



# ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

Το σύστημα ονομασίας  
περιοχών DNS

# Ονόματα των host



- Οι διευθύνσεις IP προσδιορίζουν διεπαφές υπολογιστών ή δρομολογητών
  - Η διεύθυνση IP περιέχει πληροφορία που χρησιμοποιείται για τη δρομολόγηση
- Τα ονόματα είναι αλφαριθμητικές περιγραφές αντί διευθύνσεων IP
  - π.χ. [www.telecom.ntua.gr](http://www.telecom.ntua.gr), [www.google.com](http://www.google.com), [www.ietf.org](http://www.ietf.org)
- Είναι αδύνατο μαντέψει κάποιος τις διευθύνσεις IP
  - π.χ. από το όνομα μιας ιστοθέσης

# Ονόματα των host



- Οι διευθύνσεις IP είναι δύσκολο να απομνημονεύονται από τους ανθρώπους
- Οι άνθρωποι προτιμούν να θυμούνται ονόματα αντί διευθύνσεων IP
  - Φανταστείτε να έπρεπε να θυμάστε τους αριθμούς των τηλεφώνων των φίλων σας αντί των ονομάτων τους
- Το σύστημα ονομασίας περιοχών (DNS) είναι μια κατακεμημένη βάση δεδομένων στο διαδίκτυο που επιτρέπει τη μετάφραση ανάμεσα σε ονόματα και διευθύνσεις IP



# Σύστημα ονομασίας περιοχών

## Domain Name System (DNS):

- Ο τηλεφωνικός κατάλογος του διαδικτύου
- Ο μηχανισμός του διαδικτύου για την αναφορά μέσω ονομάτων σε ότι πόρους χρησιμοποιούμε
  - Μετάφραση ονομάτων σε διευθύνσεις IP και το αντίστροφο
  - Αντιστοίχιση ονομάτων αντικειμένων σε άλλα ονόματα
  - Παγκοσμίως κατανεμημένη, επεκτάσιμη και αξιόπιστη βάση δεδομένων



# Domain Name System (DNS)

- **κατανεμημένη βάση δεδομένων που εφαρμόζεται σε μια ιεραρχία πολλών εξυπηρετητών ονομάτων**
- Περιλαμβάνει
  - το **χώρο ονομάτων**
  - τους **εξυπηρετητές** μέσω των οποίων γίνεται διαθέσιμος ο χώρος ονομάτων
  - και τους **αναλυτές (resolvers)** που ερωτούν τους εξυπηρετητές περί του χώρου ονομάτων
- Τα δεδομένα διατηρούνται τοπικά, αλλά είναι διαθέσιμα παγκόσμια ...
  - ... δεν υπάρχει υπολογιστής με όλη τη βάση DNS



# Domain Name System (DNS)

- πρωτόκολλο στρώματος εφαρμογών που επιτρέπει σε hosts, routers και name servers να επικοινωνούν για να αναλύσουν (resolve) ονόματα (μεταφράσουν ονόματα σε διεύθυνση)
  - είναι λειτουργία του κορμού του Internet
  - υλοποιείται ως πρωτόκολλο του στρώματος εφαρμογών
  - η πολυπλοκότητα βρίσκεται στο "άκρο" του δικτύου
  - οι αναζητήσεις DNS γίνονται από οποιοδήποτε μηχάνημα και οποιαδήποτε υπηρεσία
  - τα αποτελέσματα από μακρινούς εξυπηρετητές αποθηκεύονται προσωρινά σε τοπική μνήμη ώστε να βελτιωθεί η επίδοση

# Προτού υπάρξει το DNS ...



- ... υπήρχε το αρχείο hosts.txt
- Πριν το 1985 η αντιστοίχιση ονόματος σε διεύθυνση IP καταγράφονταν σε αυτό το αρχείο
  - οι υπολογιστές το κατέβαζαν από ένα κεντρικό εξυπηρετητή μέσω FTP
  - τα ονόματα στο hosts.txt δεν είχαν κάποια δομή
  - το αρχείο ακόμη υπάρχει στα περισσότερα λειτουργικά συστήματα ...
    - ... μπορεί να χρησιμοποιηθεί για τον ορισμό ονομάτων



## Χώρος ονομάτων



# Χώρος ονομάτων του DNS



- Το Internet είναι χωρισμένο νοητά σε εκατοντάδες διαφορετικές **περιοχές (domains)** υψηλού επιπέδου
  - που αναλύονται σε υπο-περιοχές (sub-domains), κ.ο.κ., με πολλούς host η καθεμία
  - Οι περιοχές μπορεί να παρασταθούν μ' ένα δέντρο
- **χώρος ονομάτων (name space)**
  - Τα ονόματα των περιοχών απαρτίζουν μια ιεραρχία κατά τρόπο που τα ονόματα να είναι μοναδικά και να απομνημονεύονται εύκολα
  - Ένας οργανισμός είναι αρμόδιος για μέρος του χώρου ονομάτων και μπορεί να προσθέσει επιπλέον επίπεδα στην ιεραρχία

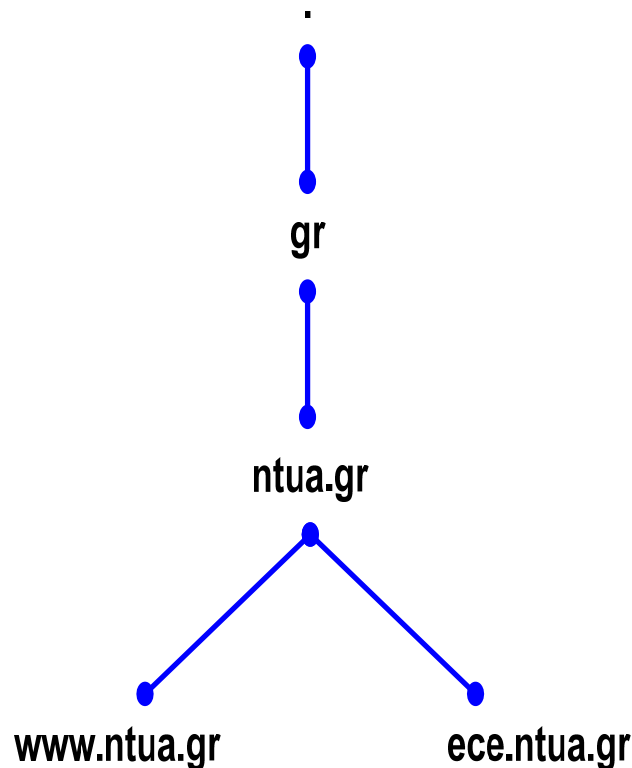


# Ιεραρχία του DNS

- Κάθε κόμβος στο δένδρο DNS αναπαριστά ένα **όνομα DNS (DNS name)**
- Κάθε κλαδί κάτω από ένα κόμβο είναι μια **περιοχή DNS (DNS domain)**
  - Η περιοχή DNS μπορεί να περιέχει hosts ή άλλες περιοχές (**subdomains**)

- Παράδειγμα περιοχών DNS

.  
gr  
ntua.gr  
cn.ece.ntua.gr



cn.ece.ntua.gr  
Δίκτυα Υπολογιστών

# Ιεραρχία του DNS



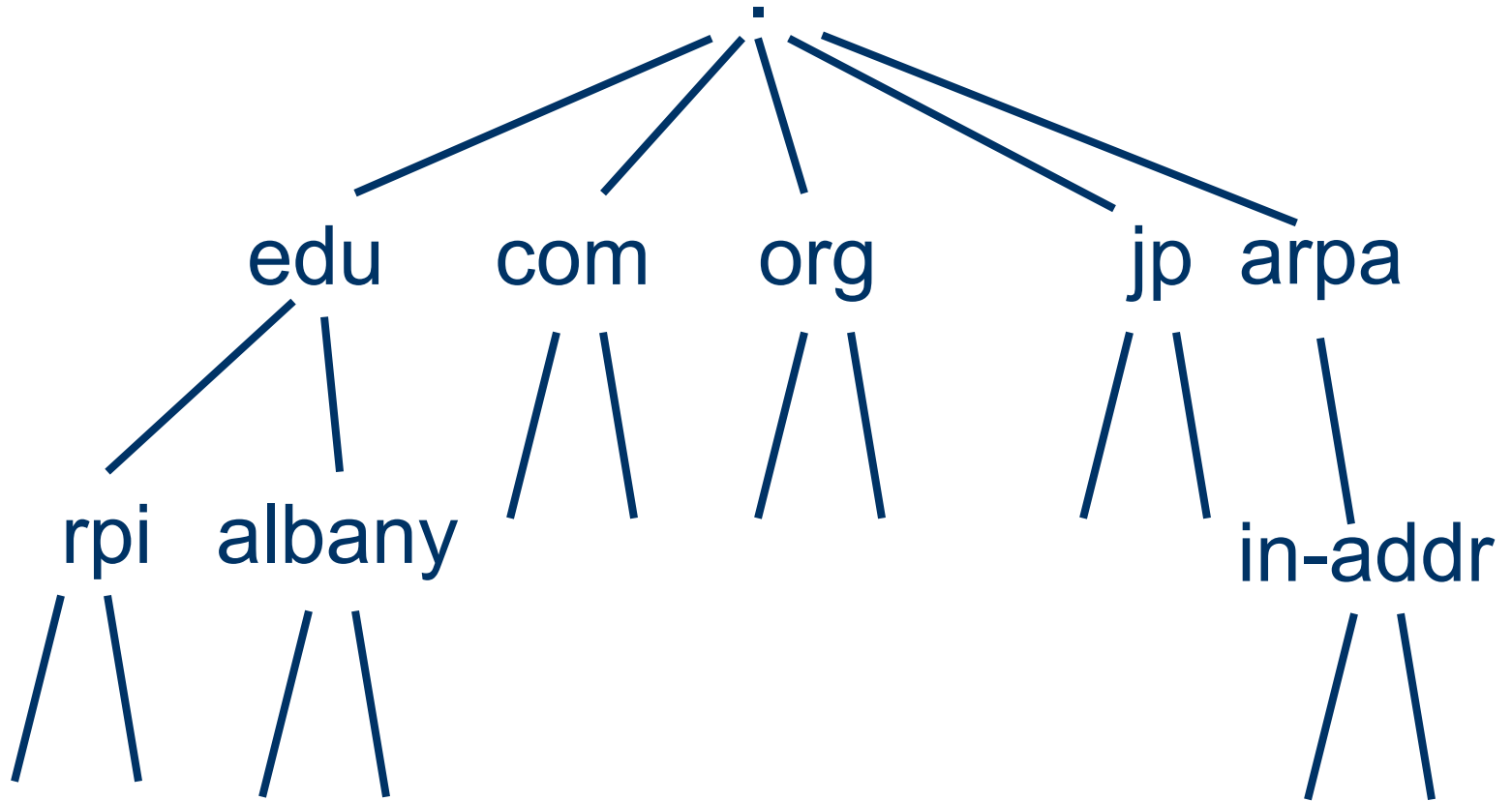
- Η κορυφή του δένδρου είναι η **ρίζα (root)** και συμβολίζεται με μία τελεία «.»
- Η IANA (Internet Assigned Numbers Authority) είναι η επίσημη αρχή του διαχειρίζεται τη ρίζα του DNS
  - Η IANA λειτουργεί υπό την επίβλεψη της ICANN (Internet Corporation for Assigned Names and Numbers)
  - Η ICANN είναι μια μη κερδοσκοπική εταιρεία που δημιουργήθηκε το 1998 με σκοπό την επίβλεψη διάφορων εργασιών σχετικών με το διαδίκτυο που προηγουμένως τις επέβλεπε άμεσα η κυβέρνηση των ΗΠΑ (μέσω της IANA)

# Ιεραρχία του DNS



- Κάτω από την κορυφή υπάρχουν οι **περιοχές ανωτάτου επιπέδου (top level domains)**
  - η διαχείριση τους (εκτός των .int και .arpa) έχει εκχωρηθεί από την IANA σε άλλους υπεύθυνους οργανισμούς, π.χ.
    - EDUCAUSE για την περιοχή .edu
    - DoD για την .mil
- Η διαχείριση του χώρου ονομάτων κάτω από τις περιοχές ανωτάτου επιπέδου έχει εκχωρηθεί σε οργανισμούς, που μπορούν να εκχωρήσουν περαιτέρω τη διαχείριση υπο-περιοχών τους

# Ιεραρχία του DNS





# Περιοχές ανώτατου επιπέδου (top-level domains - TLD)

- αρχικά (1988) υπήρχαν
  - edu, gov, com, org, mil, net, int, arpa
- μετά προστέθηκαν περιοχές για κάθε χώρα (όνομα περιοχής με 2 γράμματα).
  - gr, nl, uk, us, jp, ...
- κατόπιν (2001) εγκρίθηκαν
  - aero, biz, coop, info, museum, name, pro
- και πιο πρόσφατα (2005) εγκρίθηκαν αρκετές νέες
  - asia, cat, jobs, mobi, post, tel, travel



# Περιοχές ανώτατου επιπέδου (top-level domains - TLD)

- Η ΙΑΝΑ σήμερα ξεχωρίζει τις ακόλουθες ομάδες περιοχών ανωτάτου επιπέδου:
  - country-code top-level domains (ccTLD)
    - 248 περιοχές χωρών με όνομα αποτελούμενο από δύο γράμματα για χώρες ή επικράτειες
  - generic top-level domains (gTLD):
    - 20 γενικές περιοχές με όνομα αποτελούμενου από τρία ή περισσότερα γράμματα για οργανισμούς ή ιδιώτες

# Γενικές περιοχές ανώτατου επιπέδου



- **generic top-level domains (gTLD):**
  - **unsponsored top-level domains (uTLD)**
    - περιοχές που λειτουργούν σύμφωνα με τις πολιτικές της ICANN για το παγκόσμιο διαδίκτυο
    - biz, com, info, name, net, org, pro
  - **sponsored top-level domains (sTLD)**
    - περιοχές διαχειριζόμενες από οργανισμούς ή ιδιώτες που περιορίζουν τη συμμετοχή βάσει κανόνων
    - aero, asia, cat, coop, edu, gov, int, jobs, mil, mobi, museum, tel, travel
  - **infrastructure top-level domain**
    - περιέχει μόνο μία περιοχή που διαχειρίζεται από την IANA
    - .arpa (Address and Routing Parameter Area )



# Όνομα περιοχής



- Μια περιοχή είναι ένα υποδέντρο του παγκόσμιου δέντρου ονομάτων
- Το όνομα περιοχής (domain name) είναι η ακολουθία των ετικετών που οδηγούν από τον host (φύλλο στο δέντρο ονομάτων) στην κορυφή του παγκόσμιου δέντρου ονομάτων
  - διαβασμένο αριστερά προς δεξιά
  - έχει μέγιστο βάθος 127 επίπεδα
- Παραδείγματα:
  - whitehouse.gov
  - ntua.gr
  - εμπ.gr



# FQDN (Fully Qualified Domain Name)

- Κάθε κόμβος στο δένδρο περιοχών DNS μπορεί να προσδιορισθεί από την **πλήρη περιγραφή του ονόματος περιοχής (FQDN)**
- Η FQDN δίνει τη θέση του στο δένδρο
  - προσδιορίζει όλα τα ονόματα περιοχών κάτω από τη ρίζα
  - αποτελείται από μια ακολουθία ετικετών (labels) που χωρίζονται με τελείες
  - μπορεί να τερματίζει με μια τελεία «.» μιας και η ρίζα δεν έχει όνομα
- Παράδειγμα
  - `cs.ntua.gr` ή `cs.ntua.gr.`

# Όνομα host ή όνομα περιοχής



- Το όνομα host υπονοεί όνομα μιας περιοχής στην οποία έχουν συνδεθεί μία ή περισσότερες διευθύνσεις IP
- Π.χ. οι περιοχές [www.ntua.gr](http://www.ntua.gr) και [ntua.gr](http://ntua.gr) είναι και ονόματα host, ενώ η περιοχή gr δεν είναι



# Οργάνωση του DNS

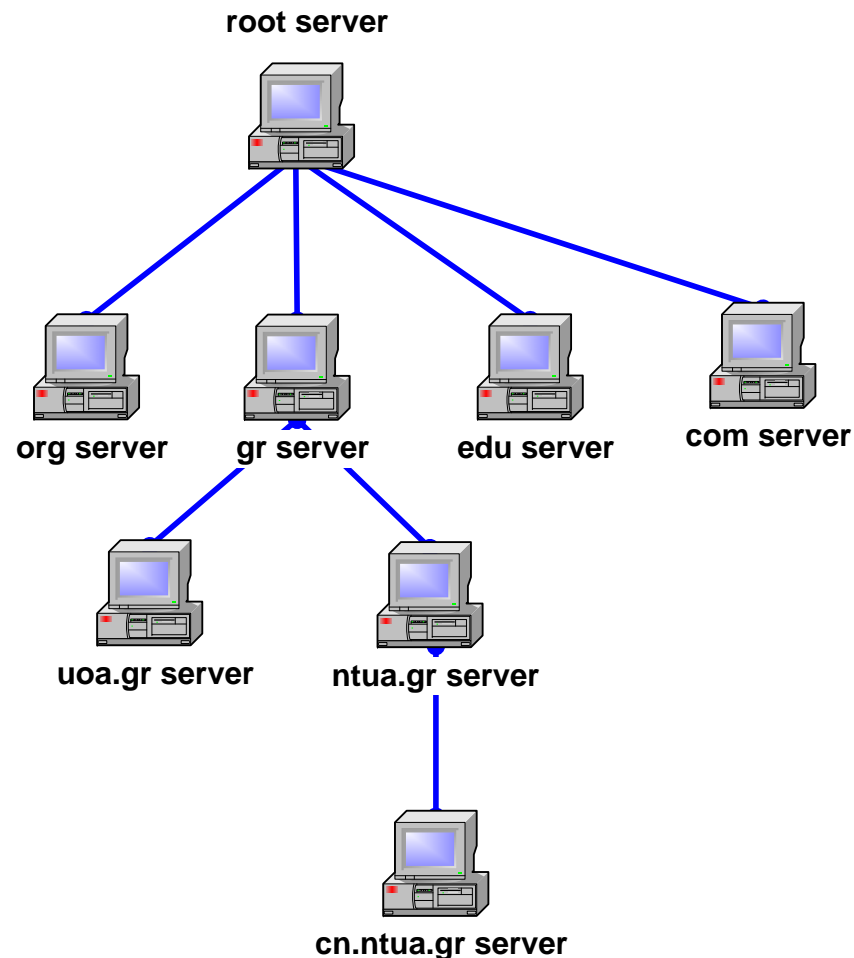


- Το DNS είναι οργανωμένο ως **μία κατανεμημένη βάση δεδομένων**
  - Χρησιμοποιεί το μοντέλο πελάτη - εξυπηρετητή
  - Κόμβοι της βάσης είναι οι εξυπηρετητές ονομάτων
- Γιατί όχι κεντρικό DNS?
  - μοναδικό σημείο αστοχίας
    - απόμακρη κεντρική βάση δεδομένων
  - όγκος κίνησης
    - δεν υπάρχει όριο στο μέγεθος της βάσης
    - δεν υπάρχει όριο στο πλήθος των ερωτήσεων
  - δυσκολία συντήρησης
  - δεν είναι επεκτάσιμο

# Ιεραρχία των εξυπηρετητών ονομάτων



- Η ιεραρχία του χώρου ονομάτων ανταποκρίνεται σε μία αντίστοιχη ιεραρχία εξυπηρετητών ονομάτων
- Κάθε εξυπηρετητής είναι υπεύθυνος για ένα συμπαγές τμήμα του χώρου ονομάτων DNS που αποκαλείται **ζώνη (zone)**
- Η ζώνη είναι μέρος του υποδένδρου
- Ο εξυπηρετητής ονομάτων απαντά σε ερωτήσεις (queries) για τους host της ζώνης του



# Αρμοδιότητα και εκχώρηση

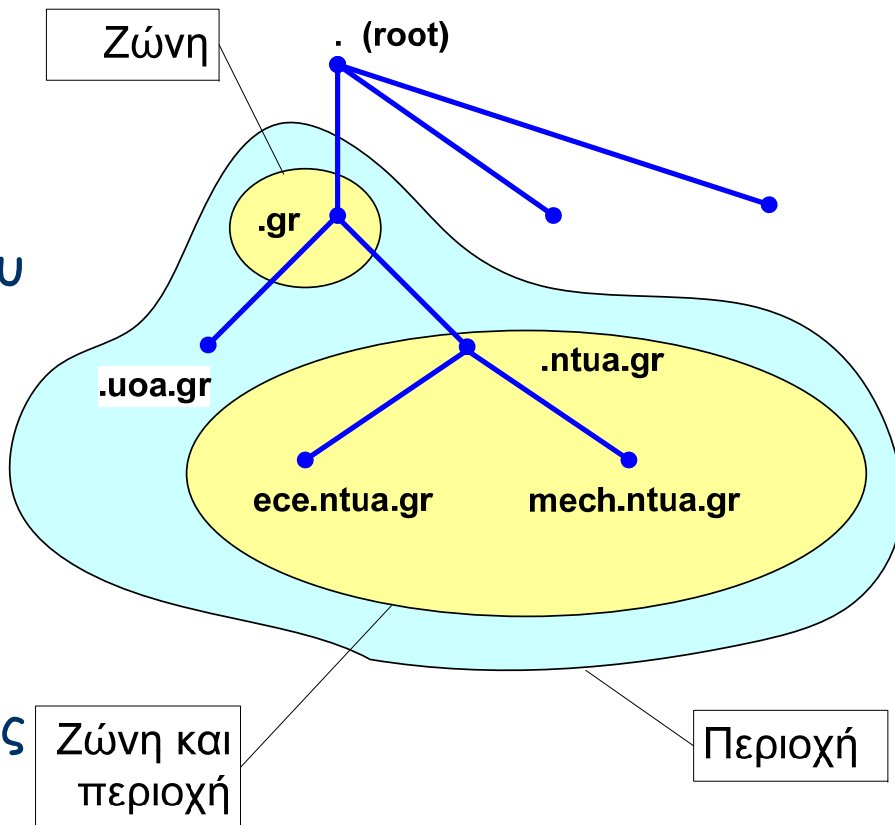


- Ο διαχειριστής μιας περιοχής μπορεί να ορίσει υπο-περιοχές για να ομαδοποιήσει τους host με
  - Γεωγραφικό, οργανωτικό, κλπ κριτήριο
- Η αρμοδιότητα για τις υπο-περιοχές μπορεί να εκχωρηθεί περαιτέρω, χωρίς αυτό να είναι υποχρεωτικό
- Η σειρά της εκχώρησης αρμοδιότητας φαίνεται διαβάζοντας το όνομα της περιοχής από δεξιά προς αριστερά
- Η μονάδα εκχώρησης είναι η ζώνη



# Περιοχή DNS και ζώνες

- Κάθε ζώνη είναι αγκυρωμένη σε ένα κόμβο του δένδρου
  - οι ζώνες δεν είναι περιοχές
  - η περιοχή DNS είναι ένας κλάδος του χώρου ονομάτων
- Η ζώνη είναι τμήμα του χώρου ονομάτων DNS που εν γένει αποθηκεύεται σε ένα αρχείο
  - Οι ζώνες είναι «διοικητικός χώρος»
- Ο εξυπηρετητής μπορεί να χωρίσει μέρος της ζώνης του και να το εκχωρήσει σε άλλους εξυπηρετητές





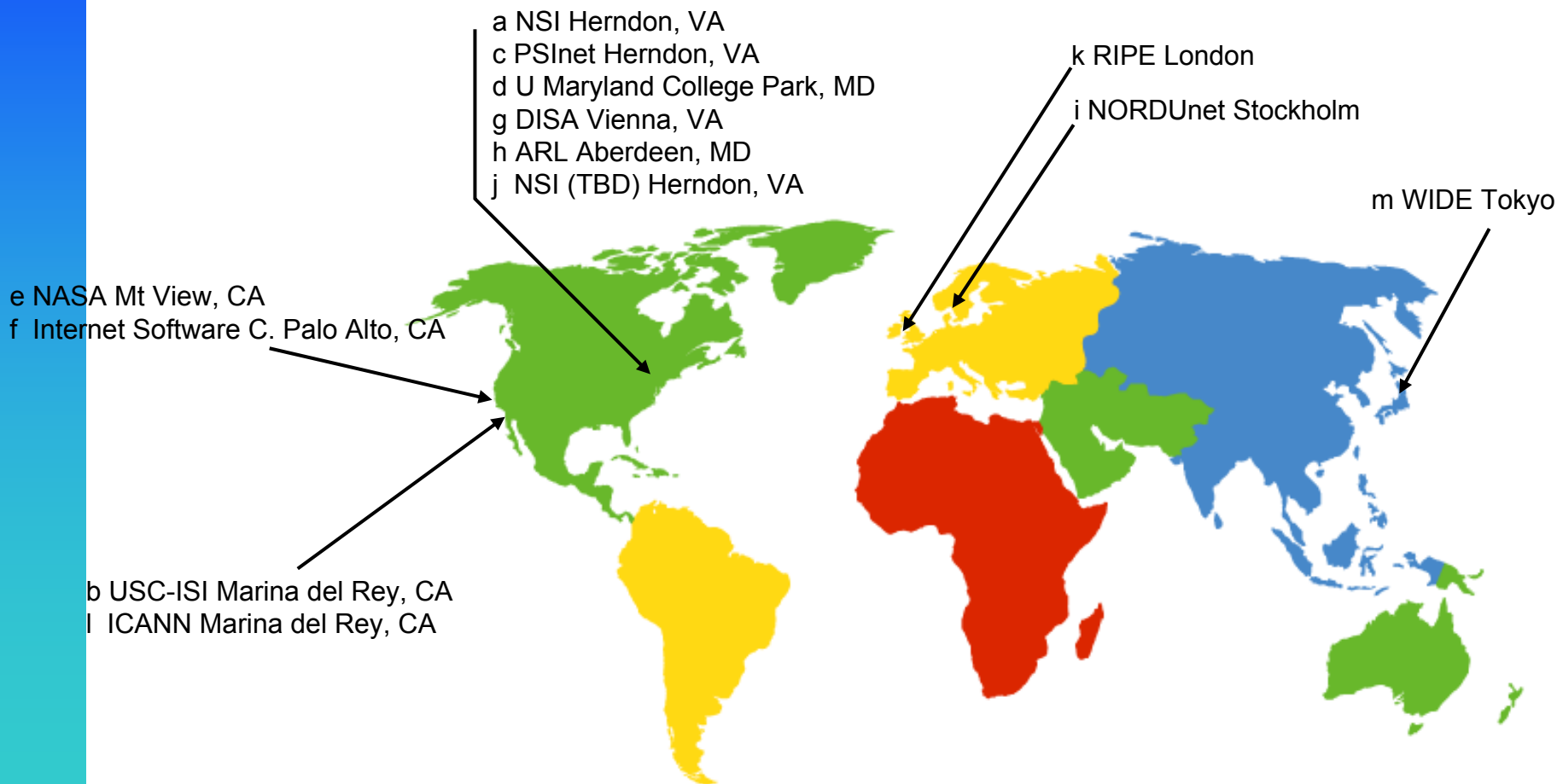


# Εξυπηρετητές κορυφής (Root name servers)

- Είναι υπεύθυνοι για τη ζώνη κορυφή «.»
- Σήμερα έχουμε 13 εξυπηρετητές κορυφής
  - {a-m}.root-servers.net
- Ερωτώνται από τους τοπικούς εξυπηρετητές ονομάτων όταν δεν μπορούν να αναλύσουν κάποιο όνομα
- Γιατί 13;
  - Συνδυασμός περιορισμών μεγέθους πακέτου IP και χαρακτηριστικών πρωτοκόλλου DNS επιτρέπει πακέτα UDP μεγέθους μέχρι 512 byte
  - Υπάρχει χώρος μόνο για 13 για εξυπηρετητές κορυφής



# 13 εξυπηρετητές κορυφής σε όλο τον κόσμο





# Διευθύνσεις των εξυπηρετητών κορυφής

A.ROOT-SERVERS.NET.	(NS.INTERNIC.NET)	198.41.0.4
B.ROOT-SERVERS.NET.	(NS1.ISI.EDU)	128.9.0.107
C.ROOT-SERVERS.NET.	(C.PSI.NET)	192.33.4.12
D.ROOT-SERVERS.NET.	(TERP.UMD.EDU)	128.8.10.90
E.ROOT-SERVERS.NET.	(NS.NASA.GOV)	192.203.23
F.ROOT-SERVERS.NET.	(NS.ISC.ORG)	192.5.5.241
G.ROOT-SERVERS.NET.	(NS.NIC.DDN.MIL)	192.112.36.4
H.ROOT-SERVERS.NET.	(AOS.ARL.ARMY.MIL)	128.63.2.53
I.ROOT-SERVERS.NET.	(NIC.NORDU.NET)	192.36.148.17
J.ROOT-SERVERS.NET.	(VeriSign)	198.41.0.10
K.ROOT-SERVERS.NET.	(RIPE NCC)	193.0.14.129
L.ROOT-SERVERS.NET.	(ICANN)	198.32.64
M.ROOT-SERVERS.NET.	(WIDE, Japan)	202.12.27.33

- Και πώς βρίσκουμε τις διευθύνσεις τους?
- Ρωτάμε τον εξυπηρετητή για το .net?
  - <http://www.internic.net/zones/named.root>

# Είναι πράγματι 13;



- Στο τέλος του 2010 ήταν 254 ([www.root-servers.org](http://www.root-servers.org))
- Χρήση anycast

# Εξυπηρετητές DNS ανώτατου επιπέδου (Top-level domain - TLD)



- Υπεύθυνοι για τις γενικές περιοχές com, org, net, edu, κλπ, και όλες τις περιοχές χωρών π.χ. uk, fr, ca, jp
- Υπάρχουν λίγοι εξυπηρετητές DNS ανώτατου επιπέδου ανά γενική περιοχή
  - Η Network Solutions διατηρεί στους εξυπηρετητές DNS για την περιοχή com
  - Η Educause διατηρεί στους εξυπηρετητές DNS για την περιοχή edu
  - Οι εξυπηρετητές κορυφής προωθούν τις ερωτήσεις προς αυτούς

# Εναλλακτικές κορυφές



- Πολλοί οργανισμοί λειτουργούν εναλλακτικές κορυφές DNS
  - Συνήθως αναφέρονται ως alt roots
- Αυτά τα εναλλακτικά συστήματα DNS λειτουργούν τους δικούς τους εξυπηρετητές κορυφής και διαχειρίζονται τους δικούς τους χώρους ονομάτων που αποτελούνται από ειδικές περιοχές ανωτάτου επιπέδου
  - Οι εναλλακτικές κορυφές εν γένει περιλαμβάνουν δείκτες προς όλους τους εξυπηρετητές περιοχών TLD που έχει εκχωρήσει η ICANN, καθώς και εξυπηρετητές για ειδικές περιοχές TLD που δεν έχουν εγκριθεί από την ICANN

# Εναλλακτικές κορυφές



- Κατά την περίοδο της έκρηξης dot-com boom, κάποιοι πάροχοι εναλλακτικών κορυφών πίστευαν ότι θα υπήρχε σημαντικό κέρδος από την παροχή εναλλακτικών TLD
  - Μόνο λίγοι από τους ISP στην πραγματικότητα χρησιμοποιούν εναλλακτικές κορυφές
  - Που οδήγησε στην εμπορική αποτυχία αρκετών εναλλακτικών παρόχων κορυφής
- Μερικές από τις λειτουργούσες εναλλακτικές κορυφές είναι
  - Public-Root, OpenNIC, UnifiedRoot, New.Net
- Πολλοί οργανισμοί διατηρούν εναλλακτικές κορυφές για το ιδιωτικό τους δίκτυο (διαθέσιμο μόνο εντός του οργανισμού)
  - Π.χ., η National Security Agency (NSA)





# Εξυπηρετητές ονομάτων





# Είδη εξυπηρετητών

- Κανένας εξυπηρετητής DNS δεν έχει όλες τις αντιστοιχίες ονομάτων σε διευθύνσεις IP
- Για να βρεθεί μία συγκεκριμένη αντιστοίχιση πιθανόν να πρέπει να γίνουν ερωτήσεις σε πολλούς εξυπηρετητές DNS
- Υπάρχουν πολλά είδη εξυπηρετητών ονομάτων
  - Επίσημοι (authoritative)
  - Κύριοι (primary), δευτερεύοντες (secondary)
  - Master, Slave
- Γίνεται και διάκριση ανάλογα με τη λειτουργία τους
  - Τοπικοί (local)
  - Προσωρινής αποθήκευσης (cache)
  - Αναδρομής (recursive)
  - Χωρίς να αποκλείεται η μείξη ρόλων και λειτουργιών

# Επίσημοι εξυπηρετητές ονομάτων



- Για μια περιοχή, ο επίσημος εξυπηρετητής (authoritative server) δίνει τις αυθεντικές απαντήσεις
  - περιέχει τις αυθεντικές εγγραφές για τους υπολογιστές μιας περιοχής, σε αντιδιαστολή με πληροφορία που έμαθε ρωτώντας άλλους
  - τον συντηρεί συνήθως ο οργανισμός που κατέχει το όνομα της περιοχής ή ο πάροχος δικτύου
  - ξέρει την απάντηση για τους υπολογιστές της περιοχής του
- Όταν εγγράφονται ονόματα περιοχών σε περιοχές ανωτάτου επιπέδου απαιτείται ο προσδιορισμός του κύριου και του δευτερεύοντα εξυπηρετητή ονομάτων
  - Για λόγους αξιοπιστίας απαιτούνται πολλαπλοί εξυπηρετητές, ώστε η περιοχή να λειτουργεί ακόμη και σε περίπτωση βλάβης ενός εξ αυτών
- Ο επίσημος εξυπηρετητής ονομάτων μπορεί να είναι ο κύριος ή ο δευτερεύων εξυπηρετητής

# Κύριοι και δευτερεύοντες εξυπηρετητές ονομάτων



- Για κάθε ζώνη πρέπει να υπάρχει ένας κύριος εξυπηρετητής και ένας αριθμός από δευτερεύοντες εξυπηρετητές
  - Ο κύριος εξυπηρετητής (*primary server*) διατηρεί ένα αρχείο ζώνης με την πρωτότυπη πληροφορία για τη ζώνη
  - Ο δευτερεύων εξυπηρετητής (*secondary server*) διατηρεί αντίγραφα των δεδομένων που αποθηκεύονται στον κύριο εξυπηρετητή
- Ο χαρακτηρισμός κύριος και δευτερεύων εξαρτάται μόνο από την προτεραιότητα που τους δίνεται κατά την εγγραφή τους στην ανώτερη περιοχή

# Master και slave εξυπηρετητές ονομάτων



- Οι κύριοι εξυπηρετητές ονομάτων συνήθως λειτουργούν ως master
- Οι δευτερεύοντες συνήθως υλοποιούνται ως slave

**ntua.gr DNS server**



**ntua.gr  
DNS DB**

**Επίσημη**



**ntua.gr  
DNS DB**

**Αντίγραφα**

# Ενημέρωση της βάσης δεδομένων DNS



- Η βάση μπορεί να ενημερωθεί δυναμικά
  - Προσθήκη, διαγραφή, τροποποίηση οποιασδήποτε πληροφορίας
- Π.χ. προσθήκη host
  - Όταν προστίθεται ένας host (π.χ. "edu-dy.cn.ntua.gr") σε μια ζώνη, ο διαχειριστής προσθέτει την πληροφορία για τον host (διεύθυνση IP και όνομα) σε ένα αρχείο του κύριου εξυπηρετητή

# Ενημέρωση της βάσης δεδομένων DNS



- Οι ενημερώσεις της πληροφορίας γίνονται στον κύριο εξυπηρετητή
  - Μόνο ο κύριος εξυπηρετητής ενημερώνεται δυναμικά
  - Μοναδικό σημείο αστοχίας
  - Οι οποιεσδήποτε αλλαγές προωθούνται στους δευτερεύοντες εξυπηρετητές
- Η βάση παραμένει πάντα εσωτερικά συνεπής
  - Κάθε εκδοχή του αρχείου ζώνης έχει ένα σειριακό αριθμό που αυξάνει με κάθε αλλαγή

# Ενημέρωση της βάσης δεδομένων DNS



- Οι τροποποιήσεις στον κύριο εξυπηρετητή σκανδαλίζουν τη διαδικασία αντιγραφής
  - Οι αλλαγές στον κύριο εξυπηρετητή αντιγράφονται στους δευτερεύοντες σύμφωνα με τον χρονισμό που επιβάλλει ο διαχειριστής

# Τοπικός εξυπηρετητής



- Κάθε οργανισμός, εταιρεία, πανεπιστήμιο, πάροχος έχει έναν
  - Είναι γνωστός και ως ο επιλεγμένος (default) εξυπηρετητής
- Όταν ο γίνει μια ερώτηση, αυτή αποστέλλεται στον τοπικό εξυπηρετητή
  - λειτουργεί ως ενδιάμεσος και προωθεί την ερώτηση εάν απαιτείται
- Αν ο τοπικός εξυπηρετητής ονομάτων δεν έχει καταλήξει στο πού θα βρει τη διεύθυνση που αντιστοιχεί στο όνομα κάποιου υπολογιστή, ρωτά τους εξυπηρετητές κορυφής
  - Μια ερώτηση μπορεί να προωθηθεί αρκετές φορές
  - Τα αποτελέσματα φυλάσσονται προσωρινά για μελλοντική χρήση



# Εξυπηρετητές προσωρινής αποθήκευσης



- Επί της αρχής, οι επίσημοι εξυπηρετητές αρκούν για τη λειτουργία του διαδικτύου
- Όμως μόνο με τους επίσημους εξυπηρετητές απαιτείται η αναδρομική λειτουργία (θα περιγραφτεί στη συνέχεια) στην πλευρά των πελατών
- Οι εξυπηρετητές ονομάτων προσωρινής αποθήκευσης (caching servers) αποθηκεύουν απαντήσεις από άλλους εξυπηρετητές
  - Τα δεδομένα αυτά εκπνέουν σύμφωνα με χρονόμετρα που θέτει ο διαχειριστής
- Με την προσωρινή αποθήκευση
  - Βελτιώνεται η επίδοση
  - Μειώνεται η κίνηση στο διαδίκτυο
  - Αυξάνει η επίδοση των εφαρμογών χρηστών



# Πρωτόκολλο DNS



# Πρωτόκολλο DNS

- Το πρωτόκολλο DNS είναι του τύπου πελάτη - εξυπηρετητή
- Ο πελάτης DNS ονομάζεται **αναλυτής (resolver)**
- Το πρωτόκολλο DNS υποστηρίζει τη μετατροπή ονομάτων σε διευθύνσεις (**ανάλυση, resolution**)
  - καθώς και την ενημέρωση των δεδομένων μεταξύ εξυπηρετητών ονομάτων

# Ανάλυση ονομάτων (name resolution)



- Είναι η διαδικασία με την οποία αναλυτές και εξυπηρετητές ονομάτων συνεργάζονται ώστε να βρουν δεδομένα εντός του χώρου ονομάτων
  - Για την ανεύρεση δεδομένων, ο εξυπηρετητής ονομάτων χρειάζεται μόνο το όνομα και τη διεύθυνση IP των εξυπηρετητών ονομάτων κορυφής
  - Οι εξυπηρετητές κορυφής ξέρουν για όλους τις περιοχές ανωτάτου επιπέδου και μπορούν να υποδείξουν τους εξυπηρετητές με τους οποίους μπορεί να γίνει επαφή



# Μετατροπή ονομάτων σε διευθύνσεις

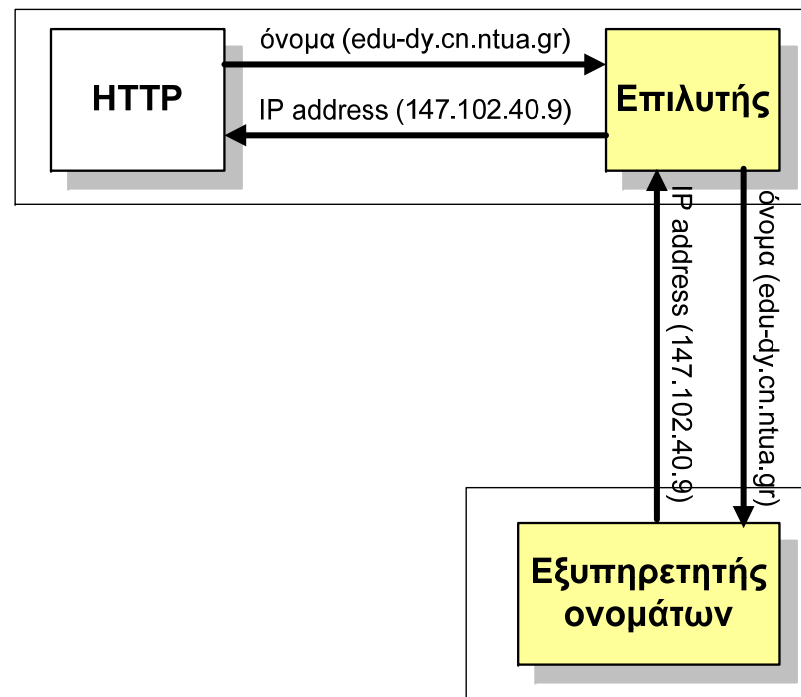
Σε συντομία η λειτουργία ανάλυσης είναι:

- το πρόγραμμα εφαρμογής καλεί μια συνάρτηση βιβλιοθήκης, τον **αναλυτή (resolver)**, στην οποία περνά το όνομα ως παράμετρο
- ο αναλυτής στέλνει την ερώτηση στον τοπικό εξυπηρετητή ονομάτων
- ο εξυπηρετητής ονομάτων επιστρέφει τη διεύθυνση IP στον αναλυτή, ο οποίος την επιστρέφει με τη σειρά του στον καλούντα
- διαθέτοντας τη διεύθυνση IP, το πρόγραμμα μπορεί στη συνέχεια να εγκαταστήσει μια σύνδεση TCP ή να στείλει πακέτα UDP



# Παράδειγμα ανάλυσης ονόματος

1. Το πρόγραμμα του χρήστη (πλοηγός ιστού) ζητά τη διεύθυνση IP ενός υπολογιστή
2. Ο τοπικός αναλυτής σχηματίζει μια **ερώτηση (DNS query)** προς τον εξυπηρετητή ονομάτων
3. Ο εξυπηρετητής ονομάτων ελέγχει το κατά πόσο γνωρίζει την απάντηση
  - a) εάν ναι, απαντά
  - b) αλλιώς, ερωτά άλλους
4. Όταν έχει την απάντηση, τη στέλνει στον αναλυτή



# Επικοινωνία μεταξύ εξυπηρετητών



- Αν ζητηθεί από έναν εξυπηρετητή DNS να δώσει την αντιστοίχιση για έναν host εκτός της περιοχής του (και η αντιστοίχιση δεν υπάρχει στην προσωρινή μνήμη):
  - Ο εξυπηρετητής βρίσκει έναν εξυπηρετητή ονομάτων της άλλης περιοχής
  - Ο εξυπηρετητής ζητά από τον εξυπηρετητή ονομάτων της άλλης περιοχής να του δώσει την αντιστοίχιση του ονόματος του host με μια διεύθυνση IP
  - Οι απαντήσεις λαμβάνονται από τους επίσημους εξυπηρετητές, αλλά προωθούνται στους πελάτες ως μη επίσημες
  - Οι απαντήσεις φυλάσσονται προσωρινά για μελλοντική χρήση

# Προσωρινή αποθήκευση



- Εάν υπάρχει εγγραφή στην προσωρινή μνήμη ικανή για να απαντηθεί μια ερώτηση, ο εξυπηρετητής δεν επικοινωνεί με άλλους εξυπηρετητές
  - Οι εγγραφές αυτές μετά από κάποιο διάστημα διαγράφονται
  - Η πληροφορία για τους εξυπηρετητές DNS ανώτατου επιπέδου εν γένει βρίσκεται στην προσωρινή μνήμη του τοπικού εξυπηρετητή DNS
    - δεν χρειάζεται ερώτηση στους εξυπηρετητές κορυφής
- Εάν δοθεί απάντηση από τα στοιχεία της προσωρινής μνήμης, η απάντηση σημαδεύεται ως **μη επίσημη** (unauthoritative)



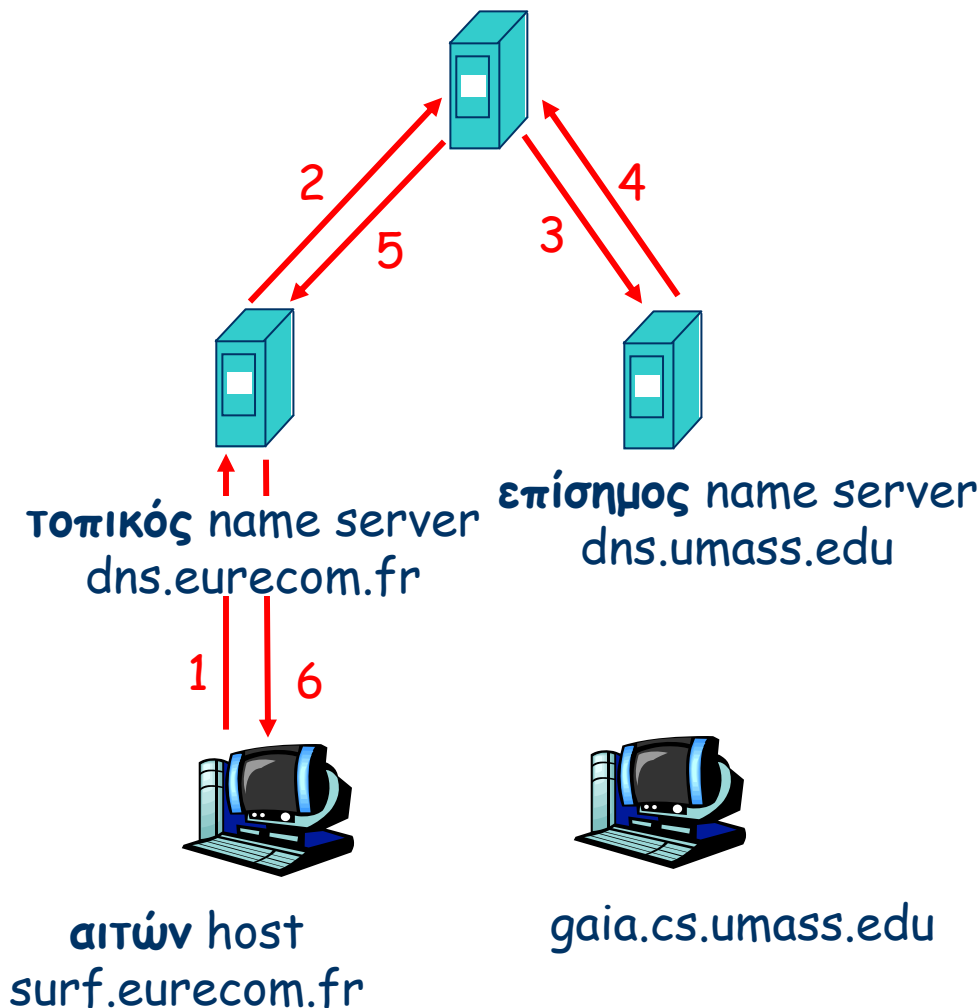


# Παράδειγμα ερώτησης DNS

εξυπηρετητής  
κορυφής

ο surf.eurecom.fr  
θέλει τη διεύθυνση IP  
του gaia.cs.umass.edu

1. επικοινωνεί με τον τοπικό εξυπηρετητή DNS (dns.eurecom.fr)
2. ο dns.eurecom.fr επικοινωνεί με τον εξυπηρετητή κορυφής, αν χρειάζεται
3. ο εξυπηρετητής κορυφής επικοινωνεί με τον επίσημο εξυπηρετητή (dns.umass.edu) αν είναι αναγκαίο



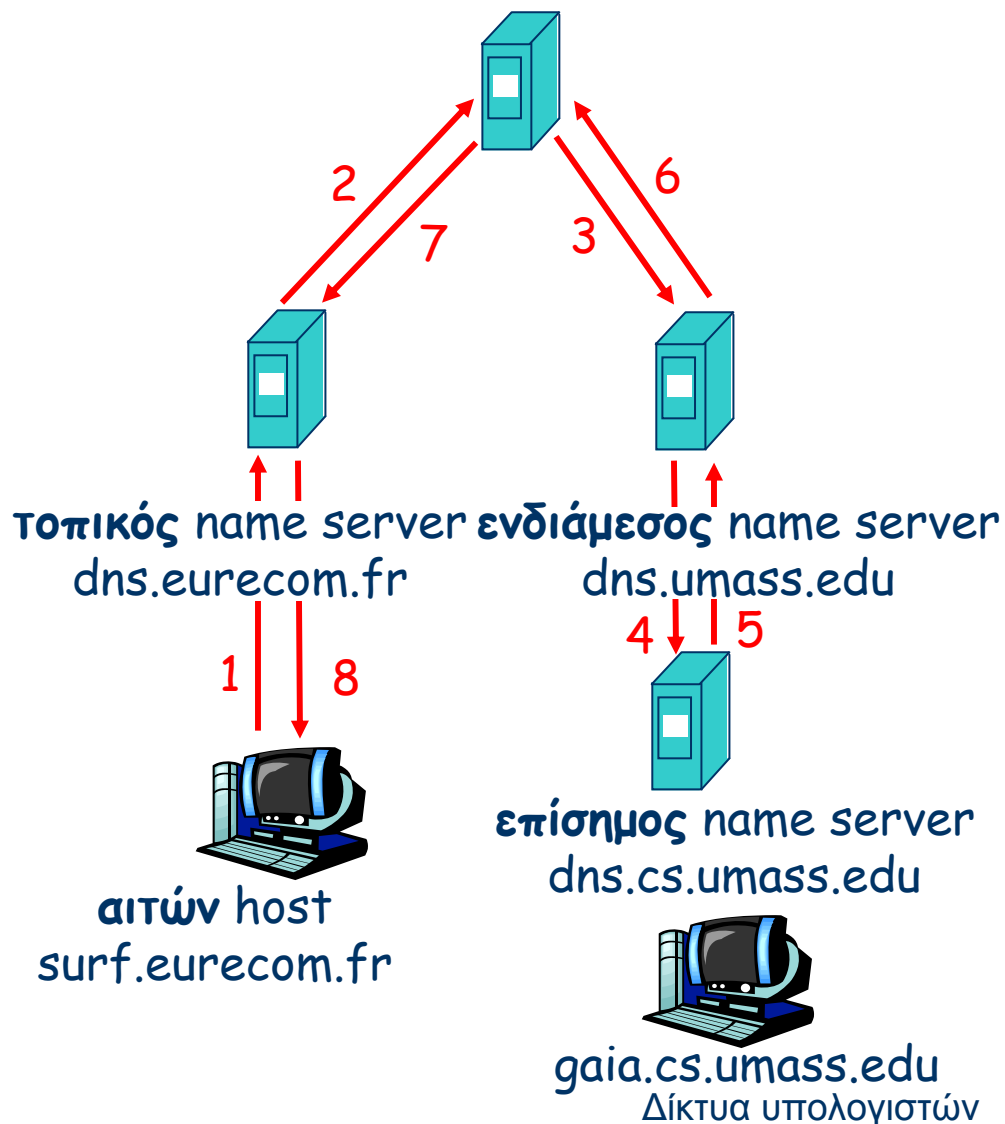


# Άλλο παράδειγμα ερώτησης

εξυπηρετητής  
κορυφής

Ο εξυπηρετητής  
κορυφής:

- μπορεί να μην γνωρίζει επίσημο name server για την περιοχή cs.umass.edu
- Γνωρίζει τον ενδιάμεσο εξυπηρετητή ονομάτων για την περιοχή umass.edu με το οποίο θα έρθει σε επαφή για να βρει επίσημο εξυπηρετητή



# Αναδρομή



- Στα προηγούμενα παραδείγματα για την αναζήτηση της διεύθυνσης IP του `gaia.cs.umass.edu` χρησιμοποιείται αναδρομή (recursion)
  - Η αίτηση του `surf.eurecom.fr` μπορεί δείχνει ότι είναι επιθυμητή μια αναδρομή
  - τούτο υποδεικνύει στον τοπικό εξυπηρετητή ονομάτων να βρει την απάντηση (πιθανώς επικοινωνώντας με άλλους εξυπηρετητές).
- Αν δεν αιτείται αναδρομή - η απάντηση μπορεί να είναι μια λίστα από άλλους εξυπηρετητές για επικοινωνία



# Αναδρομική ή επαναληπτική αναζήτηση:

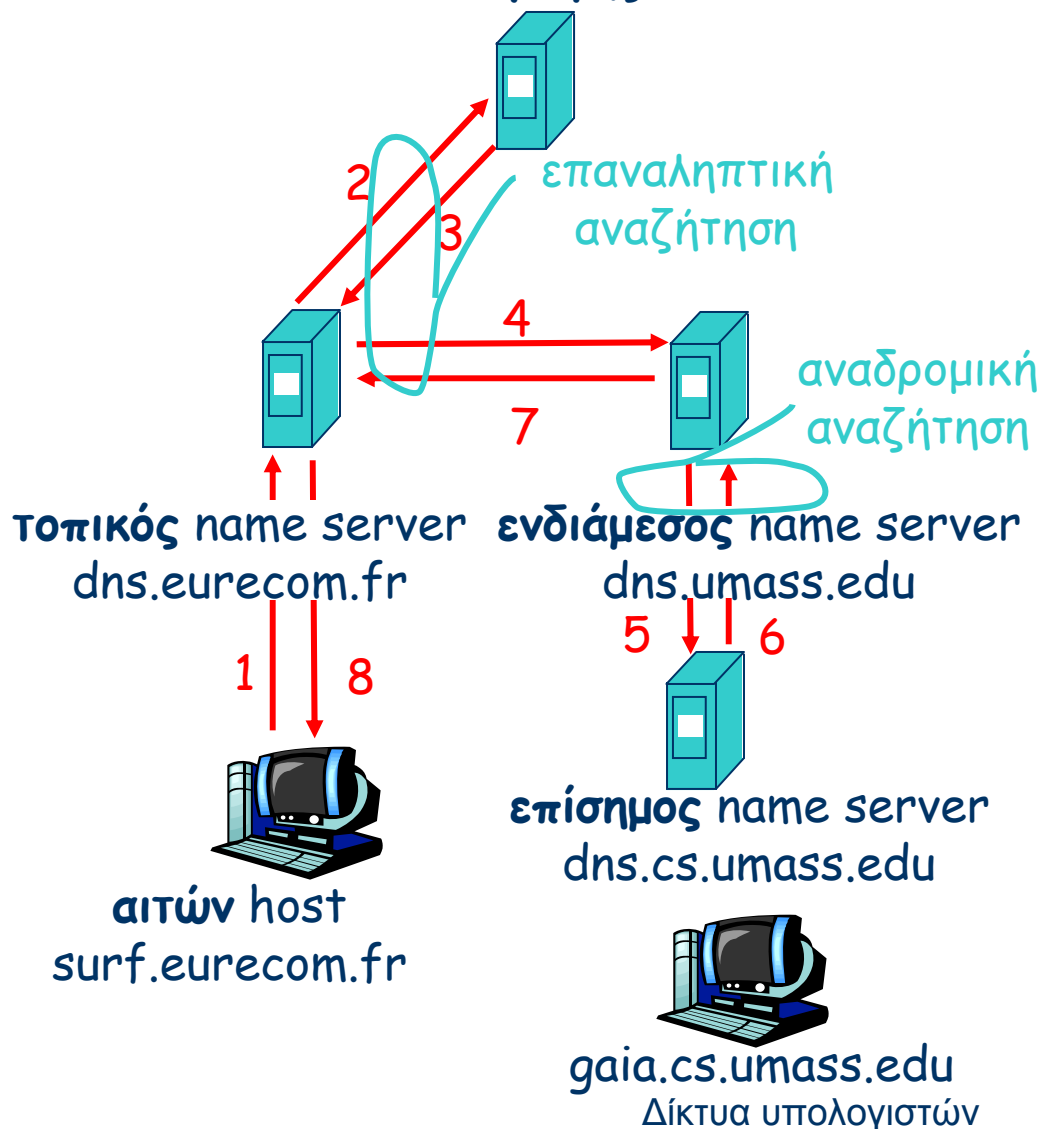
εξυπηρετητής  
κορυφής

## Αναδρομική αναζήτηση:

- επιβαρύνει τον καλούμενο name server για την ανάλυση του ονόματος
- υψηλό φορτίο

## Επαναληπτική αναζήτηση:

- ο καλούμενος name server απαντά με το όνομα του επόμενου
- επιβαρύνει τον αναλυτή



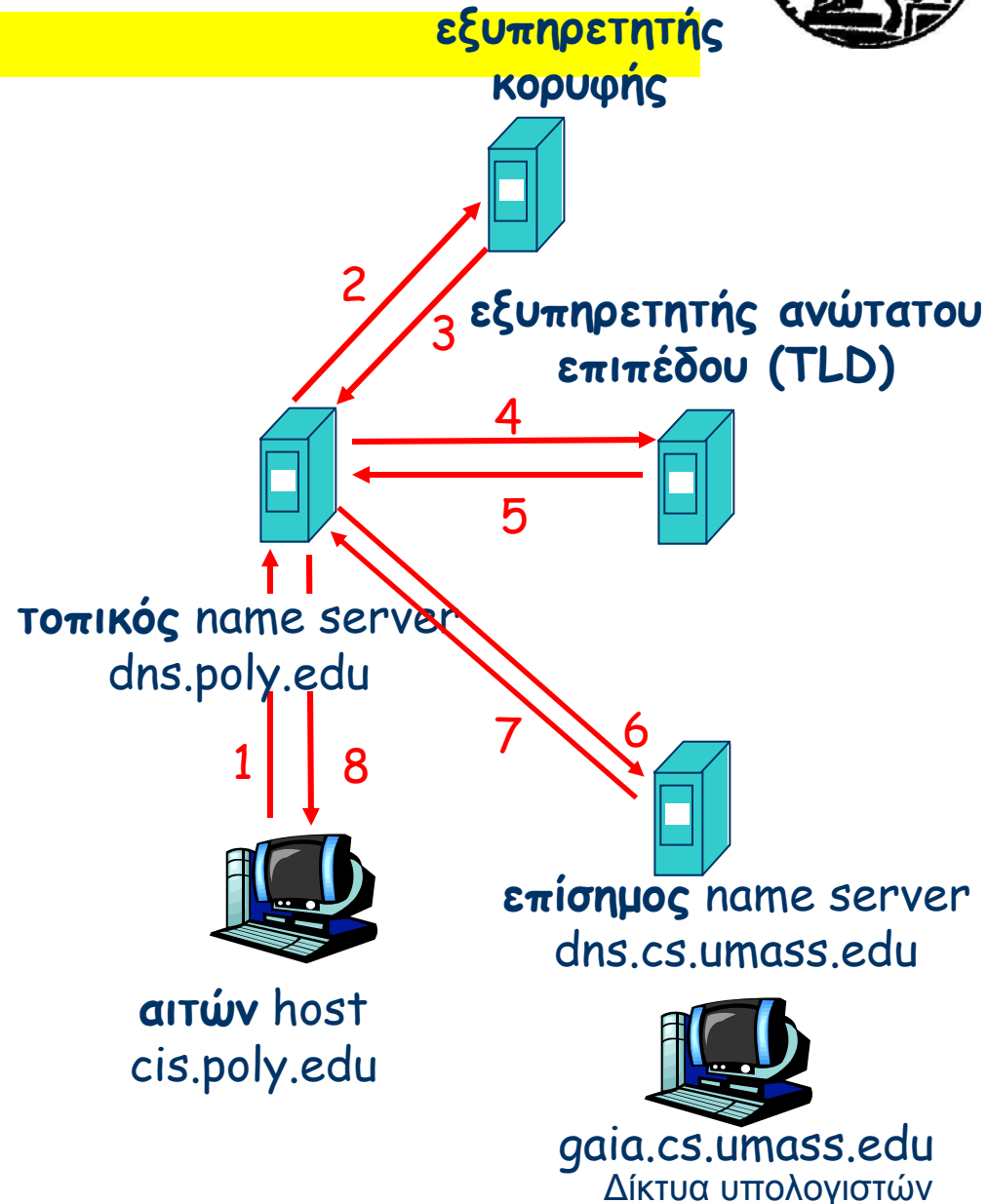


# Παράδειγμα με επαναληπτική αναζήτηση

- Υπολογιστής της περιοχής cis.poly.edu θέλει την διεύθυνση IP του υπολογιστή gaia.cs.umass.edu

## Επαναληπτική αναζήτηση:

- ο καλούμενος server απαντά με το όνομα του εξυπηρετητή ονομάτων για την επόμενη επικοινωνία
- "Δεν ξέρω αυτό το όνομα, αλλά ρώτα αυτόν τον εξυπηρετητή"





# Ανάστροφη αναζήτηση (reverse lookup)

# Διευθύνσεις IP των host



- Η δομή του δένδρου DNS είναι προσαρμοσμένη στην αναζήτηση διευθύνσεων IP δοθέντος του ονόματος ενός host
- Εάν κανείς ήθελε να βρει το όνομα του host γνωρίζοντας τη διεύθυνση IP θα πρέπει να ψάξει όλο το δένδρο
  - ανέφικτο για το σημερινό μέγεθος του διαδικτύου
- Για το σκοπό αυτό υπάρχουν οι περιοχές
  - in-addr.arpa. για IPv4
  - ip6.arpa. για IPv6
- Η διεύθυνση 147.102.40.9 μετατρέπεται στο όνομα 9.40.102.147.in-addr.arpa
  - με τη μέθοδο αυτή η αναζήτηση για μια διεύθυνση IP μετατρέπεται σε αναζήτηση για όνομα

# Η περιοχή ανωτάτου επιπέδου arpa.



- Το όνομα προέρχεται από το Advanced Research Projects Agency
  - Ο οργανισμός που χρηματοδότησε την ανάπτυξη του ARPANET, που υπήρξε ο πρόδρομος για το Internet
- Αρχικά προορίζονταν ως μεταβατική περιοχή για τους τότε κόμβους του ARPANET
  - γρήγορα όμως αυτοί μετέβησαν στο νέο τρόπο ονοματοδοσίας γενικών περιοχών .edu, .mil, .gov, κλπ ...  
... και λογικά έπρεπε να καταργηθεί αφού επιτέλεσε το έργο της
- Όμως αυτό δεν υπήρξε πρακτικό για τον κλάδο in-addr.arpa. που είχε τις αντίστροφες εγγραφές
  - Η αρχική ιδέα ήταν να αναλάβει αυτό τον ρόλο η περιοχή int.
  - Το 2000 η ιδέα εγκαταλείφτηκε και το int. παρέμεινε για διεθνείς οργανισμούς μόνο



# Περιοχές δευτέρου επιπέδου κάτω από την arpa.



- Σήμερα, η περιοχή arpa. διατηρεί τις ακόλουθες περιοχές δευτέρου επιπέδου
  - in-addr.arpa - για αντίστροφη αναζήτηση βάσει διευθύνσεων IPv4
  - ip6.arpa - για αντίστροφη αναζήτηση βάσει διευθύνσεων IPv6
  - e164.arpa - για τηλεφωνικούς αριθμούς στο DNS (ENUM)
  - iris.arpa - για το Cross Registry Information Service Protocol (CRISP), διάδοχο του WHOIS
  - uri.arpa - για δυναμική ανακάλυψη Uniform Resource Identifier (URI)
  - urn.arpa - για δυναμική ανακάλυψη Uniform Resource Name (URN)

# Αντιστοίχιση τηλεφωνικών αριθμών



- Οι τηλεφωνικοί αριθμοί οργανώνονται σύμφωνα με το πρότυπο E.164 (κωδικός χώρας, κωδικός περιοχής, αριθμός συνδρομητή)
- Το διαδίκτυο χρησιμοποιεί το DNS για την αντιστοίχιση ονομάτων σε διευθύνσεις IP και άλλες πληροφορίες
- Το πρόβλημα: Πώς να αναμείξουμε αυτούς τους δύο διαφορετικούς κόσμους;
- ENUM (ή Enum) από το E.164 NUmber Mapping είναι η βασική μέθοδος

# ENUM



- Το ENUM αντιστοιχεί τηλεφωνικούς αριθμούς E.164 σε URI ή διευθύνσεις IP που μπορούν να χρησιμοποιηθούν στο διαδίκτυο
  - αναγκαίο για την υποστήριξη VoIP
- Ακολουθεί μια οργάνωση τριών διαζωμάτων
  - Tier-0: το e164.arpa και οι εξυπηρετητές ονομάτων του
  - Tier-1: οι υπεύθυνοι εξυπηρετητές για μια "χώρα" : π.χ. 0.3.e164.arpa
    - Οι διεθνείς κωδικοί δεν είναι μόνο χώρες: δορυφορικοί πάροχοι, αριθμοί free phone, κλπ
  - Tier-2: οι υπεύθυνοι για τις εγγραφές
    - Δεν ανταποκρίνονται στους κωδικούς περιοχής (area code) όπως ίσως περίμενε κανείς



- Παράδειγμα για τον E.164 αριθμό τηλεφώνου +30 210 772 2534
  - Αφαιρούμε το "+" και τα κενά και ότι δεν είναι ψηφίο
  - Μετατρέπουμε στο FQDN  
4.3.5.2.2.7.7.0.1.2.0.3.e164.arpa.
  - Η αναζήτηση στο DNS επιστρέφει τα URI
    - sip:ceie@ntua.gr
    - mailto:stathis@mail.ntua.gr
    - sms tel:+302107722534

# Τι θέλουμε τους τηλεφωνικούς αριθμούς στο διαδίκτυο;



- Ο κόσμος ξέρει πώς να τους χρησιμοποιεί
- Τρισεκατομμύρια συσκευές έχουν μόνο αριθμητικά πληκτρολόγια
- Οι περισσότεροι πελάτες VoIP χρησιμοποιούν τους συνήθεις τηλεφωνικούς αριθμούς ή έχουν τηλέφωνα IP με πληκτρολόγια
  - URI όπως sip:user@domain δεν μπορούν να επιλεγθούν από το δημόσιο τηλεφωνικό δίκτυο
  - URI και τηλεφωνικοί αριθμοί θα συνυπάρχουν

# Γιατί DNS και όχι κάποια άλλη υπηρεσία;



- Οποιοσδήποτε μπορεί να το χρησιμοποιήσει το DNS
  - Υπάρχει
  - Δουλεύει
  - Είναι παγκόσμιο
  - Επεκτάσιμο
  - Ανοικτό
- Το ENUM μπορεί να δώσει οποιοδήποτε URI → οποιαδήποτε υπηρεσία
  - mailto, fax, video, ...
  - sms, mms, ...
  - h323, pres, im, ...
  - http, ftp, certificates, locations, ...

# Άλλες εφαρμογές



- Ονόματα host και διευθύνσεις IP δεν είναι υποχρεωτικό να αντιστοιχούν ένα προς ένα
  - Πολλά ονόματα host μπορεί να αντιστοιχούν σε μία διεύθυνση IP
    - virtual hosting: επιτρέπεται σε μία μηχανή να εξυπηρετεί πολλές ιστοθεσίες
  - Αντίστροφα, ένα όνομα host μπορεί να αντιστοιχεί σε πολλές διευθύνσεις IP
    - μεταφορά χωρίς διακοπή ιστοθέσης σε άλλη φυσική τοποθεσία
- Ανοχή σε βλάβες και κατανομή φορτίου (για εξυπηρετητές ιστού και εξυπηρετητές ηλεκτρονικού ταχυδρομείου)
  - Επιστρέφονται διαφορετικές διευθύνσεις ως απάντηση
    - δίδεται η σειρά προτεραιότητας

# Άλλες εφαρμογές



- Μαύρες λίστες για ηλεκτρονικό ταχυδρομείο (anti-spam)
  - Ο εξυπηρετητής μπορεί μέσω των μηχανισμών του DNS να ερωτήσει π.χ. την `blacklist.com` (όπως στην ανάστροφη αναζήτηση) το κατά πόσο μια συγκεκριμένη διεύθυνση IP είναι στη μαύρη λίστα
- Ενημέρωση λογισμικού
  - Πολλά εμπορικά λογισμικά (π.χ. για ιούς) χρησιμοποιούν το DNS για να εγγράψουν τις τελευταίες εκδόσεις του λογισμικού έτσι ώστε να μη χρειάζεται συνεχώς η σύνδεση με τους εξυπηρετητές αρχείων
- Δυναμικό DNS (Dynamic DNS ή DDNS)
  - Επιτρέπει στους πελάτες να ενημερώνουν για την τρέχουσα IP διεύθυνσή τους
  - Ιδιαίτερα χρήσιμο για κινητές συσκευές ή συνδέσεις ADSL όπου οι πάροχοι δε δίνουν στατικές διευθύνσεις IP





# Η βάση δεδομένων DNS

# Εγγραφές στη βάση δεδομένων DNS



- Οι εγγραφές στην κατανεμημένη βάση δεδομένων του DNS αποκαλούνται εγγραφές πόρων (**RR - resource records**)
- Οι εγγραφές πόρων αποθηκεύονται σε αρχεία (αρχεία ζώνης) στους εξυπηρετητές ονομάτων
- Οι εγγραφές πόρων αποτελούνται από τα ακόλουθα στοιχεία
  - Όνομα (Name): FQDN του κόμβου του δένδρου DNS στο οποίο αναφέρεται η εγγραφή
  - Τύπος (Type): το είδος της εγγραφής
  - Κατηγορία (Class): Για το διαδίκτυο είναι IN
  - Χρόνος ζωής (TTL)
  - RDATA: δεδομένα ανάλογα με τον τύπο

# Τύποι εγγραφών πόρων (RR)



- A: Address
- CNAME: Canonical Name
- MX: Mail Exchange
- PTR: Pointer
- NS: Name Server
- SOA: Start of Authority

# Εγγραφές πόρων



Τύπος RR: (name, type, class, ttl, rdata)

- Type = A
  - name είναι το όνομα του host
  - rdata είναι η διεύθυνση IP
- Type = NS
  - name είναι η περιοχή (πχ. foo.com)
  - rdata είναι η διεύθυνση IP του επίσημου name server για την περιοχή
- Type = CNAME
  - name είναι ψευδώνυμο για κάποιο "επίσημο" όνομα  
www.ibm.com
  - rdata είναι το επίσημο (canonical) όνομα  
www.ibm.com.cs186.net
- Type = MX
  - rdata είναι το όνομα του mail-server που σχετίζεται με το name

# Η εγγραφή πόρων SOA



- Καθορίζει την επίσημη πληροφορία για μια ζώνη DNS
  - Τον κύριο εξυπηρετητή ονομάτων
  - Τη διεύθυνση email του διαχειριστή της περιοχής
  - Τον α/α της περιοχής
  - Και πολλά χρονόμετρα (timers) σχετιζόμενα με την ανανέωση της πληροφορίας ζώνης

# Η εγγραφή πόρων NS



- Μέσω αυτής γίνεται η εκχώρηση
  - Για την περιοχή που εκχωρούμε, προσθέτουμε στον κύριο εξυπηρετητή εγγραφές NS

```
sub.goe.net. NS ns1.sub.goe.net.
sub.goe.net. NS ns2.sub.goe.net.
```
  - Για να βρούμε τους εξυπηρετητές ns1 και ns2 χρειαζόμαστε τις διευθύνσεις τους

```
ns1.sub.goe.net. A 10.0.0.1
ns2.sub.goe.net. A 10.0.0.2
```
- Είναι η εγγραφή αυτή αυθεντική (authoritative)?



# Παράδειγμα αρχείου ζώνης

db.mylab.com

```
$TTL 86400
mylab.com. IN SOA PC4.mylab.com.
master.mylab.com.
(1 ; serial
28800 ; refresh
7200 ; retry
604800 ; expire
86400 ; neg. ans. ttl
)
```

Μέγιστη ηλικία  
δεδομένων σε sec

\* Αυτός είναι ο επίσημος  
εξυπηρετητής για την περιοχή  
Mylab.com  
\* PC4.mylab.com είναι ο  
εξυπηρετητής ονομάτων  
\* master@mylab.com είναι το  
email του διαχειριστή

```
;
mylab.com. IN NS PC4.mylab.com.
;
localhost A 127.0.0.1
PC4.mylab.com. A 10.0.1.41
PC3.mylab.com. A 10.0.1.31
PC2.mylab.com. A 10.0.1.21
PC1.mylab.com. A 10.0.1.11
```

Μια εγγραφή για κάθε  
εξυπηρετητή

Μια εγγραφή για κάθε IP  
διεύθυνση host



## Ερωτήσεις DNS



# Αναδρομικές και επαναληπτικές ερωτήσεις

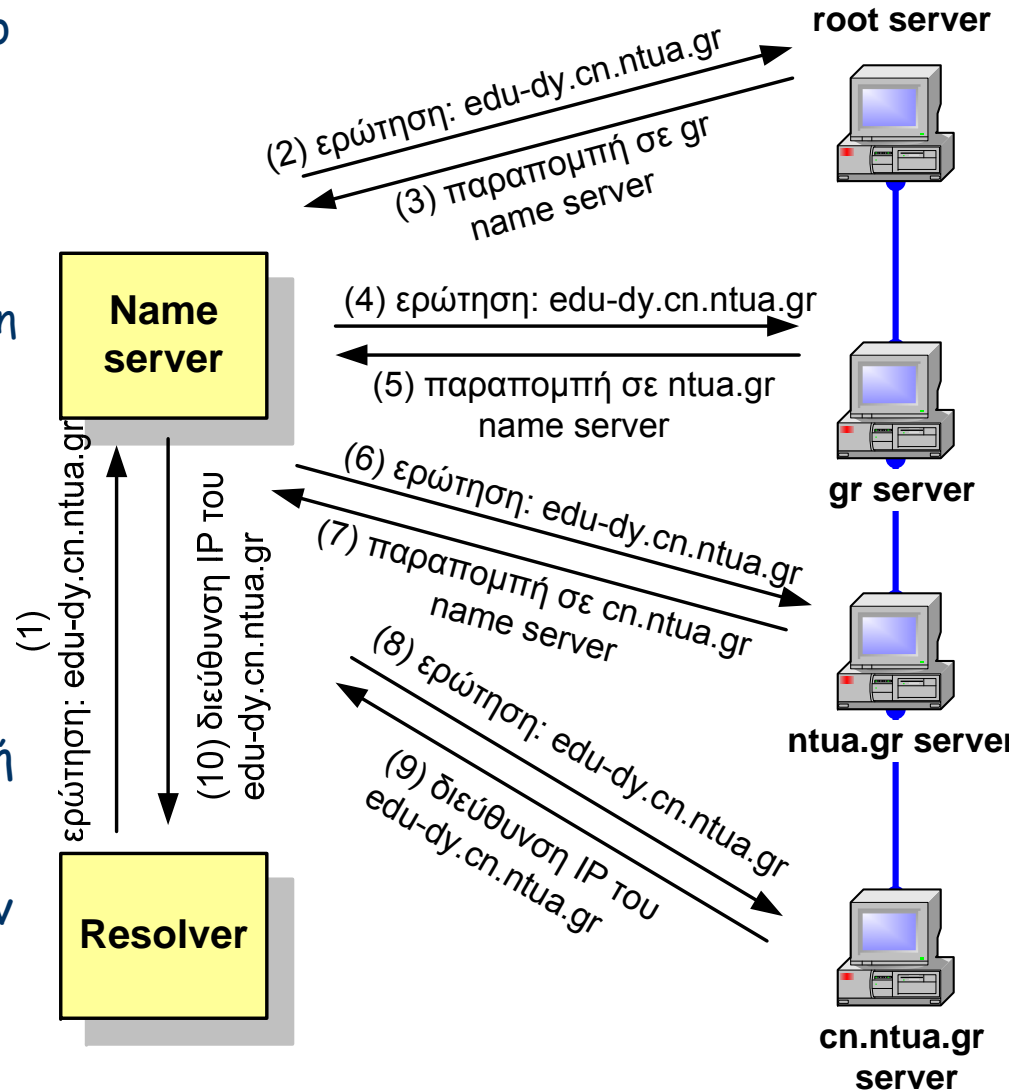


- Υπάρχουν δύο είδη ερωτήσεων DNS:
  - Αναδρομικές ερωτήσεις
  - Επαναληπτικές (μη αναδρομικές) ερωτήσεις
  - Ο τύπος της ερώτησης καθορίζεται από ένα bit στην επικεφαλίδα της ερώτησης DNS
- **Αναδρομική ερώτηση (Recursive query):**
  - Εδώ, ο εξυπηρετητής ονομάτων πρέπει να δώσει την απάντηση στην ερώτηση (ή να στείλει μήνυμα λάθους)
  - Εάν ο εξυπηρετητής ονομάτων δε γνωρίζει την απάντηση, θα ξεκινήσει μια ερώτηση σε άλλο εξυπηρετητή για να τη μάθει
- **Επαναληπτική ερώτηση (Iterative query):**
  - Εδώ, ο εξυπηρετητής ονομάτων επιστρέφει την καλύτερη δυνατή του απάντηση: (1) την ακριβή απάντηση ή (2) την παραπομπή σε άλλο εξυπηρετητή
  - Όταν ο εξυπηρετητής ονομάτων δεν έχει την ακριβή απάντηση, απαντά στον αναλυτή με παραπομπή, δηλαδή, με το όνομα ενός άλλου εξυπηρετητή ονομάτων
- Σημείωση: Οι εξυπηρετητές ρίζας και οι εξυπηρετητές ανωτάτων περιοχών (TLD) είναι ρυθμισμένοι να χειρίζονται μόνο επαναληπτικές ερωτήσεις

# Αναδρομικές ερωτήσεις



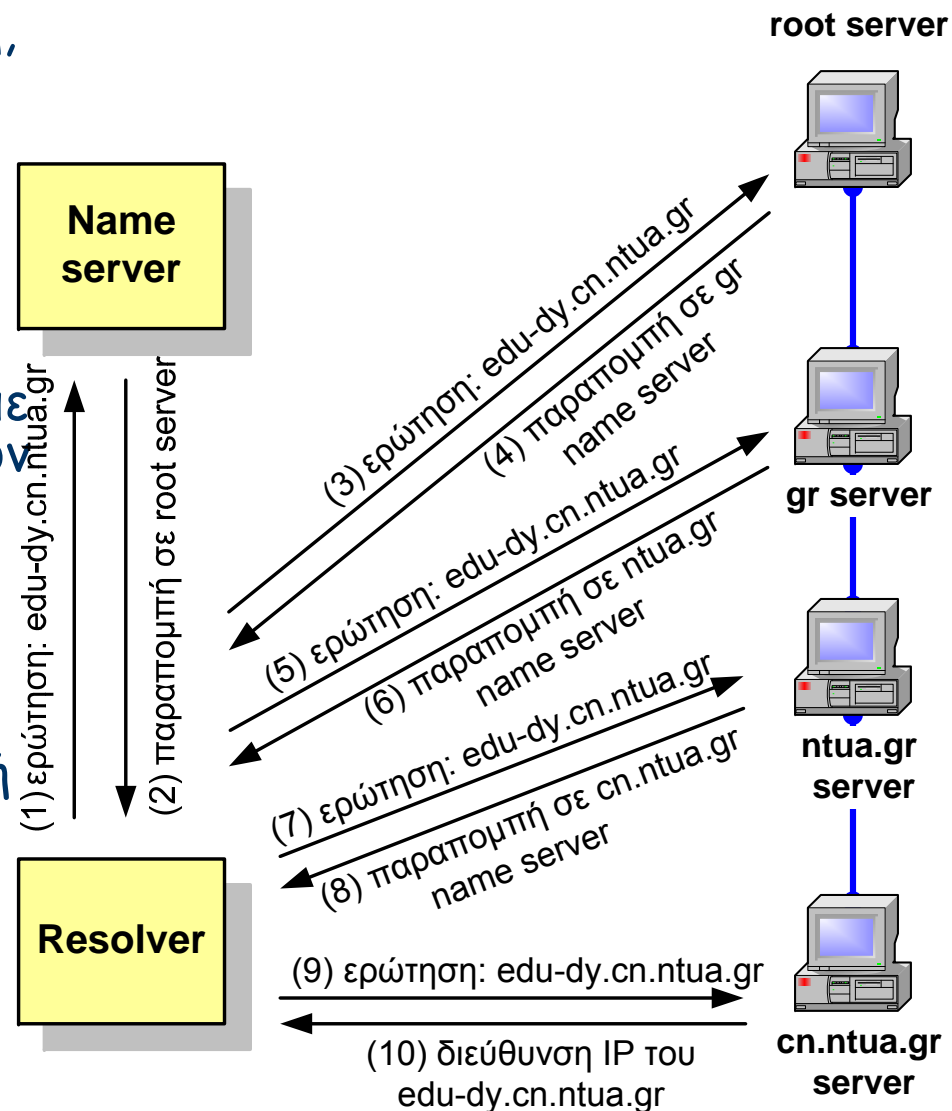
- Στις αναδρομικές ερωτήσεις ο αναλυτής αναμένει απάντηση από τον εξυπηρετητή του
- Ο εξυπηρετητής εκτελεί **επαναληπτικές** ερωτήσεις
  - Εάν δε μπορεί να δώσει απάντηση, θα στείλει ερώτηση στον πλησιέστερο γνωστό επίσημο εξυπηρετητή ονομάτων
  - Στη χειρότερη περίπτωση ο κοντινότερος γνωστός επίσημος εξυπηρετητής ονομάτων είναι ο εξυπηρετητής ρίζας
- Εδώ, ο εξυπηρετητής ρίζας παραπέμπει στον εξυπηρετητή TLD για την περιοχή "gr"
- Η ερώτηση σε αυτόν τον εξυπηρετητή παραπέμπει στον εξυπηρετητή ονομάτων της περιοχή "ntua.gr"
- ... κ.ο.κ



# Επαναληπτικές ερωτήσεις



- Στην επαναληπτική ερώτηση, ο εξυπηρετητής ονομάτων απαντά με το όνομα του πλησιέστερου γνωστού επίσημου εξυπηρετητή ονομάτων
- Εδώ, παραπέμπει στον εξυπηρετητή κορυφής, που με τη σειρά του παραπέμπει στον εξυπηρετητή TLD για την περιοχή "gr"
- Ο εξυπηρετητής TLD παραπέμπει και αυτός με τη σειρά του στον επίσημο εξυπηρετητή για την περιοχή "ntua.gr"
- ... Κ.Ο.Κ
- Η τακτική αυτή σημαίνει περισσότερη δουλειά για τον αναλυτή



# Μορφή ερώτησης (query)



- Μια ερώτηση DNS έχει τρεις παραμέτρους
  - Όνομα (Name): όνομα περιοχής ή διεύθυνση IP
  - Είδος ερώτησης (Query type): A, NS, MX, ...
  - Κατηγορία ερώτησης (Query class): 1 για IP

# Μορφή απάντησης (response)



- Η απάντηση περιλαμβάνει
  - Domain Name
  - Response type
  - Class (IP)
  - Time to live (in seconds)
  - Length of resource data
  - Resource data

# Μηνύματα DNS

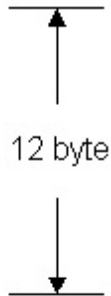


*ερωτήσεις και απαντήσεις, με την ίδια μορφή μηνύματος*

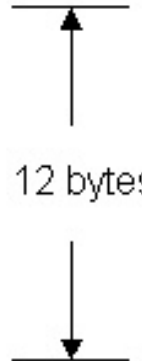
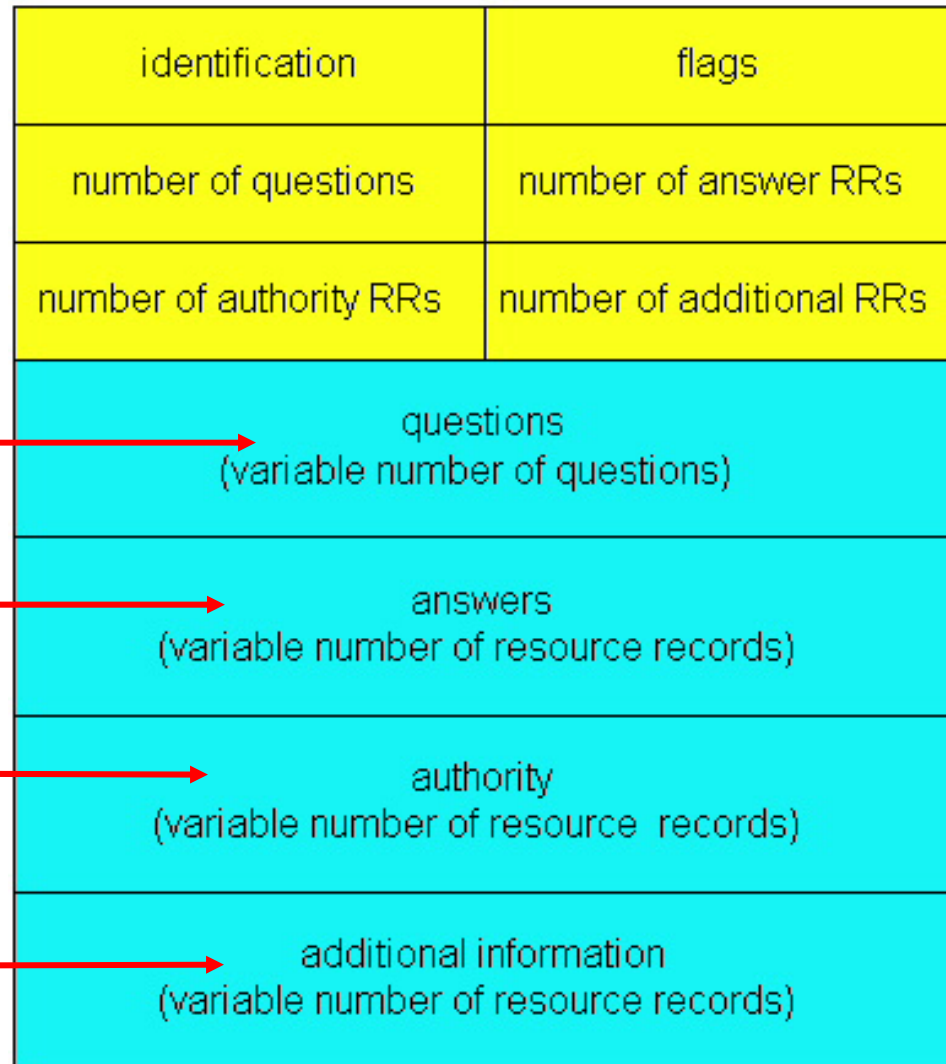
## επικεφαλίδα

- **ταυτότητα:** αριθμός 16 bit για την ερώτηση, η απάντηση χρησιμοποιεί τον ίδιο αριθμό
- **σημαίες:**
  - ερώτηση ή απάντηση
  - επιθυμητή αναδρομή
  - διαθέσιμη αναδρομή
  - η απάντηση είναι επίσημη

identification	flags
number of questions	number of answer RRs
number of authority RRs	number of additional RRs
questions (variable number of questions)	
answers (variable number of resource records)	
authority (variable number of resource records)	
additional information (variable number of resource records)	



# Μηνύματα DNS



Πεδία Name, type  
για ερώτηση

RR απάντησης  
σε ερώτηση  
εγγραφές για  
επίσημους servers

πρόσθετη "χρήσιμη"  
πληροφορία που μπορεί  
να χρησιμοποιηθεί

# Σημαίες μηνύματος



- QR: Query=0, Response=1
- AA: Authoritative Answer
- TC: response truncated (> 512 bytes)
- RD: recursion desired
- RA: recursion available
- rcode: return code



# UDP & TCP



- Το DNS χρησιμοποιεί σε αμφότερα τα πρωτόκολλα UDP και TCP
- Οι εξυπηρετητές ονομάτων ακούν στη θύρα 53
  - Το TCP χρησιμοποιείται για μεταφορές ολόκληρης της βάσης δεδομένων σε δευτερεύοντες εξυπηρετητές (αντιγραφή)
  - Το UDP χρησιμοποιείται για αναζητήσεις
  - Αν η απάντηση υπερβαίνει τα 512 byte, ο αιτών ξανα-υποβάλλει την ερώτηση χρησιμοποιώντας TCP

