QUẢN TRỊ DỊCH VỤ TÊN MIỀN (DOMAIN NAME SYSTEM - DNS)

Tổng quan

1. DNS là gì
2. Vai trò máy chủ DNS
3. Cơ sở dữ liệu của DNS
4. Cài đặt và Cấu hình DNS

Giới thiệu về DNS (Domain Name System)

- DNS là giải pháp dùng tên luận lý (tên miền) thay cho địa chỉ IP khó nhớ khi sử dụng các dịch vụ trên mạng

- **Ví dụ: www.fit.iuh.edu.vn**

- vn: Việt nam
- edu: Tổ chức thuộc lĩnh vực giáo dục
- iuh: Đại học Công Nghiệp Tp.HCM
- fit : Khoa CNTT
- www: Tên máy tính làm dịch vụ web của khoa CNTT

Giới thiệu về DNS

- Mỗi host trên Internet sẽ có 2 địa chỉ:
  - Địa chỉ IP
  - Địa chỉ tên miền
- Các tên miền được xây dựng như sau:
  - Nhóm chữ đầu tiên bên phải (còn gọi là Domain quốc gia)
    - gồm 2 chữ cái, qui định cho nước tham gia Internet.

Tên miền DNS

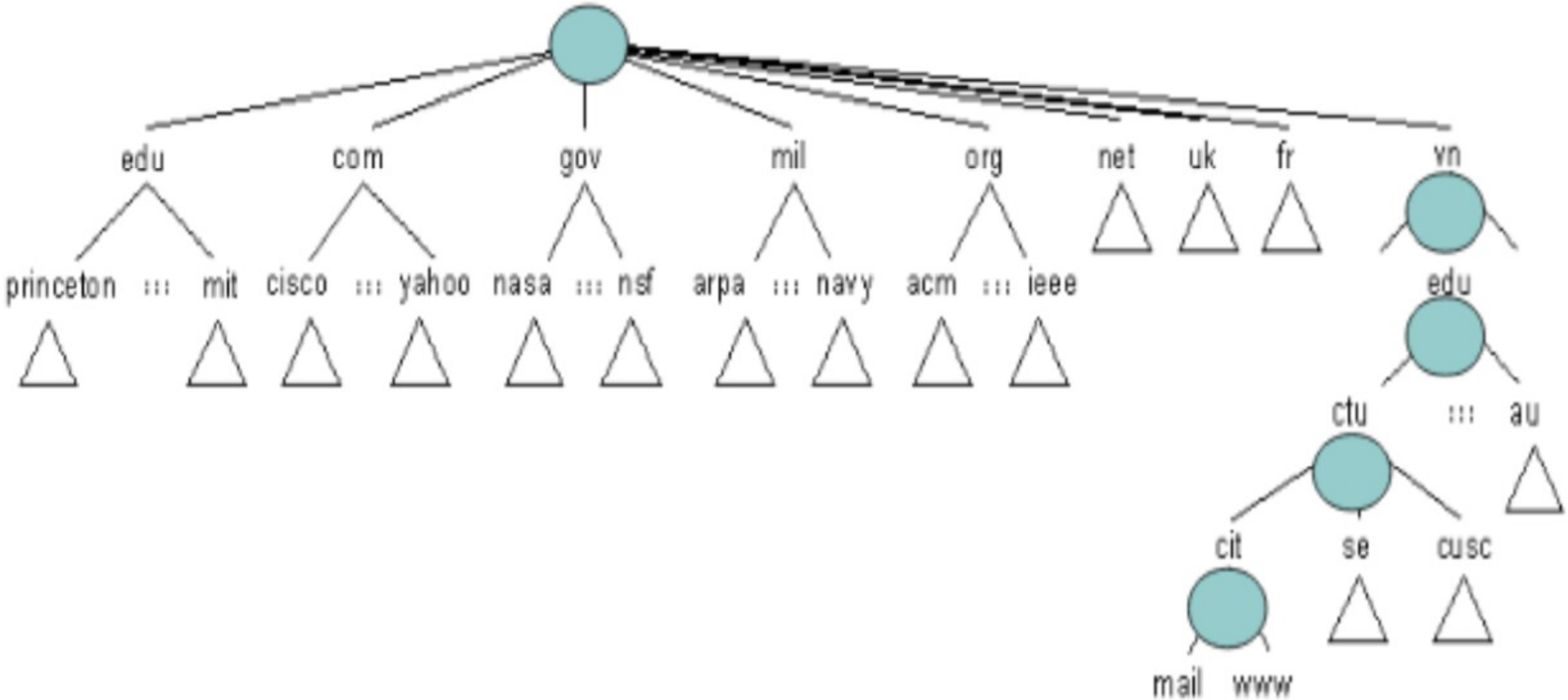
DOMAIN	QUỐC GIA
at	Áo
au	Autralia
ca	Canada
de	Đức
fr	Pháp
jp	Nhật
uk	Anh
us (hoặc không ghi)	Mỹ
vn	Việt Nam

Tên miền DNS – tổ chức

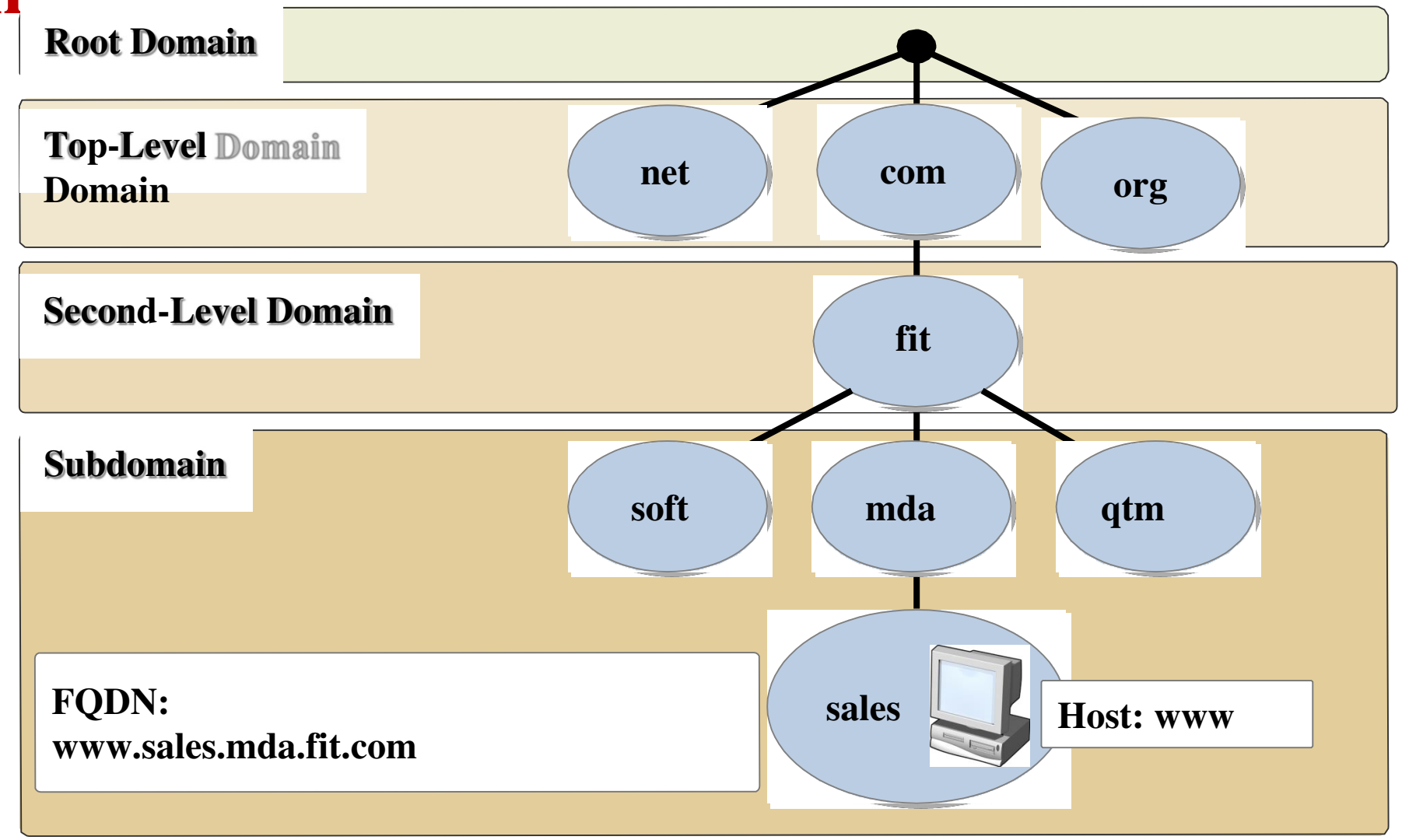
- Tên miền DNS – tổ chức
  - Nhóm chữ cái thứ hai (còn gọi là domain tổ chức) : được tính

Domain	Tổ chức
Com (commercial)	Thương mại
Edu (education)	Giáo dục
Gov (Government)	Nhà nước
Int (International)	Tổ chức quốc tế
Net (Networking)	Tài nguyên trên mạng
Org(organization)	Các tổ chức khác
Mil (military)	Tên miền sử dụng cho quân đội

Name Server trên Internet



Tổng quan về hệ thống không gian tên miền



Cải tiến DNS trong Windows Server 2012

- Những tính năng mới của DNS trong WServer 2012:
  - Tải vùng ở chế độ nền
  - Hỗ trợ IPv6
  - Hỗ trợ read-only domain controllers
  - Tên toàn cầu duy nhất

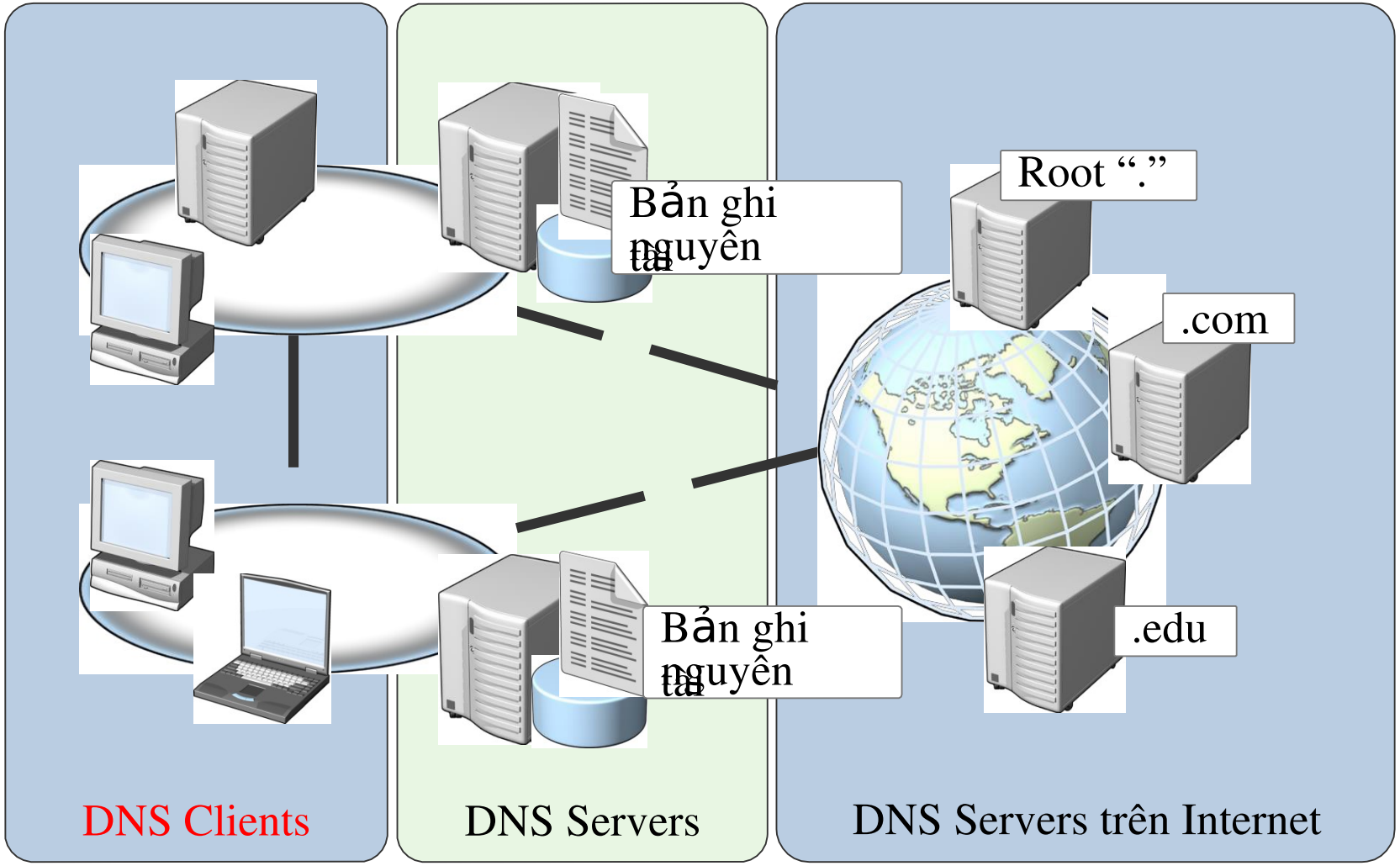
Triển khai máy chủ DNS

- Tài khoản người dùng phải là thành viên của nhóm quản trị
  hoặc tương đương
- Cấu hình máy chủ DNS sử dụng IP tĩnh
- Không nên thay đổi máy chủ và tập tin khởi động
- Sử dụng DNS console hoặc dnscmd
- Vùng DNS tích hợp với Active Directory không thể quản lý bằng cách sử dụng một công cụ soạn thảo

Cấu hình vai trò máy chủ DNS

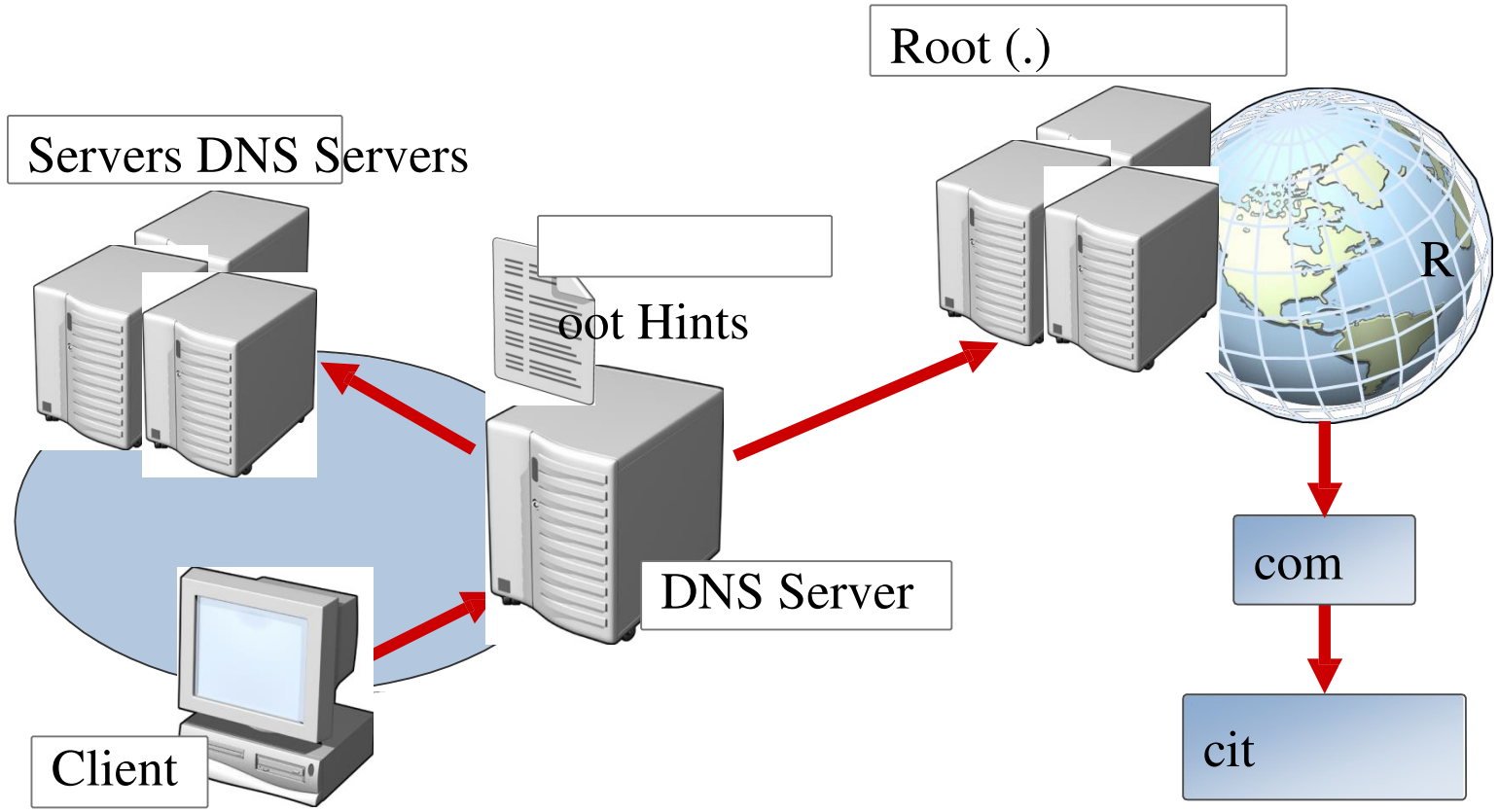
- Các thành phần của một giải pháp DNS là gì?
- Bản ghi tài nguyên DNS
- Root Hints là gì?
- Một truy vấn DNS là gì?
- Truy vấn đệ quy là gì?
- Truy vấn lặp là gì?
- Chuyển tiếp (Forwarder) là gì?
- Chuyển tiếp có điều kiện là gì?
- Lưu trữ đệm làm việc thế nào

Các thành phần của một giải pháp DNS là gì?



Root Hints là gì?

Root hints chứa địa chỉ IP cho máy chủ DNS gốc



Một truy vấn DNS là gì?

- Truy vấn là một yêu cầu phân giải tên được gởi đến một máy chủ DNS
  - Có 2 loại truy vấn: đệ quy và lặp
  - Máy trạm DNS và máy chủ DNS cả hai bắt đầu truy vấn
  - Các máy chủ DNS có hoặc không có thẩm quyền trên một không gian tên miền
  - Một máy chủ DNS có thẩm quyền đối với không gian tên miền sẽ:
    - Trả về địa chỉ IP yêu cầu
    - Trả về một quyền "No"
  - Một máy chủ DNS không có thẩm quyền đối với không gian tên miền sẽ:
    - Kiểm tra bộ nhớ cache của nó
    - Sử dụng chuyển tiếp

Cơ chế hoạt động của DNS

- User yêu cầu máy cục bộ truy cập dịch vụ nào đó của 1 host trên internet bằng tên miền đã biết của host đó.

- Máy tính chỉ liên lạc bằng đc IP, nên khi nhận lệnh này, bước đầu tiên là phải điều tra xem IP của cái gọi là www.guci.com là bao nhiêu
- Đó là khi cỗ máy DNS bắt đầu vận hành.

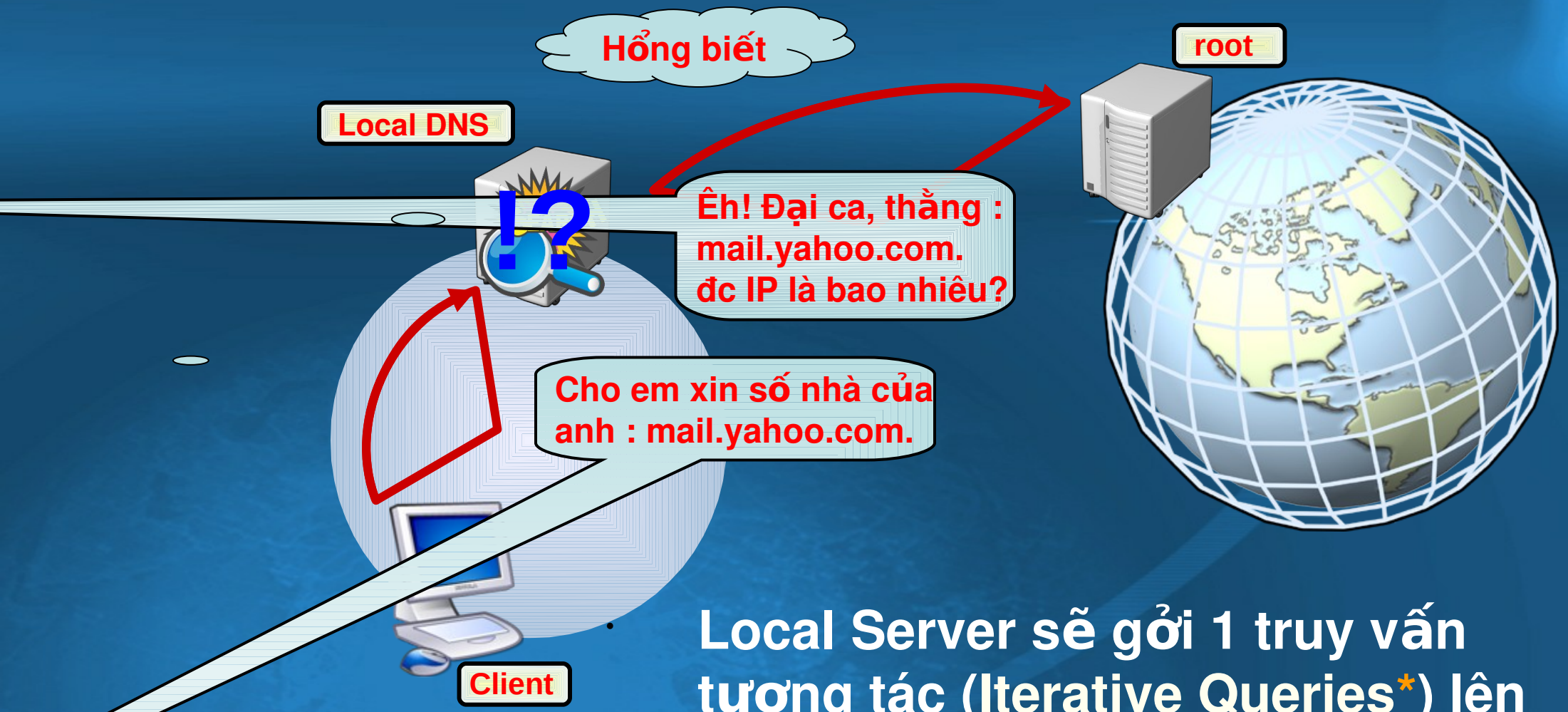
- Host gởi lên Local DNS Server một truy vấn đệ quy (Recursive Queries*) nhờ giải đáp .
- Lúc này đối với Local Server DNS có 2 trường hợp xảy ra.

1. Máy này nằm trong Zone nó quản lý, hoặc trong cache của nó đã có thông tin : Đã có.
2. Máy này không nằm trong Zone nó quản lý, và trong cache của nó không có thông tin nào về máy này : Chưa có.

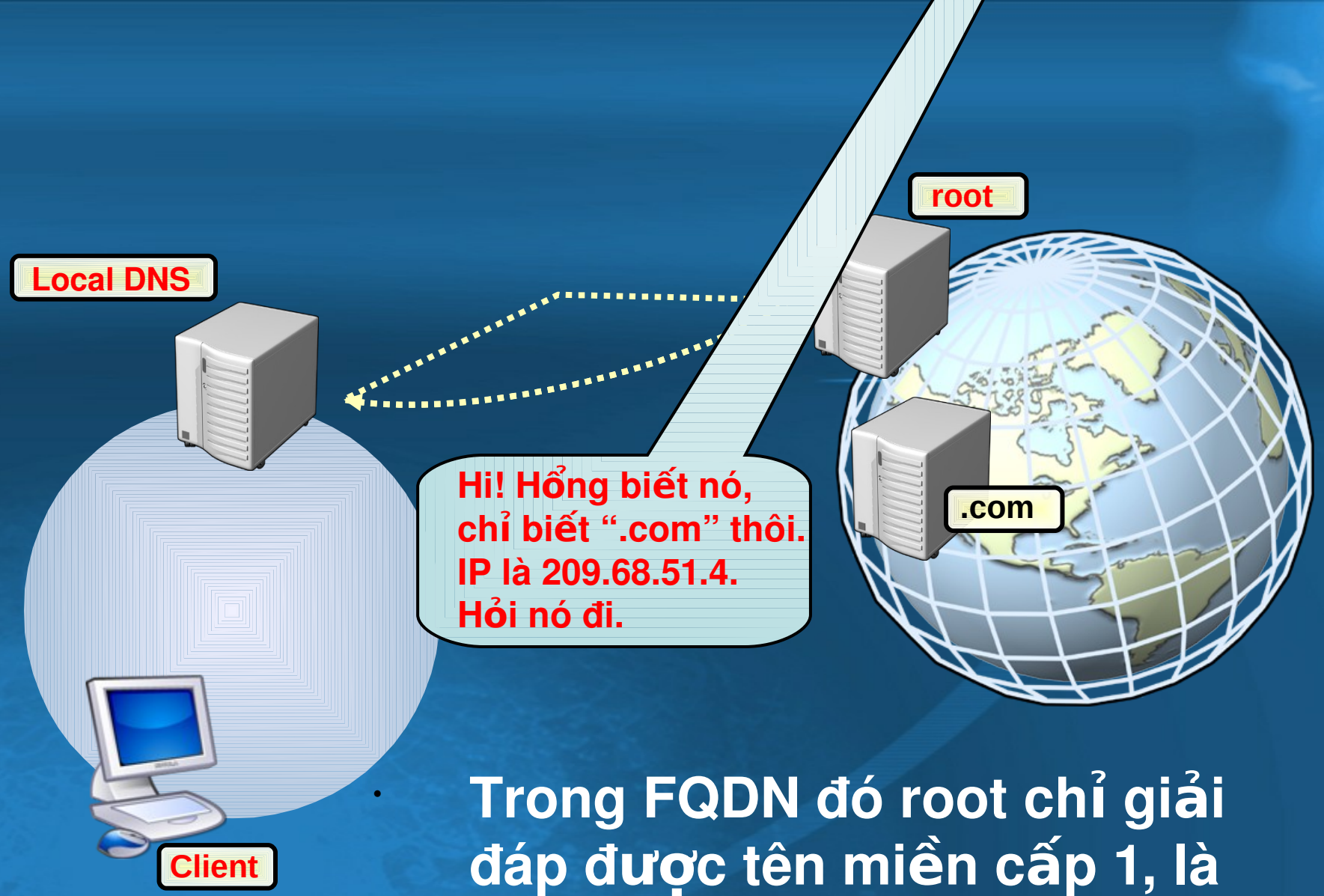
* TRƯỜNG HỢP 1 .

- Khi nhận được truy vấn từ client, DNS server sẽ tìm trong cache hoặc trong CSDL của nó đcIP tương ứng của host mà client cần truy vấn, rồi hồi đáp lại cho client.

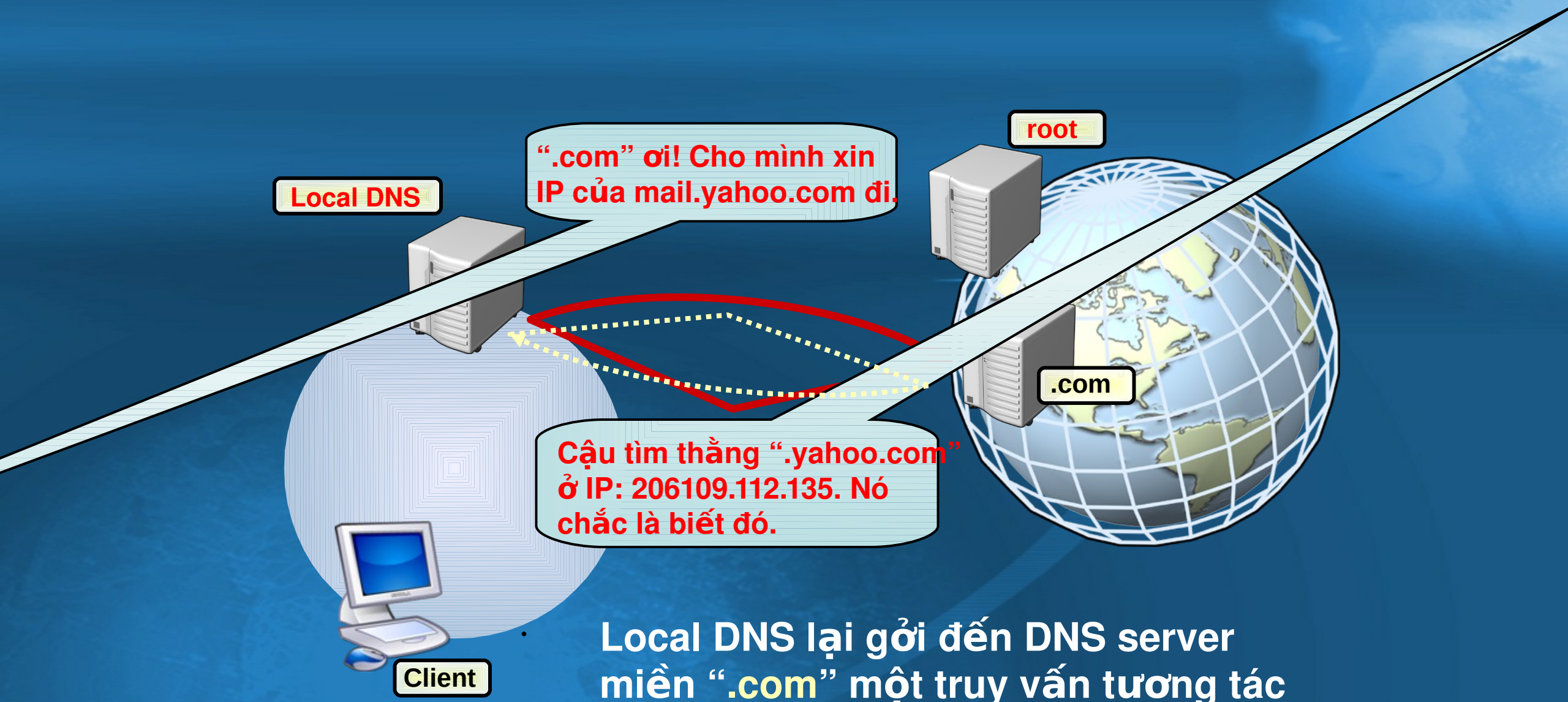
* TRƯỜNG HỢP 2 .



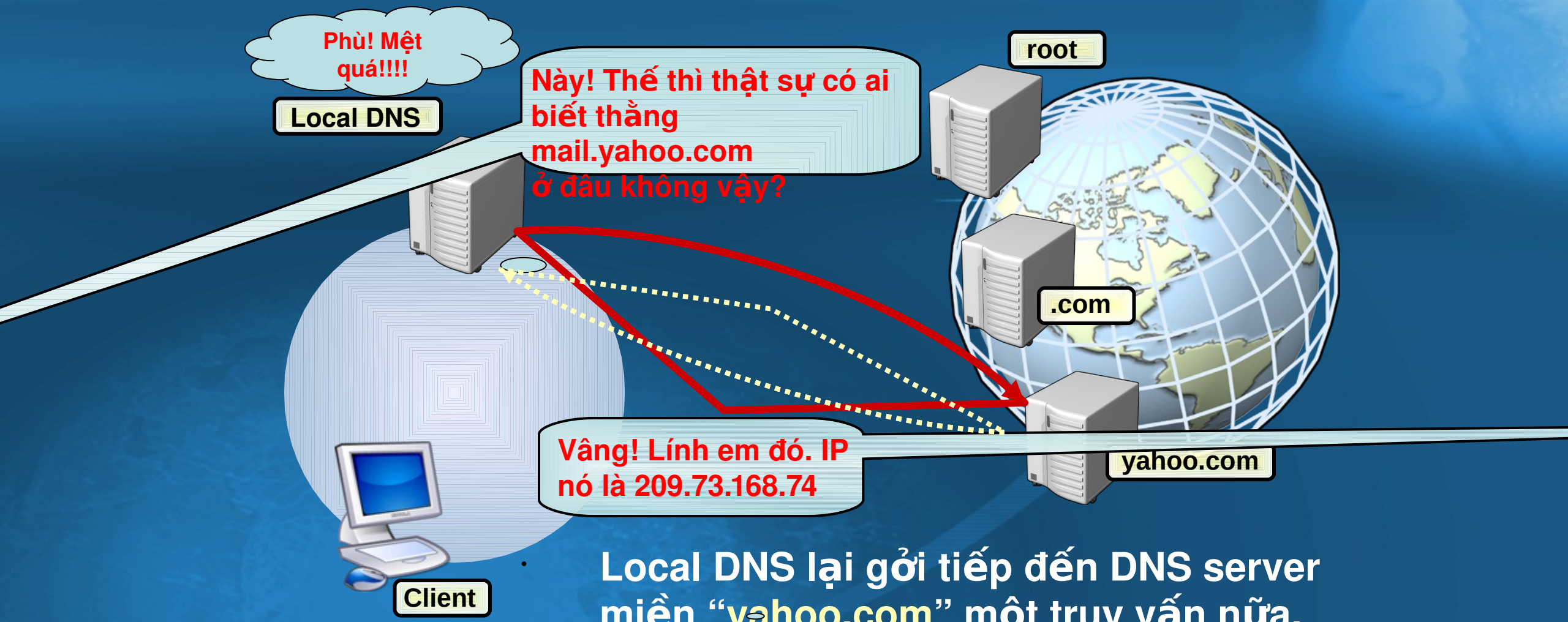
Local Server sẽ gởi 1 truy vấn tương tác (Iterative Queries*) lên Root Hints, hỏi địa chỉ của mail.yahoo.com



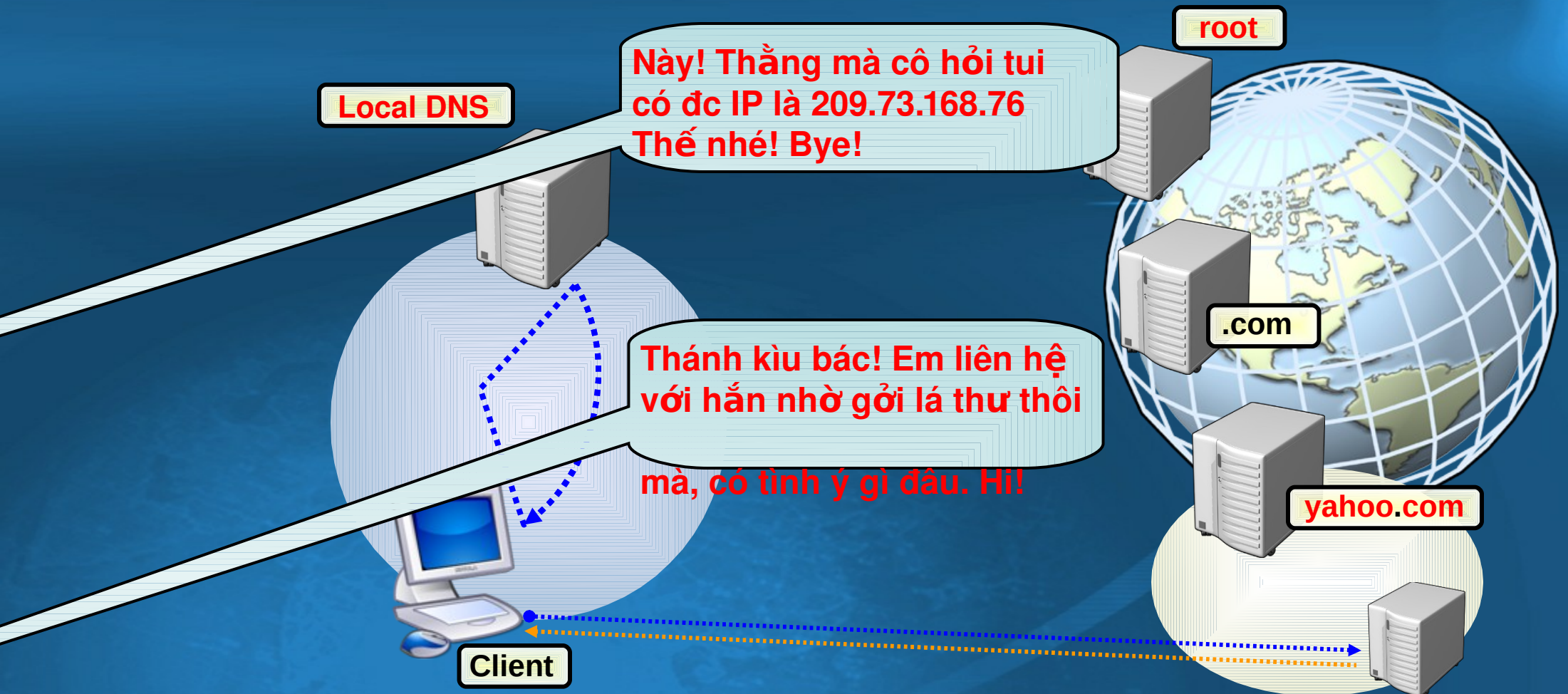
- Trong FQDN đó root chỉ giải đáp được tên miền cấp 1, là miền nó quản lý. Đó là kết quả tốt nhất mà nó biết.



- Local DNS lại gởi đến DNS server miền “.com” một truy vấn tương tác
- Và server này cũng trả lời bằng kết quả tốt nhất mà nó có.

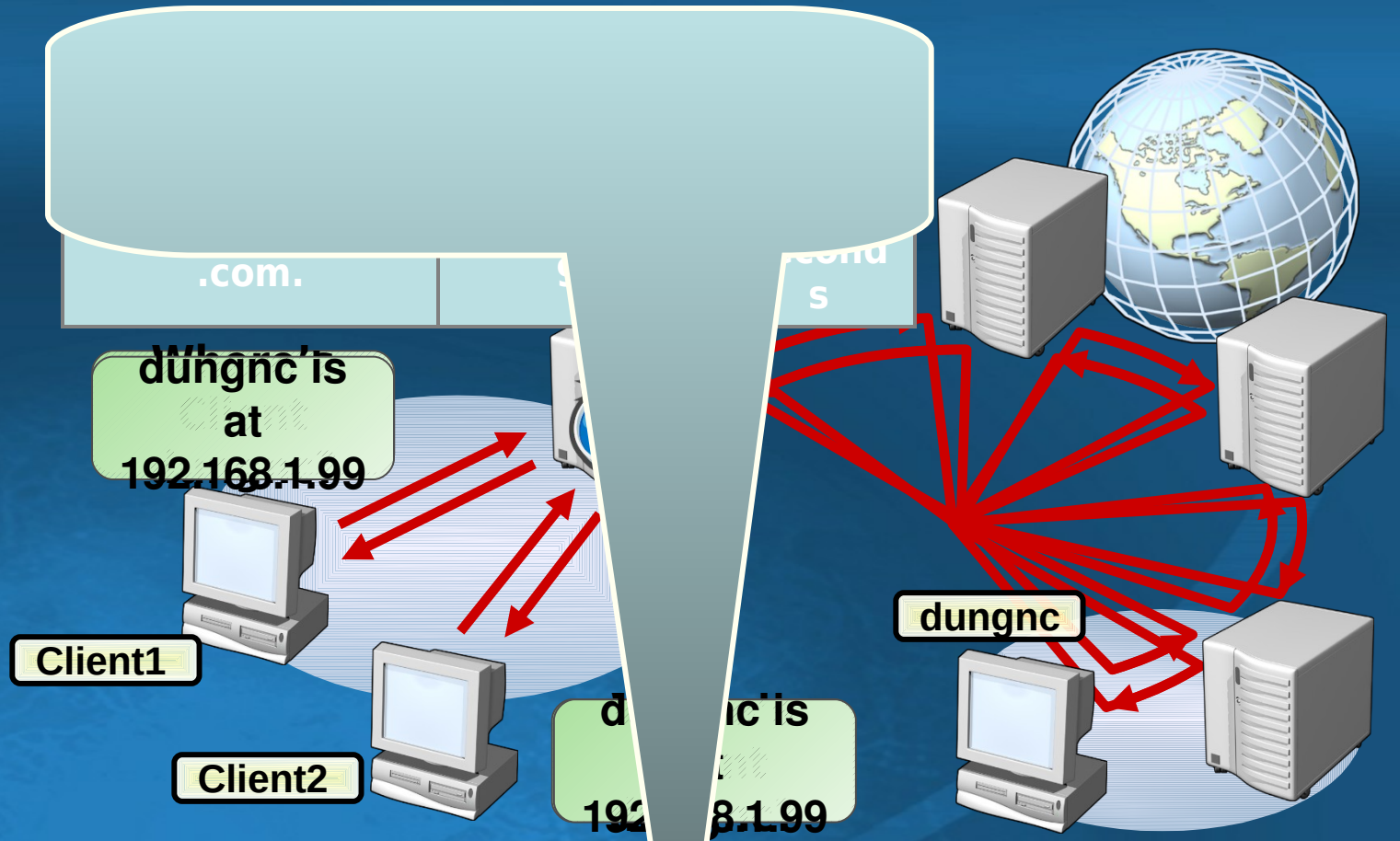


- Local DNS lại gởi tiếp đến DNS server miền "yahoo.com" một truy vấn nữa.
- Zone này do nó quản lý, nên Name Server này trả lời chính xác được truy vấn đó.



- Bây giờ Local DNS đã biết chính xác IP của mail.yahoo.com để trả lời cho client.

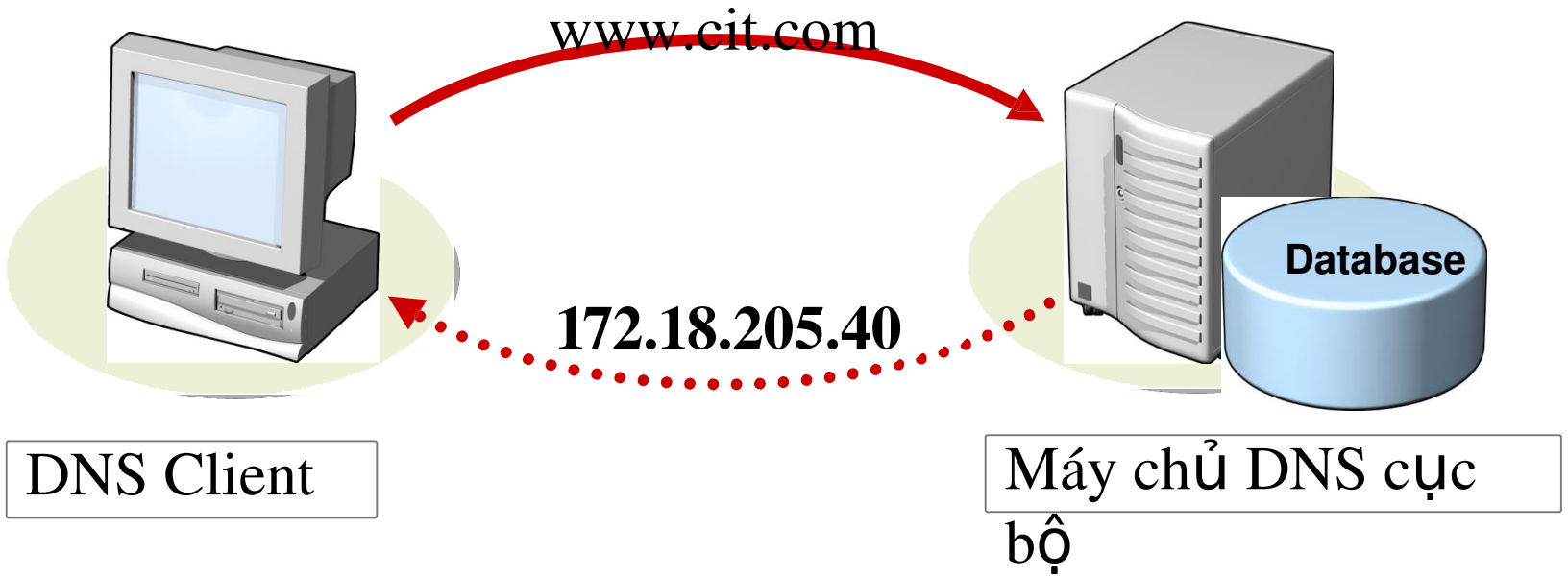
* caching.



Caching là một phương pháp lưu giữ những thông tin vừa được truy cập gần đây vào trong bộ nhớ riêng biệt của hệ thống, để lần sau nếu truy cập lại địa chỉ này sẽ nhanh hơn vì không phải tìm một lần nữa.

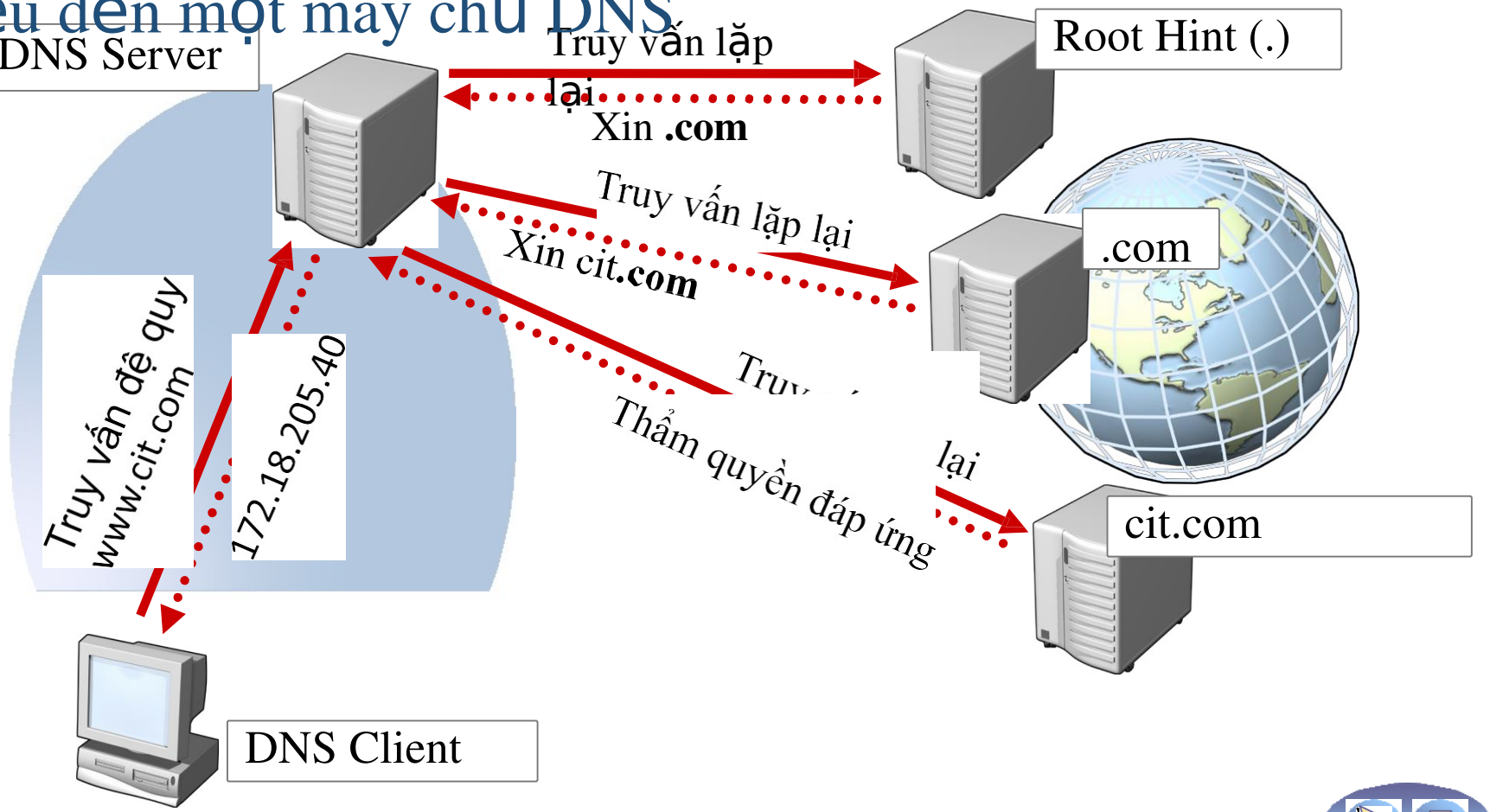
Truy vấn đệ quy là gì?

Một câu truy vấn đệ quy được gửi tới một máy chủ DNS và yêu cầu một câu trả lời hoàn chỉnh



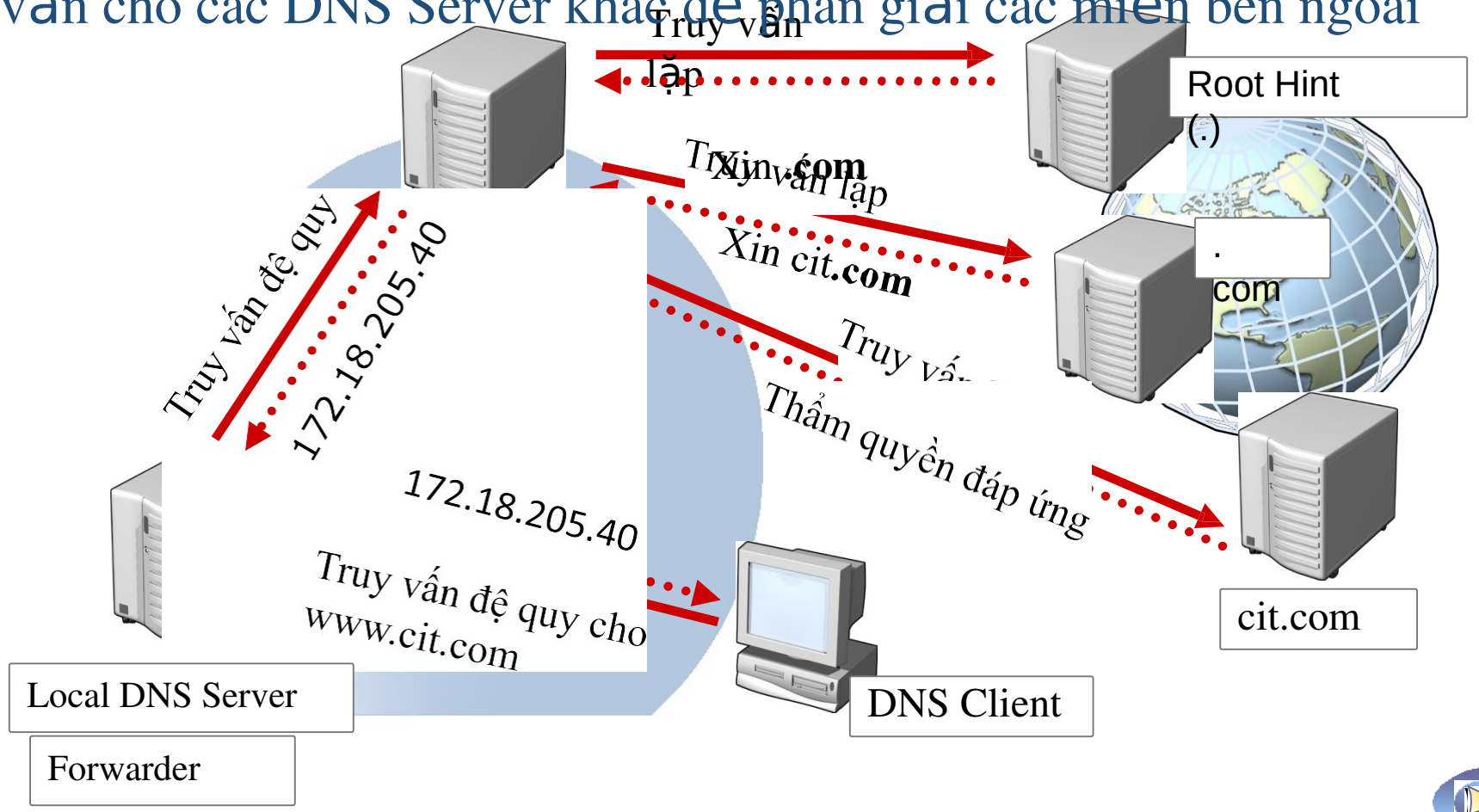
Truy vấn lặp là gì?

Một truy vấn lặp gởi đến một máy chủ DNS có thể được trả lời với một
giới thiệu đến một máy chủ DNS



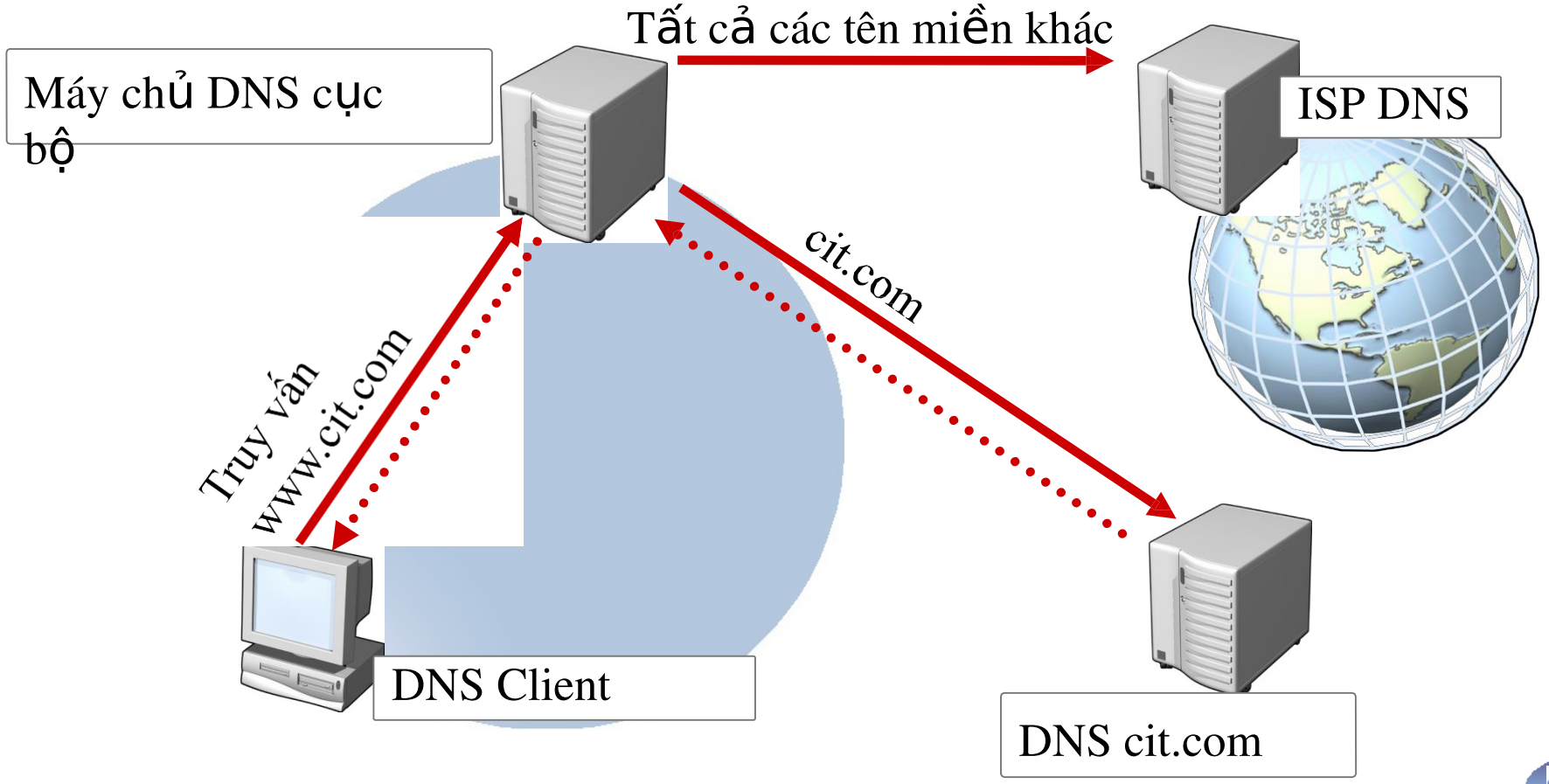
Chuyển tiếp là gì?

Chuyển tiếp (forwarder) là kỹ thuật cho phép DNS Server cục bộ chuyển yêu cầu
truy vấn cho các DNS Server khác để phân giải các miền bên ngoài



Chuyển tiếp có điều kiện là gì?

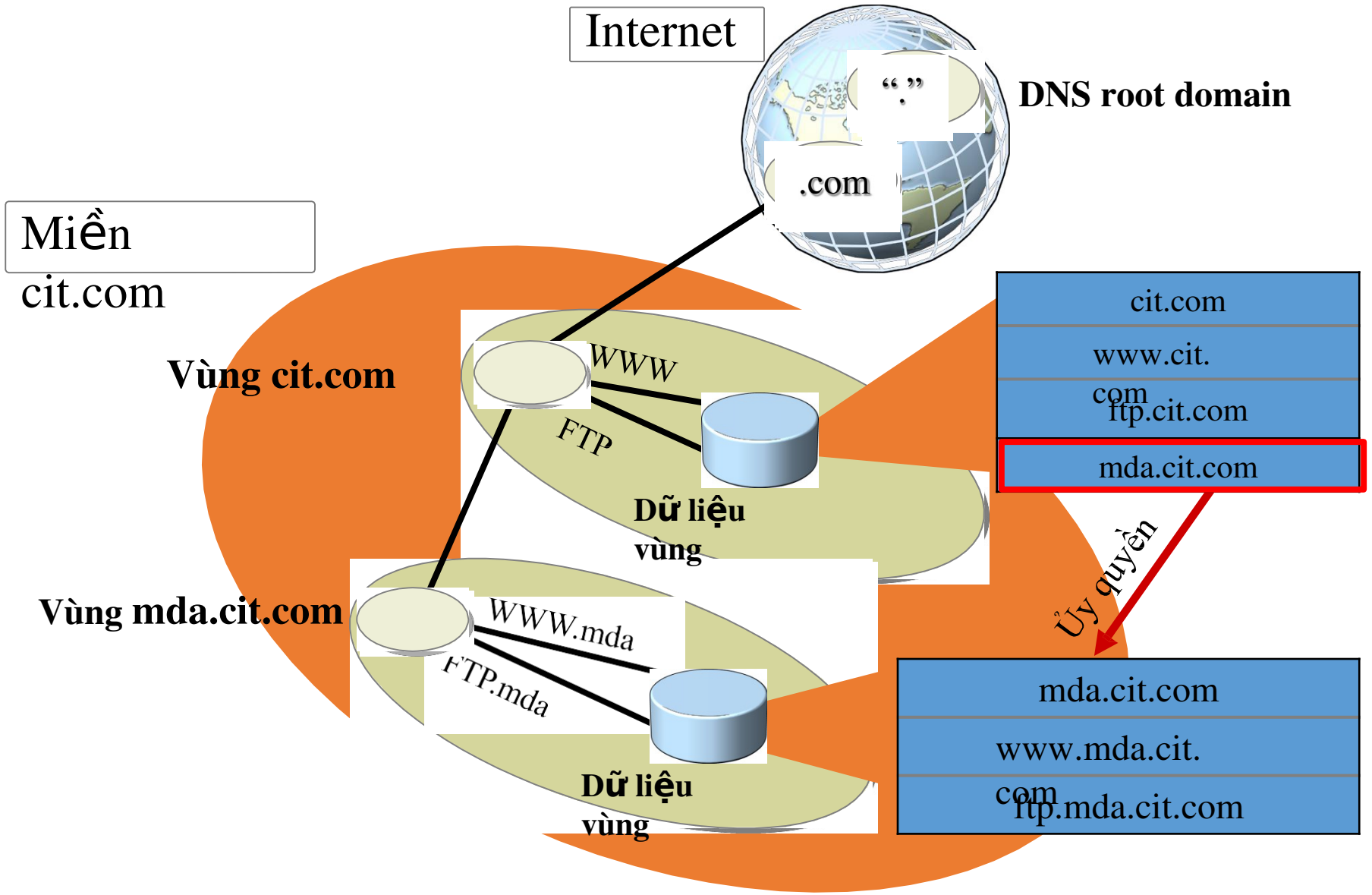
Chuyển tiếp có điều kiện cho phép DNS cục bộ chuyển tiếp các yêu cầu phân giải theo tên miền trong truy vấn yêu cầu



Cấu hình vùng DNS

- Vùng DNS là gì?
- Các loại vùng DNS
- Vùng truy vấn tới và vùng truy vấn lùi là gì?
- Stub Zones là gì?
- Vùng DNS ủy quyền

Vùng DNS là gì?



Các loại DNS Server trên Internet

- Primary name server: Duy trì một cơ sở dữ liệu về ZOA do
  mình phụ trách
- Secondary name server: Sao chép dự phòng dữ liệu ZOA của các primary name server vào cơ sở dữ liệu của mình
- Caching domain name server: trữ lại các yêu cầu phân tích
  tên đã giải quyết để tăng tốc độ phân tích tên

Name Server trên Internet

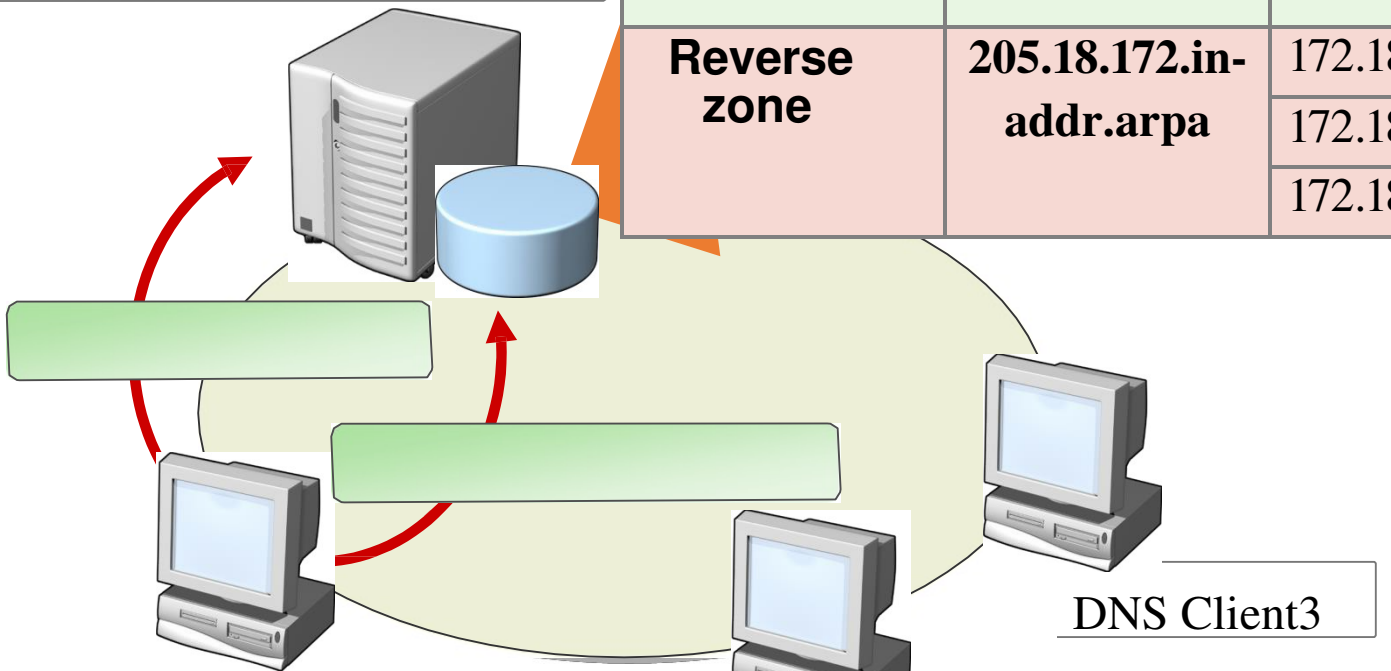
- Phân tích tên (Resolving Names):
  - Là tiến trình ánh xạ từ dạng tên miền sang địa chỉ IP (forward lookup)
- Phân tích địa chỉ (Resolving IP Addresses)
  - Là tiến trình ánh xạ từ địa chỉ IP sang tên của một máy tính (reverse lookup)
- Name Server đảm nhận 2 vai trò này
- Vùng có thẩm quyền (ZOA-Zones of Authority):
  - Là một phần của không gian tên mà một Name Server nào đó có nhiệm vụ thực hiện tiến trình phân tích tên và địa chỉ
  - Một ZOA chứa ít nhất một Domain, gọi là miền gốc và có thể có

Vùng truy vấn tới và vùng truy vấn lùi là gì?

Không gian: mda.cit.com

Forward zone	**mda**	DNS Client1	172.18.205.45
		DNS Client2	172.18.205.46
		DNS Client3	172.18.205.47
Reverse zone	**205.18.172.in-addr.arpa**	172.18.205.45	DNS Client1
		172.18.205.46	DNS Client2
		172.18.205.47	DNS Client3

Máy chủ DNS được ủy quyền mda



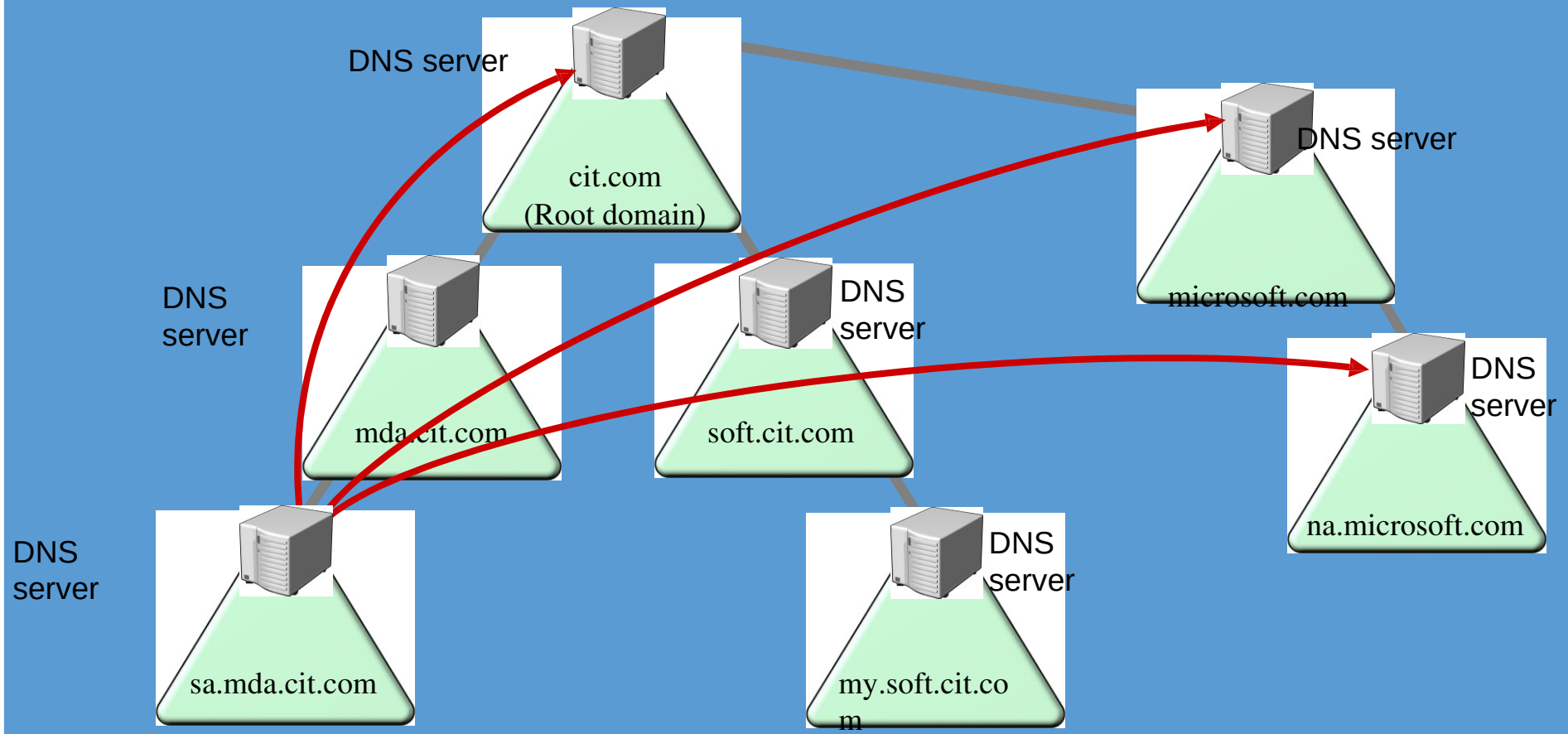
DNS Client3

DNS Client1

NS Client2

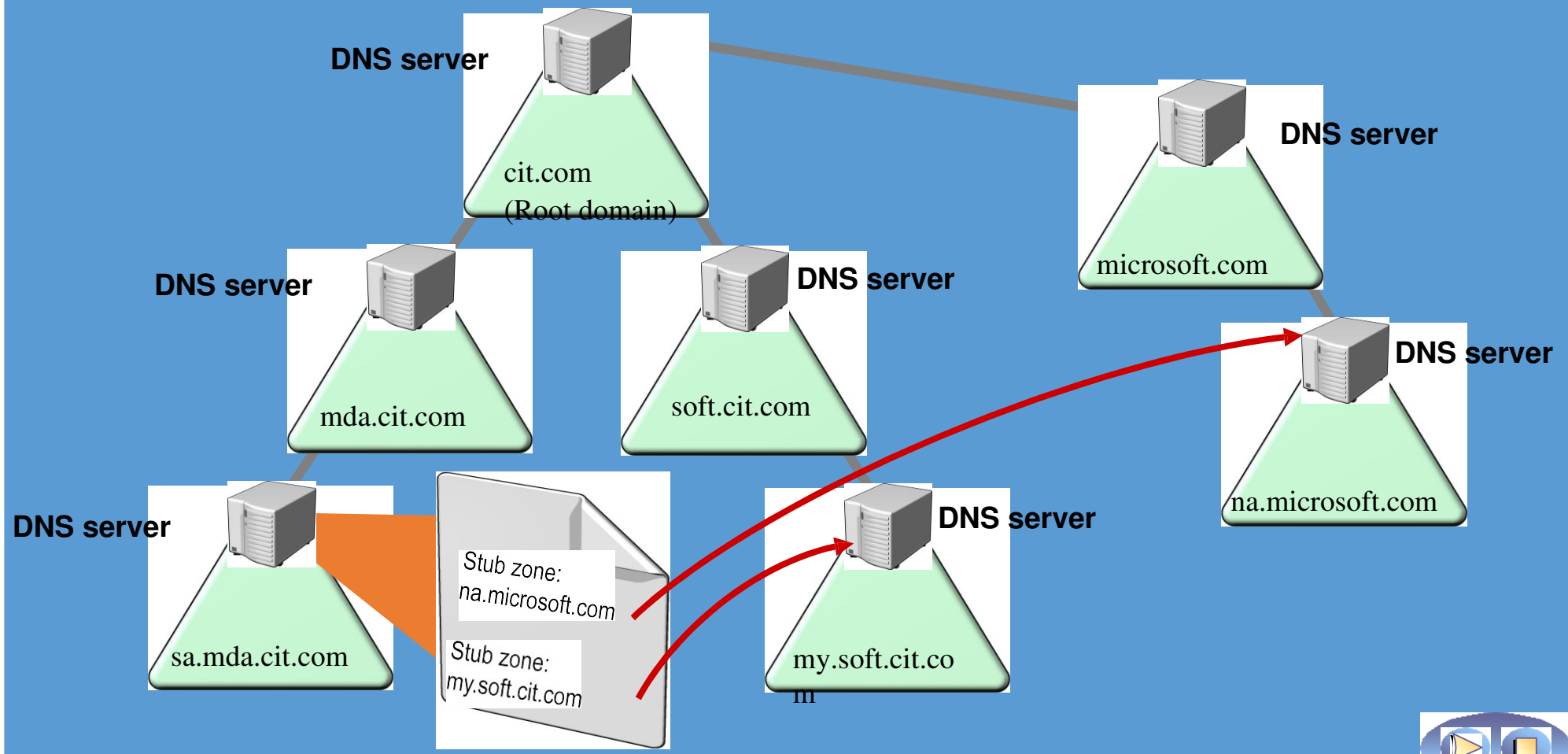
Stub Zones là gì?

Nếu không có stub zone, máy chủ sa.mda.cit.com phải truy vấn đến một số máy chủ để tìm ra máy chủ vùng na.microsoft.com

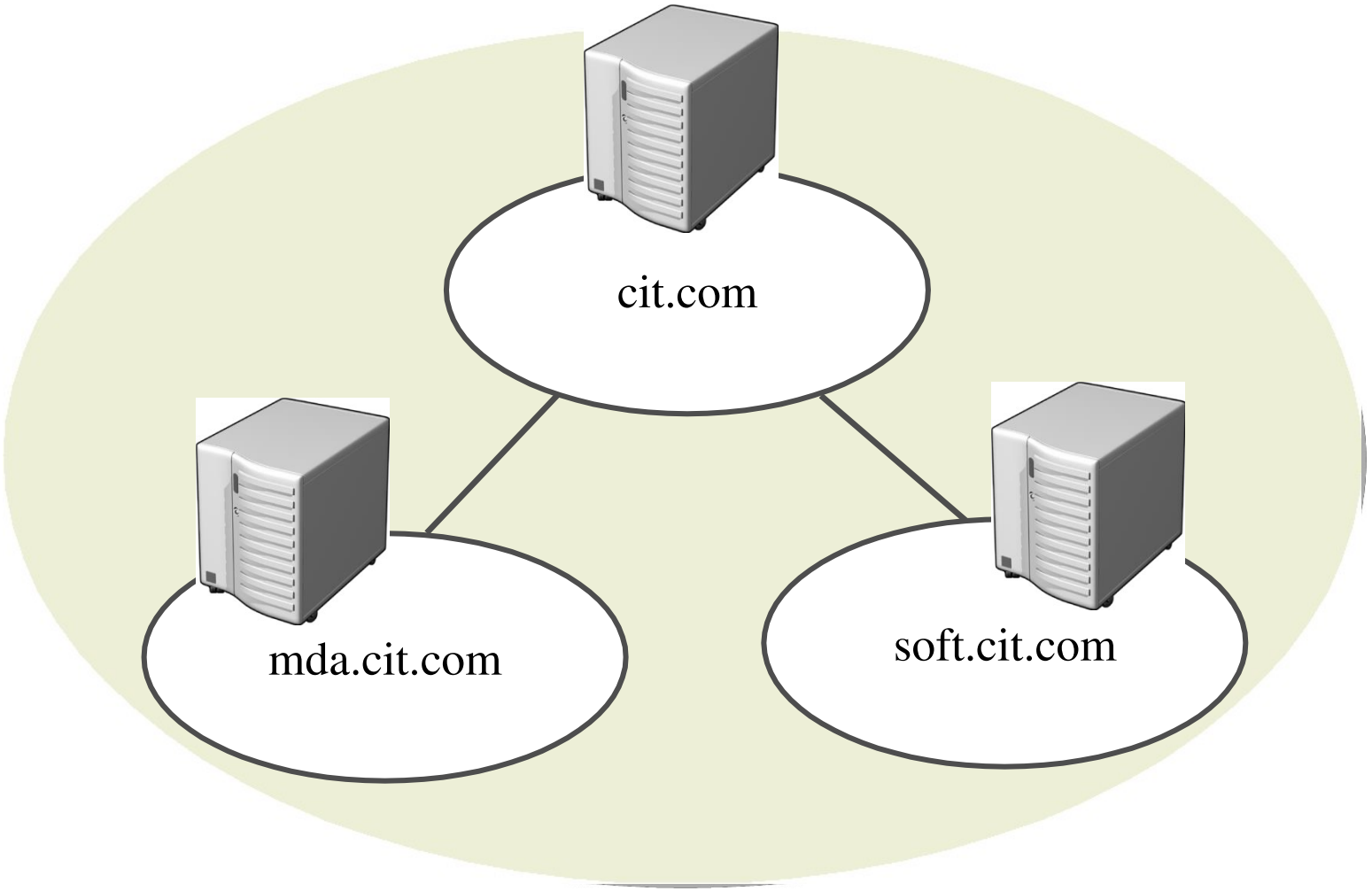


Stub Zones là gì?

Khi đã định nghĩa stub zone, vị trí của máy chủ vùng na.microsoft.com được biết đến mà không cần truy vấn nhiều máy chủ DNS khác



Vùng DNS ủy quyền



Các công cụ để xác định vấn đề với DNS

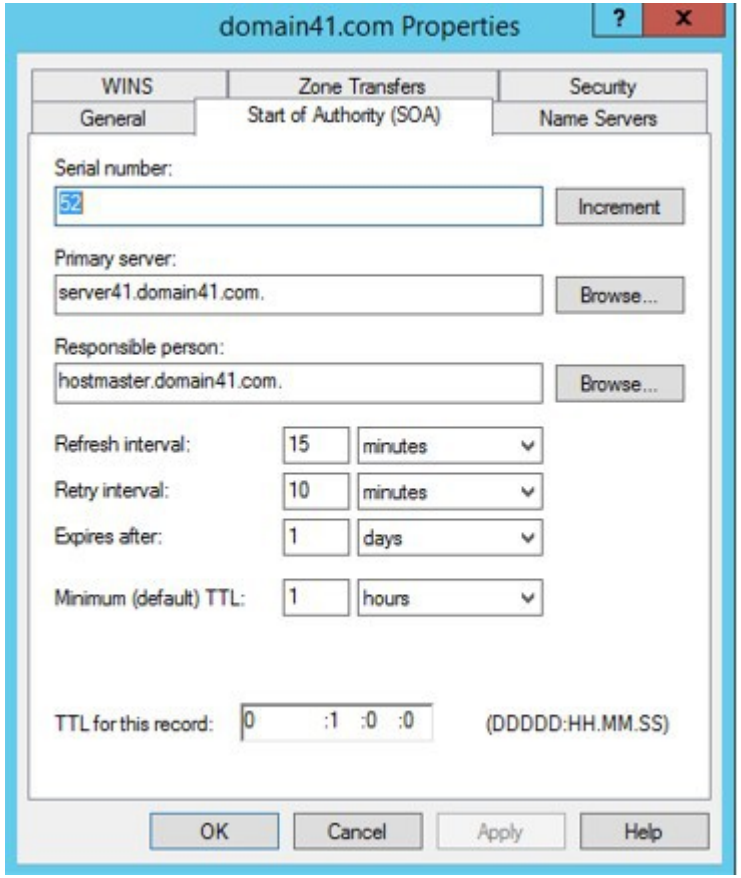
Công cụ	Sử dụng để:
Nslookup	Khắc phục sự cố các vấn đề về DNS
Dnscmd	Chỉnh sửa cấu hình DNS
Dnslint	Chẩn đoán các vấn đề DNS

Cơ sở dữ liệu của DNS

- (Tên, Giá trị, Kiểu, Lớp, TTL)
  - **Tên** ánh xạ **Giá trị**
    - www.cit.ctu.edu -> 203.162.36.146
  - Kiểu: Chỉ ra cách thức mà **Giá trị** được thông dịch
  - Lớp: Cho phép thêm vào các thực thể không do NIC quản lý
  - TTL: Thời gian sống

Bản ghi tài nguyên DNS

- Bản ghi tài nguyên DNS bao gồm:
  - SOA: Start of Authority
  - A: Host Record
  - CNAME: Alias Record
  - MX: Mail Exchange Record
  - SRV: Service Resources
  - NS: Name Servers

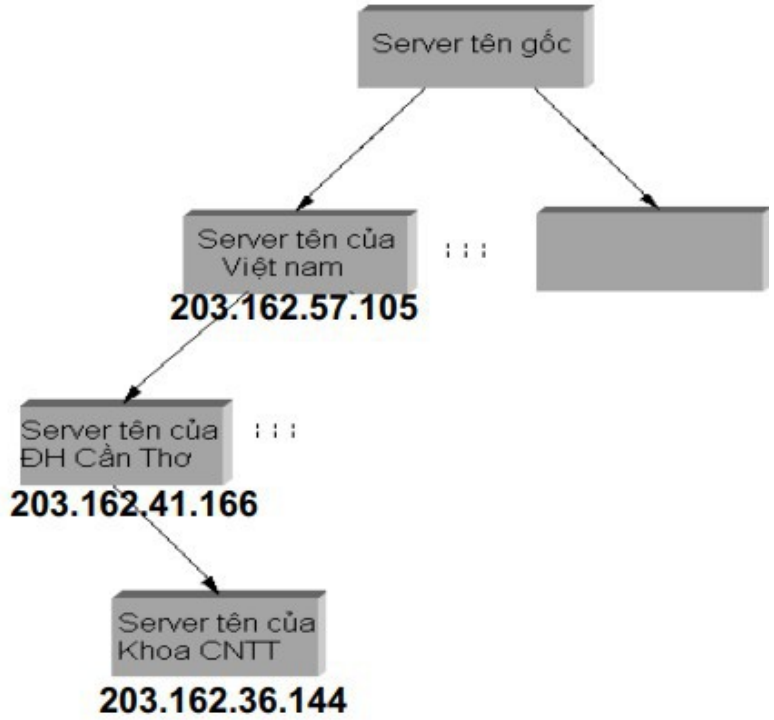


Cơ sở dữ liệu của DNS

- (Tên, Giá trị, Kiểu, Lớp, TTL)
  - Kiểu A: Tên miền sang địa chỉ IP
    - (ns.ctu.edu.vn, 203.162.41.166, **A**, IN)
  - Kiểu NS: Tên miền và Name Server của có
    - (ctu.edu.vn, ns.ctu.edu.vn, **NS**, IN)
  - Kiểu CNAME: Đặt bí danh cho một tên máy tính đã có
    - (dns.ctu.edu.vn, ns.ctu.edu.vn, **CNAME**, IN)
  - Kiểu MX: Tên miền và Mail Server cho miền
    - (ctu.edu.vn, mail.ctu.edu.vn, MX, IN)

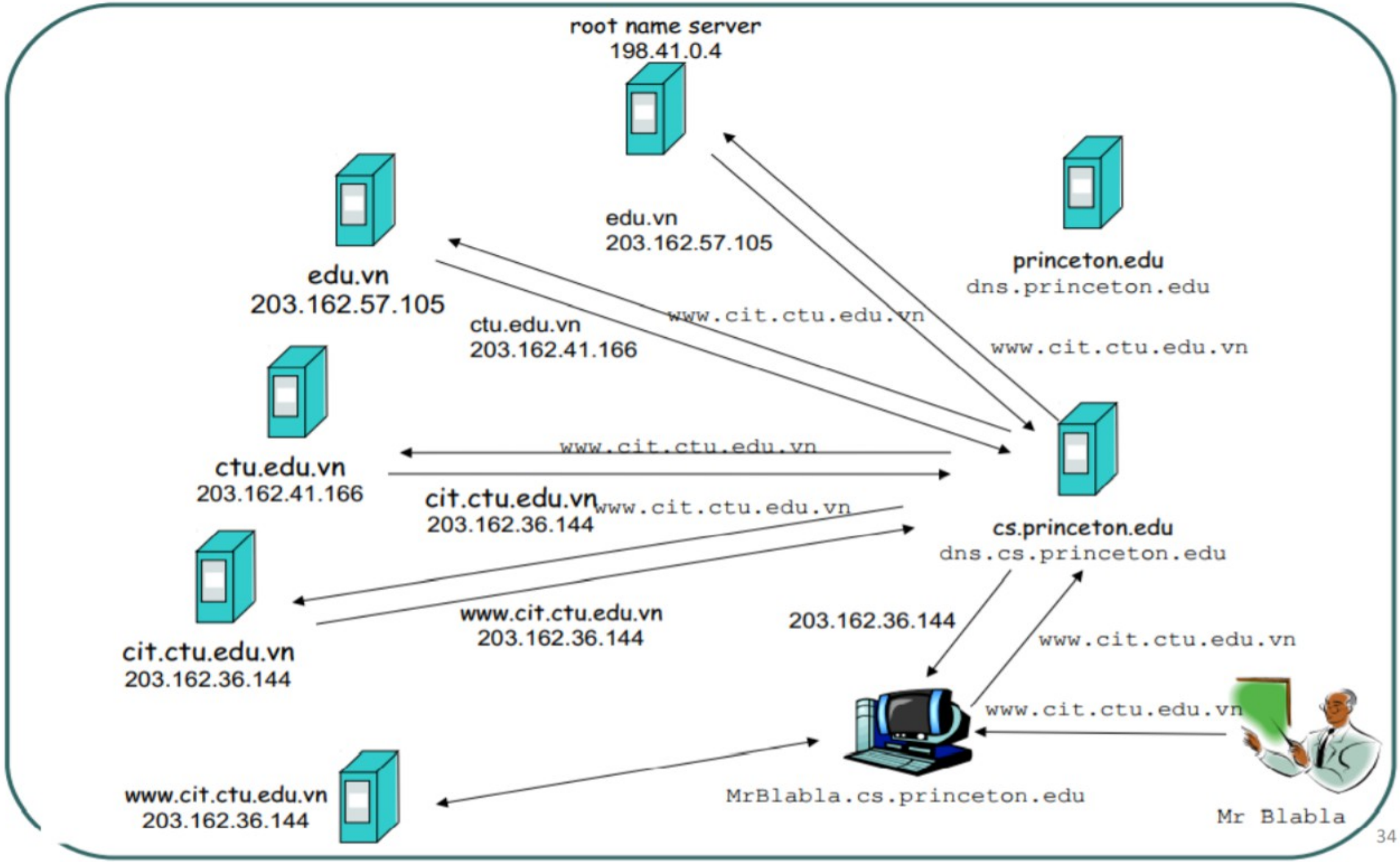
Cơ sở dữ liệu của DNS

- Root name server chứa
  - Chứa một mẫu tin **NS** cho mỗi server cấp hai.
  - Một mẫu tin **A** để thông dịch từ một tên server cấp hai sang địa chỉ IP của nó.
  - (edu.vn, dns1.vnnic.net.vn, NS, IN);
  - (dns1.vnnic.net.vn, **203.162.57.105**, A, IN)
- Tương tự cho các Name Server thứ cấp
  - dns1.vnnic.net.vn:
    - (ctu.edu.vn, ns.ctu.edu.vn, NS, IN)
    - (ns.ctu.edu.vn, **203.162.41.166**, A, IN)
  - ns.ctu.edu.vn:
    - (cit.ctu.edu.vn, ns.cit.ctu.edu.vn, NS, IN)
    - (**ns**.cit.ctu.edu.vn, **203.162.36.144**, A, IN)
    - (ctu.edu.vn, mail.ctu.edu.vn, MX, IN)
    - (mail.ctu.edu.vn, 203.162.139.21, A, IN)
    - (www.ctu.edu.vn, mail.ctu.edu.vn, CNAME, IN)



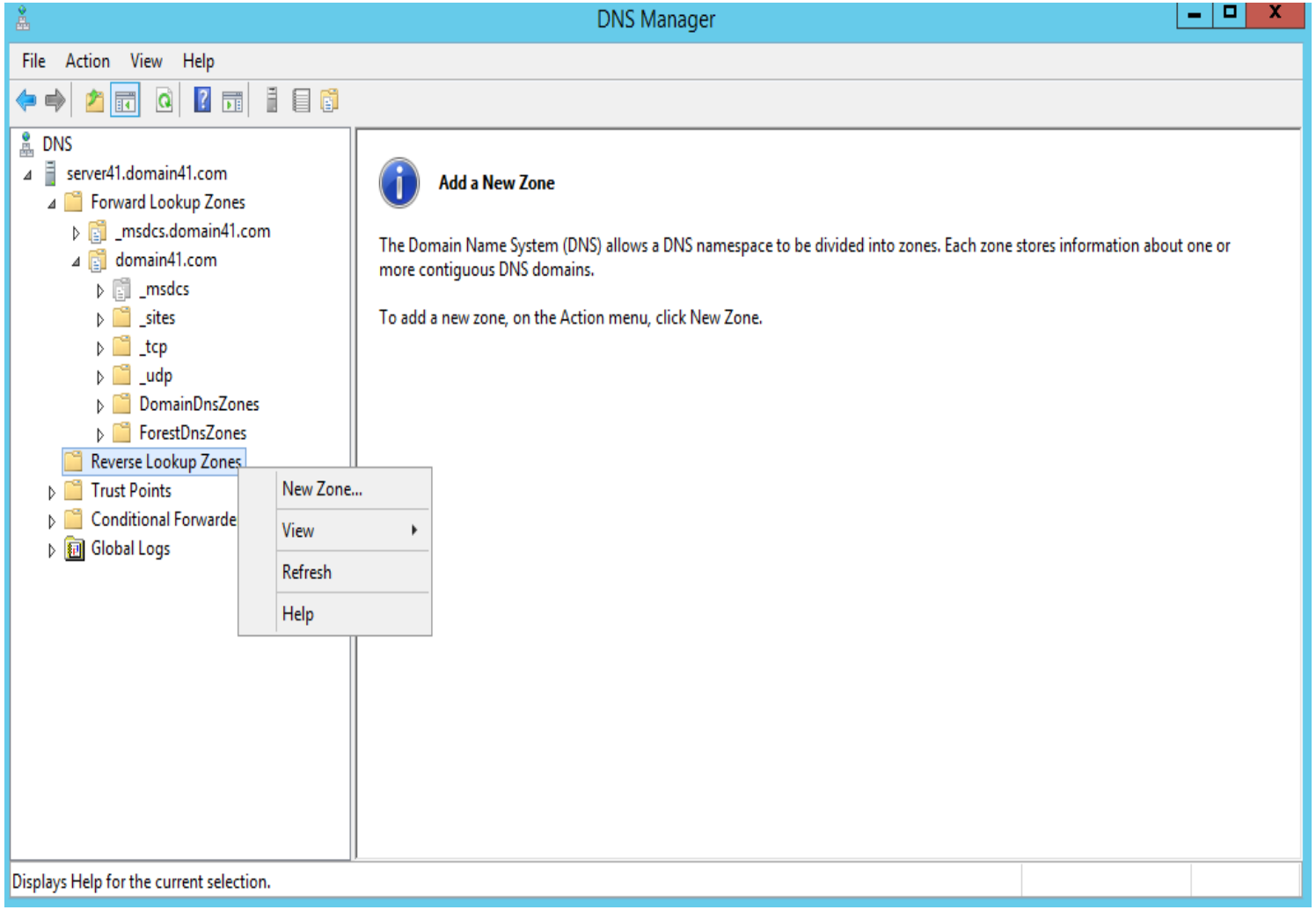
Tiến trình phân tích tên

- Mỗi Name Server biết địa chỉ của ít nhất một Root Name Server:
  - (. , a.root-servers.net, NS, IN)
    (a.root-server.net, 198.41.0.4, A, IN)

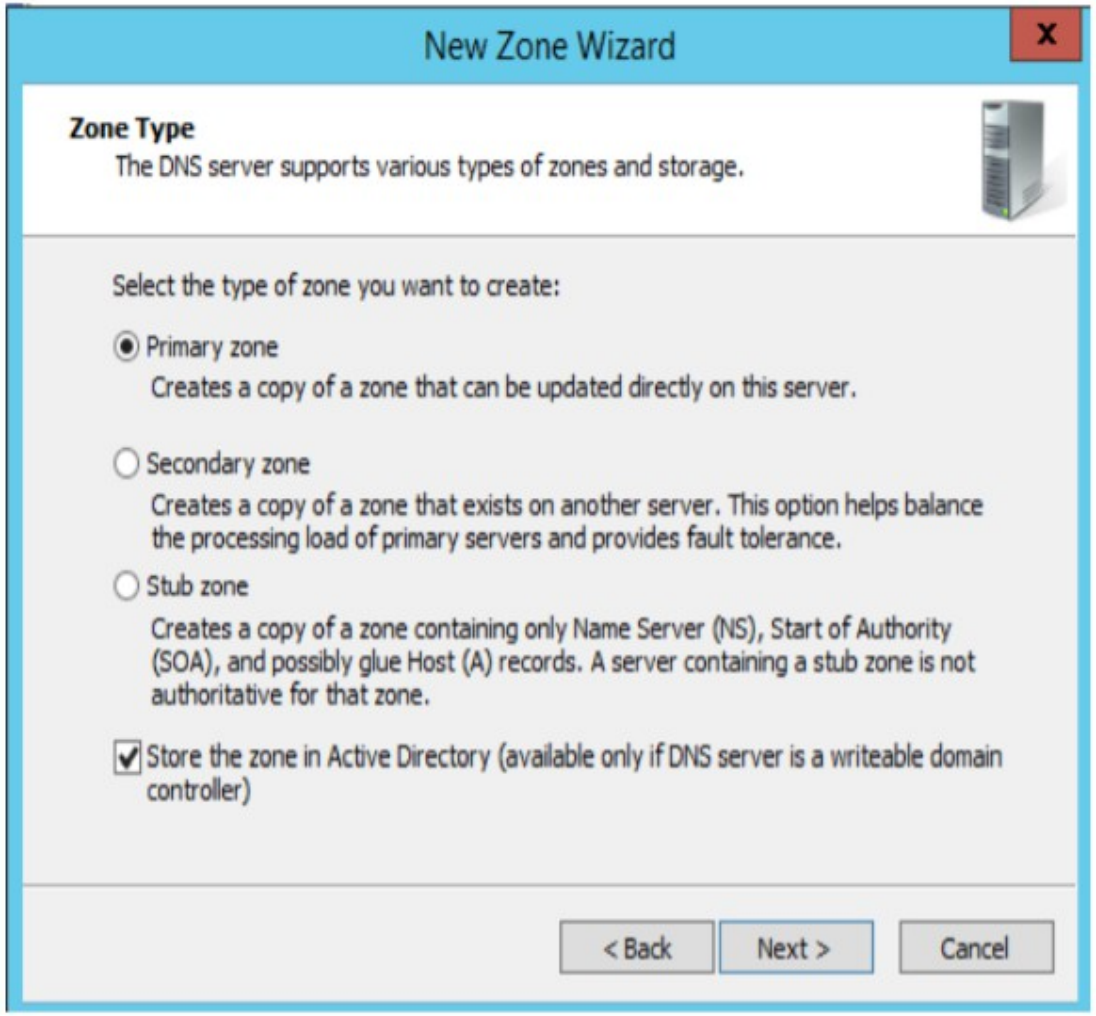

root name server
198.41.0.4
edu.vn
203.162.57.105
edu.vn
203.162.57.105
princeton.edu
dns.princeton.edu
www.cit.ctu.edu.vn
ctu.edu.vn
203.162.41.166
www.cit.ctu.edu.vn
ctu.edu.vn
203.162.41.166
www.cit.ctu.edu.vn
cit.ctu.edu.vn
203.162.36.144
www.cit.ctu.edu.vn
cs.princeton.edu
dns.cs.princeton.edu
cit.ctu.edu.vn
203.162.36.144
www.cit.ctu.edu.vn
203.162.36.144
203.162.36.144
www.cit.ctu.edu.vn
www.cit.ctu.edu.vn
www.cit.ctu.edu.vn
203.162.36.144
MrBlabla.cs.princeton.edu
Mr Blabla

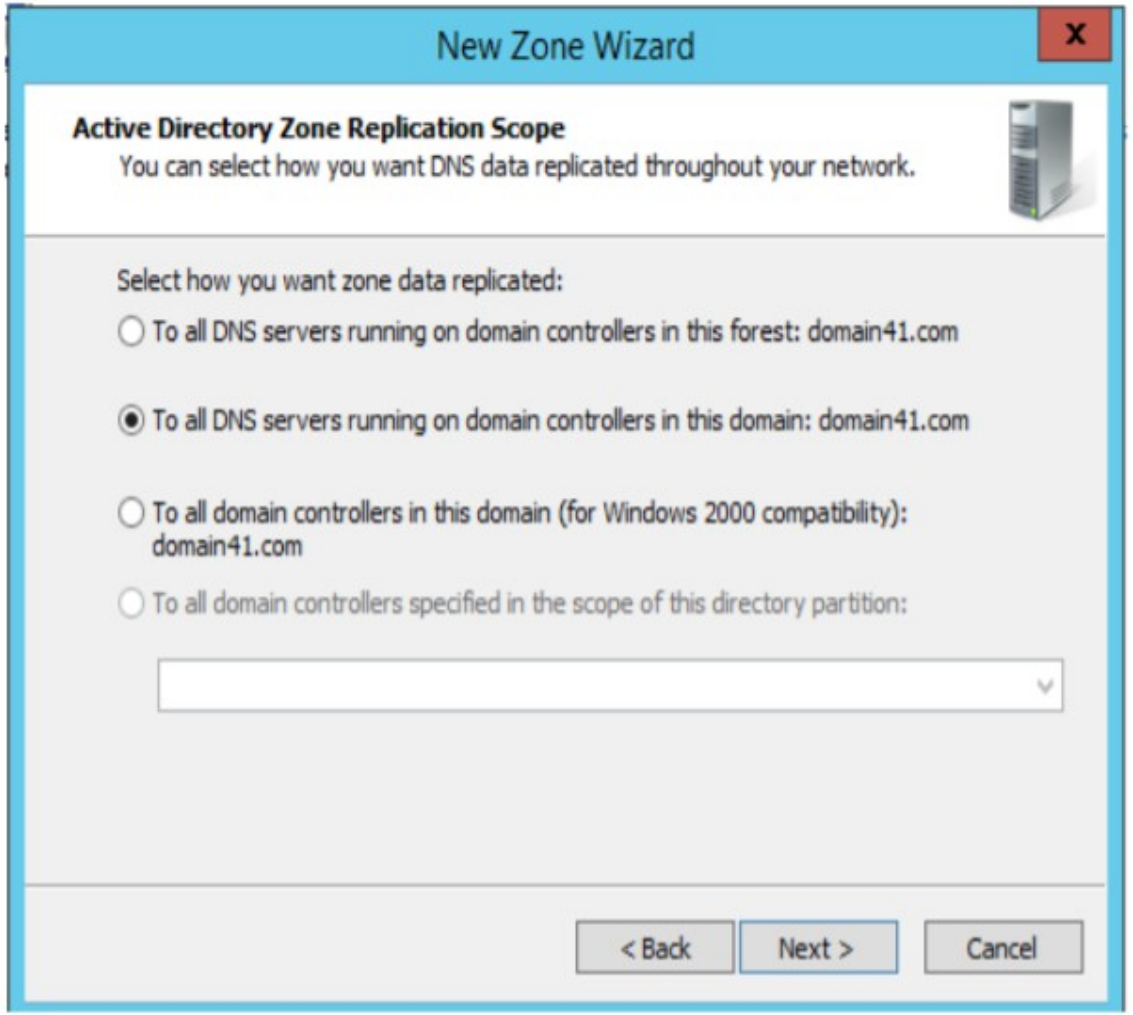
Cài đặt và Cấu hình DNS

- Khởi động và cấu hình DNS mở **Server manager -> Tools-> DNS**
- Click vào nút mở rộng **Reverse Lookup** chọn **New Zone** để cài đặt

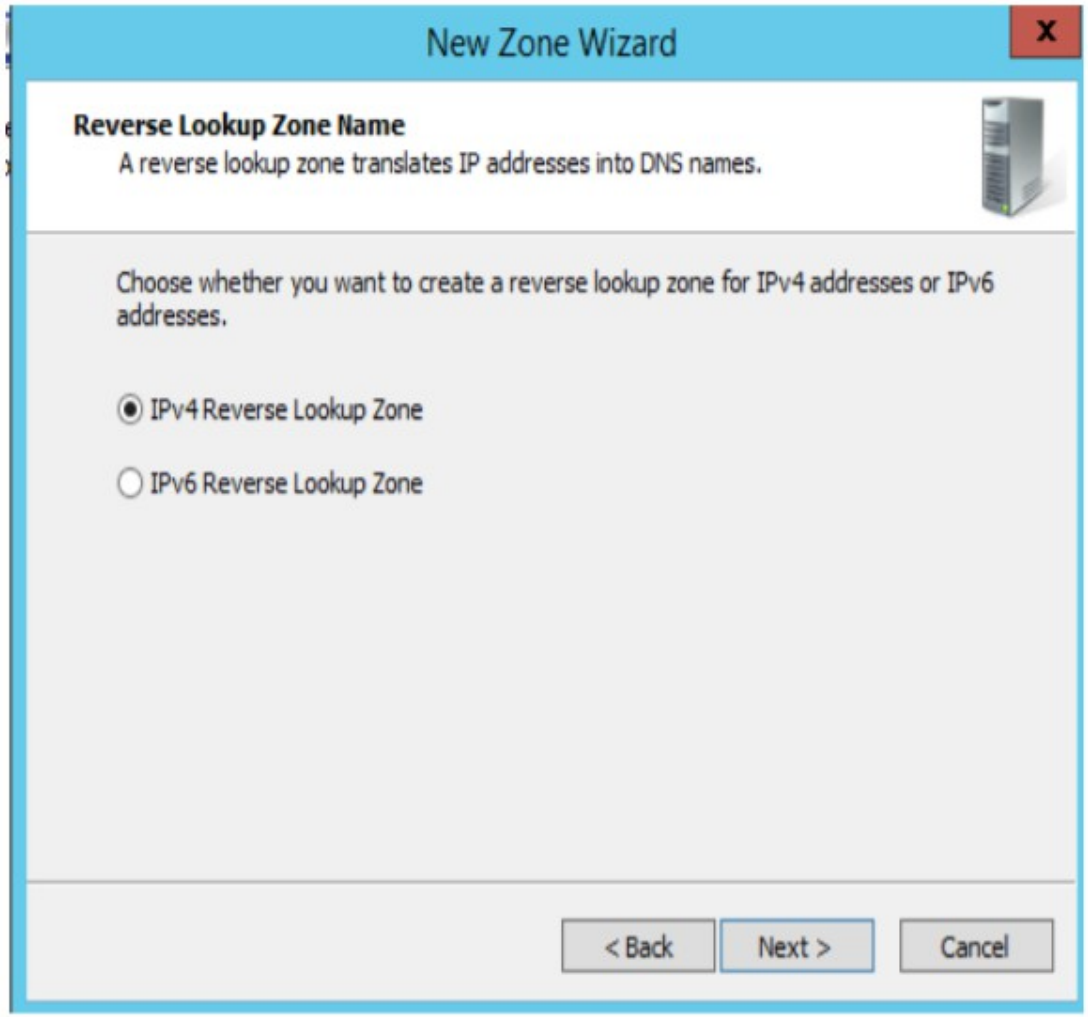


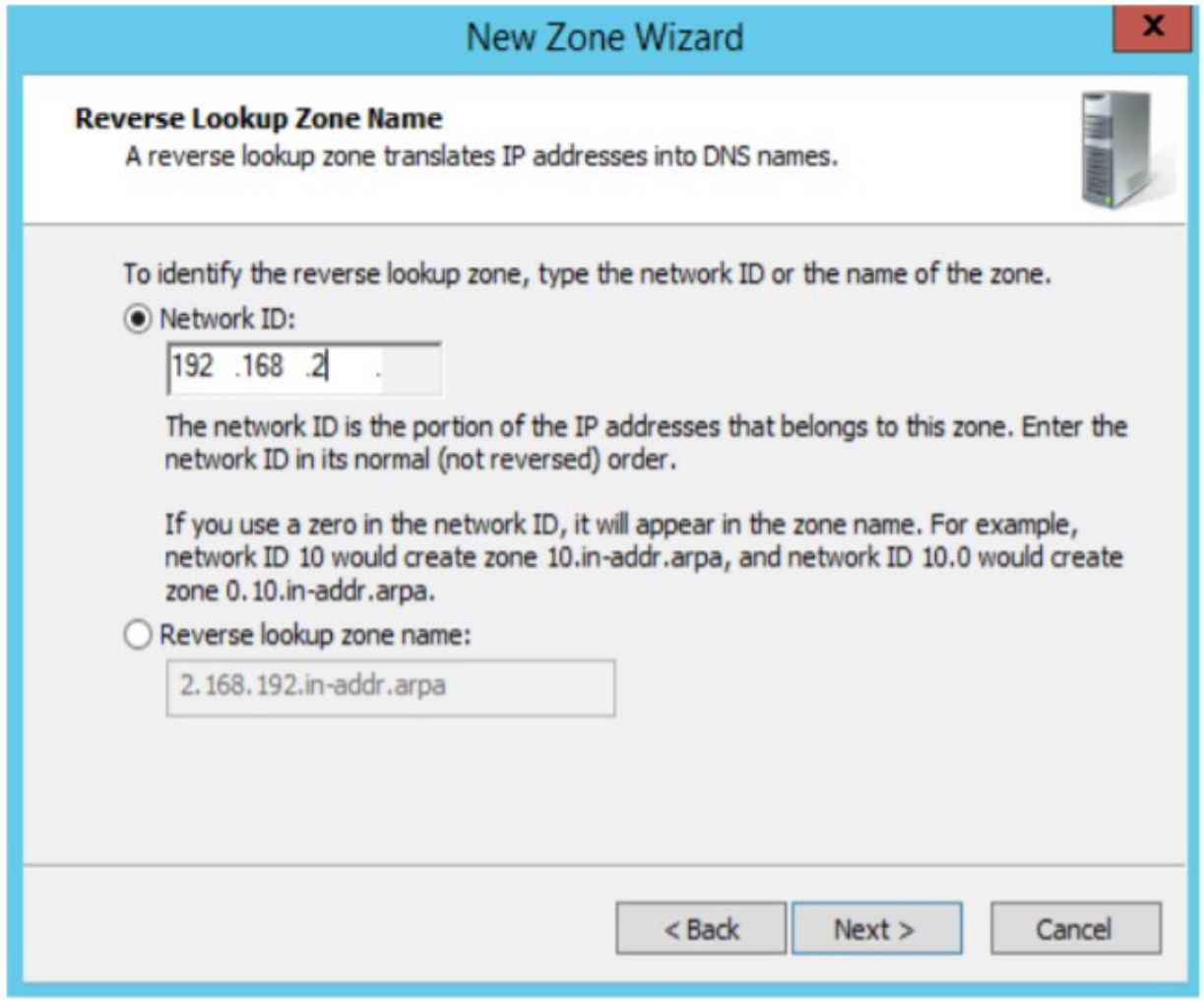
Cài đặt và Cấu hình DNS



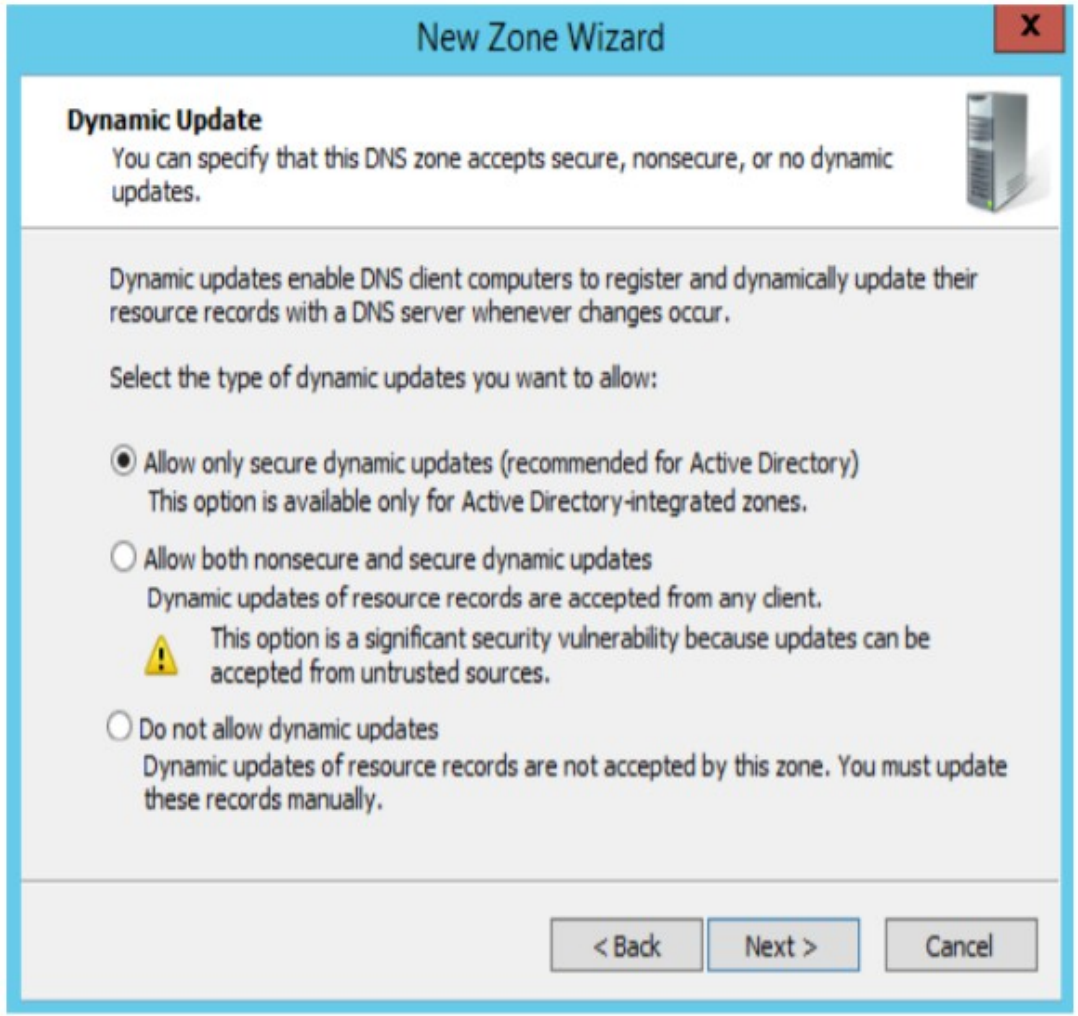


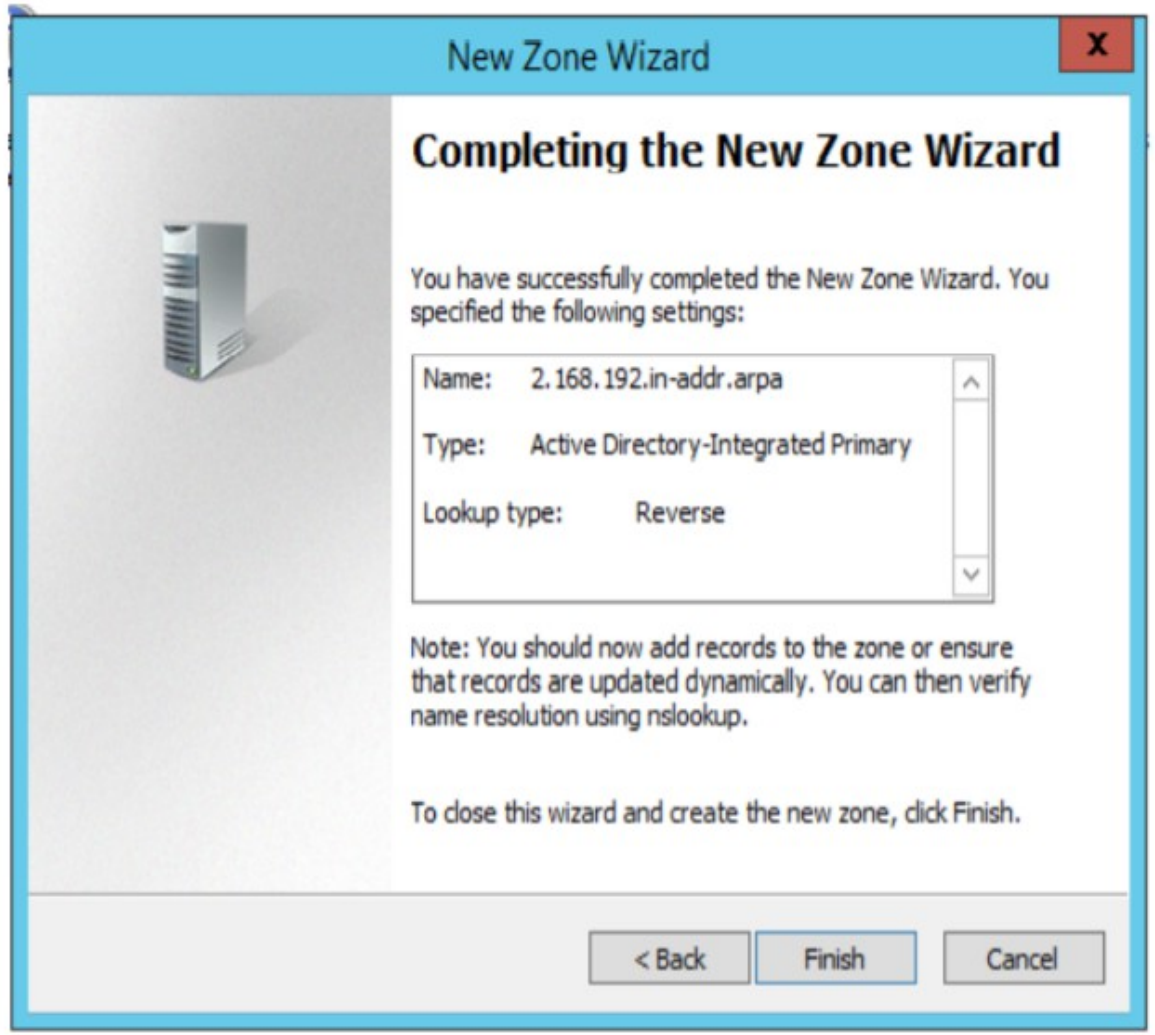
Cài đặt và Cấu hình DNS



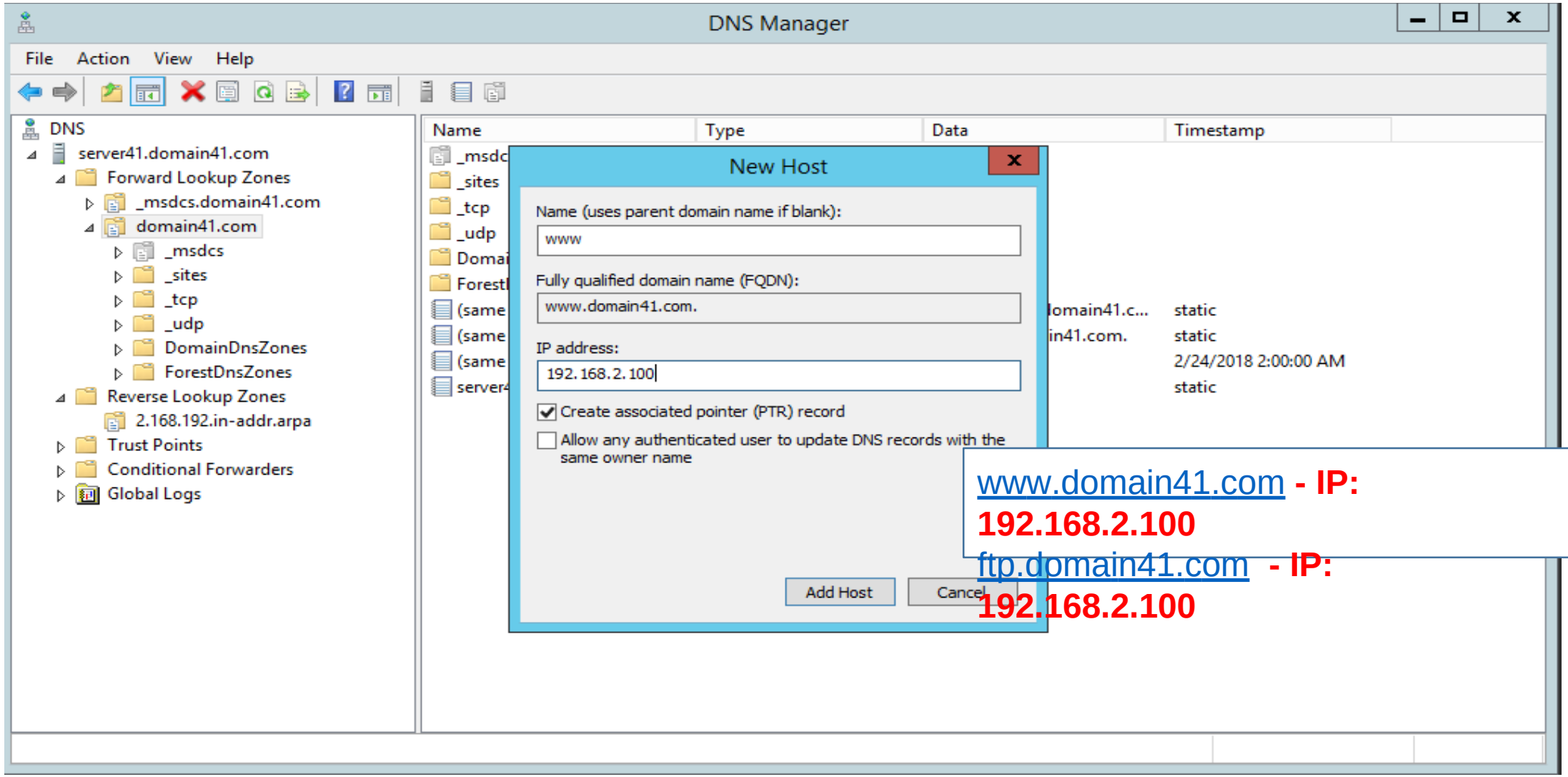


Cài đặt và Cấu hình DNS





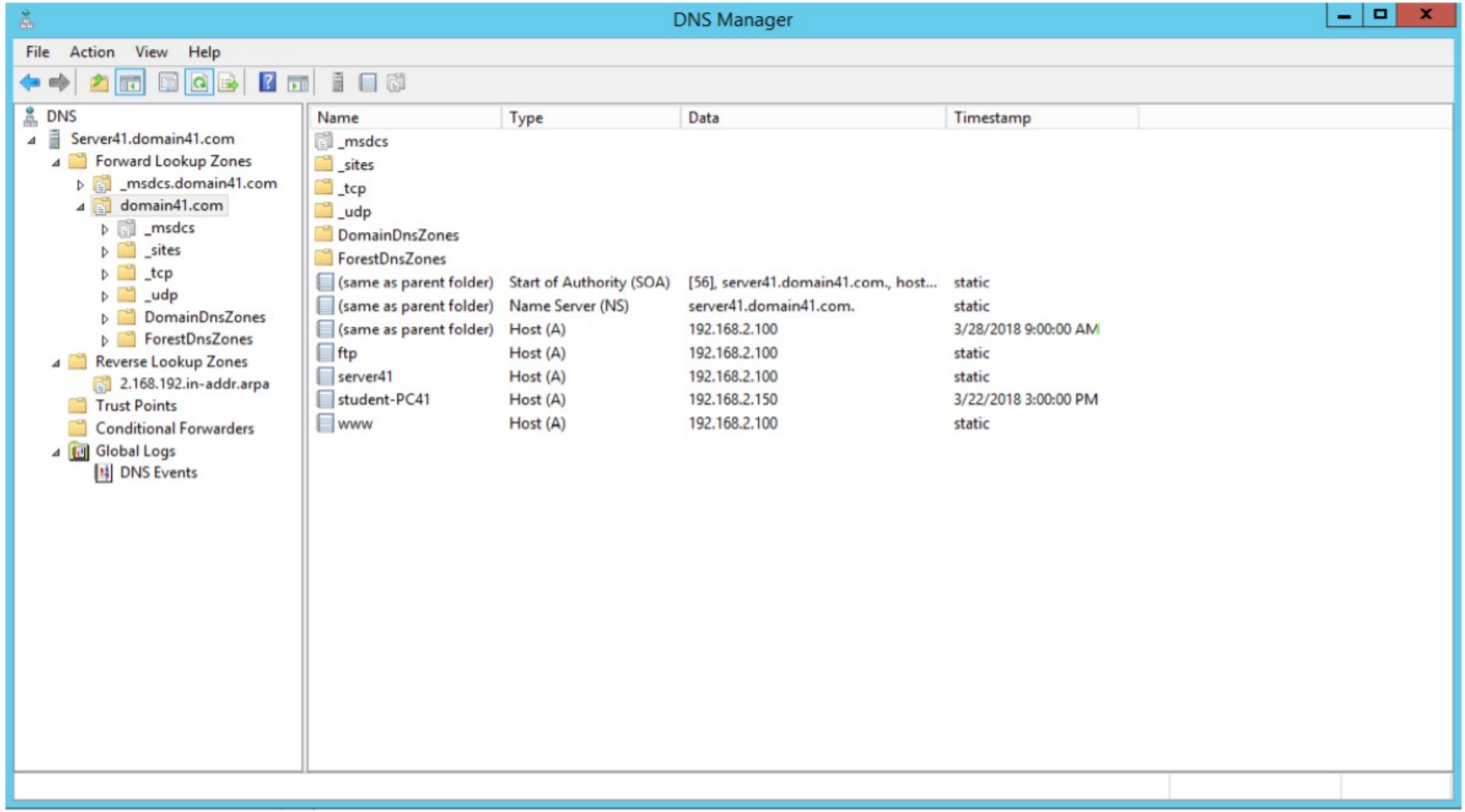
Cài đặt và Cấu hình DNS



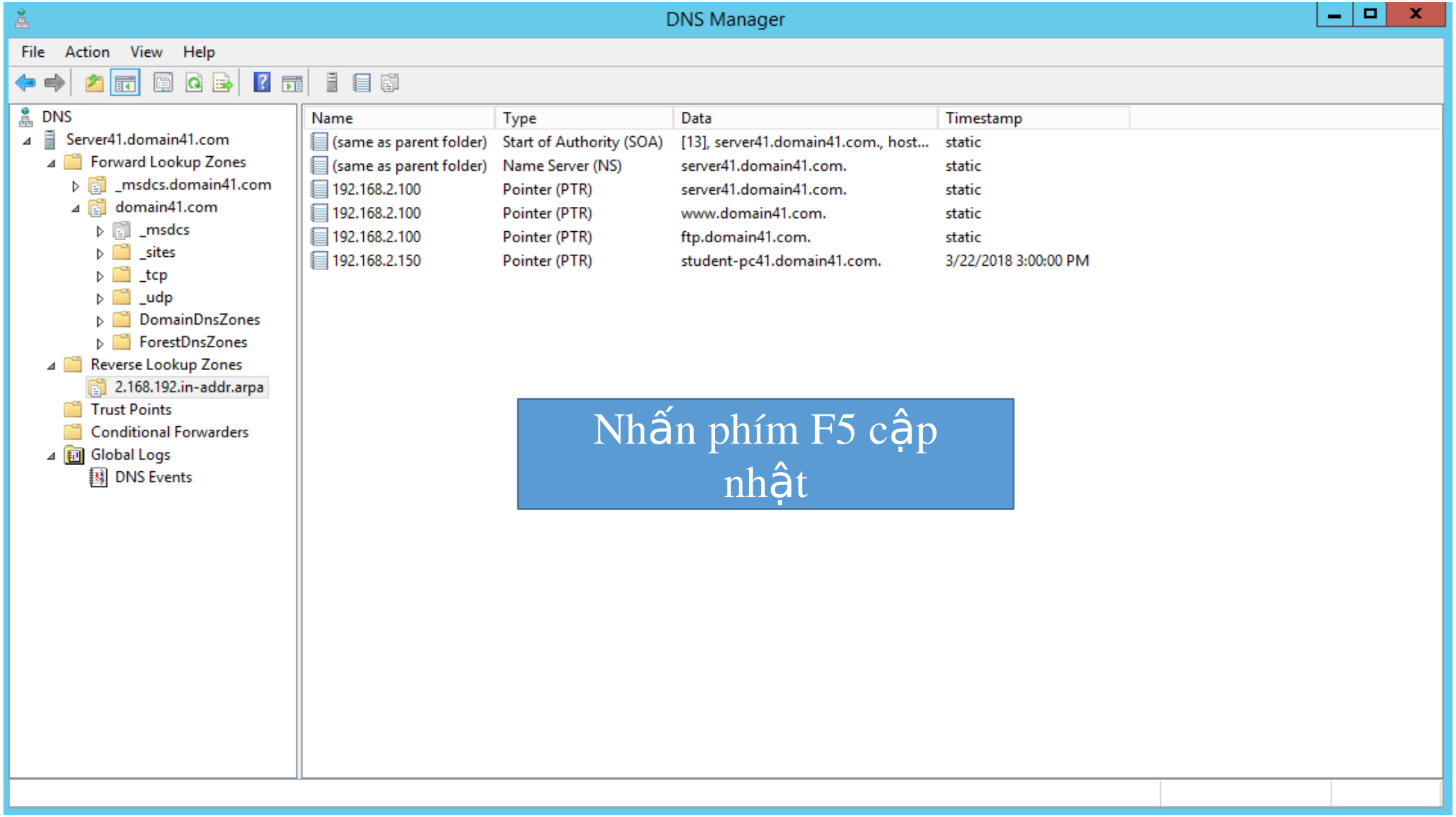
www.domain41.com - **IP: 192.168.2.100**

ftp.domain41.com - **IP: 192.168.2.100**

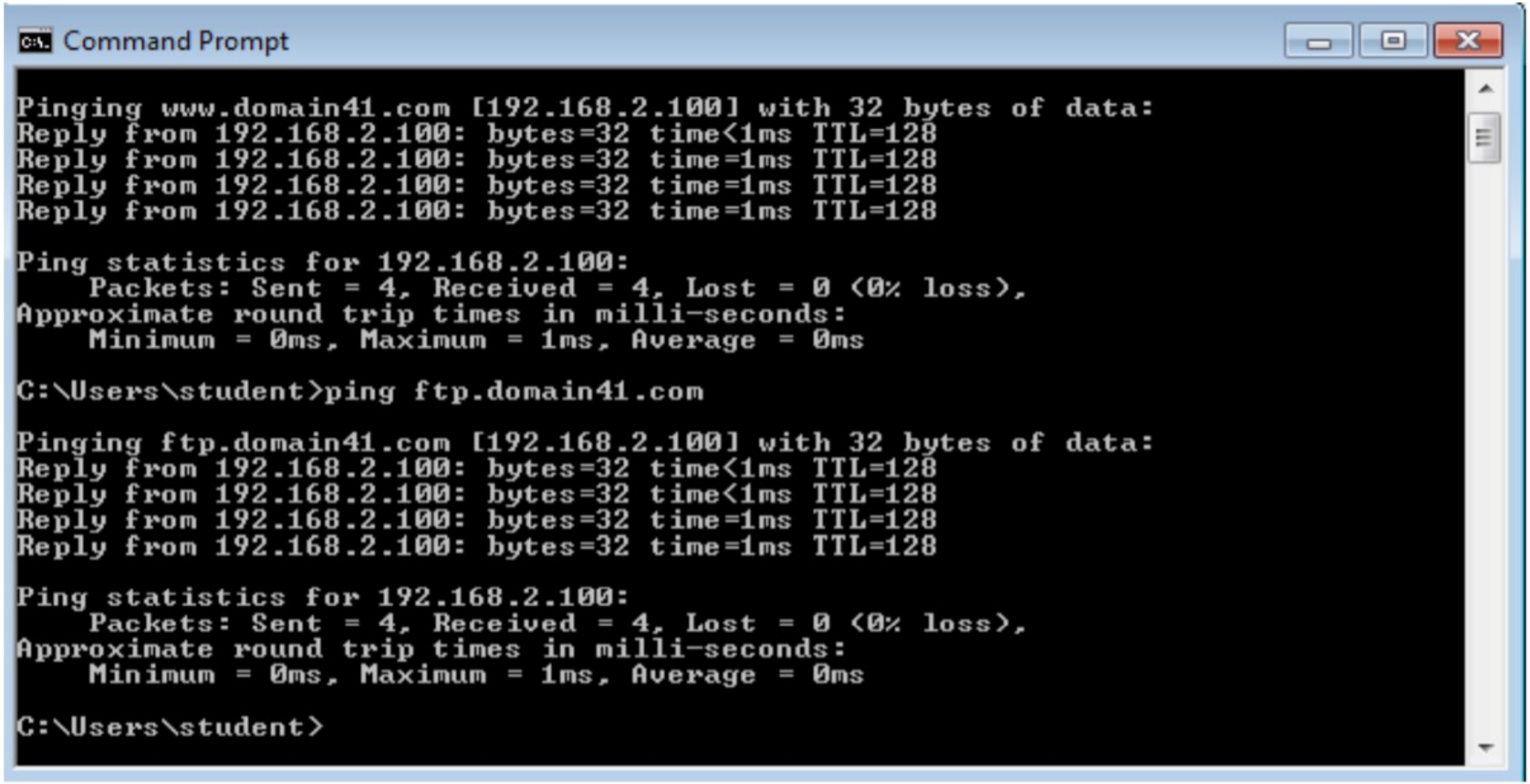
Forward Lookup Zones



Reverse Lookup Zones



Kiểm tra DNS


Command Prompt
Pinging www.domain41.com [192.168.2.100] with 32 bytes of data:
Reply from 192.168.2.100: bytes=32 time<1ms TTL=128
Reply from 192.168.2.100: bytes=32 time=1ms TTL=128
Reply from 192.168.2.100: bytes=32 time=1ms TTL=128
Reply from 192.168.2.100: bytes=32 time=1ms TTL=128
Ping statistics for 192.168.2.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\Users\student>ping ftp.domain41.com
Pinging ftp.domain41.com [192.168.2.100] with 32 bytes of data:
Reply from 192.168.2.100: bytes=32 time<1ms TTL=128
Reply from 192.168.2.100: bytes=32 time<1ms TTL=128
Reply from 192.168.2.100: bytes=32 time=1ms TTL=128
Reply from 192.168.2.100: bytes=32 time=1ms TTL=128
Ping statistics for 192.168.2.100:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 1ms, Average = 0ms
C:\Users\student>