Chương 2: Nội dung

DNS: Hệ thống tên miền (domain name system)

Con người: có nhiều định danh:
- CMT, tên, số hộ chiếu

Các host và router trên Internet:
- Địa chỉ IP (32 bit) – được dùng để gán địa chỉ cho các gói tin
- "tên miền", ví dụ: www.yahoo.com – được con người sử dụng

Hỏi: Làm cách nào để ánh xạ giữa địa chỉ IP và tên miền, và ngược lại?

Hệ thống tên miền:
- *Cơ sở dữ liệu phân tán* được cài đặt phân cấp với nhiều *server tên miền*
- *Giao thức tầng ứng dụng:* để các host, các server tên miền truyền thông được thì cần phải *phân giải* các tên miền (diễn dịch địa chỉ/tên miền)
  - Chú ý: chức năng lõi của Internet, được cài đặt như giao thức tầng ứng dụng
  - Phức tạp tại "phần cạnh" của mạng

DNS: các dịch vụ và cấu trúc

Các dịch vụ của DNS
- Dịch tên host thành địa chỉ IP
- Bí danh của host
  - Các tên đúng chuẩn, các tên là bí danh
- Bí danh mail server
- Phân tán tải
  - Nhân rộng các máy chủ Web: nhiều địa chỉ IP tương ứng với một tên

Tại sao không tập trung hóa trong DNS?
- Một điểm chịu lỗi
- Lưu lượng
- Cơ sở dữ liệu tập trung ở xa
- Bảo trì

Trả lời: Không thể thực hiện với quy mô lớn!
- Chỉ riêng máy chủ DNS Comcast: 600 tỷ truy vấn DNS/ngày
- Riêng máy chủ DNS Akamai: 2,2T truy vấn DNS/ngày

Một số vấn đề của DNS

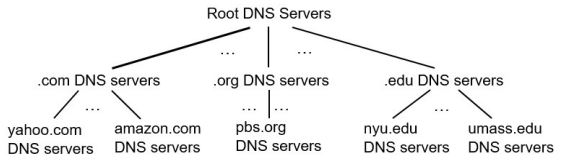
Cơ sở dữ liệu phân tán khổng lồ:
- ~ tỷ bản ghi, mỗi bản ghi đơn giản.

Xử lý hàng nghìn tỷ truy vấn mỗi ngày:
- Số lượng truy vấn đọc *nhiều hơn* truy vấn ghi
- *Các vấn đề về hiệu năng:* hầu hết mọi giao dịch Internet đều tương tác với DNS – tính theo mili giây!

Không tập trung về mặt tổ chức và vật lý:
- hàng triệu tổ chức khác nhau chịu trách nhiệm về bản ghi của họ

Vấn đề: độ tin cậy, bảo mật

DNS: cơ sở dữ liệu phân tán và phân cấp



Root

Top Level Domain

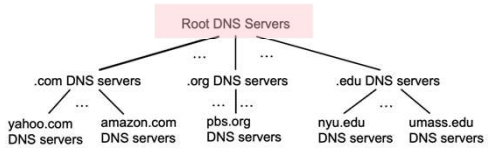
Authoritative

client muốn có đị chỉ IP cho www.amazon.com:

- client truy vấn server gốc để tìm com DNS server
- client truy vấn .com DNS server để lấy amazon.com DNS server
- client truy vấn amazon.com DNS server để lấy địa chỉ IP của www.amazon.com

DNS: Các server tên gốc

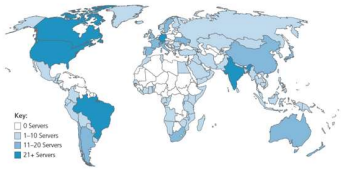
- Là nơi liên hệ cuối cùng, chính thức, khi mà các server tên miền không thể phân giải tên.



DNS: Các server tên gốc

- Là nơi liên hệ cuối cùng, chính thức, khi mà các server tên miền không thể phân giải tên.
- Chức năng Internet *vô cùng quan trọng*
  - Internet không thể hoạt động nếu thiếu nó!
  - DNSSEC – cung cấp bảo mật (xác thực, tính toàn vẹn của thông điệp)
- ICANN (Internet Corporation for Assigned Names and Numbers) quản lý tên miền DNS gốc

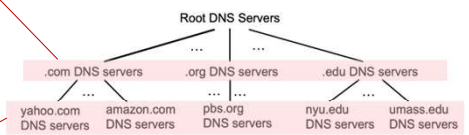
13 logical root name "servers" worldwide each "server" replicated many times (~200 servers in US)



Các server TLD và server có thẩm quyền

Các server top-level domain (TLD) :

- Chịu trách nhiệm cho tên miền .com, .org, .net, .edu, .aero, .jobs, .museums, và tất cả các tên miền cấp cao nhất thuộc quốc gia như: .cn, .uk, .fr, .ca, .jp
- Network Solutions: cơ quan đăng ký có thẩm quyền cho .com, .net TLD
- Educause: .edu TLD



Các server DNS có thẩm quyền:

- (Các) máy chủ DNS của chính tổ chức, cung cấp tên máy chủ có thẩm quyền để ánh xạ IP cho các máy chủ được đặt tên của tổ chức
- có thể được duy trì bởi tổ chức hoặc nhà cung cấp dịch vụ

Server tên DNS cục bộ

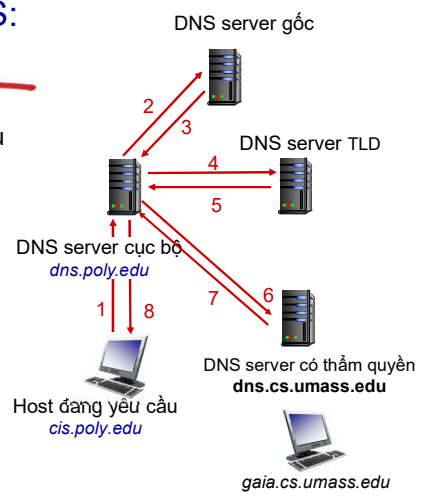
- Khi máy chủ thực hiện truy vấn DNS, nó sẽ được gửi đến máy chủ DNS *cục bộ* của nó
  - Máy chủ DNS cục bộ trả lời:
    - từ thông tin có trong bộ đệm cục bộ của các cặp tên-địa chỉ (có thể đã bị cũ!)
    - chuyển tiếp yêu cầu vào hệ thống phân cấp DNS để giải quyết
  - Mỗi ISP có máy chủ tên DNS cục bộ:
    - MacOS: `% scutil --dns`
    - Windows: `>ipconfig /all`
- Máy chủ DNS cục bộ không hoàn toàn thuộc về hệ thống phân cấp.

Phân giải tên DNS: Truy vấn lặp

- Ví dụ: Host tại cis.poly.edu muốn lấy địa chỉ IP của gaia.cs.umass.edu

Truy vấn lặp:

- Server được hỏi sẽ trả lời với tên của server sẽ có thể hỏi được tiếp
- "Tôi không biết tên đó, nhưng có thể hỏi server này"

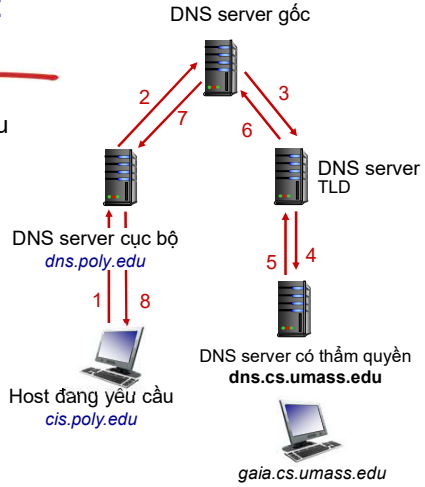


Phân giải tên DNS: Truy vấn đệ quy

- Ví dụ: Host tại cis.poly.edu muốn lấy địa chỉ IP của gaia.cs.umass.edu

Truy vấn đệ quy:

- Đặt trách nhiệm phân giải tên lên server tên được hỏi
- Tải nặng tại các cấp cao hơn trong hệ thống phân cấp?



DNS: lưu và cập nhật các bản ghi

- Khi server tên học cách ánh xạ, nó sẽ *lưu* ánh xạ vào bộ nhớ đệm, và ngay lập tức sẽ phản hồi truy vấn với ánh xạ này.
  - Việc lưu trong bộ đệm sẽ giúp cải thiện thời gian phản hồi
  - Mục lưu sẽ bị quá hạn (bị xóa) sau một thời gian (TTL)
  - Các server TLD thường được lưu trong các server tên cục bộ
    - Do đó, các server tên gốc sẽ không thường xuyên được truy cập
- Các mục được lưu trong bộ đệm có thể bị *quá hạn*
  - Nếu host thay đổi địa chỉ IP, thì Internet sẽ có thể không biết được cho đến khi TTL hết hạn
  - Sử dụng cơ chế best effort để dịch tên-địa chỉ!

Bản ghi DNS (DNS records)

DNS: cơ sở dữ liệu phân tán lưu trữ các bản ghi nguồn (resource records - RR)

Định dạng RR: `(name, value, type, ttl)`

type=A

- **name** là tên máy
- **Value** là địa chỉ IP

type=NS

- **name** là tên miền (ví dụ: foo.com)
- **value** là tên host của server có thẩm quyền cho tên miền này

type=CNAME

- **name** là tên bí danh của tên "chuẩn" (tên thật)
- `www.ibm.com` tên thật là `servereast.backup2.ibm.com`
- **value** là tên chuẩn

type=MX

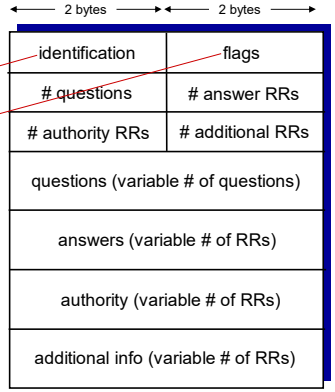
- **value** là tên của mail server được kết hợp với **name**

Giao thức, thông điệp DNS

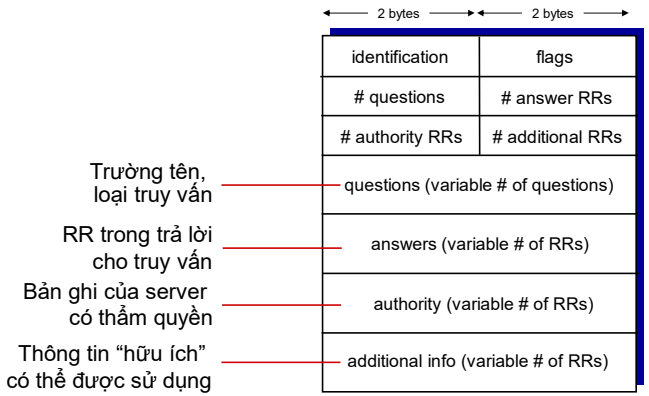
- Các thông điệp *truy vấn* và *trả lời* đều có cùng *định dạng thông điệp*

Tiêu đề thông điệp

- identification: 16 bit cho truy vấn/trả lời
- flags:
  - Truy vấn hoặc trả lời
  - Đệ quy chờ
  - Đệ quy sẵn sàng
  - Trả lời có thẩm quyền



Giao thức, thông điệp DNS



Đưa thông tin vào trong DNS

- Ví dụ: Tạo mới "Network Utopia"
- Đăng ký tên miền networkuptopia.com tại *DNS registrar* (Ví dụ: Network Solutions)
  - Cung cấp tên, địa chỉ IP của server tên có thẩm quyền (sơ cấp và thứ cấp)
  - registrar chèn 2 bản ghi NS, A vào server .com TLD:

```
(networkutopia.com, dns1.networkutopia.com, NS)
(dns1.networkutopia.com, 212.212.212.1, A)
```

- Tạo server có thẩm quyền cục bộ với địa chỉ IP `212.212.212.1`
  - Bản ghi loại A cho `www.networkuptopia.com`
  - Bản ghi loại MX cho `networkutopia.com`

Bảo mật DNS

Tấn công DDoS

- Tấn công server gốc với lưu lượng lớn
  - Không thành công cho đến nay
  - Lọc lưu lượng
  - DNS server cục bộ cache IP của TLD server, cho phép bỏ qua server gốc
- Tấn công TLD servers với lưu lượng lớn
  - Tiềm tàng nhiều nguy cơ hơn

Tấn công giả mạo

- Chặn các truy vấn DNS, trả về các câu trả lời không có thật
- Đầu độc bộ đệm DNS
  - Gửi trả lời giả mạo đến DNS server, mà các server này có thể cache lại

RFC 4033: Dịch vụ xác thực DNSSEC