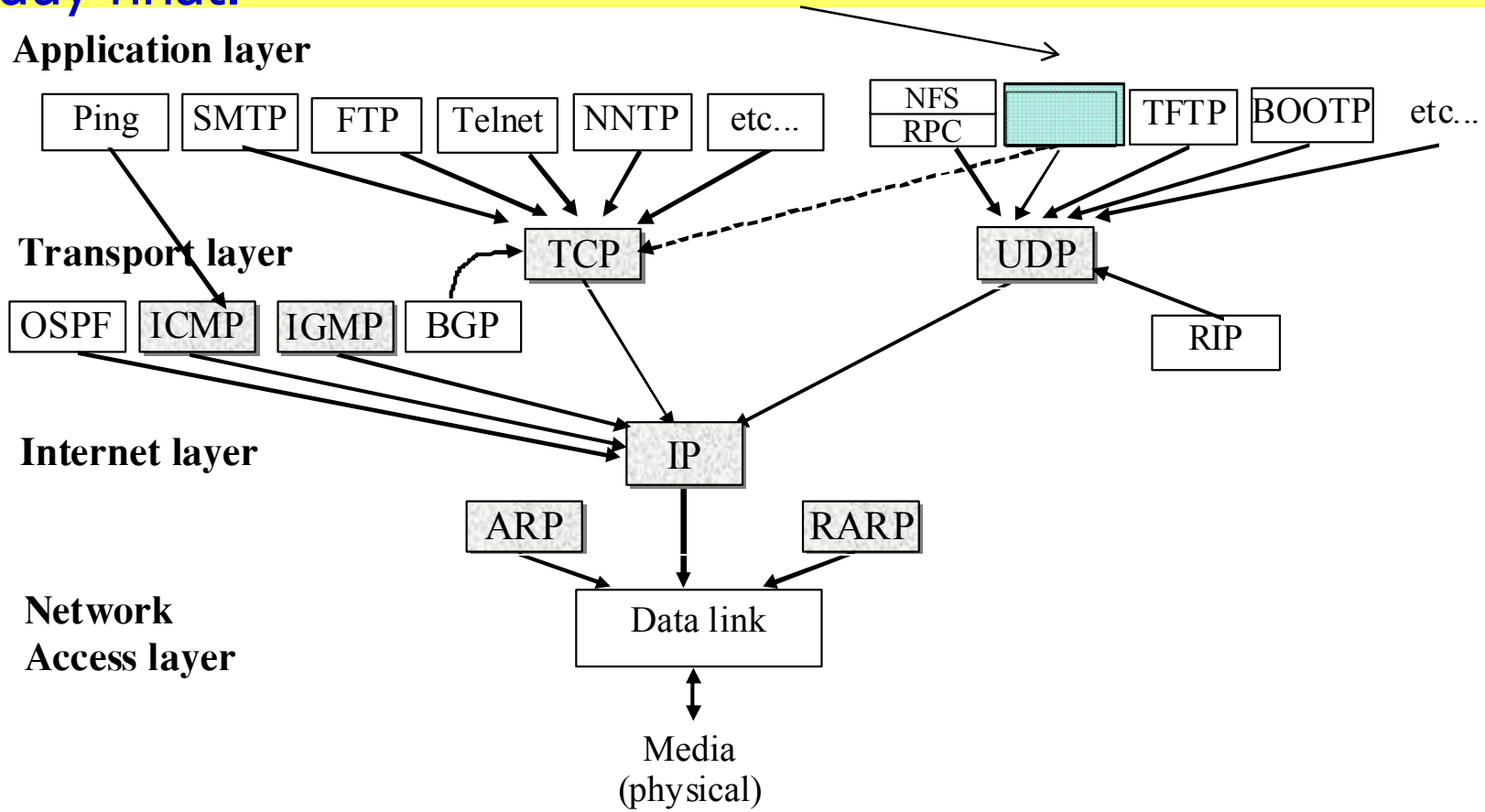
HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

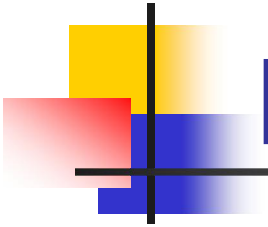
Internet và giao thức

Internet and Protocols

Chương 4: DNS - Hệ thống tên miền

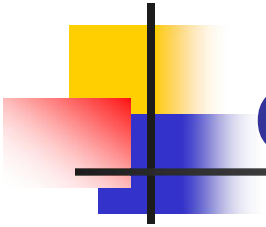
- DNS (Domain Name System) – Hệ thống tên miền là ứng dụng client-server, nhận dạng mỗi host có địa chỉ IP ứng với một tên duy nhất.





DNS

- Dùng cổng 53
- Có thể sử dụng UDP (chủ yếu) hoặc TCP (hiếm khi, chỉ khi bản tin phản hồi có kích thước lớn hơn 512 byte)
- DNS được định nghĩa trong các RFC 1034 và 1035



Chương 4: DNS - Hệ thống tên miền

- DNS là giao thức hỗ trợ cho các ứng dụng (support protocol).
- tana@128.111.24.41 là tên và địa chỉ gắn vào một server có IP cố định. Nếu ISP chuyển server này sang một máy tính khác, ở địa điểm khác thì địa chỉ này phải thay đổi sang giá trị mới → rất bất tiện.
- tana@art.ucsb.edu – tên dạng ASCII, thiết bị hiểu dạng địa chỉ số, vì thế cần phải có thiết bị thực hiện chức năng chuyển đổi giữa địa chỉ dạng ASCII với địa chỉ dạng số.

Chương 4: DNS - Hệ thống tên miền

Con người: có nhiều kiểu nhận dạng như

- tên (name)
- số CMT, hộ chiếu (passport) …

Trạm, router trên Internet :

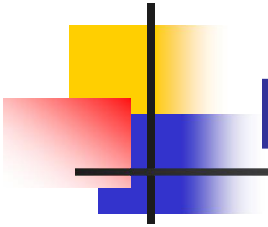
- Địa chỉ IPv4 (32 bit) sử dụng cho gói dữ liệu
- Tên host, (mail.yahoo.com) … sử dụng cho con người

Q: ánh xạ giữa địa chỉ IP và tên như thế nào

Hệ thống tên miền (DNS):

- *Cơ sở dữ liệu phân tán* được thực hiện trong phân cấp máy chủ tên miền *(name servers)*
- *Giao thức lớp ứng dụng* host (trạm), router, name server truyền thông để phân giải tên (phiên dịch giữa địa chỉ/tên)
  - Chú ý: đây là chức năng cốt lõi của Internet
  - Phức tạp ở biên mạng

Q: Tại sao không tập trung DNS



DNS

Dịch vụ DNS

- Phiên dịch địa chỉ IP và tên trạm
- Bí danh host
- Bí danh server thư
- Phân tải
  - Các server Web được nhân rộng ra: tập các địa chỉ IP cho một tên chính tắc

Tại sao không tập trung DNS?

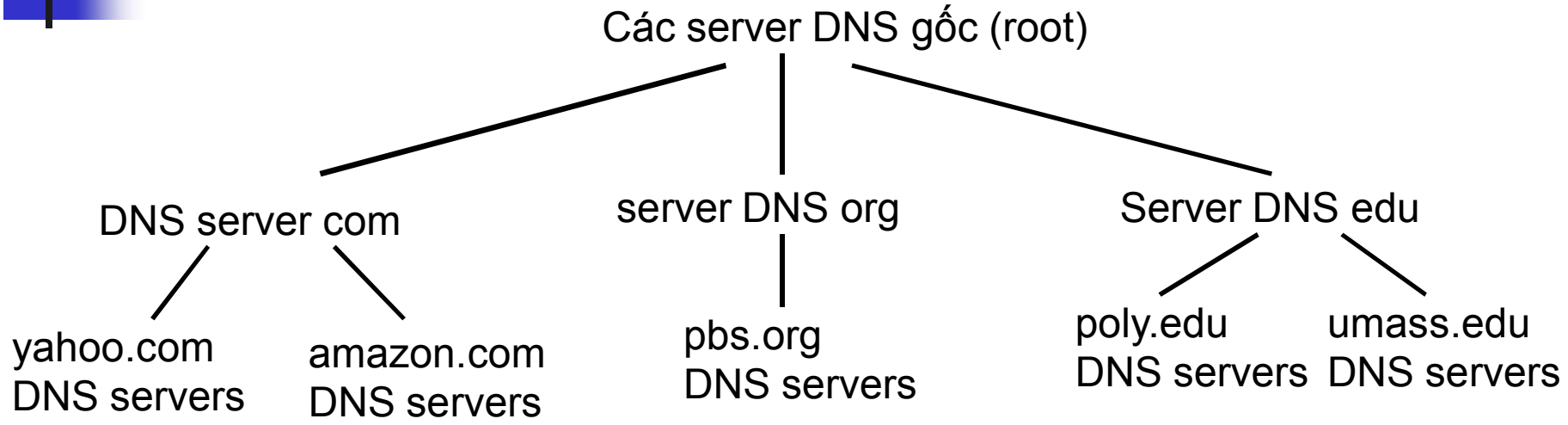
- Khi có lỗi ở 1 điểm thì cả hệ thống lỗi
- Lưu lượng tập trung vào một DNS server sẽ quá lớn
- Khoảng cách tới cơ sở dữ liệu ở xa
- Duy trì và cập nhật

Không đáp ứng quy mô mạng

Tên: Name
Địa chỉ: Address

Alias: bí danh

Cơ sở dữ liệu phân cấp, phân tán

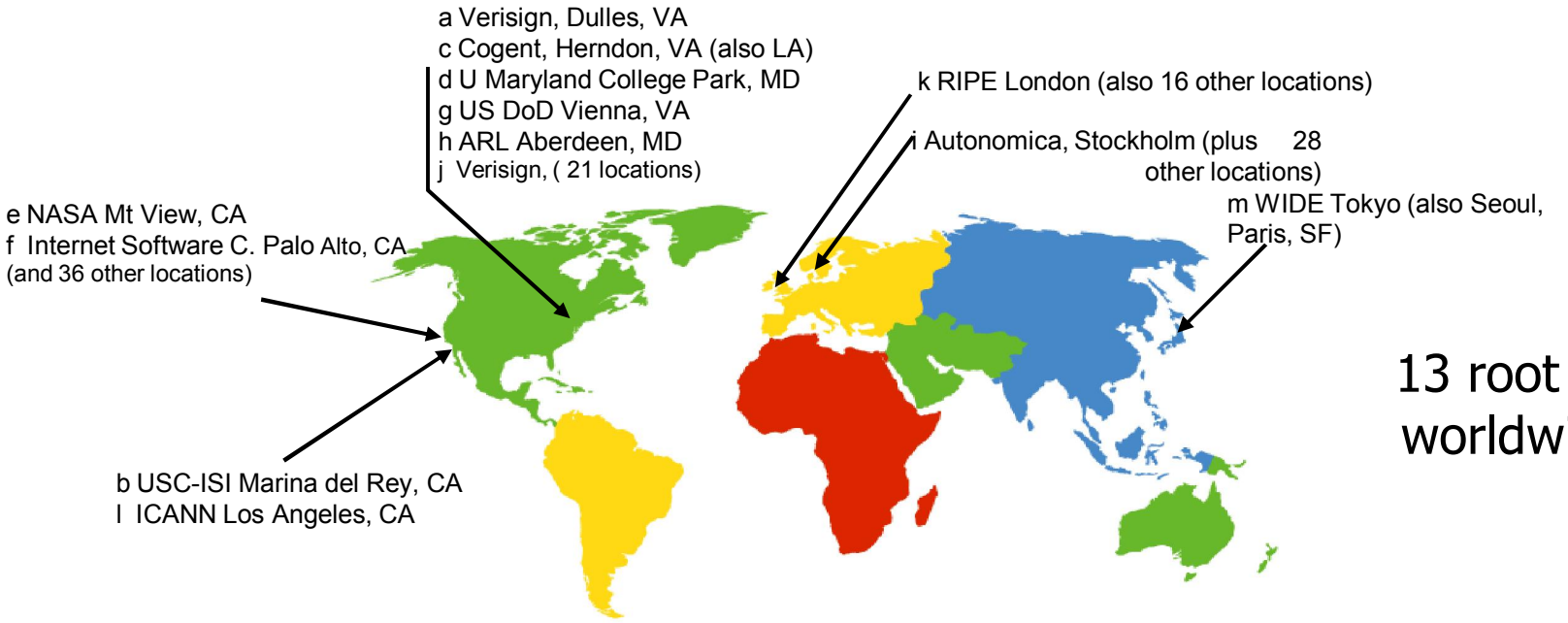


Client muốn tìm địa chỉ IP cho trang www.amazon.com

- client yêu cầu root server tìm server DNS com
- client yêu cầu server DNS com tìm server DNS amazon.com
- client yêu cầu server DNS amazon.com lấy địa chỉ IP của www.amazon.com

DNS: Server tên gốc

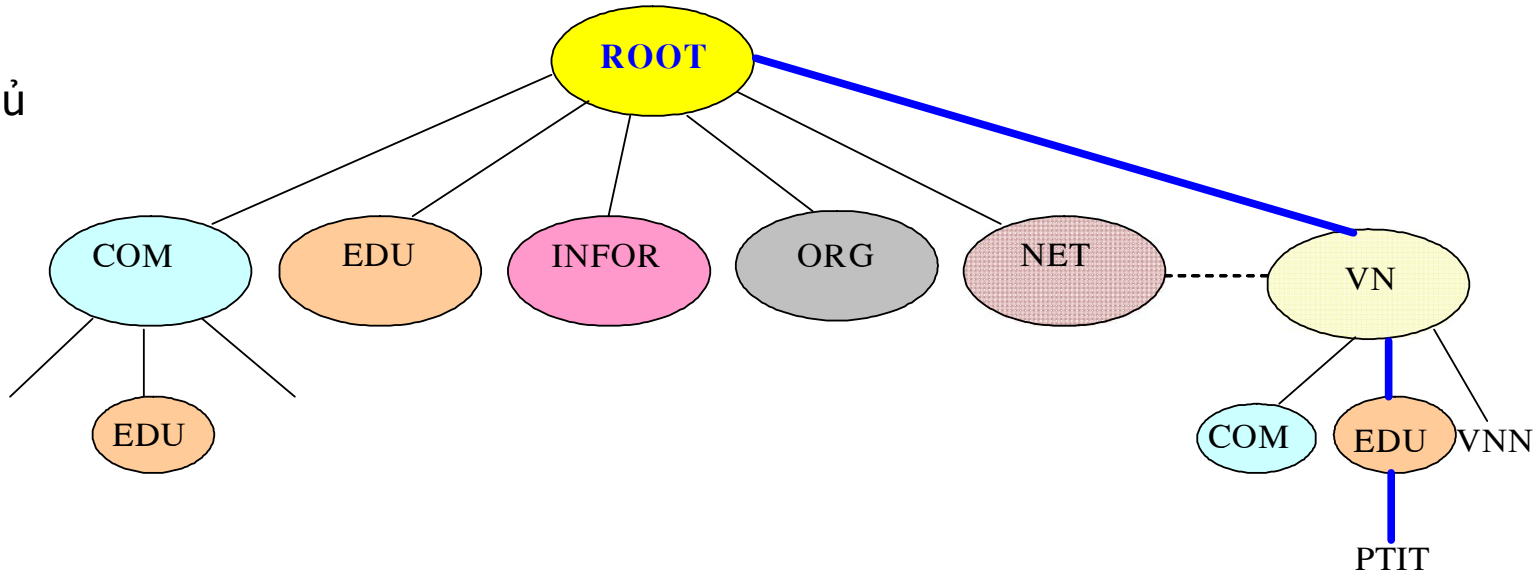
- Được kết nối với server tên khu vực (cục bộ) khi máy chủ này không thể xử lý được tên miền
- Máy chủ tên gốc (root name server):
  - Kết nối server tên có thẩm quyền nếu không biết ánh xạ tên
  - Lấy kết quả ánh xạ
  - Trả về kết quả ánh xạ cho server tên khu vực

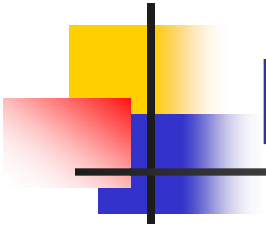


13 root name servers worldwide

Mạng Internet: Dịch vụ DNS

- Server tên miền mức cao (TLD) :
  là server cho com, org, net, edu, … và tất cả tên miền cấp quốc gia uk, fr, ca, us, jp, cn, vn ...
- Server DNS thẩm quyền:
  Server DNS của các tổ chức, cung cấp ánh xạ tên trạm được cấp quyền với địa chỉ của server các tổ chức (ví dụ: trang Web, mail).
  Do nhà cung cấp dịch vụ hoặc tổ chức duy trì.
- Ví dụ:
  ptit.edu.vn
  - ptit: Tên máy chủ
  - edu: Tên miền mức hai (Do tổ chức quản lý mạng quốc gia quy định)
  - vn: Tên miền mức cao nhất (Mã quốc gia)





Máy chủ tên miền cục bộ

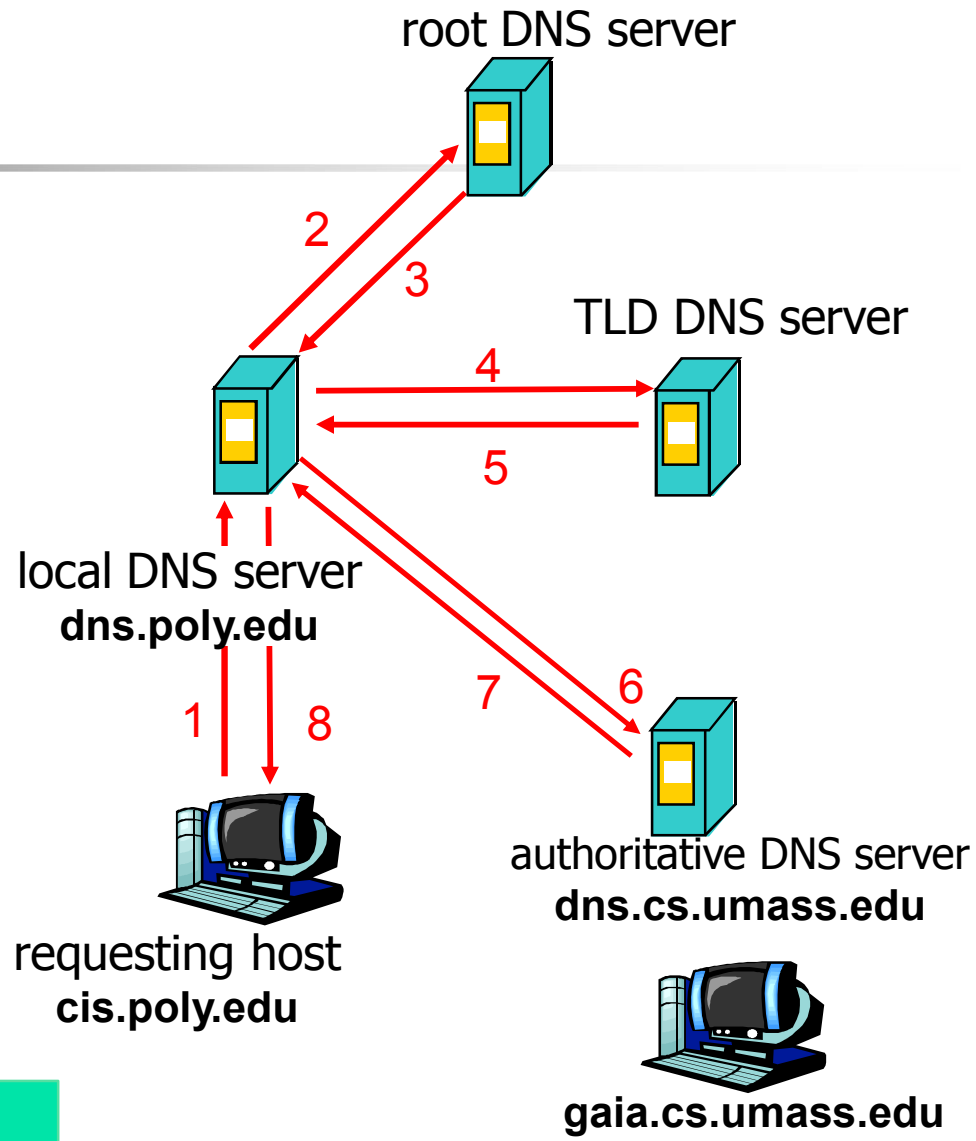
- Không thuộc phân cấp DNS
- Mỗi ISP (ISP dân cư, công ty, trường đại học) chỉ có một máy chủ tên miền cục bộ, được gọi là server tên miền mặc định
- Khi host truy vấn DNS, truy vấn được gửi tới server DNS cục bộ.
- Hoạt động như proxy, chuyển tiếp truy vấn vào hệ thống phân cấp

Ví dụ về tên miền

- Trạm (host) ở cis.poly.edu muốn tìm địa chỉ IP của gaia.cs.umass.edu

Truy vấn lặp lại :

- Server được kết nối (liên hệ) trả lại tên miền của server cần để kết nối
- "Tôi không biết tên miền này, nhưng hãy hỏi server này"



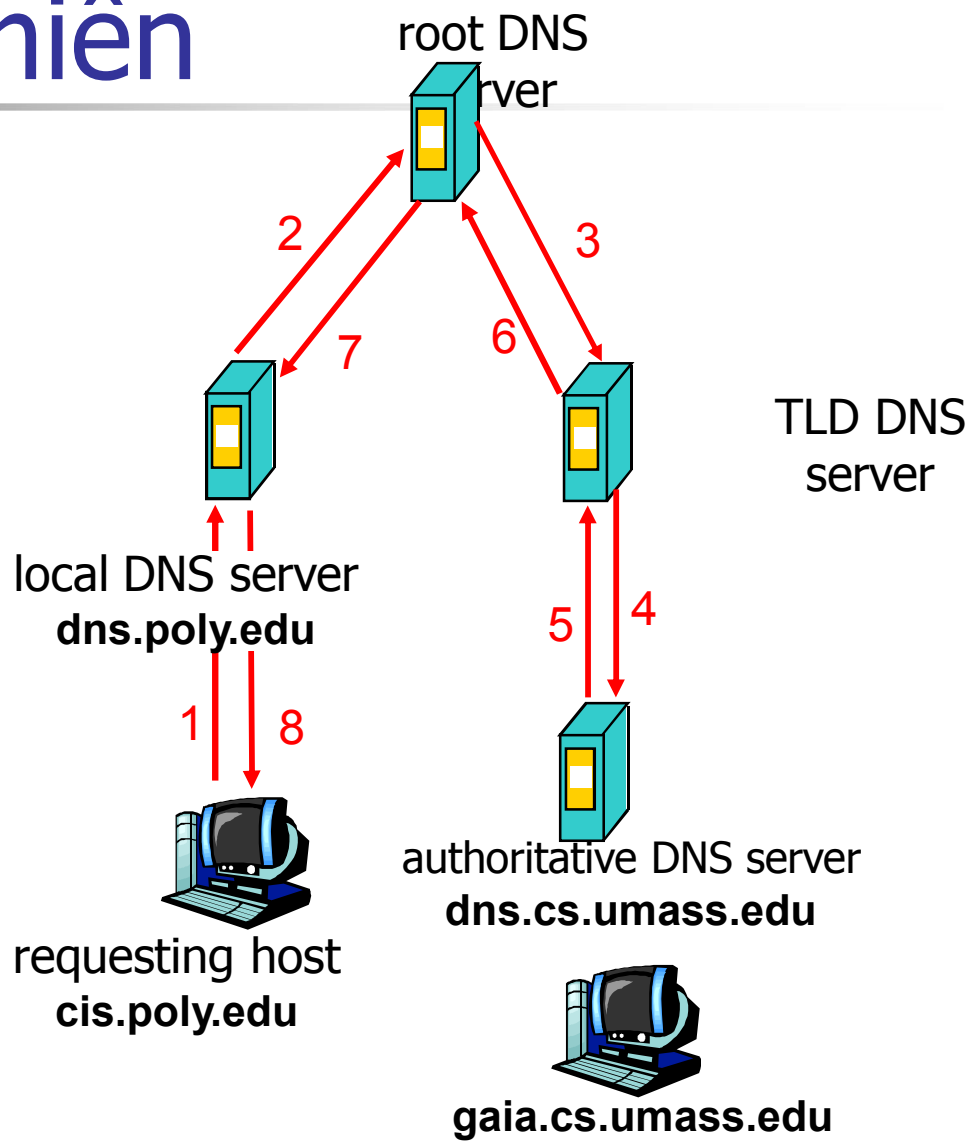
Q: Phân tích trình tự truy vấn từ mail.yahoo.com đến ptit.edu.vn

Ví dụ về tên miền

- Truy vấn đệ quy trong DNS

  Đưa trọng trách xử lý tên miền cho server được kết nối.

  Tải cao?



Bản ghi DNS

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

Khuôn dạng RR : **(name, value, type, ttl)**

- TTL – Time to live (t/g sống)

- Type=A
  - **name** is hostname (tên trạm)
  - **value** is IP address (địa chỉ IP)

- Type=NS
  - **name** is domain – tên miền (e.g. foo.com)
  - **value** is hostname (tên trạm) của máy chủ tên miền thẩm quyền cho tên miền này

- Type=CNAME
  - **name** is alias name (bí danh) cho "canonical" (the real) name (tên chính tắc)
    `www.ibm.com` **là bí danh của** `servereast.backup2.ibm.com`
  - **value** is canonical name (tên chính tắc)

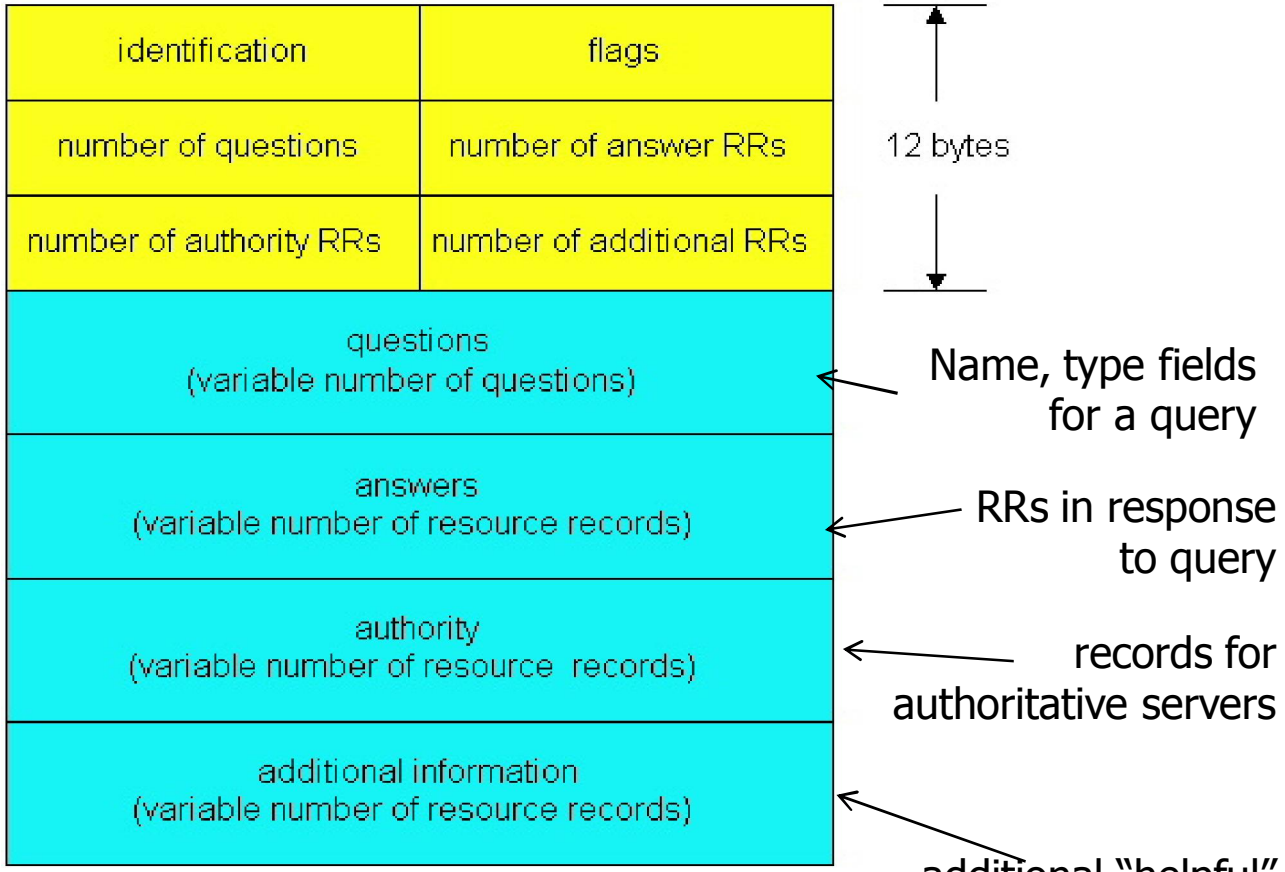
- Type=MX
  - **value** is tên of mailserver gắn với **name**

Giao thức và bản tin DNS

Giao thức DNS: bản tin truy vấn - *query* và trả lời - *reply* có cùng khuôn dạng

msg header

- identification: 16 bit # định danh truy vấn.
- flags:
  - Truy vấn hay trả lời
  - Thẩm quyền
  - Đệ quy
  - Đệ quy sẵn sàng



Message format: Khuôn dạng bản tin

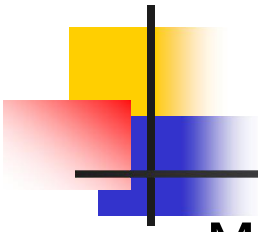
Recursion: đệ quy

Chèn bản ghi vào DNS

- Ví dụ: Mở công ty mới có tên "Network Utopia"
- Đăng ký tên miền networkuptopia.com tại *DNS registrar* (Ví dụ: Network Solutions)
  - Cung cấp các tên miền, các địa chỉ IP của server tên miền thẩm quyền (sơ cấp và thứ cấp)
  - Chèn đăng ký hai RR vào server tên miền mức cao - TLD:

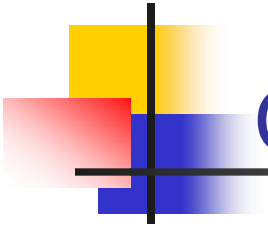
```
(networkutopia.com, dns1.networkutopia.com, NS)
(dns1.networkutopia.com, 212.212.212.1, A)
```

- Trên server thẩm quyền tạo: Bản ghi loại A cho www.networkuptopia.com; Bản ghi loại MX cho mail server networkutopia.com
- Làm thế nào để có địa chỉ về Web site này?



DNS: lưu đệm (caching)

- Mỗi lần server tên miền học được ánh xạ, nó sẽ lưu đệm ánh xạ đó
  - Các mục lưu đệm quá thời hạn bị loại bỏ (biến mất) sau một thời gian
  - Server tên miền mức cao (TLD) thường lưu đệm trong các server tên miền khu vực (cục bộ)
    - Như vậy server tên miền gốc không thường xuyên bị truy vấn



Các điểm yếu an toàn DNS

- Tấn công tràn ngập băng thông DDoS
- Gửi lượng truy vấn DNS rất lớn tới các máy chủ TLD
- Kiểu tấn công người trung gian (man-in-the-middle)
- Khai thác cơ sở hạ tầng DNS để khởi động tấn công DDoS chống lại trạm chủ mục tiêu.

Tổng kết

1. *Khái niệm về DNS.*
2. *Khuôn dạng bản ghi, bản tin DNS.*

- *Việc đệm (caching) sẽ giúp ích gì cho hệ thống DNS khi bị tấn công?*

- Nội dung về nhà và học buổi tới:
  - Chương 5: Ứng dụng ngang hàng P2P

DNS – why & how

- In the ARPANET, there was simply a file, *hosts.txt, that listed all the hosts and their IP addresses.*
- Every night, all the hosts would fetch it from the site at which it was maintained. For a network of a few hundred large timesharing machines, this approach worked reasonably well.
- However, when thousands of minicomputers and PCs were connected to the net, everyone realized that this approach could not continue to work forever. For one thing, the size of the file would become too large. However, even more important, host name conflicts would occur constantly unless names were centrally managed, something unthinkable in a huge international network due to the load and latency. To solve these problems, **DNS (the Domain Name System) was invented.**