

DNS: Domain Name System

Hệ thống tên miền

- ❑ DNS là một hệ thống được sử dụng trên Internet để dịch tên của các miền và các nút mạng được quảng cáo công cộng của chúng thành các địa chỉ IP.
- ❑ Một miền là một nhóm các máy tính được kết hợp với nhau bởi vị trí địa lý hay loại công việc/kinh doanh của chúng.
- ❑ Hệ thống tên miền được thiết lập theo một hệ thống phân cấp, tạo ra các DNS server ở các cấp độ khác nhau.
- ❑ Ví dụ: <http://www.ntu.edu.vn/cntt/>

DNS: Hệ thống tên miền

Người: nhiều định danh:

- CMND, tên, số hộ chiếu

Internet hosts, routers:

- Địa chỉ IP (32 bits) - được sử dụng để đánh địa chỉ cho các gói dữ liệu
- "tên", ví dụ, `www.yahoo.com` - được sử dụng bởi con người

Q: ánh xạ giữa địa chỉ IP và tên?

Domain Name System:

- *cơ sở dữ liệu phân tán* được cài đặt dựa trên hệ thống phân cấp của nhiều *name servers*
- *giao thức ở tầng ứng dụng* để cho các host, routers, name servers giao tiếp để *phân giải* names (dịch địa chỉ/tên)
 - lưu ý: một chức năng cốt lõi của Internet, được cài đặt như là giao thức tầng ứng dụng
 - độ phức tạp tại "biên" của mạng

DNS

Các dịch vụ của DNS

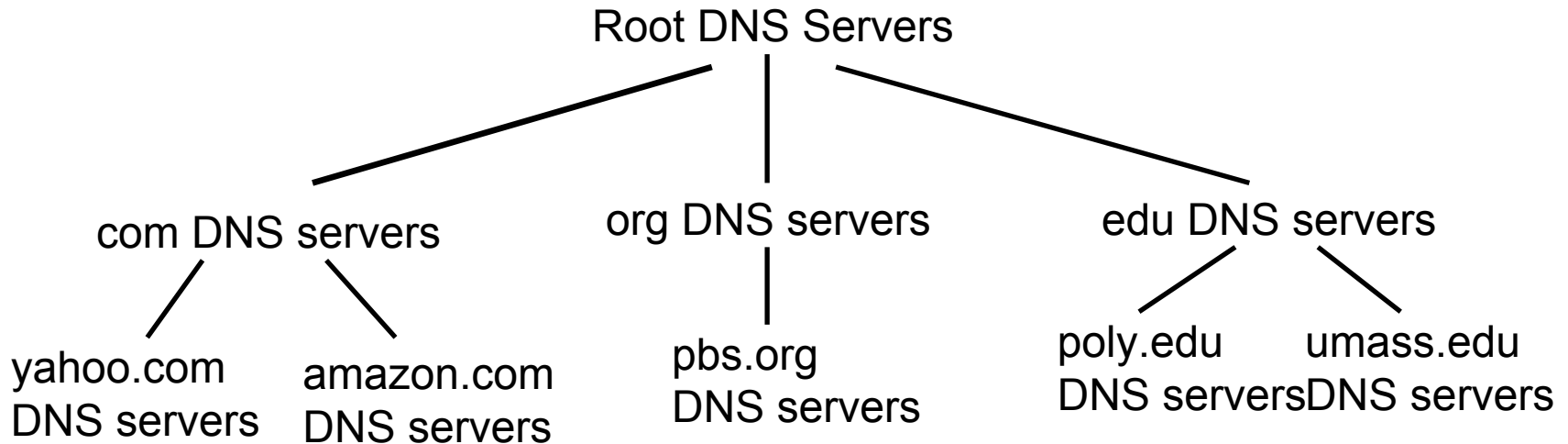
- ❑ Dịch tên của trạm thành địa chỉ
- ❑ Bí danh (aliasing) cho trạm
 - các tên chuẩn (canonical) và bí danh
- ❑ Bí danh cho mail server
- ❑ Phân phối tải
 - các Web servers bản sao: **tập các địa chỉ IP** cho một tên chuẩn/tên thật (canonical name)

Tại sao không tập trung DNS?

- ❑ hư hỏng tại một điểm đơn
- ❑ khối lượng lưu lượng
- ❑ cơ sở dữ liệu tập trung ở xa
- ❑ vấn đề duy trì

không mở rộng được!

Cơ sở dữ liệu phân cấp, phân tán

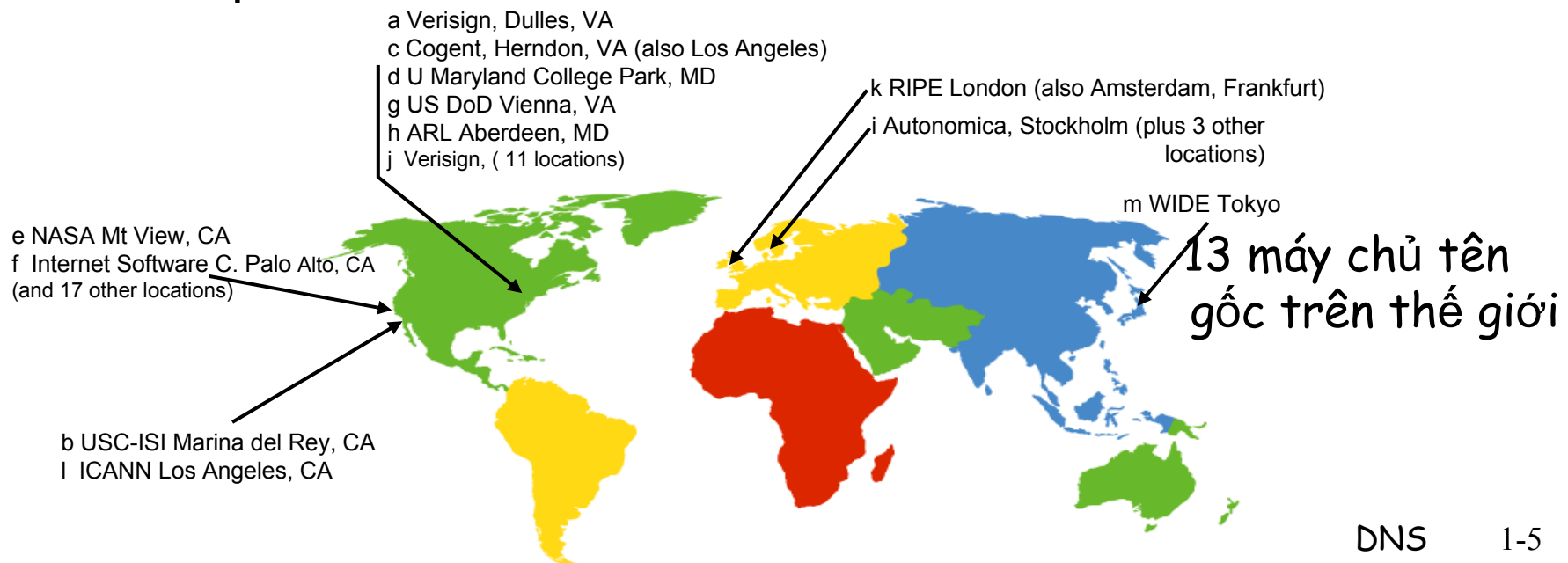


Client muốn địa chỉ IP của **www.amazon.com**:

- ❑ Client truy vấn một máy chủ gốc (root server) để tìm **com DNS server**
- ❑ Client truy vấn **com DNS server** để có được **amazon.com DNS server**
- ❑ Client truy vấn **amazon.com DNS server** để có được địa chỉ IP của **www.amazon.com**

DNS: Các máy chủ tên gốc (root name servers)

- ❑ được liên hệ bởi máy chủ tên cục bộ (local name server) khi nó không thể phân giải tên
- ❑ máy chủ gốc có thể hoạt động như sau:
 - liên hệ với máy chủ tên có thẩm quyền (authoritative name server) nếu ánh xạ tên không được biết đến
 - lấy ánh xạ tên
 - trả lại ánh xạ tên cho máy chủ tên cục bộ
 - Nhận xét?



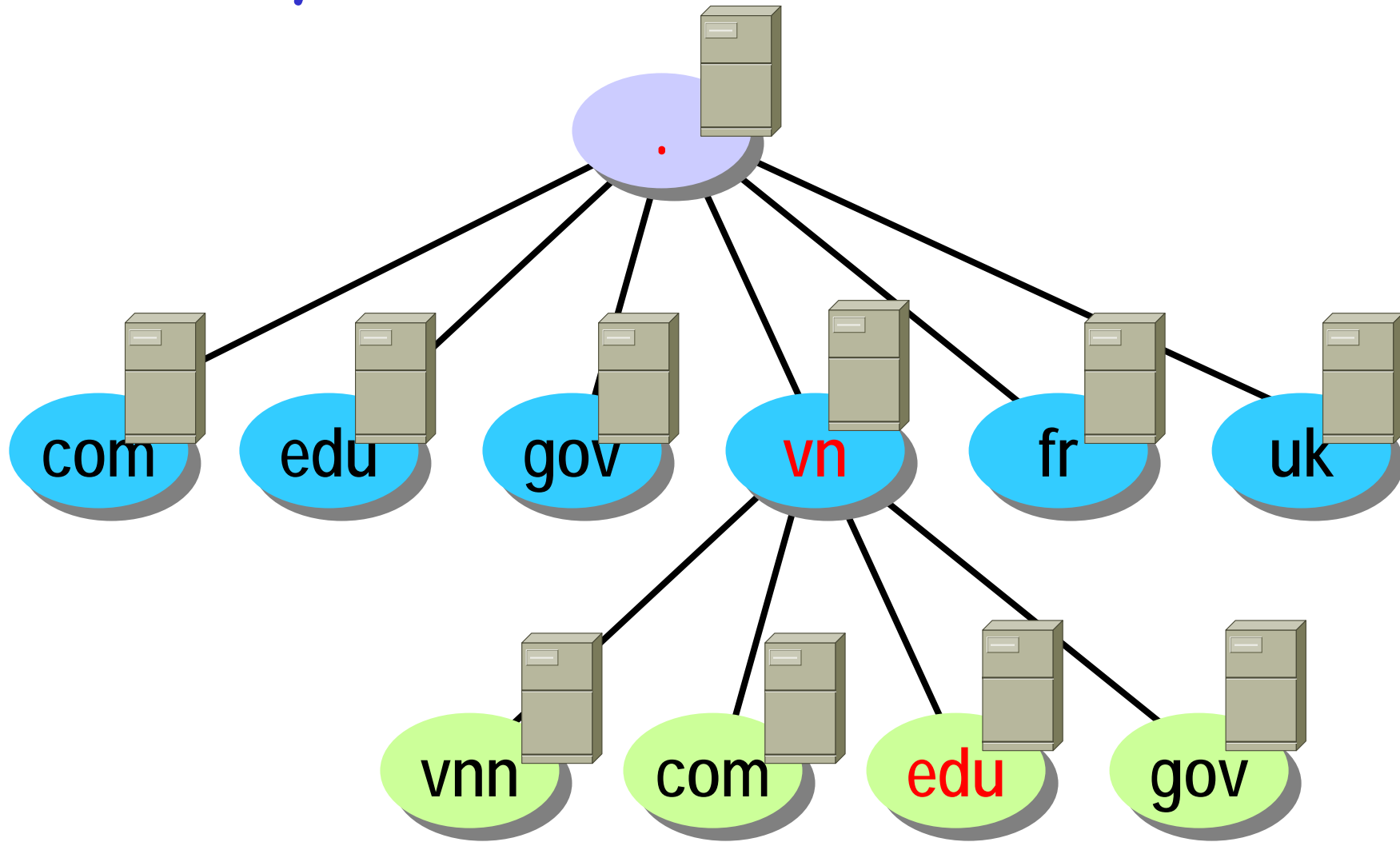
TLD và Authoritative Servers

- ❑ **Top-level domain (TLD) servers:** chịu trách nhiệm cho các tên miền com, org, net, edu, vv..., và tất cả các tên miền quốc gia cấp cao nhất như vn, kr, uk, fr, ca, jp.
 - Network solutions duy trì các máy chủ tên cho com TLD
 - Educause cho edu TLD
- ❑ **Authoritative DNS servers:** các máy chủ DNS của các tổ chức, cung cấp sự ánh xạ theo thẩm quyền giữa tên trạm và địa chỉ IP cho các máy chủ của tổ chức (vd, Web và mail server).
 - Có thể được duy trì bởi tổ chức hoặc nhà cung cấp dịch vụ

Máy chủ tên cục bộ (Local Name Server)

- ❑ Không hoàn toàn thuộc về hệ thống phân cấp
- ❑ Mỗi ISP (ISP cấp địa phương, công ty, trường đại học...) có một máy chủ tên cục bộ.
 - Còn được gọi là "default name server"
- ❑ Khi một trạm thực hiện một truy vấn DNS, truy vấn đó sẽ được gửi đến máy chủ tên cục bộ của nó
 - Đóng vai trò như là một proxy (ủy quyền), chuyển tiếp truy vấn đến hệ thống phân cấp.

DNS: System



Phân giải tên

- ❑ http://www.microsoft.com/technet/itsolutions/network/evaluate/technol/tcpipfund/tcpipfund_ch08.mspx

Resolver/Thiết bị giải

- ❑ Các chương trình DNS client được dùng để tra cứu thông tin tên DNS.

Name Resolution/Phân giải tên

- ❑ Hai loại truy vấn mà một thiết bị giải tên DNS (một DNS client hay một DNS server khác) có thể sử dụng để truy vấn một DNS server:

Recursive queries/Các truy vấn đệ quy

- ❑ Trong một truy vấn đệ quy, name server bị truy vấn được yêu cầu trả lời với dữ liệu được yêu cầu hoặc với một lỗi nói về dữ liệu của loại được yêu cầu hoặc tên miền được chỉ định là không tồn tại.
- ❑ Name server không thể chỉ chuyển DNS resolver đến một name server khác.
- ❑ Một **DNS client** thường gọi loại truy vấn này.

Iterative queries/Truy vấn lặp lại

- ❑ Trong một **iterative query**, name server bị truy vấn có thể trả lại câu trả lời tốt nhất mà hiện tại nó có cho DNS resolver.
- ❑ Câu trả lời tốt nhất có thể là tên được phân giải hoặc một sự chuyển đến name server khác mà nó gần hơn để đáp ứng yêu cầu gốc của DNS client.
- ❑ **DNS servers** thường gọi **iterative queries** để truy vấn các DNS servers khác.

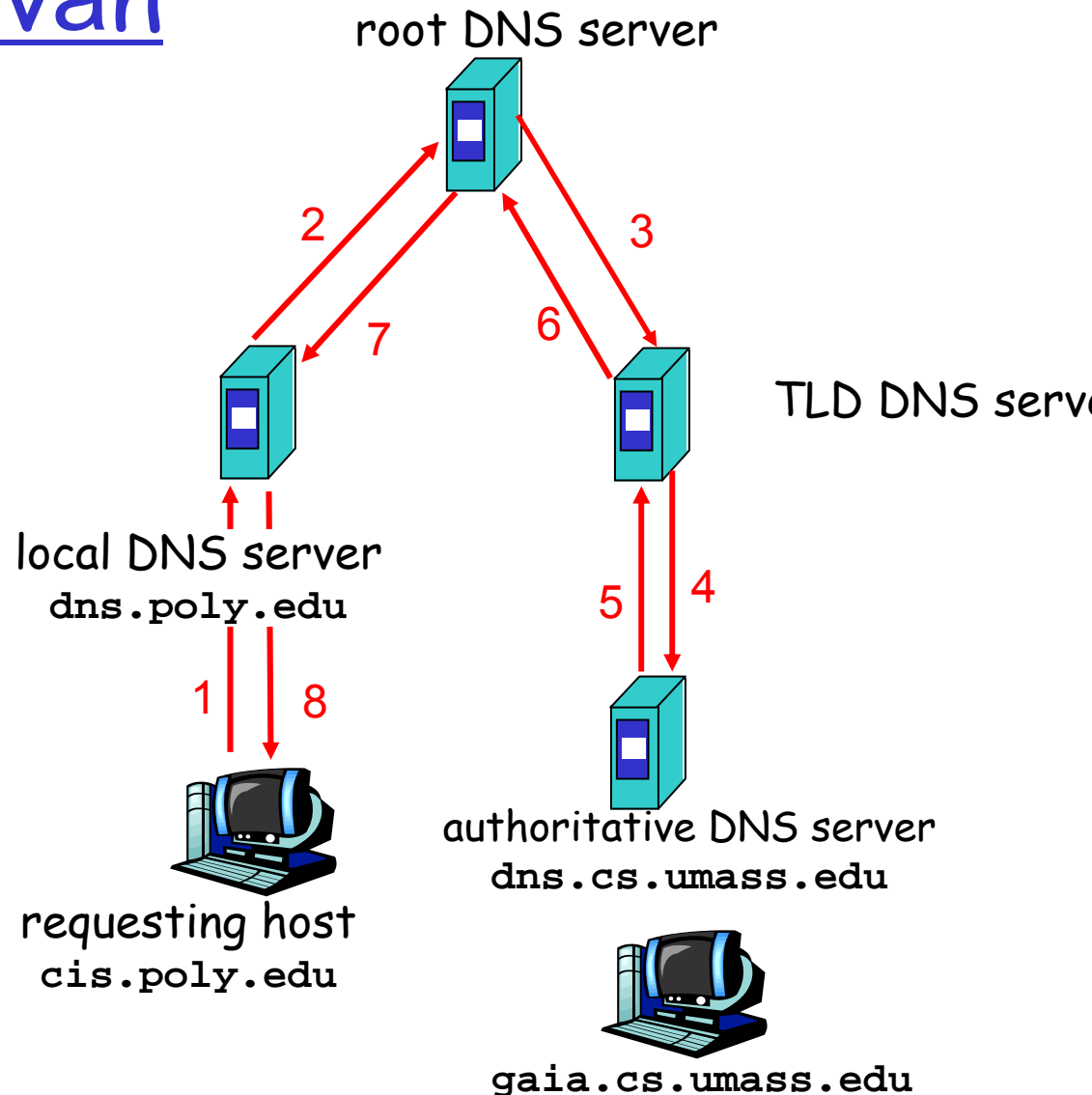
Các loại truy vấn

truy vấn đệ quy:

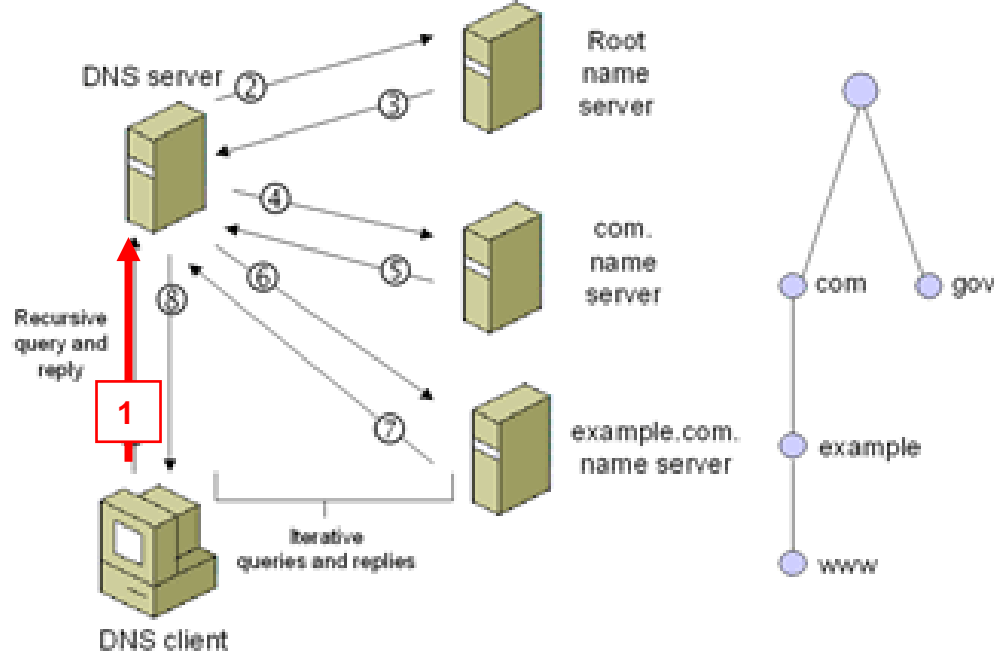
- ❑ đặt gánh nặng phân giải tên lên máy chủ tên được liên hệ
- ❑ tải nặng?

truy vấn lặp lại:

- ❑ máy chủ được liên hệ trả lời với tên của máy chủ khác để liên hệ
- ❑ “tôi không biết tên đó, nhưng hỏi máy chủ này”

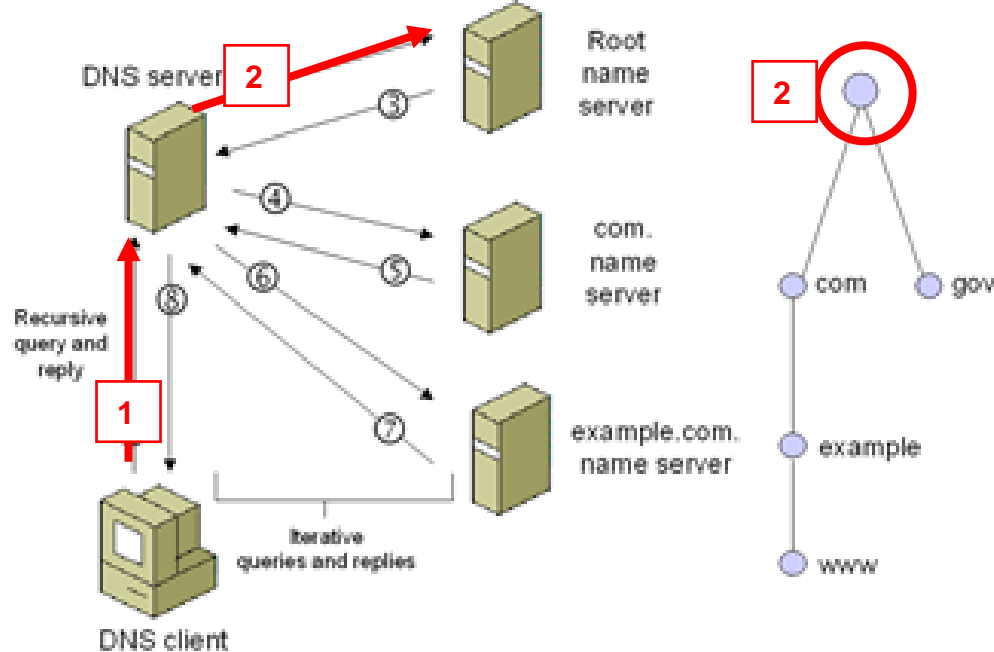


Ví dụ về phân giải tên DNS



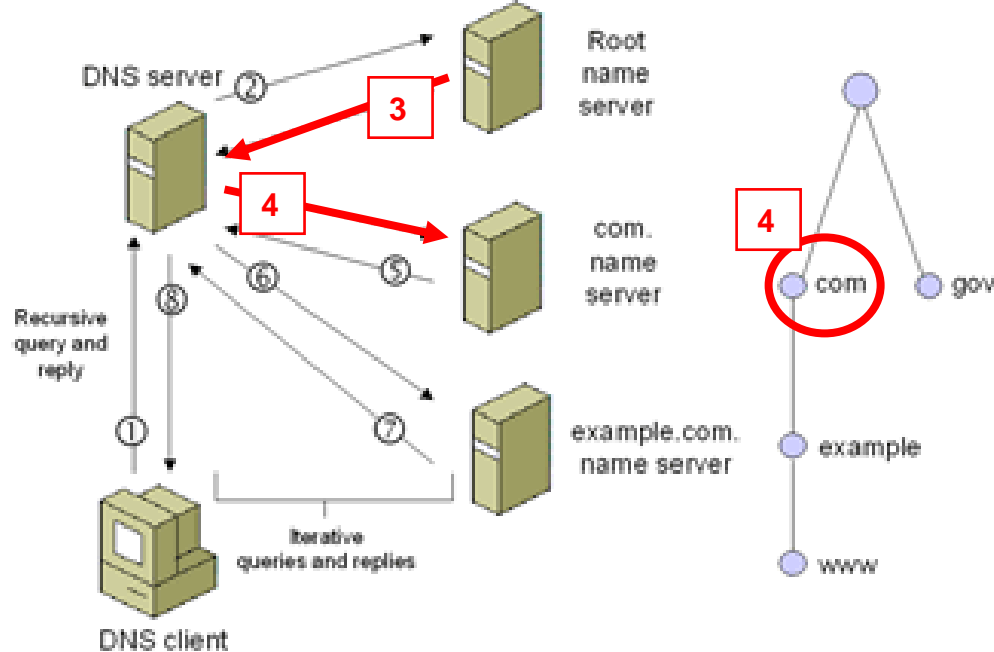
- ❑ Để thấy được các truy vấn đệ quy và truy vấn lặp lại được sử dụng như thế nào trong các phân giải tên DNS phổ biến, xem xét một máy tính chạy hệ điều hành Microsoft Windows® XP hoặc Windows Server 2003 được kết nối vào Internet.
- ❑ Một người sử dụng gõ **http://www.example.com** trong trường địa chỉ/Address của trình duyệt Internet explorer.
- ❑ Khi người sử dụng nhấn phím ENTER, trình duyệt thực hiện một lời gọi hàm Windows Sockets, hoặc là *gethostbyname()* hay *getaddrinfo()*, để phân giải tên **www.example.com** thành địa chỉ IP.
- ❑ Về phần DNS của tiến trình phân giải tên trong Windows, những bước sau diễn ra:

Ví dụ về phân giải tên DNS



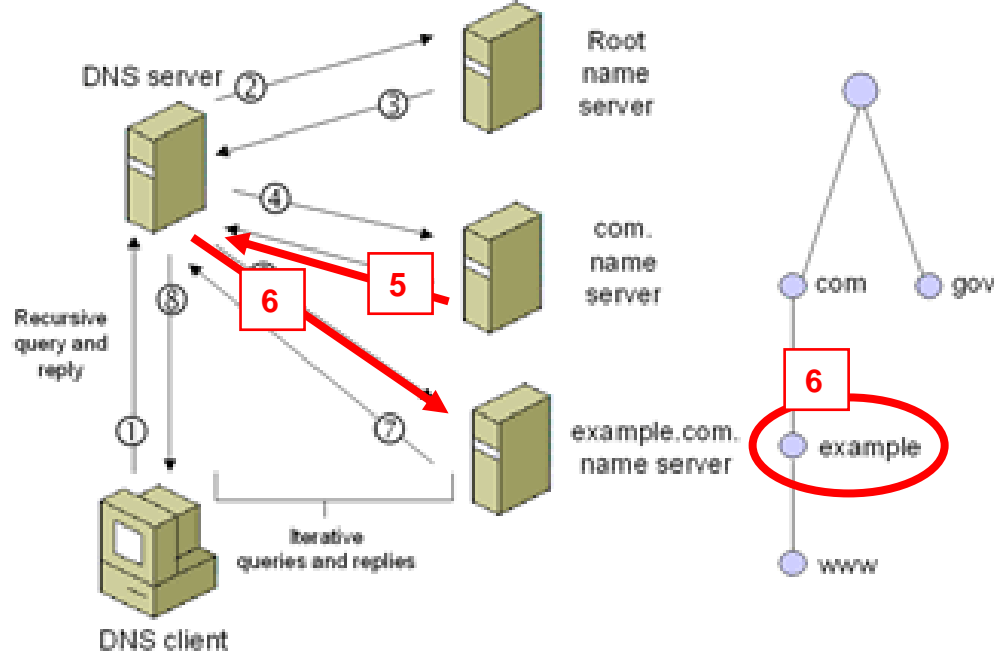
- ❑ 1. DNS resolver trên DNS client gửi một **recursive query** đến DNS server đã được cấu hình trước của nó, yêu cầu địa chỉ IP cho tên tương ứng "**www.example.com**".
 - DNS server của client đó chịu trách nhiệm phân giải tên và không thể chuyển DNS client đó đến một DNS server khác.
- ❑ 2. DNS server nhận được **recursive query** ban đầu đó kiểm tra vùng/zone của nó và không tìm thấy vùng tương ứng với tên miền được yêu cầu; DNS server này không phải DNS có thẩm quyền/authoritative cho miền **example.com**.
 - Bởi vì DNS server này không có thông tin về địa chỉ IP của các DNS servers là thẩm quyền **example.com** hay **com**, nó gửi một **iterative query** cho **www.example.com** đến một máy chủ tên gốc/root name server.

Ví dụ về phân giải tên DNS



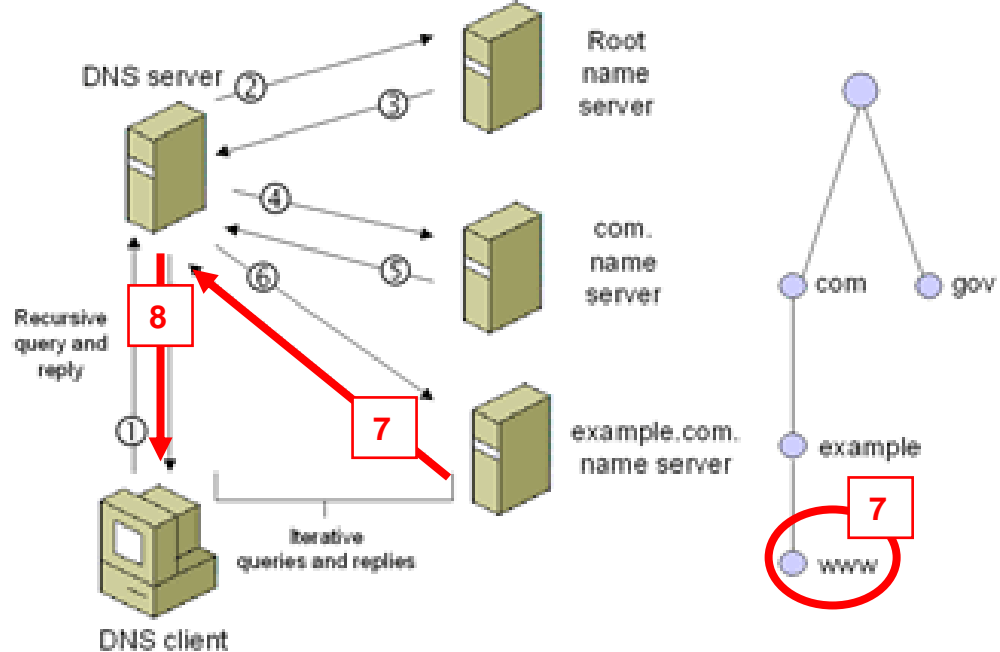
- ❑ 3. **Máy chủ tên gốc** có thẩm quyền cho miền gốc và có thông tin về các máy chủ tên là thẩm quyền của của cho các tên miền cấp đỉnh/top-level domain names.
 - Nó **không** có thẩm quyền cho tên miền **example.com**..
 - Do đó, root name server này trả lời với địa chỉ IP của một máy chủ tên cho top-level domain **com**..
- ❑ 4. **DNS server** của DNS client đó gửi một **iterative query** cho **www.example.com** đến máy chủ tên là thẩm quyền cho top-level domain **com**..

Ví dụ về phân giải tên DNS



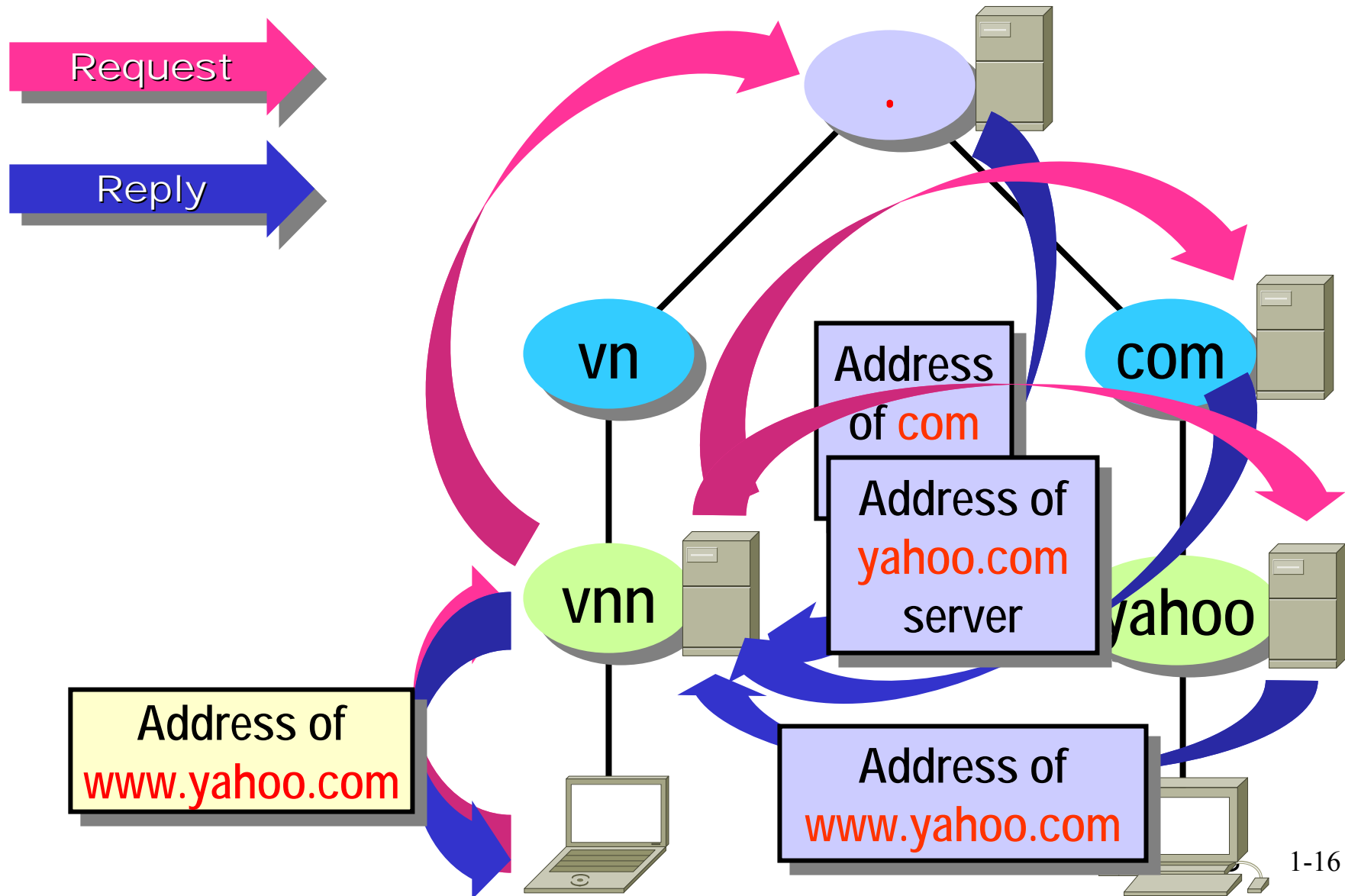
- ❑ 5. **com. name server** là **thẩm quyền** cho miền **com**. và có thông tin về các địa chỉ IP của các máy chủ tên là thẩm quyền cho các tên miền cấp hai/second-level domain names của miền **com**.
 - Nó **không** là thẩm quyền cho miền **example.com**..
 - Do đó, **com. name server** trả lời với địa chỉ IP của máy chủ tên là thẩm quyền cho miền **example.com**..
- ❑ 6. **DNS server** của DNS gửi một **iterative query** cho **www.example.com**. đến máy chủ tên là thẩm quyền của miền **example.com**..

Ví dụ về phân giải tên DNS



- ❑ 7. **example.com.** name server trả lời với địa chỉ IP tương ứng với tên miền tiêu chuẩn đầy đủ/**FullyQualifiedDomainName** **www.example.com.**
- ❑ 8. DNS server gửi địa chỉ IP của **www.example.com** cho DNS client.

DNS: Resolve `www.yahoo.com`



DNS: cất trữ (caching) và cập nhật các bản ghi

- ❑ mỗi khi name server học một ánh xạ, nó *cất trữ (caches)* ánh xạ đó
 - các mục được cache sẽ hết hiệu lực (biến mất) sau một khoảng thời gian nào đó: *trạng thái mềm*
 - các TLD servers thường được cache trong các local name servers
 - do đó các root name servers thường ít bị đến thăm
- ❑ các cơ chế cập nhật/thông báo được thực hiện theo sự chỉ định của IETF
 - RFC 2136
 - <http://www.ietf.org/html.charters/dnsind-charter.html>

Các bản ghi DNS

DNS: cơ sở dữ liệu phân tán lưu giữ các bản ghi tài nguyên - resource records- (RR)

khuôn dạng RR: (name, value, type, ttl)

❑ Type=A

- name là tên trạm
- value là địa chỉ IP

❑ Type=NS

- name là miền (ví dụ foo.com)
- value là tên trạm của máy chủ tên có thẩm quyền (authoritative name server) của tên miền đó

❑ Type=CNAME

- name là tên bí danh cho một số tên "chuẩn" ("canonical" - tên thật)

www.ibm.com thật ra là
servereast.backup2.ibm.com

- value là tên thật

❑ Type=MX

- value là tên của mailserver được kết hợp với name

Giao thức DNS, các thông điệp

Giao thức DNS: các thông điệp *request* và *reply*, cả hai dạng có cùng *khuôn dạng thông điệp*

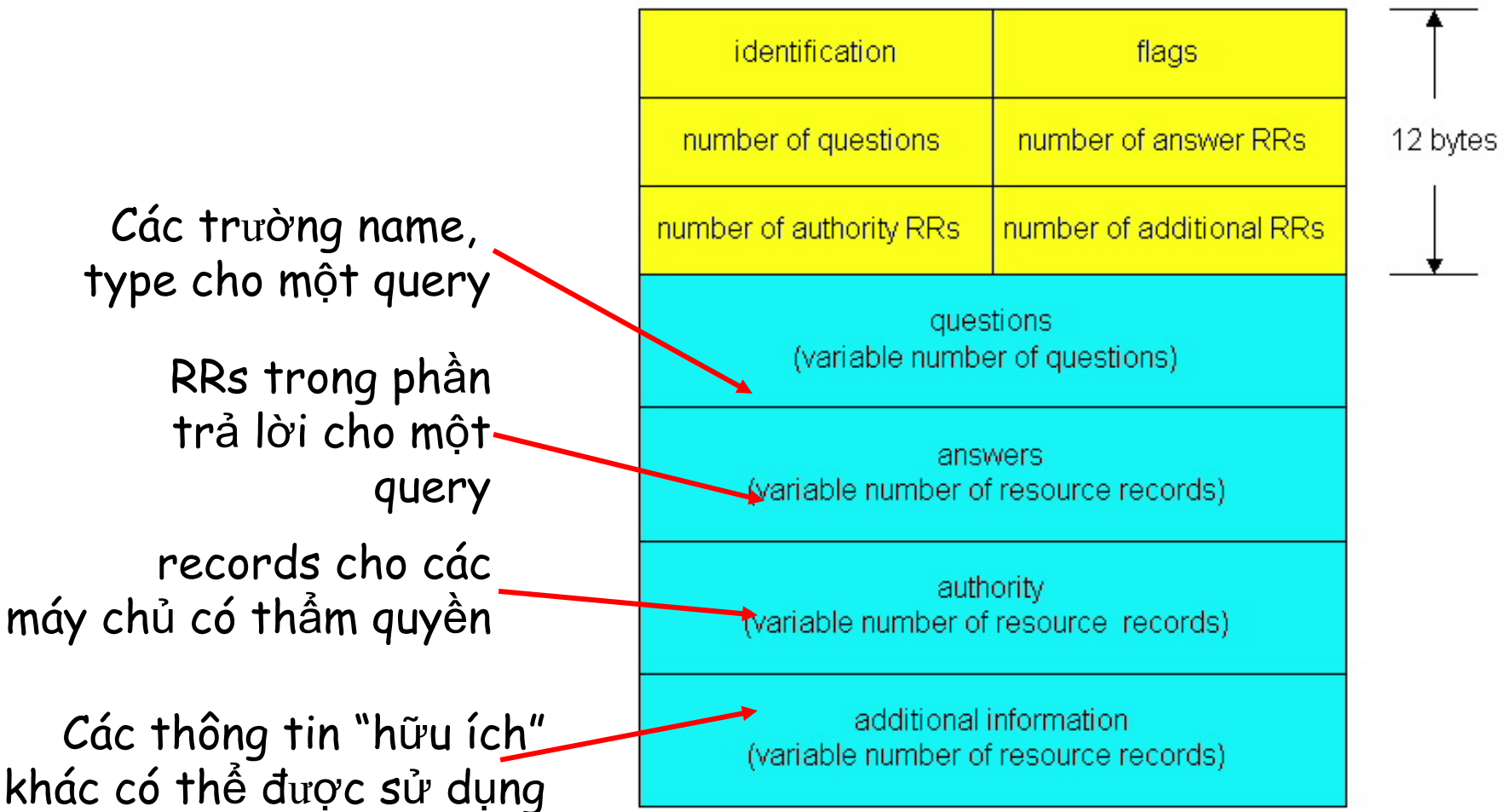
phần đầu của thông điệp

- ❑ **identification**: số 16 bits định danh cho query, reply cho query này sử dụng cùng số
- ❑ **flags**:
 - query hay reply
 - đệ quy được đề nghị
 - đệ quy sẵn có
 - reply là chính thức (có thẩm quyền)

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)	



Giao thức DNS, các thông điệp



Chèn các bản ghi vào DNS

- ❑ Ví dụ: mạng "Network Utopia" vừa mới được khởi động
- ❑ Đăng ký tên networkutopia.com tại một **nhà đăng ký - registrar** (ví dụ, Network Solutions)
 - Cần phải cung cấp cho registrar các thông tin về tên và địa chỉ IP **authoritative name server** của bạn (primary và secondary)
 - Registrar chèn hai RRs và trong **com TLD server**:

(networkutopia.com, dns1.networkutopia.com, NS)

(dns1.networkutopia.com, 212.212.212.1, A)

- ❑ Thêm vào máy chủ có thẩm quyền bản ghi loại/Type A cho www.networkutopia.com và bản ghi Type MX cho networkutopia.com
- ❑ **Làm thế nào để mọi người lấy địa chỉ IP của Web site chúng ta?**