κυρίως σε εφαρμογές web και e-mail που έχουν πολύ κίνηση.
- Το DNS καθορίστηκε αρχικά στα *RFC's 1034* και *1035*.

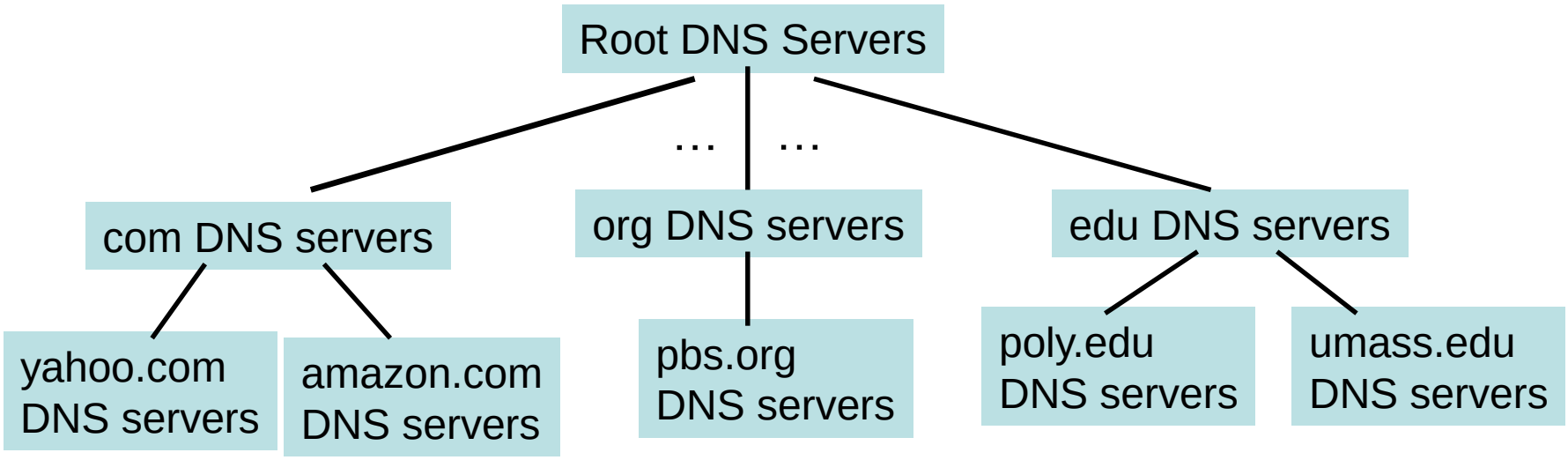
Το DNS δεν είναι κεντρικοποιημένο

- Σε μια κεντρικοποιημένη σχεδίαση του DNS οι πελάτες θα απεύθυναν όλα τους τα ερωτήματα σε ένα μοναδικό κεντρικό εξυπηρετητή DNS.
- Μια τέτοια σχεδίαση θα είχε κάποια προβλήματα:
  - *μοναδικό σημείο αποτυχίας* (κατάρρευση του DNS server θα είχε σαν αποτέλεσμα τη κατάρρευση του Διαδικτύου),
  - *μεγάλος όγκος κίνησης* (πρέπει να ικανοποιηθούν εκατοντάδες εκατομμύρια αιτήσεις),
  - *απομακρυσμένη κεντρικοποιημένη βάση δεδομένων* (η βάση δεν μπορεί να είναι ταυτόχρονα κοντά σε όλους τους πελάτες που υποβάλουν ερωτήματα – καθυστέρηση),
  - *συντήρηση* (τεράστια βάση δεδομένων με πολύ συχνές ενημερώσεις στις εγγραφές της).
  - Δεν *κλιμακώνεται* εύκολα.

Το DNS είναι κατανεμημένο από τη σχεδίαση του

- Χρησιμοποιείται ένα μεγάλο σύνολο εξυπηρετητών που είναι οργανωμένοι *ιεραρχικά* και βρίσκονται διασπαρμένοι σε όλο τον κόσμο.
- Οι αντιστοιχίσεις των ονομάτων είναι κατανεμημένες σε αυτούς τους εξυπηρετητές (κατανεμημένη βάση δεδομένων)
- Υπάρχουν 3 βασικοί τύποι εξυπηρετητών:
  - *Εξυπηρετητές ρίζας DNS* (root DNS servers)
  - *Εξυπηρετητές DNS ανωτάτου επιπέδου* (Top-Level Domain –TLD servers)
  - *Αυθεντικοί εξυπηρετητές* DNS (Authoritative DNS servers)
- Επίσης, υπάρχουν και *Τοπικοί εξυπηρετητές DNS* (Local DNS name servers) που όμως δεν ανήκουν με τη στενή έννοια στη ιεραρχία των εξυπηρετητών DNS.

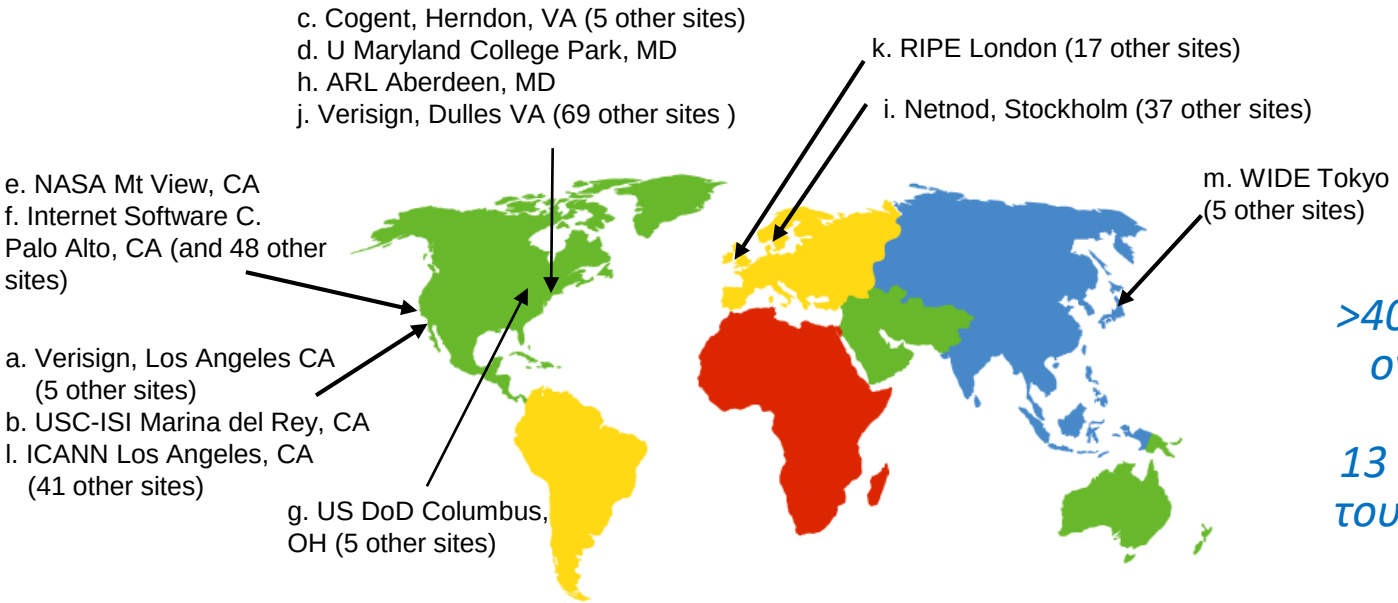
Κατανεμημένη, Ιεραρχική Βάση Δεδομένων



- Ο πελάτης θέλει τη διεύθυνση IP για το www.amazon.com:
  - Ο πελάτης ρωτά έναν εξυπηρετητή *ρίζας* (root server) για να βρει τον εξυπηρετητή DNS του *ανώτατου τομέα com* (com DNS server)
  - Ο πελάτης ρωτά τον εξυπηρετητή DNS του ανώτατου τομέα com (TLD server) για να πάρει τον *αυθεντικό εξυπηρετητή DNS amazon.com* (amazon.com DNS server)
  - Ο πελάτης ρωτά τον αυθεντικό εξυπηρετητή DNS amazon.com (amazon.com DNS server) για να πάρει τη διεύθυνση IP του *www.amazon.com*.

DNS: Εξυπηρετητές ονομάτων ρίζας (root name servers)

- Με αυτούς έρχεται σε επαφή ο τοπικός εξυπηρετητής ονομάτων που δεν μπορεί να μεταφράσει το όνομα.
- Ο εξυπηρετητής ονομάτων ρίζας:
  - έρχεται σε επαφή με τον *αυθεντικό* (authoritative) εξυπηρετητή ονομάτων, αν η αντιστοιχία του ονόματος δεν είναι γνωστή,
  - παίρνει την αντιστοιχία,
  - επιστρέφει την αντιστοιχία στον τοπικό εξυπηρετητή ονομάτων.



>400 εξυπηρετητές ονομάτων ρίζας παγκοσμίως, 13 οργανισμοί που τους διαχειρίζονται (2016)

TLD και Αυθεντικοί εξυπηρετητές

- Εξυπηρετητές τομέων ανώτερου επιπέδου (Top Level Domain servers):
  - Είναι υπεύθυνοι για τους τομείς com, org, net, edu, κλπ, και όλους τους ανώτερου επιπέδου τομείς χωρών uk, fr, ca, jp, gr κλπ. Για παράδειγμα:
    - Η Verisign Global Registry διατηρεί εξυπηρετητές για τους com TLD.
    - η Educause για τους edu TLD.
    - Το Ινστιτούτο Πληροφορικής του ITE (ICS-FORTH GR) για τους gr TLD.
  - Παρέχουν τις IP διευθύνσεις για τους αυθεντικούς DNS servers.
- Αυθεντικοί εξυπηρετητές DNS (Authoritative DNS servers):
  - Οι εξυπηρετητές DNS κάθε οργανισμού που παρέχουν αυθεντικές (authoritative) αντιστοιχίσεις ονομάτων υπολογιστών σε διευθύνσεις IP για τους εξυπηρετητές ενός οργανισμού (π.χ., Web, mail).
  - Κάθε οργανισμός που έχει δημόσια προσπελάσιμους servers πρέπει να παρέχει δημόσια τις αντιστοιχίσεις του.
  - Μπορεί να διατηρείται από τον ίδιο τον οργανισμό ή το πάροχο υπηρεσιών.

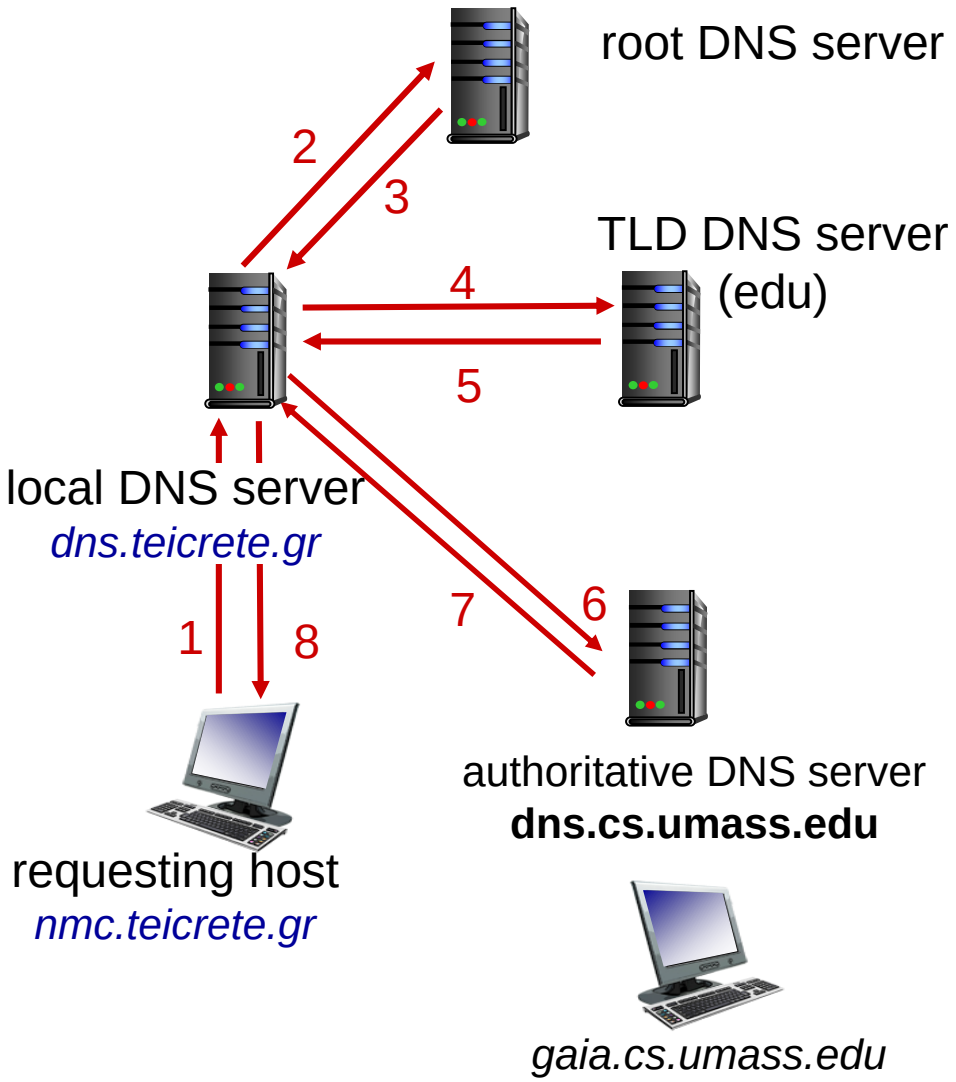
Τοπικοί Εξυπηρετητές Ονομάτων (Local Name Server)

- Δεν ανήκουν αυστηρά στην ιεραρχία.
- Παίζουν σημαντικό ρόλο στη αρχιτεκτονική και στη λειτουργία του DNS.
- Κάθε ISP (περιφερειακός ISP, εταιρία, πανεπιστήμιο) έχει έναν Τοπικό Εξυπηρετητή Ονομάτων.
- Καλείται επίσης «*προεπιλεγμένος εξυπηρετητής ονομάτων*» (“default name server”).
- Κάθε ISP παρέχει στα hosts που εξυπηρετεί, τις διευθύνσεις ενός ή περισσοτέρων τοπικών εξυπηρετητών DNS.
- Όταν ένας υπολογιστής πραγματοποιεί ένα ερώτημα DNS, το ερώτημα στέλνεται σε αυτόν τον τοπικό εξυπηρετητή DNS.
- Λειτουργεί ως *πληρεξούσιος* (proxy), προωθεί τα ερωτήματα στην ιεραρχία.

Παράδειγμα μετάφρασης ονόματος DNS

- Ο υπολογιστής στο nmc.teicrete.gr θέλει να βρει τη διεύθυνση IP του gaia.cs.umass.edu
- *Επαναληπτικό ερώτημα* (iterated query).

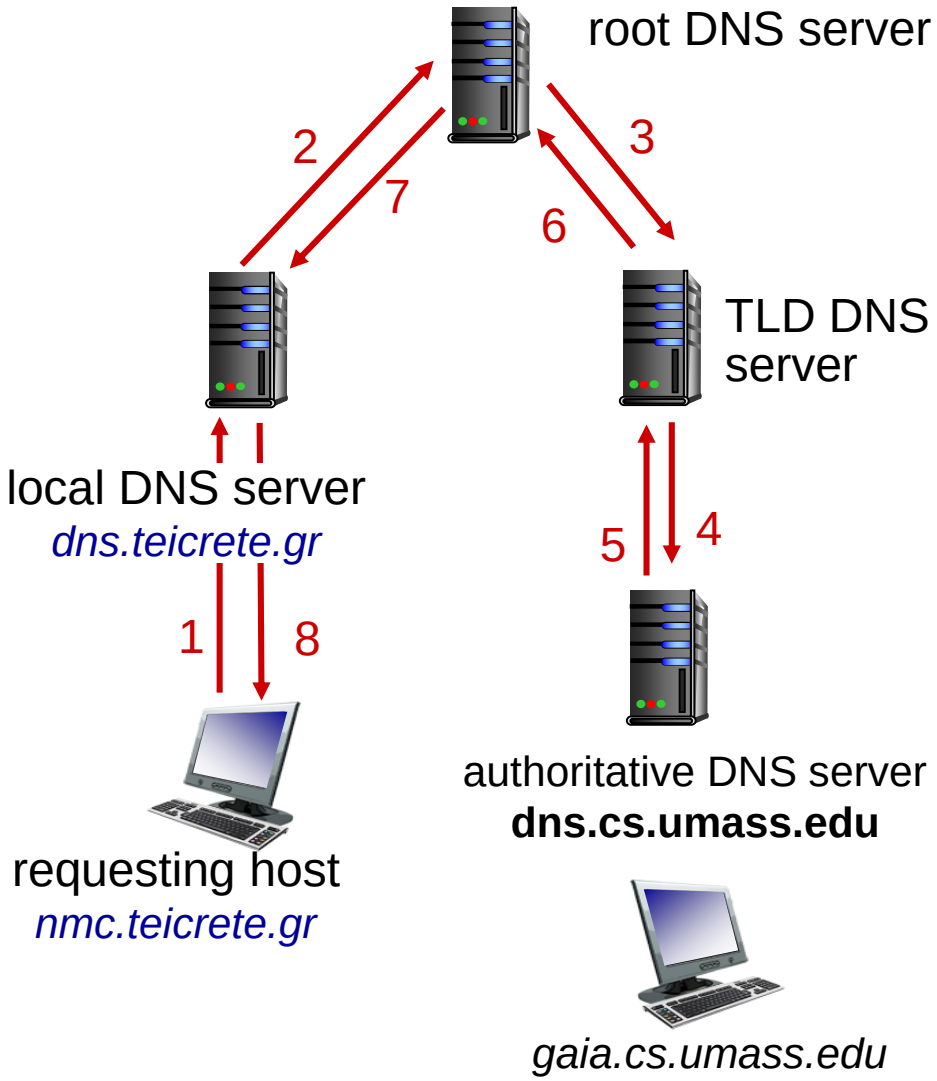
  Ο εξυπηρετητής που ρωτήθηκε απαντά:
  - με το όνομα του εξυπηρετητή που πρέπει να ρωτηθεί ή
  - «Δεν ξέρω το όνομα αλλά ρώτα αυτόν τον εξυπηρετητή».
- *Αναδρομικό ερώτημα* (recursive query):
  - Εναποθέτει το βάρος της μετάφρασης ονόματος στον εξυπηρετητή που ρωτήθηκε.



Το ίδιο παράδειγμα με αναδρομικά ερωτήματα

- Μήπως είναι βαρύ φορτίο για τους ψηλά ιεραρχικά εξυπηρετητές?

- Δείτε στη ενότητα σύνδεσμοι, επίδειξη με αναδρομικά / επαναληπτικά ερωτήματα στο DNS.
- Δοκιμάστε την εντολή nslookup.

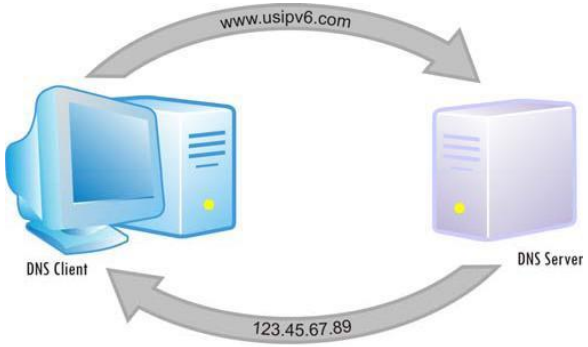


Προσωρινή αποθήκευση και ενημέρωση εγγραφών

- Για να βελτιώσει τις καθυστερήσεις το DNS χρησιμοποιεί τεχνικές *caching* (προσωρινή αποθήκευση εγγραφών).
- Όταν ο (οποιοσδήποτε) εξυπηρετητής DNS μάθει μια αντιστοίχιση την αποθηκεύει προσωρινά στη τοπική του μνήμη.
- Τα περιεχόμενα της προσωρινής μνήμης (cache) λήγουν (εξαφανίζονται) μετά από κάποιο χρονικό διάστημα.
- Οι εγγραφές των εξυπηρετητών TLD τυπικά αποθηκεύονται προσωρινά σε τοπικούς εξυπηρετητές DNS.
- Οι τοπικοί εξυπηρετητές DNS, αν έχουν την αντιστοίχιση απαντούν άμεσα.
- Με αυτό τον τρόπο οι εξυπηρετητές ρίζας δεν δέχονται συχνά αιτήματα.

Εγγραφές DNS

- Οι εξυπηρετητές DNS αποθηκεύουν εγγραφές πόρων (resource records - RR) που έχουν τα εξής πεδία:
  - *Όνομα (name),*
  - *Τιμή (value),*
  - *Τύπος (type),*
  - *Χρονικό διάστημα παραμονής της εγγραφής* (*TTL*).



- Η σημασία των πεδίων «Όνομα» και «Τιμή» εξαρτάται από το πεδίο «Τύπος».
- Το πεδίο *TTL* (*Time To Live*) καθορίζει πότε ένας πόρος πρέπει ν' αφαιρεθεί από τη προσωρινή μνήμη (cache).
- Κάθε μήνυμα απόκρισης DNS μεταφέρει μια ή περισσότερες εγγραφές πόρων.

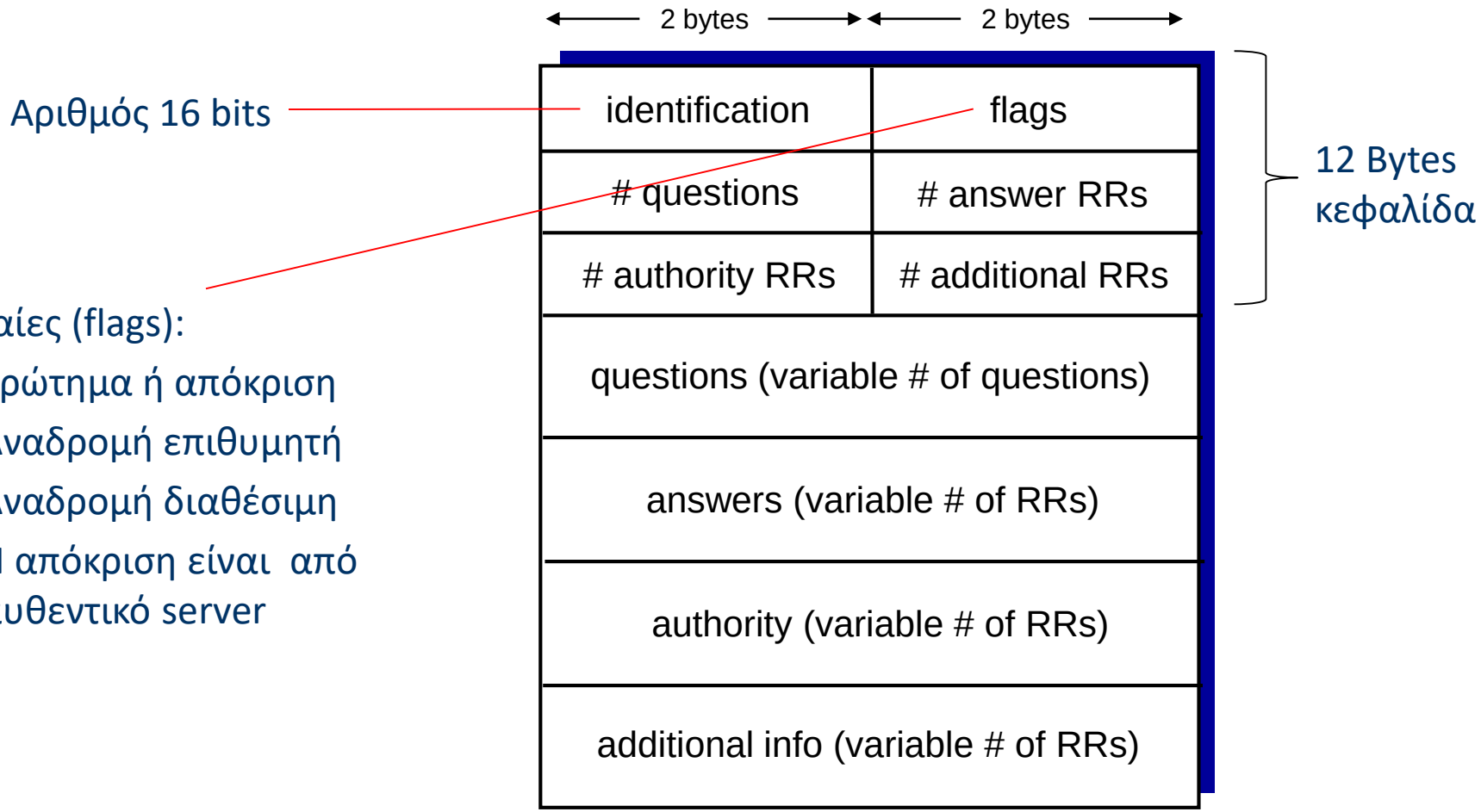
Το πεδίο «Τύπος» (type) της RR

- *Type=A*
  - name είναι το όνομα του υπολογιστή
  - value είναι η διεύθυνση IP
- *Type=NS*
  - name είναι τομέας (domain π.χ. foo.com)
  - value είναι το όνομα υπολογιστή (hostname) του αυθεντικού εξυπηρετητή ονομάτων για αυτόν τον τομέα.
- *Type=CNAME*
  - name είναι ψευδώνυμο (alias name) για κάποιο κανονικό (canonical) όνομα. Π.χ. το www.ibm.com είναι στην πραγματικότητα servereast.backup2.ibm.com
  - value είναι το κανονικό όνομα
- *Type=MX*
  - value είναι το όνομα του εξυπηρετητή mail που σχετίζεται με το name

Όνομα (name),
Τιμή (value),
Τύπος (type)

Τα μηνύματα του DNS

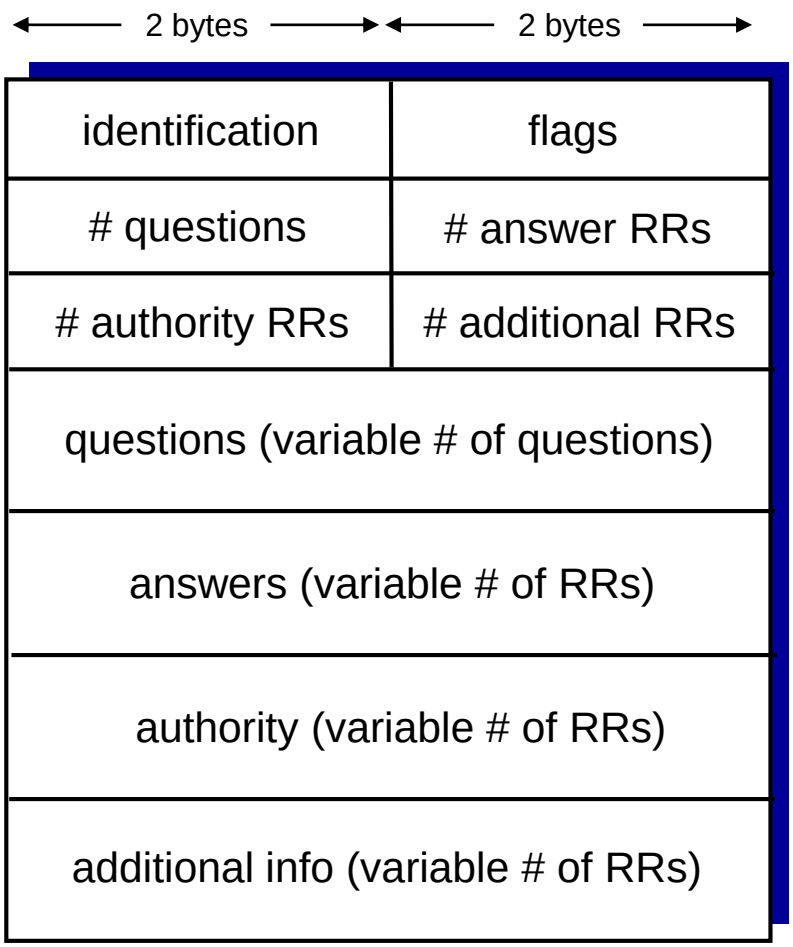
- Τα μηνύματα ερωτήματος (query) και απόκρισης (reply) έχουν και τα δύο την ίδια μορφή μηνύματος (message format)



Σημαίες (flags):

- Ερώτημα ή απόκριση
- Αναδρομή επιθυμητή
- Αναδρομή διαθέσιμη
- Η απόκριση είναι από αυθεντικό server

Τα μηνύματα του DNS



12 Bytes κεφαλίδα

Πεδία ονόματος, τύπου για ένα ερώτημα

RR για απόκριση στο ερώτημα

Εγγραφές για αυθεντικούς εξυπηρετητές

Πρόσθετες "χρήσιμες" πληροφορίες που μπορούν να χρησιμοποιηθούν

- Παράδειγμα: νέα startup εταιρία “Network Utopia”
- Εγγράφει το όνομα networkuptopia.com σε ένα DNS καταγραφέα (registrar) πχ. την Network Solutions.
- Πως γίνεται αυτό:
  - Η εταιρεία παρέχει ονόματα, διευθύνσεις IP του αυθεντικού εξυπηρετητή ονομάτων (κύριου και δευτερεύοντα)
  - Ο registrar εισάγει δύο RRs στον εξυπηρετητή TLD com:

    (networkutopia.com, dns1.networkutopia.com, NS)

    (dns1.networkutopia.com, 212.212.212.1, A)
- Επίσης, δημιουργείται εγγραφή αυθεντικού εξυπηρετητή τύπου A για το www.networkuptopia.com και εγγραφή τύπου MX για το mail.networkutopia.com αν χρειαστεί.