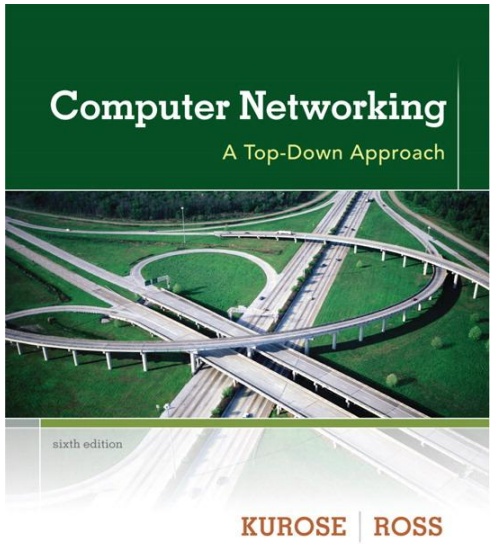
Network administration and Monitoring

د/عبدالملك الجمهوري

Chapter 2
Application Layer



A note on the use of these ppt slides:

We're making these slides freely available to all (faculty, students, readers). They're in PowerPoint form so you see the animations; and can add, modify, and delete slides (including this one) and slide content to suit your needs. They obviously represent a *lot* of work on our part. In return for use, we only ask the following:

- If you use these slides (e.g., in a class) that you mention their source (after all, we'd like people to use our book!)
- If you post any slides on a www site, that you note that they are adapted from (or perhaps identical to) our slides, and note our copyright of this material.

Thanks and enjoy! JFK/KWR

©All material copyright 1996-2012
J.F Kurose and K.W. Ross, All Rights Reserved

Computer Networking: A Top Down Approach
6th edition
Jim Kurose, Keith Ross
Addison-Wesley
March 2012

Chapter 2: outline

2.1 principles of network applications
- app architectures
- app requirements

2.2 Web and HTTP

2.3 FTP

2.4 electronic mail
- SMTP, POP3, IMAP

2.5 DNS

2.6 P2P applications

2.7 socket programming with UDP and TCP

DNS: domain name system (نظام أسماء النطاقات)

- هو عبارة عن قاعدة بيانات كبيرة وظيفتها تحويل الأسماء المفهومة من قبل البشر إلى أسماء مفهومة من قبل الجهاز والعكس

people: many identifiers:

- SSN, name, passport #

Internet hosts, routers: (الأجهزة لها نوعين من الأسماء)

- IP address (32 bit) - used for addressing datagrams
- "name", e.g., www.yahoo.com - used by humans

Q: how to map between IP address and name, and vice versa ? (كيف يمكن التحويل بين هذه الأسماء)

Domain Name System:

- *distributed database* implemented in hierarchy of many *name servers* (قاعدة بيانات موزعة وتبنى بشكل هرمي)
- *application-layer protocol:* hosts, name servers communicate to *resolve* names (address/name translation) (موجود في الأجهزة الطرفية فقط)
  - note: core Internet function, implemented as application-layer protocol (وظيفة مركزية للانترنت)
  - complexity at network's "edge" (طالما وهي عملية معقدة فنبقيها قريبة من الأجهزة الطرفية وبعيدة عن أجهزة الموجهات)

DNS: services, structure

DNS services

- hostname to IP address translation
- host aliasing (أسماء وهمية)
  - canonical, alias names
- mail server aliasing
- load distribution (توزيع الحمل)
  - replicated Web servers: many IP addresses correspond to one name (كل سيرفر عنده أكثر من عنوان وفي مواقع مختلفة فيتم تحويل الطلب الى السيرفر الأقل حمل)

why not centralize DNS?

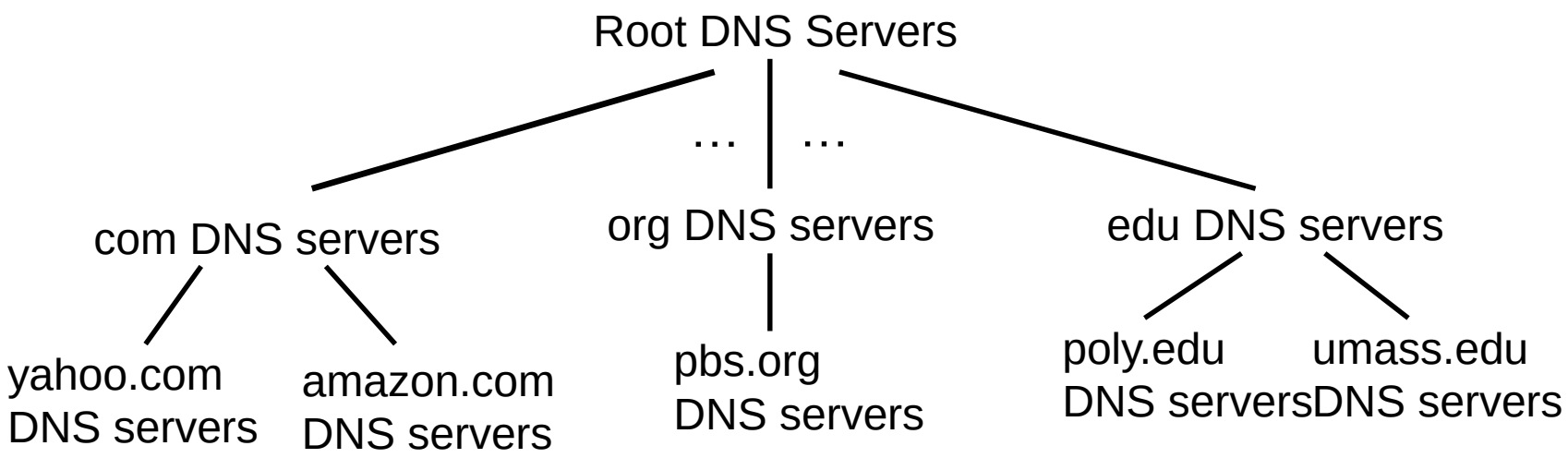
(هيكل هرمي وليس مركزي (مخدم وحيد))

- single point of failure
- traffic volume (حجم الطلبات)
- distant centralized database (بطئ في الاستجابة)
- maintenance

A: doesn't scale!

(إذا كان جهاز واحد لا يستطيع تحمل عدد كبير من الطلبات)

DNS: a distributed, hierarchical database



client wants IP for www.amazon.com; 1st approx:

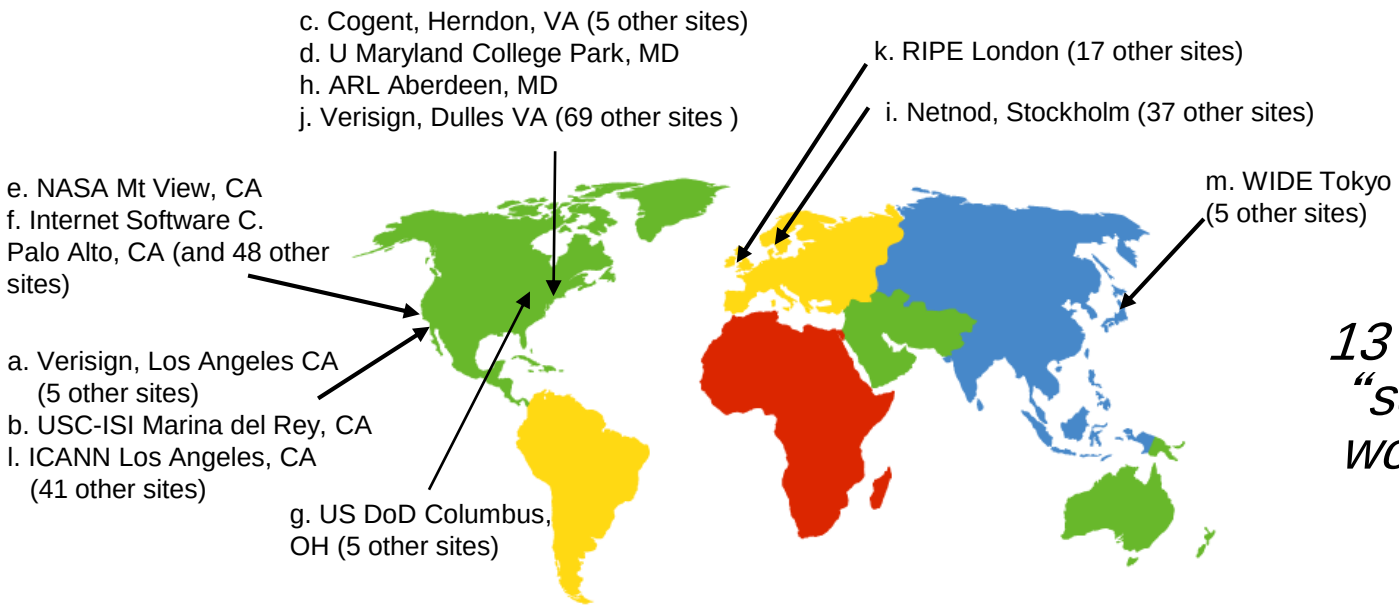
- client queries root server to find com DNS server
- client queries .com DNS server to get amazon.com DNS server
- client queries amazon.com DNS server to get IP address for www.amazon.com

- العملية السابقة تحدث بأجزاء من الثانية بدون أن يشعر المستخدم

DNS: root name servers

- contacted by local name server that can not resolve name
- root name server:
  - contacts authoritative name server if name mapping not known
  - gets mapping (التحويل بين الـهوست والعنوان)
  - returns mapping to local name server

- بسبب وجود 10 مخدمات جذرية في الولايات المتحدة فإن معظم الـ Traffic العالمي سوف يمر بالولايات المتحدة الأمريكية لذلك يقال أن أمريكا تتحكم بالأنترنت عبر العالم



13 root name "servers" worldwide

TLD, authoritative servers

• بما أنها هرمية فإن الطبقة التي تأتي بعد الـ Root مباشرة تسمى TLD

top-level domain (TLD) servers:

- responsible for com, org, net, edu, aero, jobs, museums, and all top-level country domains, e.g.: uk, fr, ca, jp
- Network Solutions maintains servers for .com TLD (تدار من قبل شركات)
- Educause for .edu TLD

authoritative DNS servers:

• النوع التالي في الهرمية بعد الـ TLD هو الـ authoritative servers

- organization's own DNS server(s), providing authoritative hostname to IP mappings for organization's named hosts (مملوك لشركة أو مؤسسة خاصة، الادارة محلية يوفر تحويل الاسماء الى عناوين للاجهزة المحلية المتصلة بهذه المنظومة)
- can be maintained by organization or service provider (يدار من قبل قسم الأي تي في الشركة عند عمل مخدم محلي، أما عند استئجار مخدم من مزود الخدمة الموجود في الكلود فيد من قبل مزود الخدمة)

Local DNS name server

- does not strictly belong to hierarchy (ليس بالضرورة أن يكون جزء من الهرمية لأنه قد يكون في شبكة منزلية أو ماشابه، وقد ينظم بشكل مؤقت للهرم وقد يغادر في أي وقت)
- each ISP (residential ISP, company, university) has one (أول مخدم تتصل به الاجهزة عندما تطلب عنوان معين)
  - also called "default name server"
- when host makes DNS query, query is sent to its local DNS server
  - has local cache of recent name-to-address translation pairs (but may be out of date!)
  - acts as proxy, forwards query into hierarchy (يعمل كوسيط حيث يحول الطلبات من جهاز المستخدم إلى مخدمات الهرمية)

DNS name resolution example

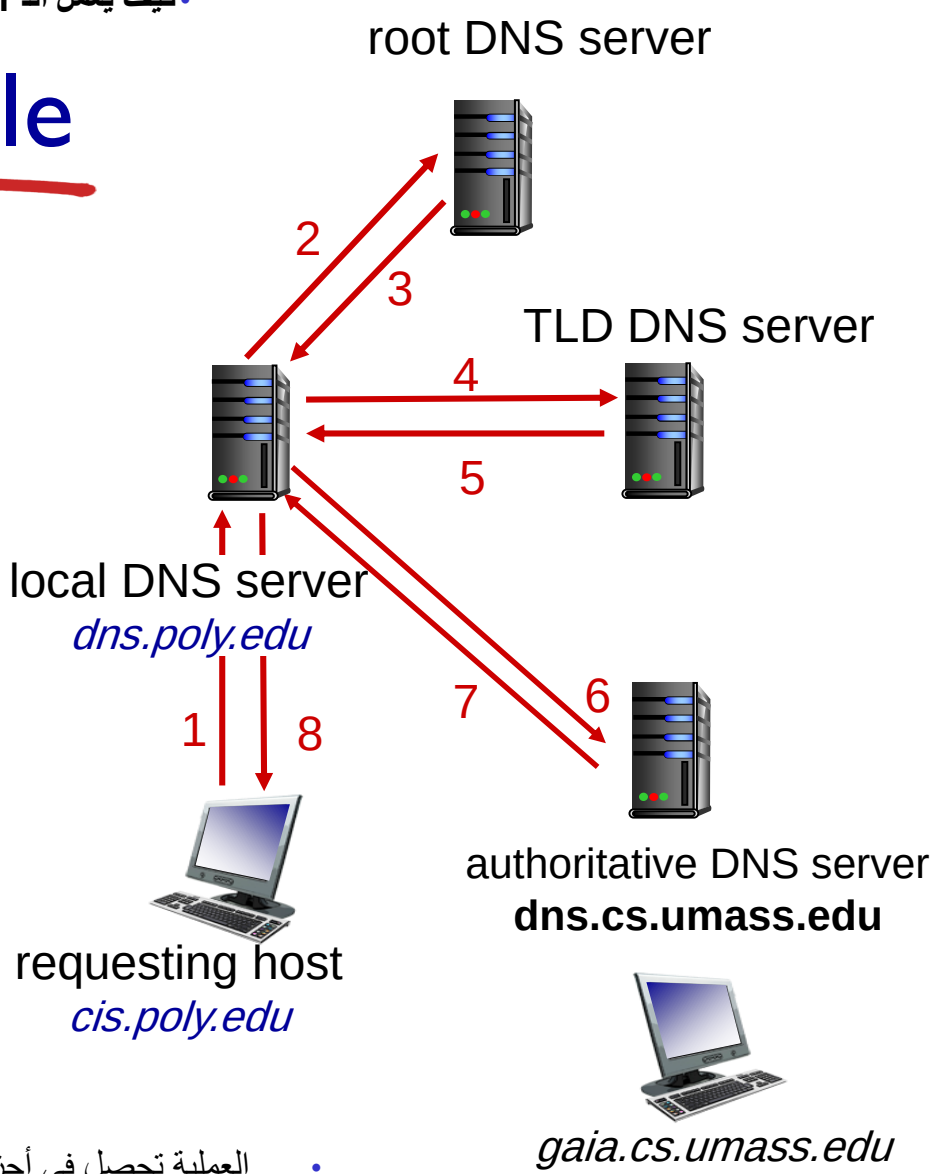
• كيف يعمل الـ DNS server

- host at cis.poly.edu wants IP address for gaia.cs.umass.edu

• يوجد نوعين من الطلبات

iterated query: (الطلب التكراري)

- contacted server replies with name of server to contact
- "I don't know this name, but ask this server"

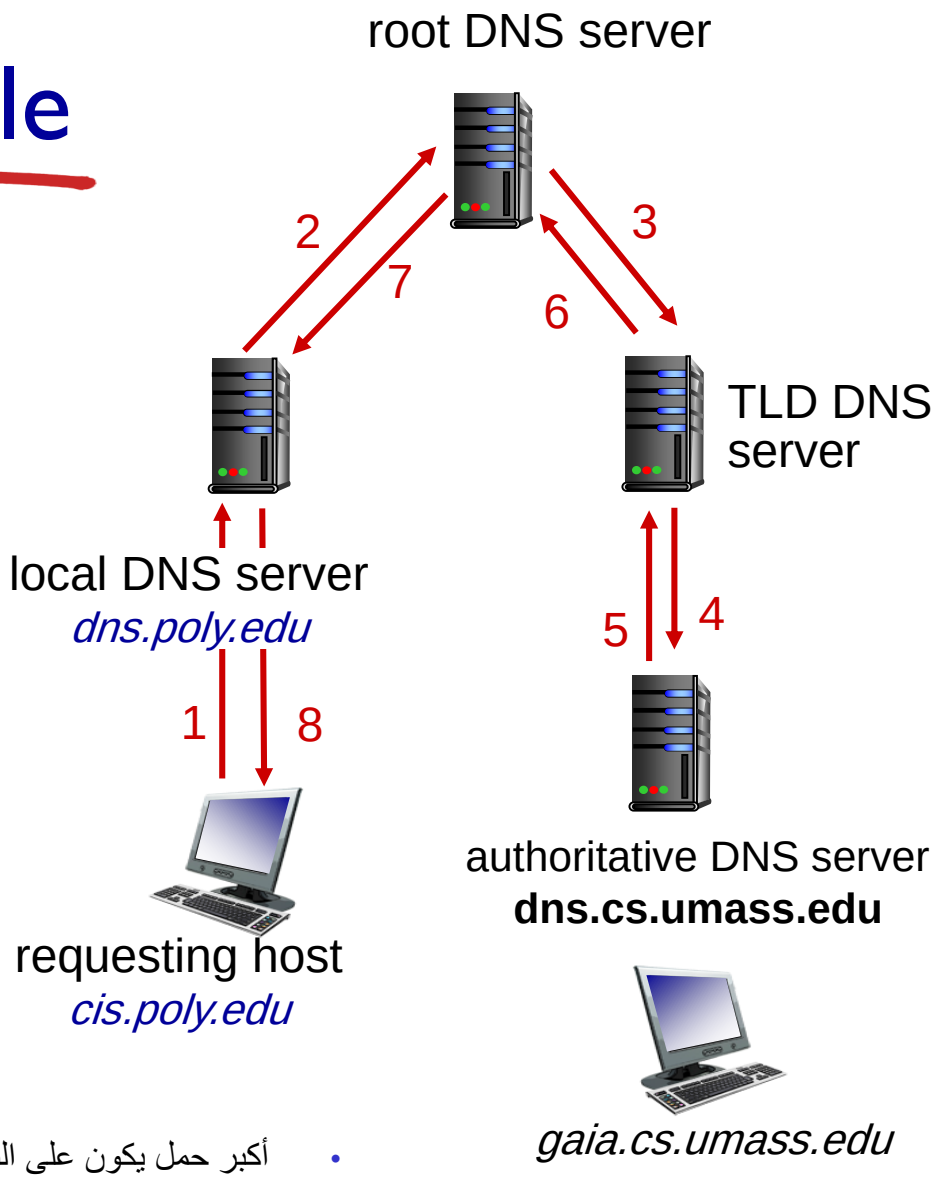


• العملية تحصل في أجزاء من الثانية
• كل الحمل كان على السيرفر المحلي

DNS name resolution example

recursive query:

- puts burden of name resolution on contacted name server
- heavy load at upper levels of hierarchy?



- أكبر حمل يكون على السيرفر الجذري

DNS: caching, updating records

- once (any) name server learns mapping, it *caches* mapping (كيف يتم المحافظة على بيانات الكاش حقيقية ومحدثة)
  - cache entries timeout (disappear) after some time (TTL) (كل الحقول في الكاش بعد إنتهاء فترة زمنية معينة تنتهي وتطلب تحديث البيانات من جديد، كل حقل له رقم معين بإسم تي تي ال)
  - TLD servers typically cached in local name servers
    - thus root name servers not often visited

• المعلومات غالباً ما تجدها في الـ TLD
ونادراً ما يتم زيارة الـ Root servers

- cached entries may be *out-of-date* (best effort name-to-address translation!)
  - if name host changes IP address, may not be known Internet-wide until all TTLs expire
- update/notify mechanisms proposed IETF standard
  - RFC 2136

DNS records (*)

DNS: distributed db storing resource records (RR)

RR format: `(name, value, type, ttl)`

•كل سجل في قاعدة بينات الـ DNS يحتوي على البيانات التالية

type=A

- **`name`** is hostname
- **`value`** is IP address

type=NS

- **`name`** is domain (e.g., foo.com) (قد يكون مخصص لدوين خاصة بشبكة محلية أو شركة أو جامعة)
- **`value`** is hostname of authoritative name server for this domain

type=CNAME

- **`name`** is alias name for some "canonical" (the real) name
- **`www.ibm.com`** is really **`servereast.backup2.ibm.com`**
- **`value`** is canonical name (**`www.ibm.com`**)

type=MX

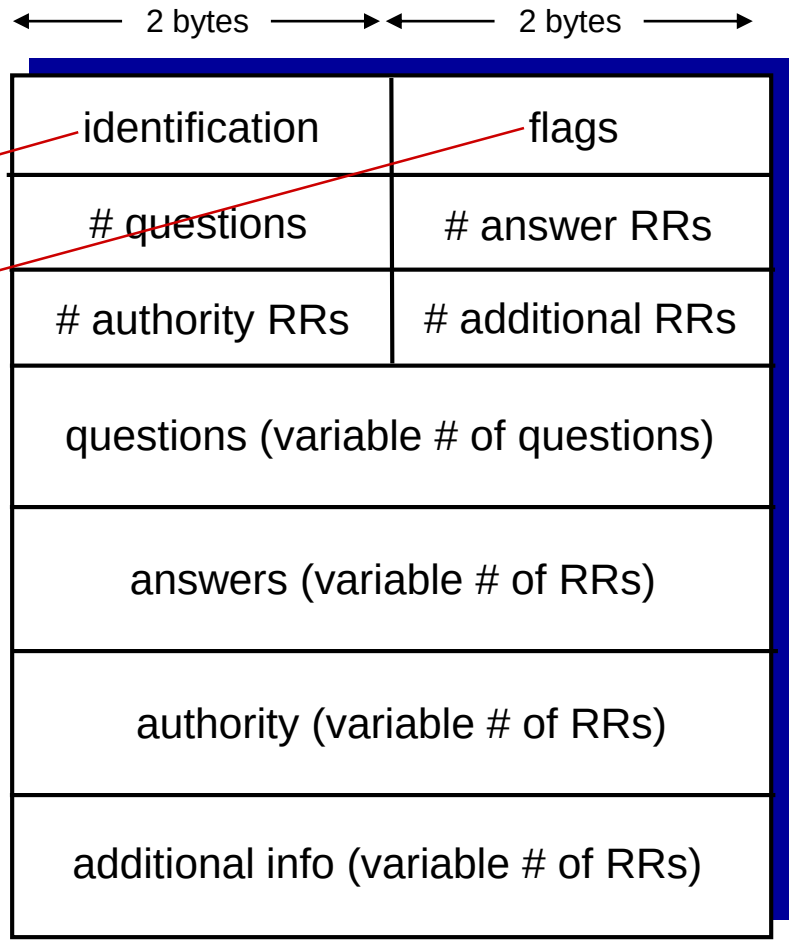
- **`Value`** `(Maile1.google.com)` is name of mailserver associated with **`name`** `(www.google .com)`

DNS protocol, messages (*)

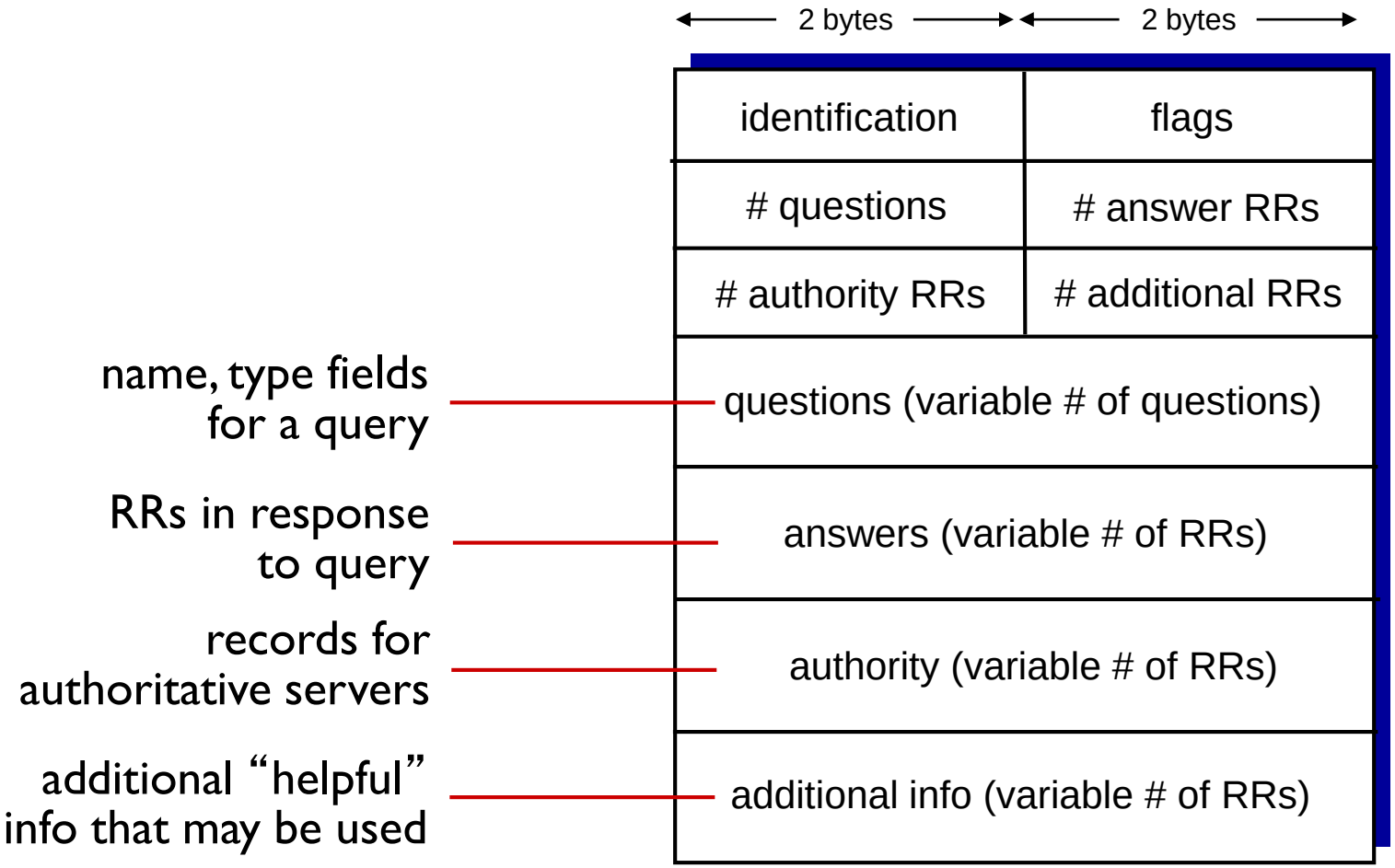
- *query* and *reply* messages, both with same *message format*

msg header

- identification: 16 bit # for query, reply to query uses same #
- flags:
  - query or reply
  - recursion desired
  - recursion available
  - reply is authoritative



DNS protocol, messages (*)



Inserting records into DNS (*)

- example: new startup "Network Utopia" •إذا ظهر موقع جديد بإسم
- register name networkuptopia.com at *DNS registrar* (e.g., Network Solutions)
  - provide names, IP addresses of authoritative name server (primary and secondary)
  - registrar inserts two RRs into .com TLD server:
    (networkutopia.com, dns1.networkutopia.com, NS)
    (dns1.networkutopia.com, 212.212.212.1, A)
- create authoritative server type A record for www.networkuptopia.com; type MX record for networkutopia.com

•حصل مسبقاً هجوم على بعض مخدمات الـ DNS مما جعلها خارج الخدمة لبعض من الوقت وهذا أدى إلى خسائر بمئات الملايين من الدولارات للعديد من الشركات

Attacking DNS (*)

DDoS attacks (distributed DOS)

- Bombard root servers with traffic
  - Not successful to date (حتى اليوم لم ينجح أي هجوم من هذا النوع على مخدمات الروت)
  - Traffic Filtering (بسبب وجود العديد من الفلاتر مثل الفيرول وغيرها)
  - Local DNS servers cache IPs of TLD servers, allowing root server bypass (ولان معظم الطلبات غالباً ما يتم الرد عليها من المخدمات في الهرمية الأدني)
- Bombard TLD servers
  - Potentially more dangerous (هنا الهجوم عليها أخطر لأن الترافيك المار عليها كثير)

Redirect attacks (هجوم إعادة التوجيه)

- Man-in-middle
  - Intercept queries
- DNS poisoning
  - Send bogus relies to DNS server, which caches

Exploit DNS for DDoS (استخدامه في الهجوم)

- Send queries with spoofed source address: target IP
- Requires amplification