Υλοποίηση Δικτυακών Υποδομών και Υπηρεσιών: Υπηρεσία Domain Name Service

Δρ. Απόστολος Γκάμας

Διδάσκων (407/80)

gkamas@uop.gr

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ
ΤΜΗΜΑ ΕΠΙΣΤΗΜΗΣ ΚΑΙ ΤΕΧΝΟΛΟΓΙΑΣ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

Εισαγωγή

- Επικοινωνία συσκευών δικτύου
- Επικοινωνία ανθρώπων και συσκευών
- Ονοματολογία & πληροφορίες όσον αφορά
  - τη γεωγραφική θέση (gr, jp, fi)
  - τις προσφερόμενες υπηρεσίες (mail, www)
  - το είδος του οργανισμού (edu, com, mil, net)

Παραδείγματα

HTTP αίτηση από πελάτη προς HTTP server www.teithe.gr

Διαδικασίες DNS

HTTP αίτηση από πελάτη προς HTTP server 193.92.235.36

Παραδείγματα

- alpha.noc.uop.gr συσκευή στην Ελλάδα
- www.funet.fi συσκευή στη Φιλανδία
- www.teithe.gr εξυπηρετητής υπηρεσίας HTTP στην Ελλάδα
- pop.teithe.gr εξυπηρετητής υπηρεσίας POP στην Ελλάδα
- www.pasteur.edu.gr συσκευή που ανήκει σε εκπαιδευτικό ίδρυμα στην Ελλάδα

Τι είναι το Domain Name System

- Κατανεμημένη βάση δεδομένων
- Κατανομή ευθύνης συντήρησης της βάσης του Domain Name System
- Δικτυακοί πόροι & αντιστοίχηση ονομάτων
- Ερωτήσεις (resolvers) απαντήσεις (dns servers)

Ιστορία της ονοματολογίας

- 1970's ARPANET
  - Host.txt διαχειριζόταν SRI-NIC
  - Ήταν αποθηκευμένο σε ένα μηχάνημα
  - Προβλήματα
    - Προβλήματα κίνησης και φόρτου
    - Συγκρούσεις ονομάτων (Name collisions)
    - Συνέπεια (Consistency)
- Το DNS δημιουργήθηκε το 1983 από τον Paul Mockapetris (RFCs 1034 και 1035), και έχει γραφτεί μεγάλος αριθμός σχετικών RFCs

DNS: Domain Service Name

- Για την αναγνώριση των hosts, routers στο Διαδίκτυο χρησιμοποιούνται:
  - IP διευθύνσεις (150.140.141.24) (διευκολύνει τις συσκευές)
  - «Όνομα» (www.uop.gr) (διευκολύνει τους ανθρώπους)
- Domain Service Name
  - Υπηρεσία καταλόγου που μεταφράζει hostnames σε διεύθυνση IP
  - Αποτελεί μια κατανεμημένη βάση δεδομένων που υλοποιείται από μια ιεραρχία από πολλούς name servers

DNS: Domain Service Name

- Πρωτόκολλο επιπέδου εφαρμογής hosts και name servers επικοινωνούν για την ανάλυση ονομάτων σε διευθύνσεις IP και αντίστροφα
  - Αποτελεί λειτουργία του πυρήνα του Διαδικτύου που υλοποιείται ως πρωτόκολλο του επιπέδου εφαρμογής
  - Πολυπλοκότητα στο άκρο του δικτύου
- Χρησιμοποιεί UDP, port 53
- Ακολουθεί το μοντέλο client/server
- Το DNS χρησιμοποιείται από άλλα πρωτόκολλα εφαρμογών π.χ. HTTP

DNS: Domain Service Name

- Υπηρεσίες DNS
  - Μετάφραση ονόματος host σε διεύθυνση IP
  - Ψευδώνυμο host (κανονικό (canonical) όνομα και ψευδώνυμα)
  - Ψευδώνυμο mail server
  - Κατανομή φορτίου
    - Πολλαπλοί web servers: σε ένα κανονικό όνομα αντιστοιχούν περισσότερες από μία διευθύνσεις IP
- Γιατί όχι κεντρικοποιημένο DNS?
  - Μοναδικό σημείο αστοχίας
  - Όγκος κίνησης
  - Κεντρικοποιημένη βάση δεδομένων σε μεγάλη απόσταση
  - Συντήρηση τεράστιας βάσης δεδομένων με συχνές ενημερώσεις

Χαρακτηριστικά του DNS : Global Distribution

- Τα δεδομένα αποθηκεύονται τοπικά αλλά είναι διαθέσιμα globally
  - Κανένας υπολογιστής δεν έχει όλα τα DNS δεδομένα
- Τα απομακρυσμένα DNS δεδομένα αποθηκεύονται τοπικά για βελτίωση της απόδοσης

Χαρακτηριστικά του DNS: Loose Coherency

- Η βάση δεδομένων είναι πάντα εσωτερικά συνεπής
  - Κάθε έκδοση ενός subset της βάσης (μια zone) έχει ένα serial number
  - Το serial number αυξάνεται σε κάθε αλλαγή
- Οι αλλαγές στην βάση δεδομένων αντιγράφονται με κανόνες που ορίζει ο διαχειριστής του zone
- Τα δεδομένα τα οποία αποθηκεύονται τοπικά (Cached data) λήγουν μετά από timeout που ορίζει ο διαχειριστής του zone

Χαρακτηριστικά του DNS: Κλιμάκωση (Scalability)

- Δεν υπάρχει περιορισμός στο μέγεθος της βάσης δεδομένων
  - Ένας server μπορεί να έχει πάνω από 20,000,000 εγγραφές (κάτι το οποίο βέβαια δεν είναι καλή ιδέα)
- Δεν υπάρχει όριο στο αριθμό των queries
  - 24,000 queries per second χειρίζονται εύκολα
  - 2,000-4,000 qps είναι πιο νορμάλ
- Τα queries κατανέμονται μεταξύ masters, slaves, και caches servers

Χαρακτηριστικά του DNS: Αξιοπιστία

- Τα δεδομένα είναι replicated
  - Δεδομένα από ένα master server αντιγράφονται σε πολλούς slaves servers
- Οι Clients υποβάλλουν query
  - Στο Master server
  - Σε ένα από slave servers
- Οι Clients συνήθως αποθηκεύουν τοπικά query (local caches)

Χαρακτηριστικά του DNS: Δυναμικότητα (Dynamicity)

- Η βάση δεδομένων μπορεί να ενημερωθεί δυναμικά
  - Προσθήκη/διαγραφή/αλλαγή σχεδόν όλων των εγγραφών
- Αλλαγές στην master βάση δεδομένων μεταδίδονται στους slaves
  - Μόνο ο master server μπορεί να ενημερωθεί δυναμικά
  - Υπάρχει single point of failure

Θεωρητική οργάνωση της βάσης

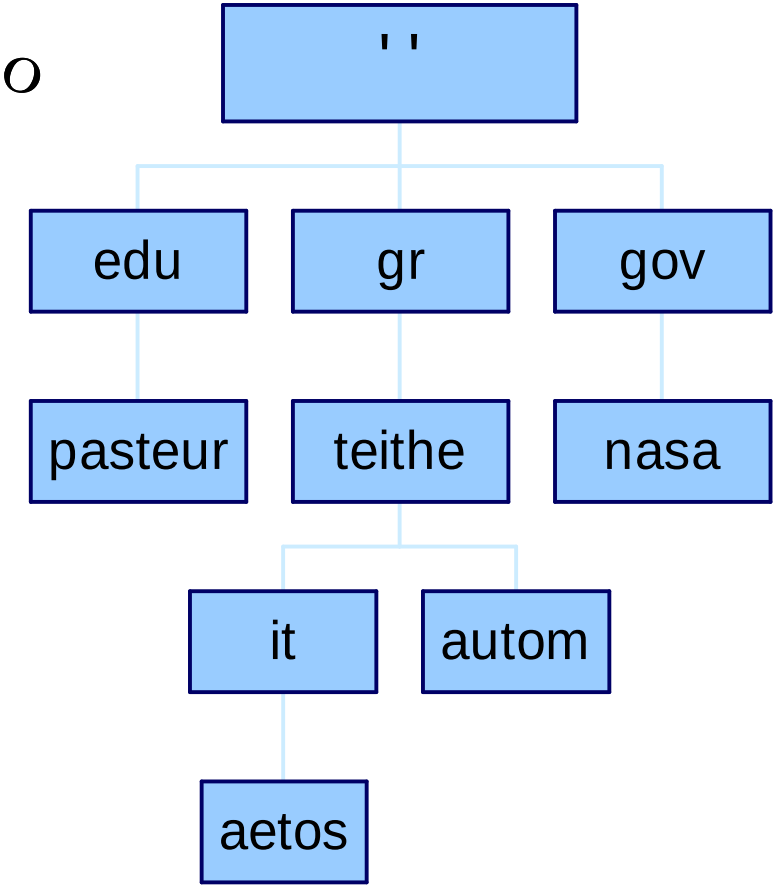
Περιοχή πρώτου επίπεδο

Δευτέρου επιπέδου

Τρίτου επιπέδου

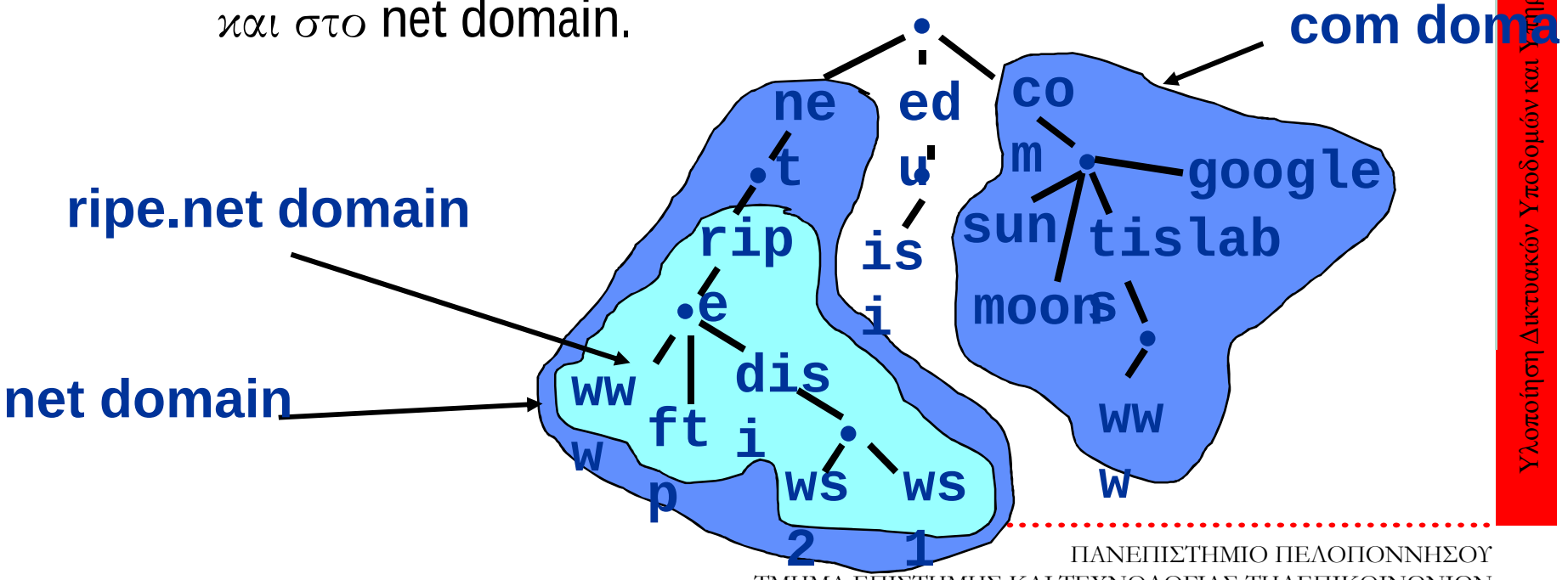
υποπεριοχές

υποπεριοχές



Domains

- Τα Domains είναι περιοχές ονομάτων “namespaces”
- Οτιδήποτε κάτω από το .com είναι στο com domain.
- Οτιδήποτε κάτω από το ripe.net is είναι στο ripe.net domain και στο net domain.

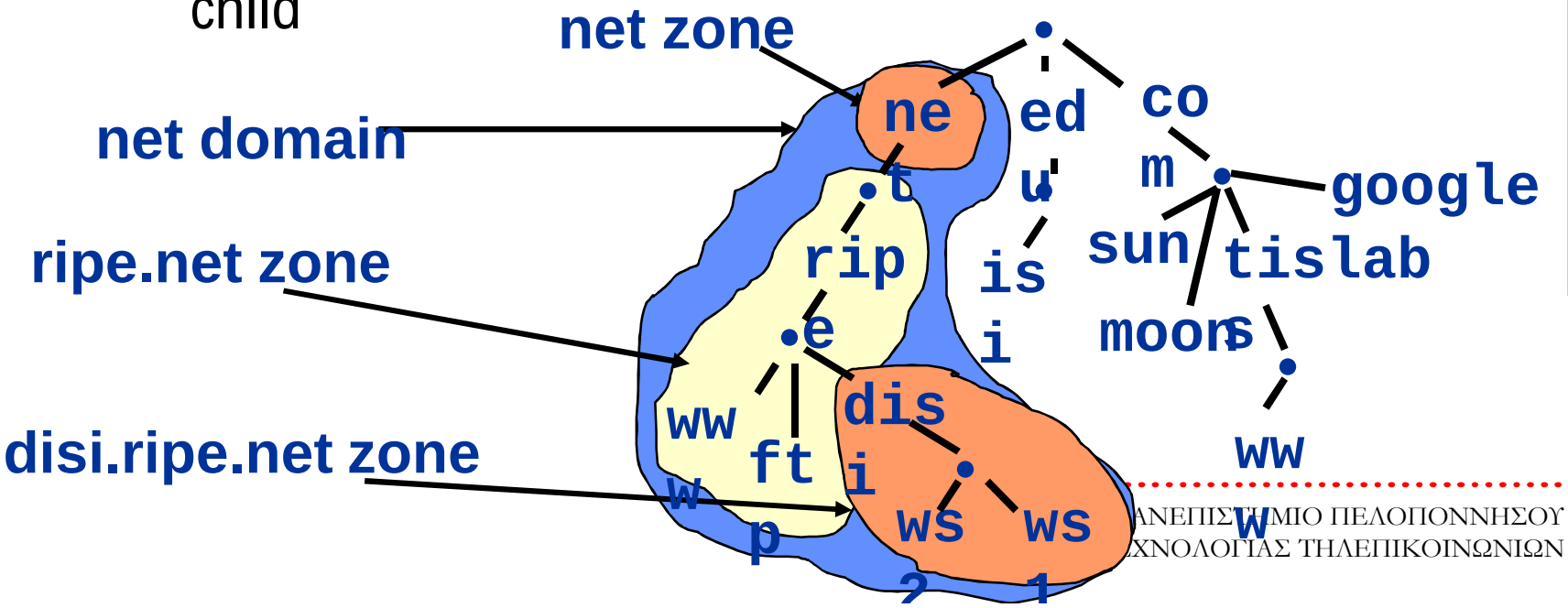


Delegation

- Οι διαχειριστές μπορούν να δημιουργήσουν subdomains για την ομαδοποίηση hosts
  - Σύμφωνα με γεωγραφικά χαρακτηριστικά, ανάγκες οργάνωσης ή άλλα κριτήρια
- Ο διαχειριστής ενός domain μπορεί να ορίζει κάποιο υπεύθυνο για την διαχείριση του subdomain
  - Αυτό δεν είναι απαραίτητο

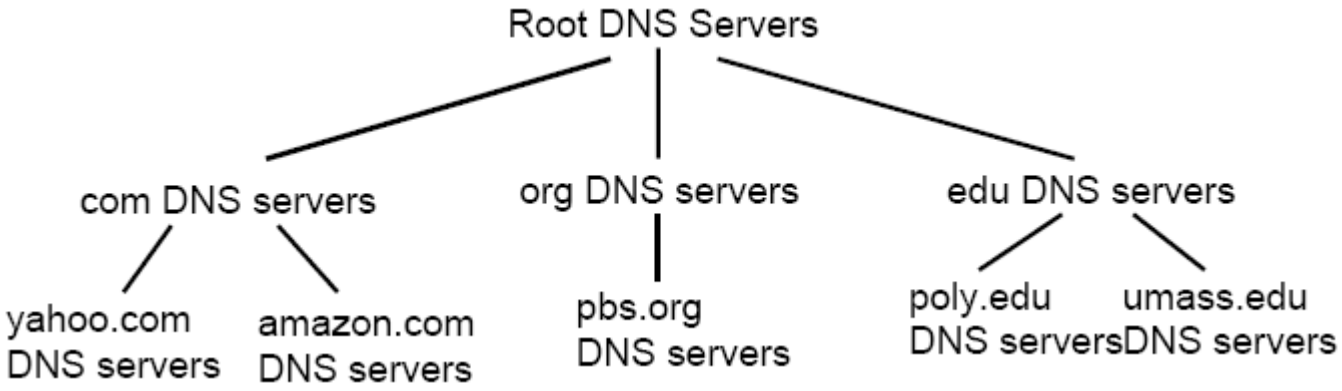
Zones και Delegations

- Zones είναι "administrative spaces"
- Οι διαχειριστές των Zone είναι υπεύθυνοι για ένα μέρος του domain's name space
- Δικαιώματα διαχείρισης ορίζονται από ένα parent σε ένα child



Κατανεμημένη, ιεραρχική βάση δεδομένων

- Ένας client επιθυμεί τη διεύθυνση IP του host www.amazon.com (χονδρική προσέγγιση):
  - Ο client στέλνει ερώτημα σε ένα root server αναζητώντας τον DNS server του domain com
  - Ο client στέλνει ερώτημα σε ένα DNS server του domain com αναζητώντας τον DNS server του subdomain amazon.com
  - Ο client στέλνει ερώτημα στον DNS server του amazon.com αναζητώντας την διεύθυνση IP του host www.amazon.com



DNS Name Servers

- Κανένας server δεν γνωρίζει όλα τα ζεύγη hostname-διεύθυνση IP
- Local name server
  - Κάθε ISP, εταιρία έχει ένα local (default) name server
  - Σε μια DNS query ο host απευθύνεται πρώτα στον local name server

DNS Root name servers

- Σε αυτούς απευθύνονται οι τοπικοί (local) name servers που δεν μπορούν να μεταφράσουν ένα hostname

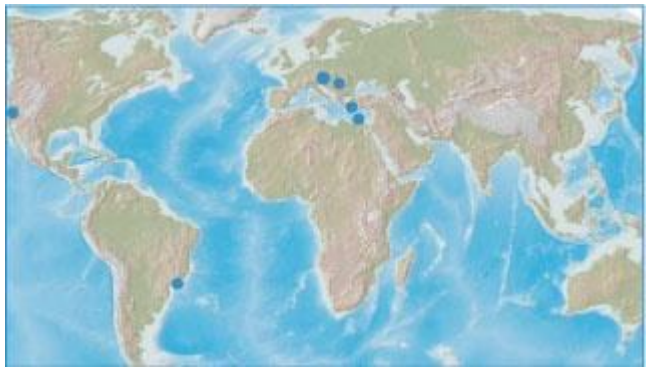
13 root name servers παγκοσμίως

TLD Servers και Authoritative Servers

- Top-level domain (TLD) servers: υπεύθυνοι για τα domains com, org, net, edu κλπ καθώς και για όλα τα top-level domains των κρατών: π.χ. gr, uk, fr, ca, jp
  - Η εταιρία Network solutions διαχειρίζεται τους servers του TLD com
  - Η εταιρία Educause διαχειρίζεται τους servers του TLD edu
- Authoritative DNS server: Οι DNS server ενός οργανισμού, που παρέχουν τις αντίστοιχιες hostname σε διεύθυνση IP για τους servers του οργανισμού (π.χ. Web και Mail servers).
  - Μπορεί να διατηρούνται από τον οργανισμό τον ίδιο ή από service provider

TLD server για το .gr

- Το TLD gr το διαχειρίζεται το ΙΤΕ-ΙΠ (περισσότερες πληροφορίες http://www.gr)
- Κόμβοι του .gr εγκατεστημένοι στον διεθνή χώρο
  - Ελλάδα: Ηράκλειο, Κρήτης (3) - Αθήνα. Μελλοντικές εγκαταστάσεις: Πάτρα, Ιωάννινα
  - Αυστρία: Βιέννη
  - Γερμανία: Φρανκφούρτη
  - Βραζιλία: Ρίο
  - Ηνωμένες Πολιτείες Αμερικής: Καλιφόρνια



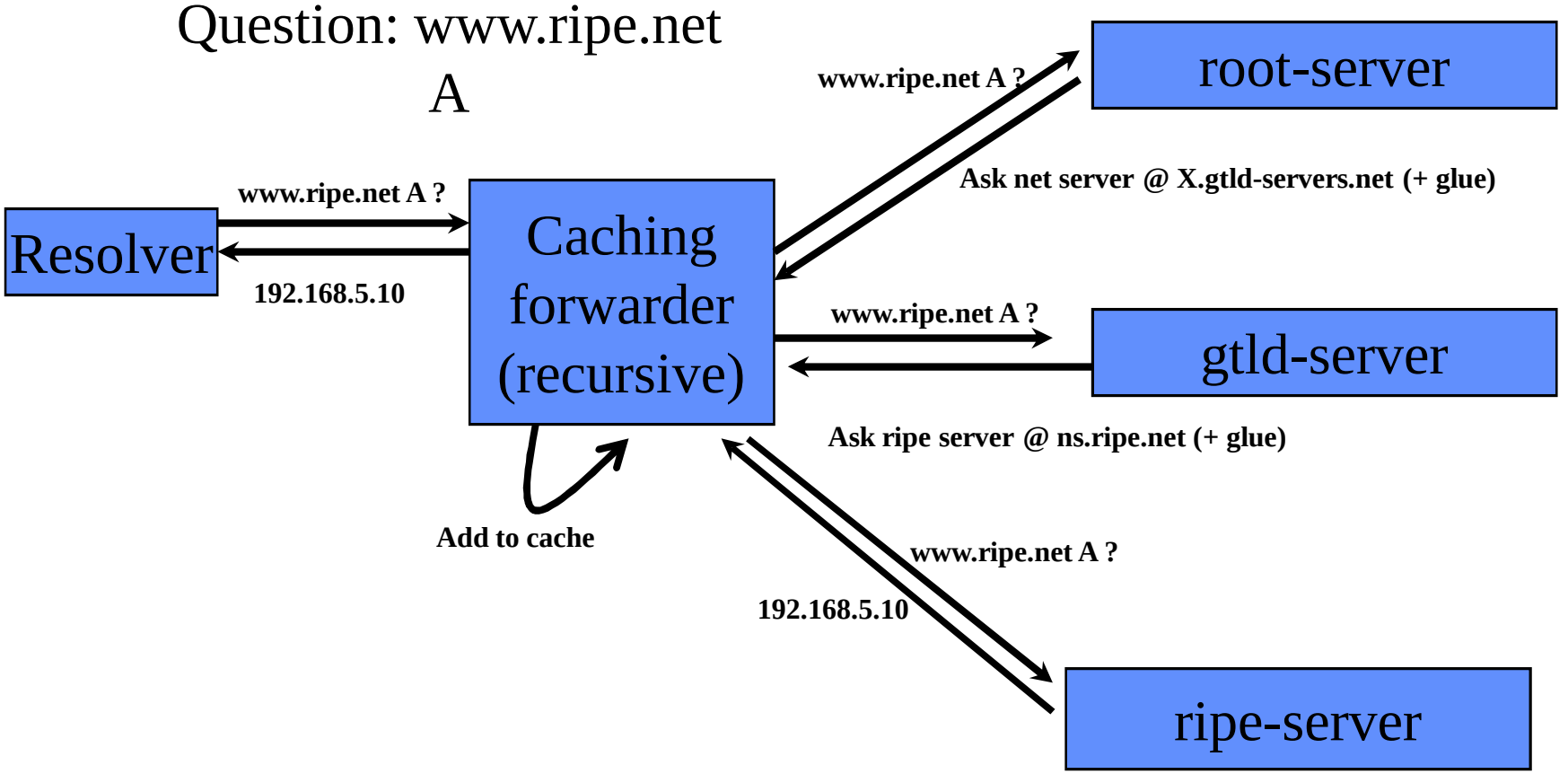
Local Name Server

- Δεν ανήκει αυστηρά στην ιεραρχία των DNS servers
- Κάθε ISP (εταιρία, πανεπιστήμιο) έχει ένα τοπικό name server ο οποίο καλείται επίσης και «default name server»
- Όταν ένα host κάνει ένα ερώτημα (query) DNS, το ερώτημα στέλνεται στον τοπικό του DNS server
  - Ο τοπικός name server προωθεί το ερώτημα στην ιεραρχία

Resolvers

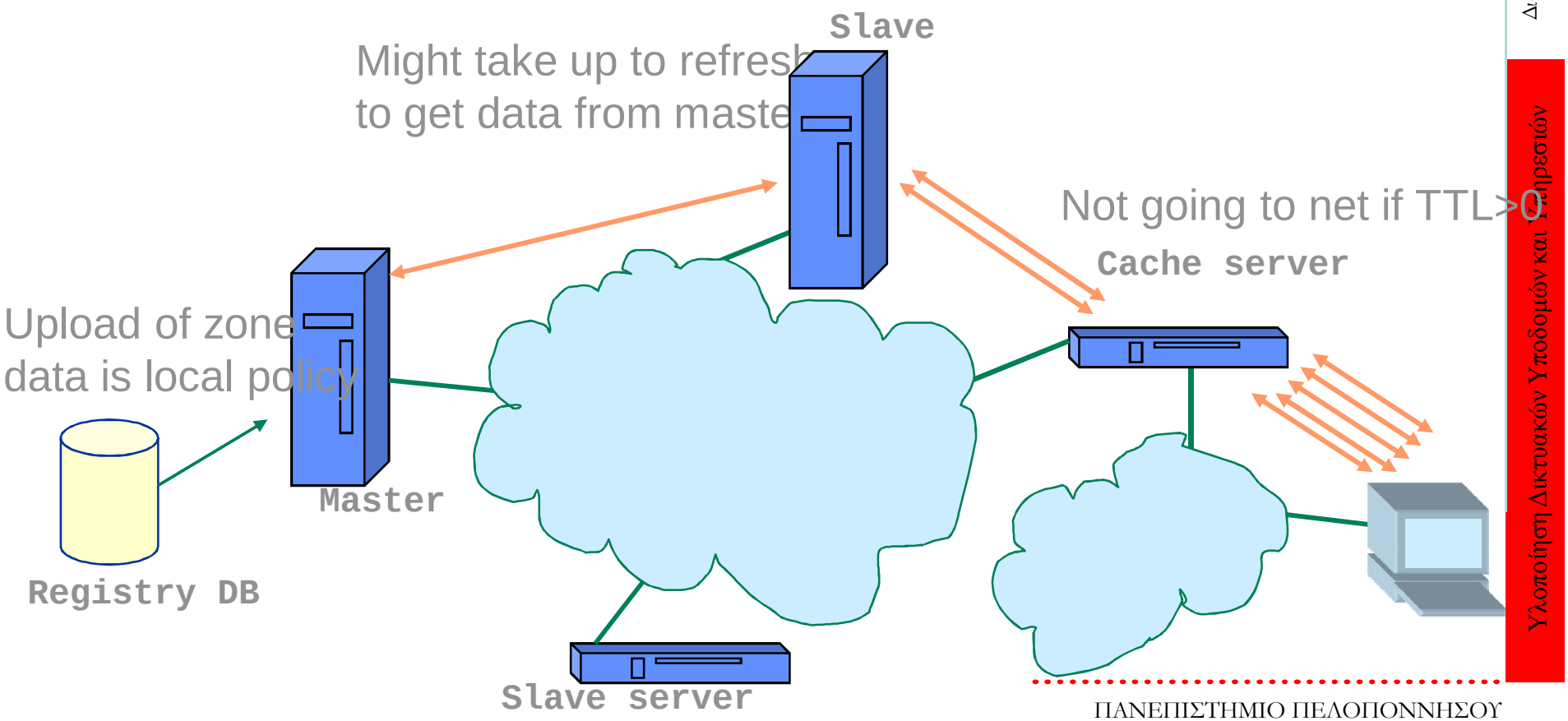
- Δέχονται ερωτήσεις από προγράμματα
- Απευθύνουν τις ερωτήσεις στον name server
- Ερμηνεύουν τις απαντήσεις από τους name servers
- Δίνουν την τελική απάντηση στην ερώτηση στο πρόγραμμα που ρώτησε

Resolving process & Cache



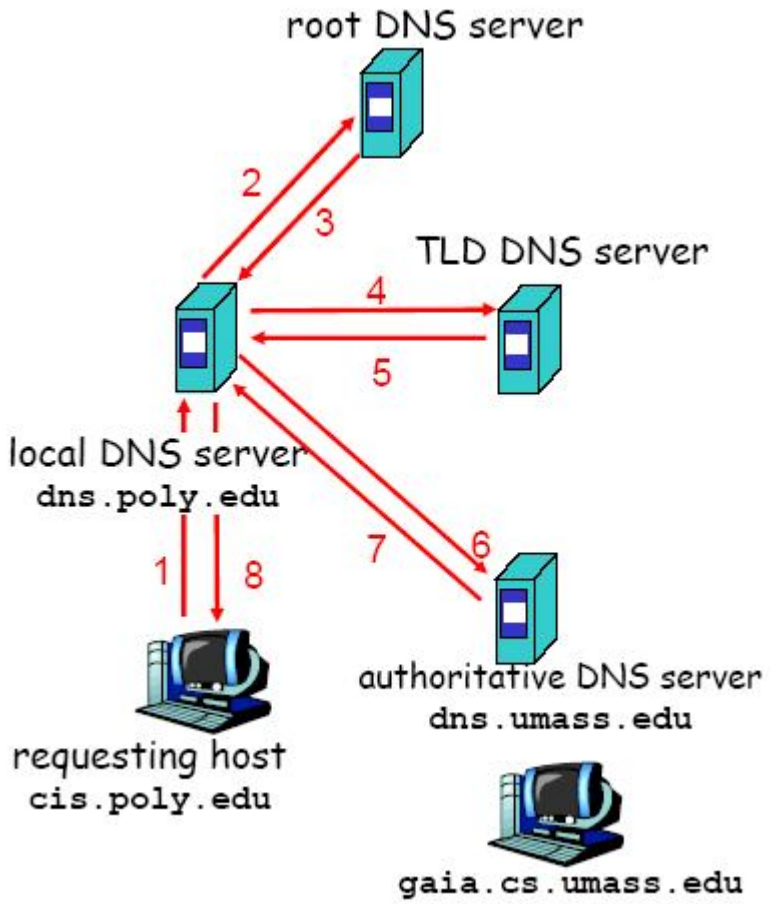
Που αποθηκεύονται τα DNS δεδομένα?

Changes in DNS do not propagate instantly!



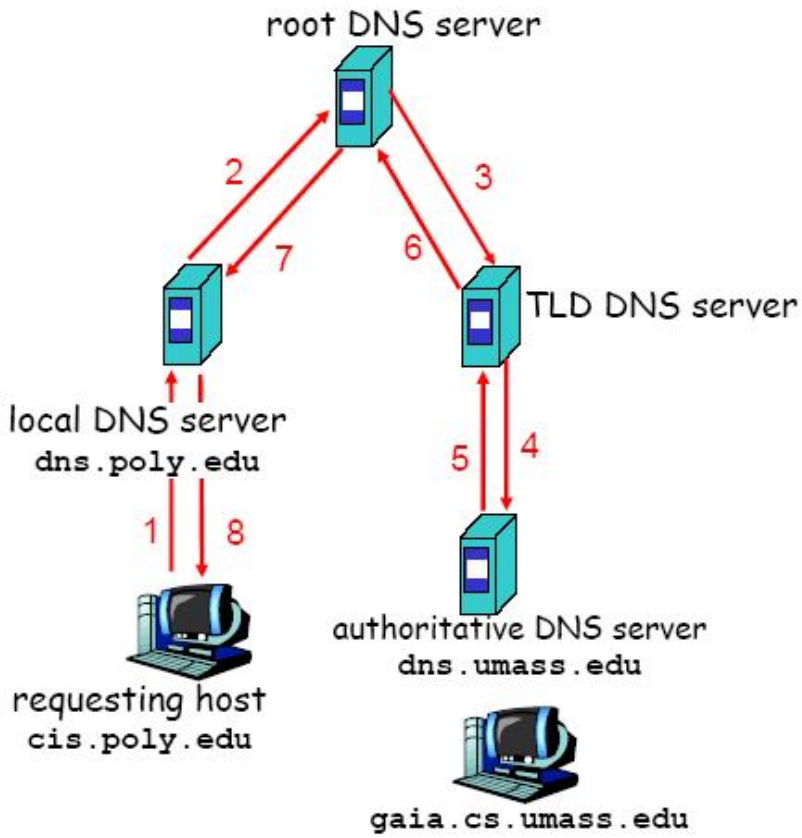
Παράδειγμα

- Ο host cis.poly.edu θέλει τη διεύθυνση IP του gaia.cd.umass.edu



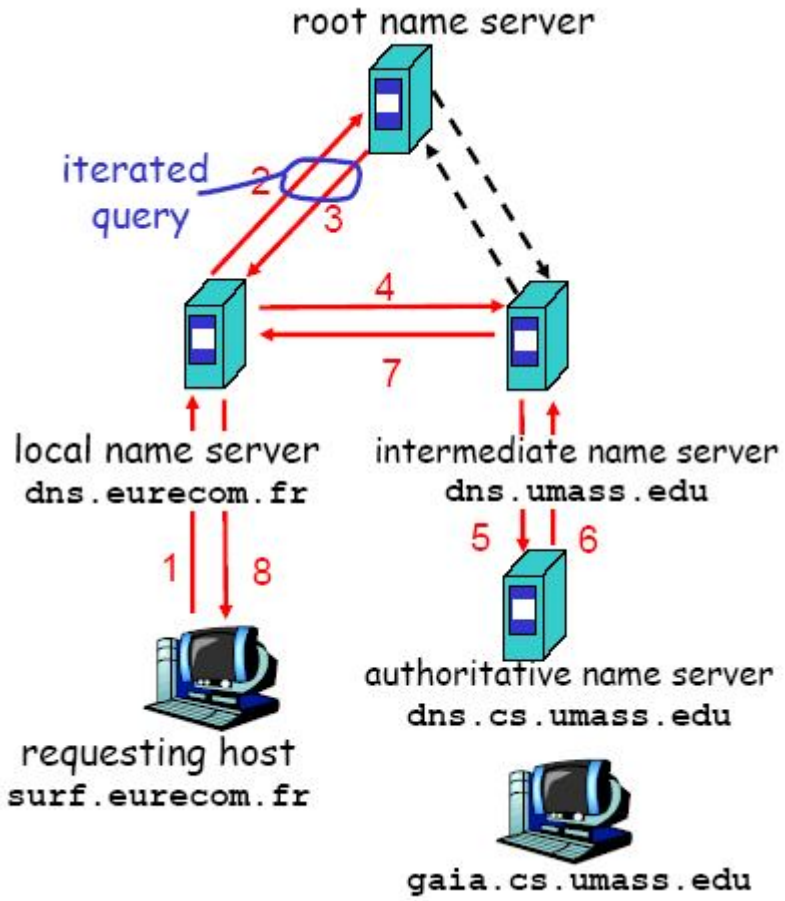
DNS: Recursive queries

- Recursive query (αναδρομικό ερώτημα)
  - Αναθέτει τη μετάφραση του ονόματος στον name server στον οποίο απευθύνεται
  - Υψηλό φορτίο
- Iterated query (επαναληπτικό ερώτημα)
  - Ο ερωτηθείς name server παραπέμπει σε άλλο name server
  - "Δεν γνωρίζω αυτό το όνομα, ρώτα αυτόν το server"



DNS: iterated queries

- Recursive query
  - Αναθέτει τη μετάφραση του ονόματος στον name server στον οποίο απευθύνεται
  - Υψηλό φορτίο
- Iterated query
  - Ο ερωτηθείς name server παραπέμπει σε άλλο name server
  - "Δεν γνωρίζω αυτό το όνομα, ρώτα αυτόν το server"



DNS: caching και ενημέρωση records

- Για την βελτίωση των καθυστερήσεων και του αριθμού DNS queries στο δίκτυο:
  - Όταν (οποιοσδήποτε) name server λάβει ένα record, καταχωρεί αντίγραφο σε μια cache
    - Η καταχώρηση της cache εξαφανίζεται (timeout) μετά από κάποιο χρόνο
    - Καταχωρήσεις για τους TLD servers υπάρχουν συνήθως στην cache του τοπικού name server (οι root name servers δεν δέχονται συχνές επισκέψεις)
- Η εισαγωγή δεδομένων στην βάση γίνονται μέχρι πρόσφατα στατικά από τον διαχειριστή
  - Υπό σχεδίαση (IETF) βρίσκονται δυναμικοί μηχανισμοί ενημέρωσης που χρησιμοποιούν μηνύματα DNS

Οργάνωση των πληροφοριών

- domain name [ttl] [class] type value
  - domain name (δείκτης)
  - ttl (time to live)
  - class (IN)
  - type
  - value

Τύποι Resource

- Ip address
  - knuth.it.teithe.gr IN A 193.92.235.39
- Host information
  - knuth.it.teithe.gr IN HINFO ‘VAX 4000’ ‘VMS’
- Pointer
  - 29.235.92.193.in-addr.arpa IN PTR knuth.it.teithe.gr
- Name servers
  - it.teithe.gr IN NS knuth.it.teithe.gr.

Τύποι Resource

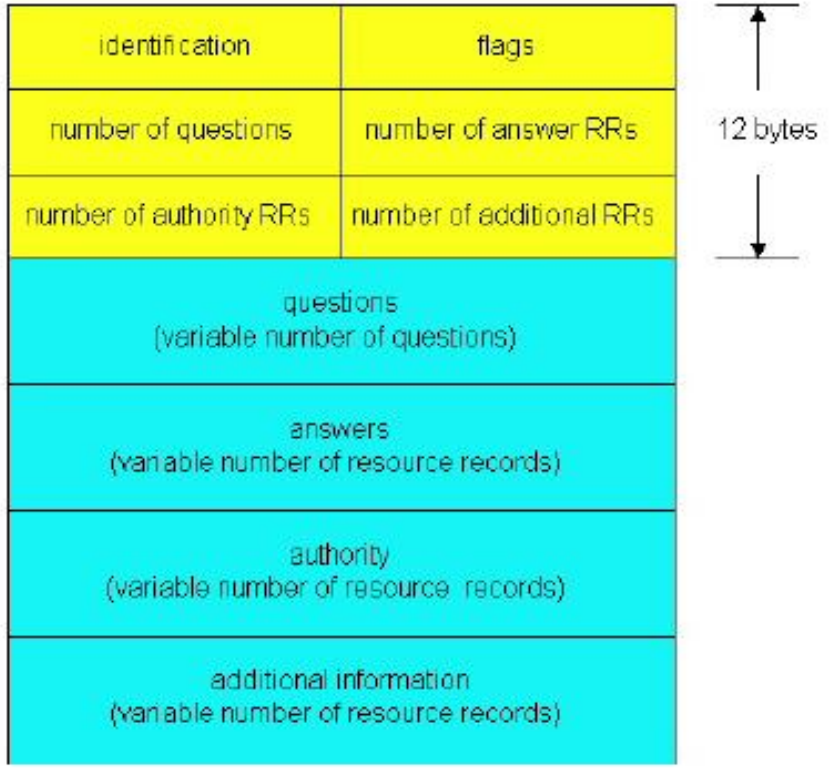
- Canonical Name
  - www.teithe.gr IN CNAME knuth.it.teithe.gr.
- Mail exchanger
  - it.teithe.gr IN MX 10 knuth.it.teithe.gr.
- Well known servises
  - knuth.it.teithe.gr IN WKS TCP smtp teltnet

DNS records

- DNS: Κατανεμημένη βάση δεδομένων αποθηκεύει resource records (RR)
- RR Format: (name, value, type, ttl)
- Type=A: name: hostname και value: IP address
- Type=NS: name ψευδώνυμο (alias name) για κάποιο «canonical» name (πραγματικό όνομα) (π.χ. www.ibm.com στην πραγματικότητα servereast.backup2.ibm.com) και value: canonical name
- Type=MX: name: ψευδώνυμο mail server και value: «canonical» name mail server

Πρωτόκολλο DNS, μηνύματα

- Πρωτόκολλο DNS: μηνύματα **query** και **reply** έχουν το ίδιο **format**
- Επικεφαλίδα μηνύματος
  - **Identification**: αριθμός από 16 **bits** που προσδιορίζει το ερώτημα **(query)**, η απόκριση σε ένα ερώτημα χρησιμοποιεί τον ίδιο αριθμό
  - **Flags**
    - Query ή reply
    - Recursion desired
    - Recursion available
    - Reply is authoritative



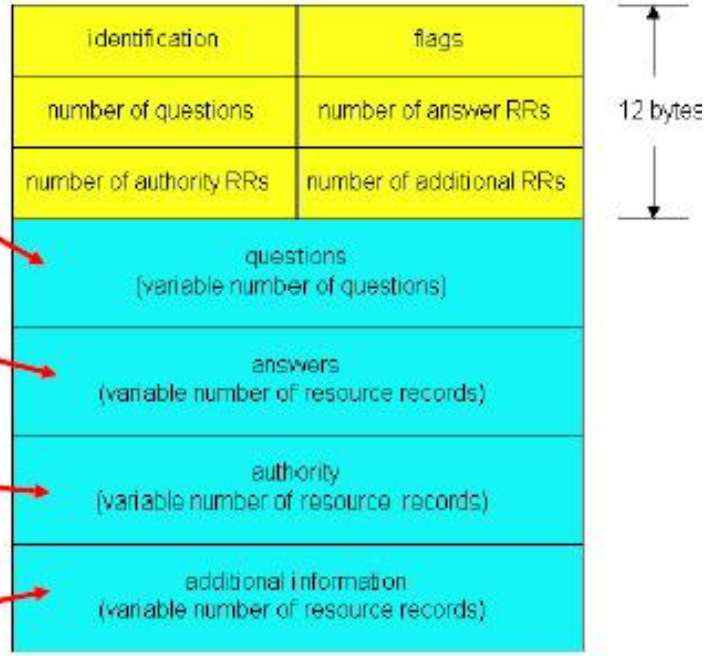
Πρωτόκολλο DNS, μηνύματα

Name, type fields for a query

RRs in response to query

records for authoritative servers

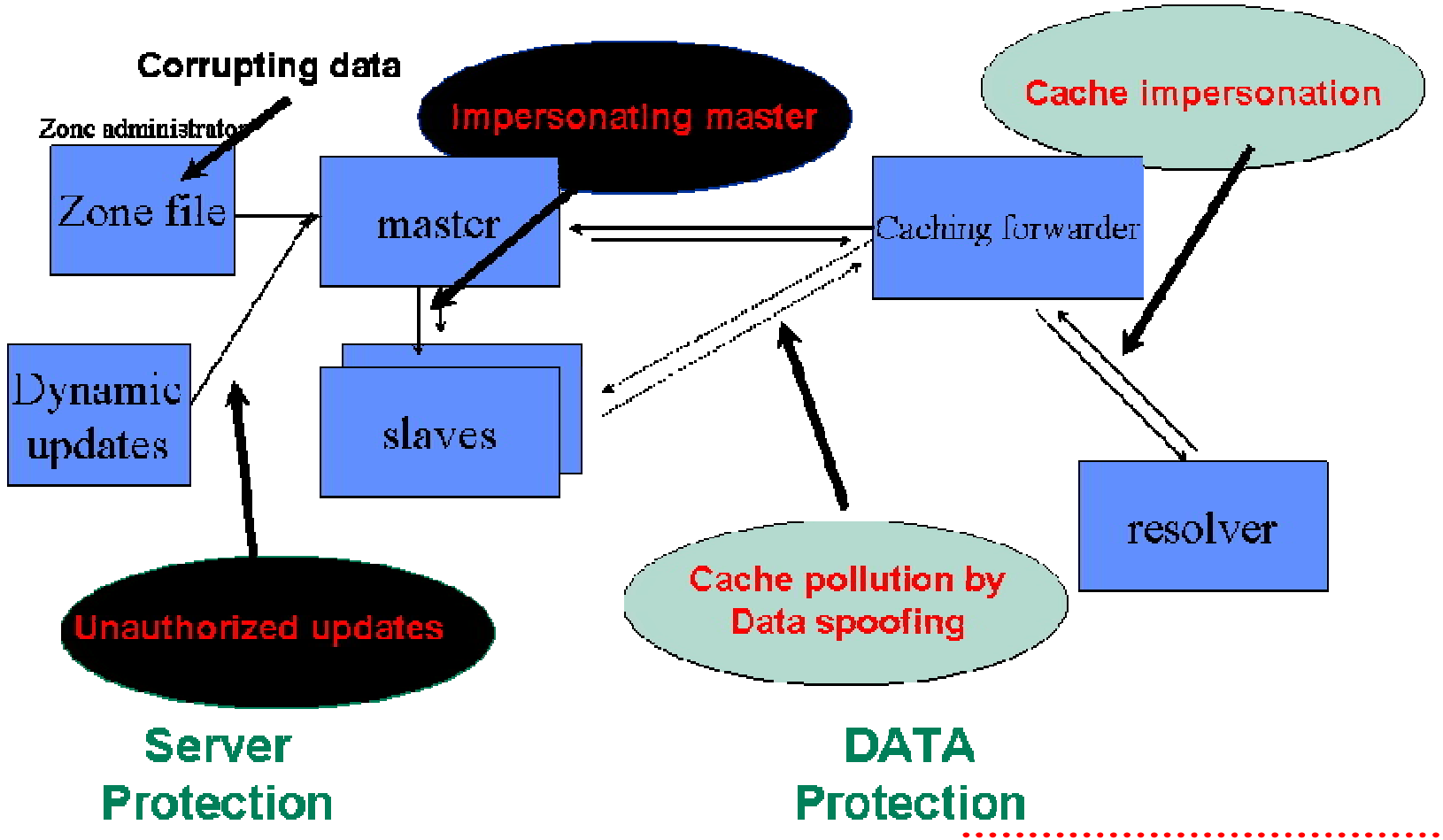
additional "helpful" info that may be used



Προβλήματα ασφάλειας στο DNS

- Τα DNS δεδομένα μπορεί να αλλοιωθούν (spoofed, corrupted) κατά την μετάδοση από τον server στο resolver
- Το DNS protocol δεν παρέχει μηχανισμού για το έλεγχο της εγκυρότητας των DNS δεδομένων.
- Πως ένας slave server γνωρίζει ότι μιλά με τον κατάλληλο master server

Προβλήματα ασφάλειας στο DNS



Η λύση είναι το DNSSEC

- Το DNSSEC προστατεύει στην αλλοίωση των δεδομένων (spoofing και corruption)
- Το DNSSEC παρέχει μηχανισμούς για την πιστοποίηση servers
- Το DNSSEC παρέχει μηχανισμούς για έλεγχο αυθεντικότητας και integrity