

# 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](http://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	Australia
ca	Canada
de	Đức
fr	Pháp
jp	Nhật
uk	Anh
us (hoặc không ghi)	Mỹ
vn	Việt Nam

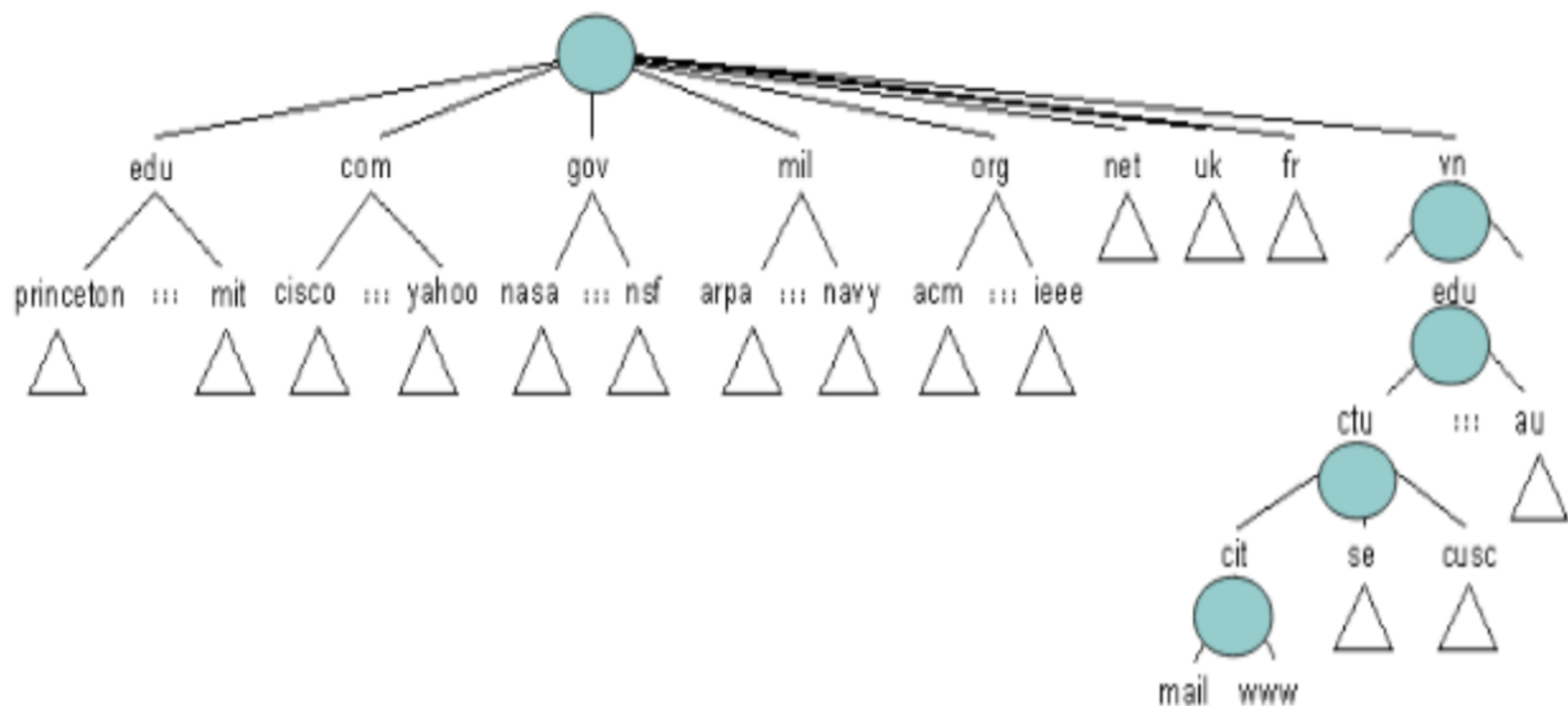
# Tên miền DNS – tổ chức

## ❖ Tên miền DNS – tổ chức

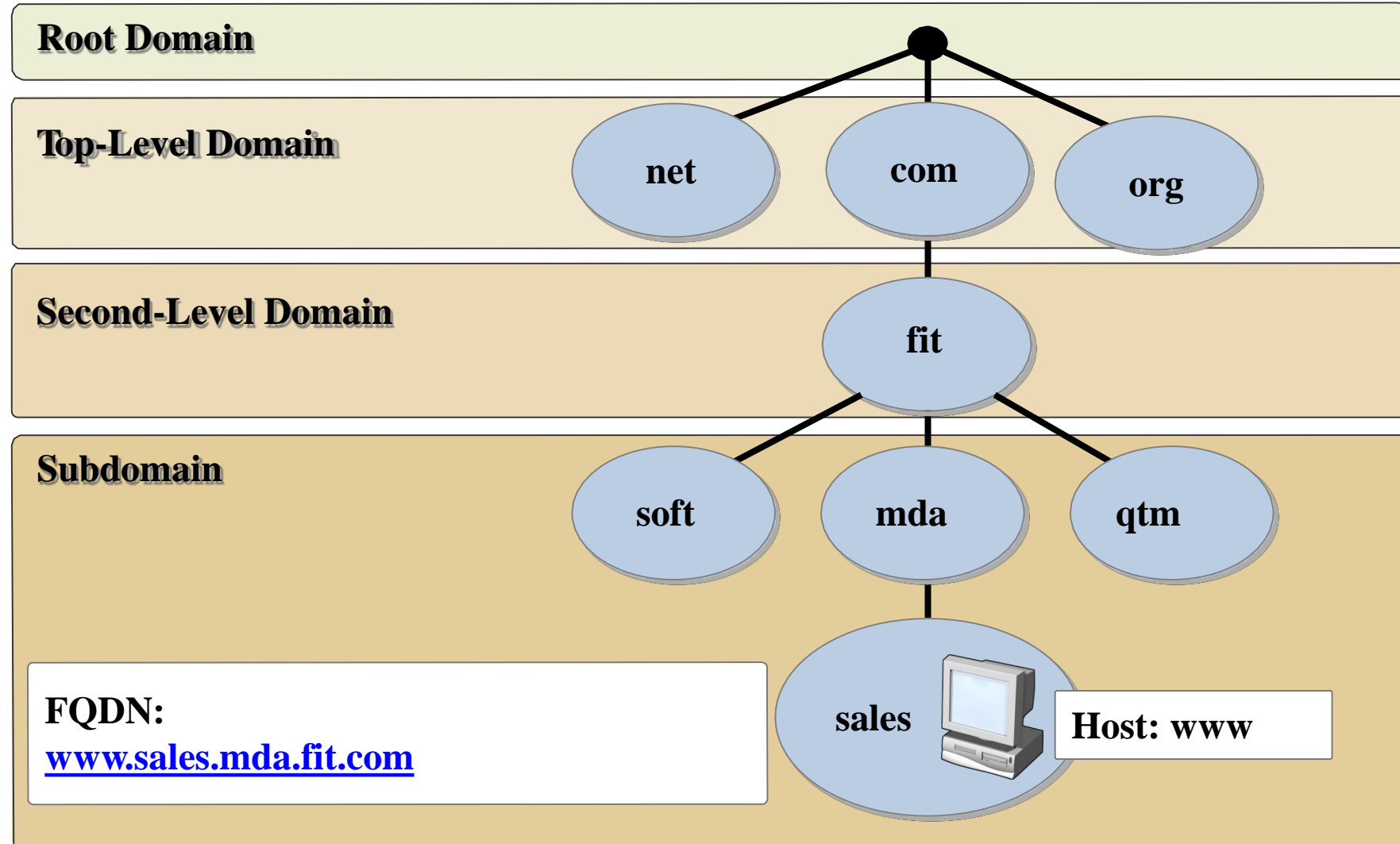
- ❑ Nhóm chữ cái thứ hai (còn gọi là domain tổ chức) : được tính từ phải sang trái, chỉ ra nghề nghiệp, tổ chức .

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

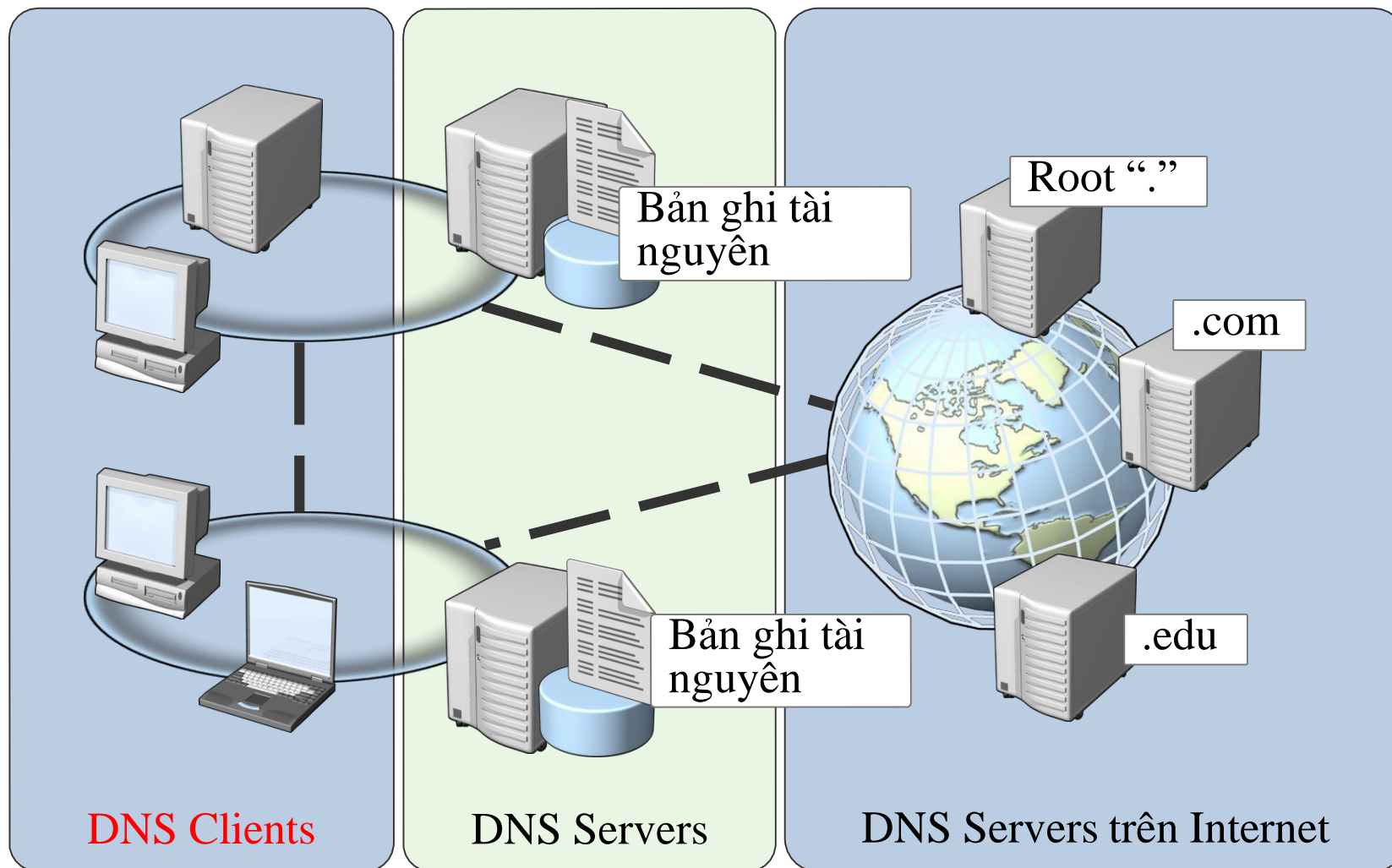
# Triển khai máy chủ DNS

- ❖ 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

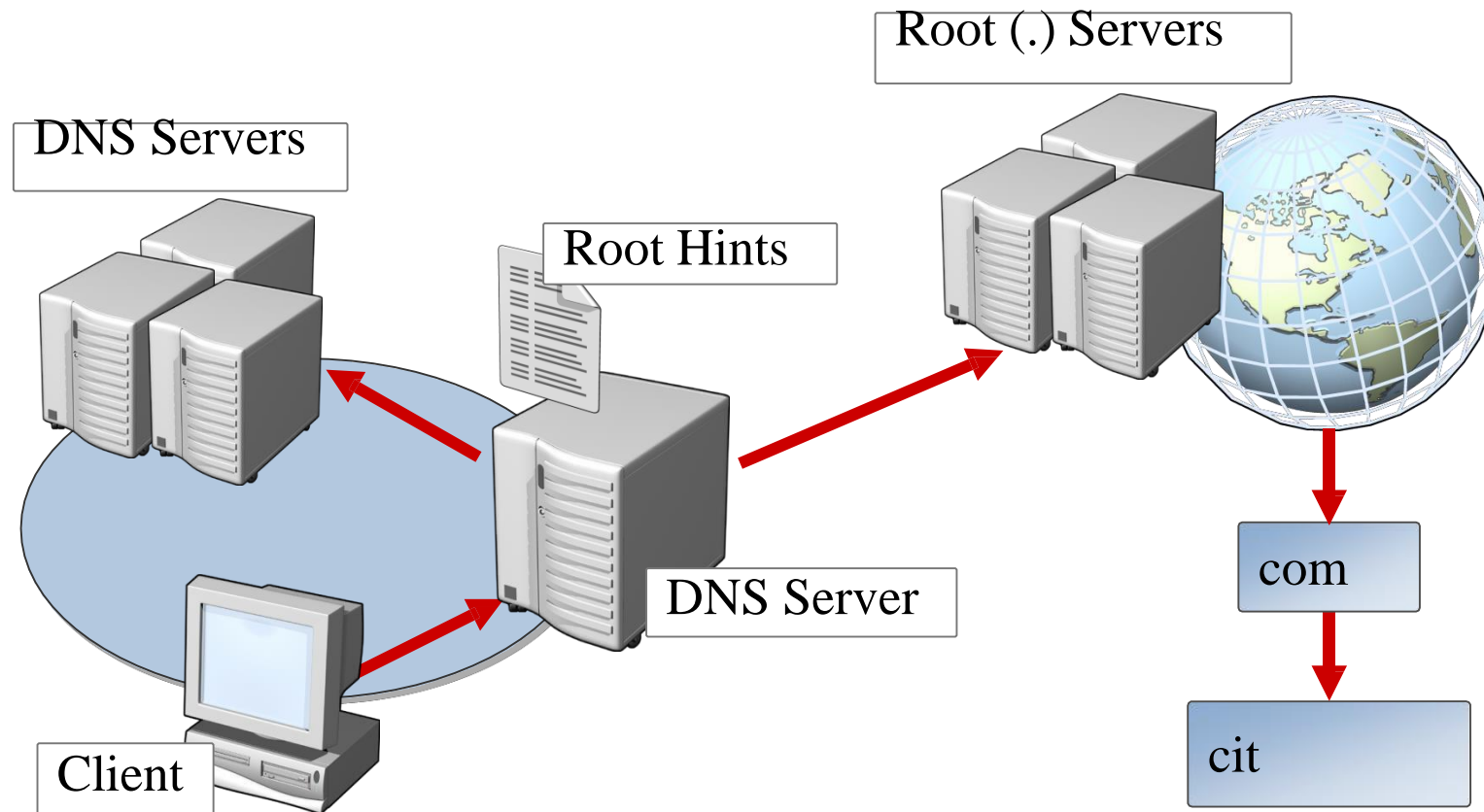
- ❖ Các thành phần của một giải pháp DNS là gì?
- ❖ Bản ghi tài nguyên DNS
- ❖ Root Hints là gì?
- ❖ Một truy vấn DNS là gì?
- ❖ Truy vấn đệ quy là gì?
- ❖ Truy vấn lặp là gì?
- ❖ Chuyển tiếp (Forwarder) là gì?
- ❖ Chuyển tiếp có điều kiện là gì?
- ❖ Lưu trữ đệm làm việc thế nào

# 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 gửi 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
    - Sử dụng root hints

# 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](http://www.guci.com) là bao nhiêu
- Đó là khi cỗ máy DNS bắt đầu vận hành.

Em muốn mở trang [www.guci.com](http://www.guci.com) để xem mấy mẫu giày mới nhất. Hi!





- Host gửi 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 .

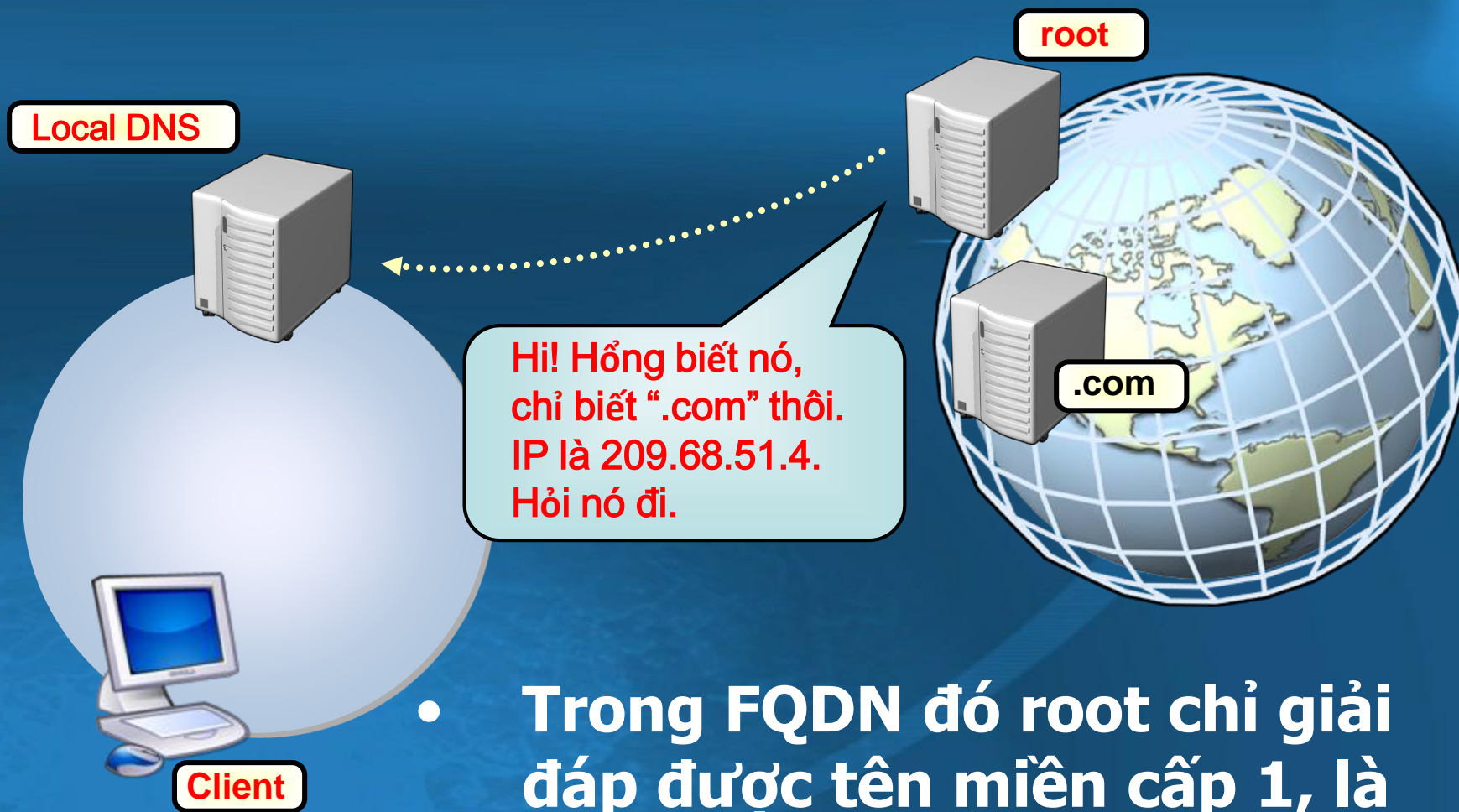
- Khi nhận được truy vấn từ client, DNS server sẽ tìm trong cache hoặc trong CSDL của nó để IP tương ứng của host mà client cần truy vấn, rồi hồi đáp lại cho client.



## \* TRƯỜNG HỢP 2 .

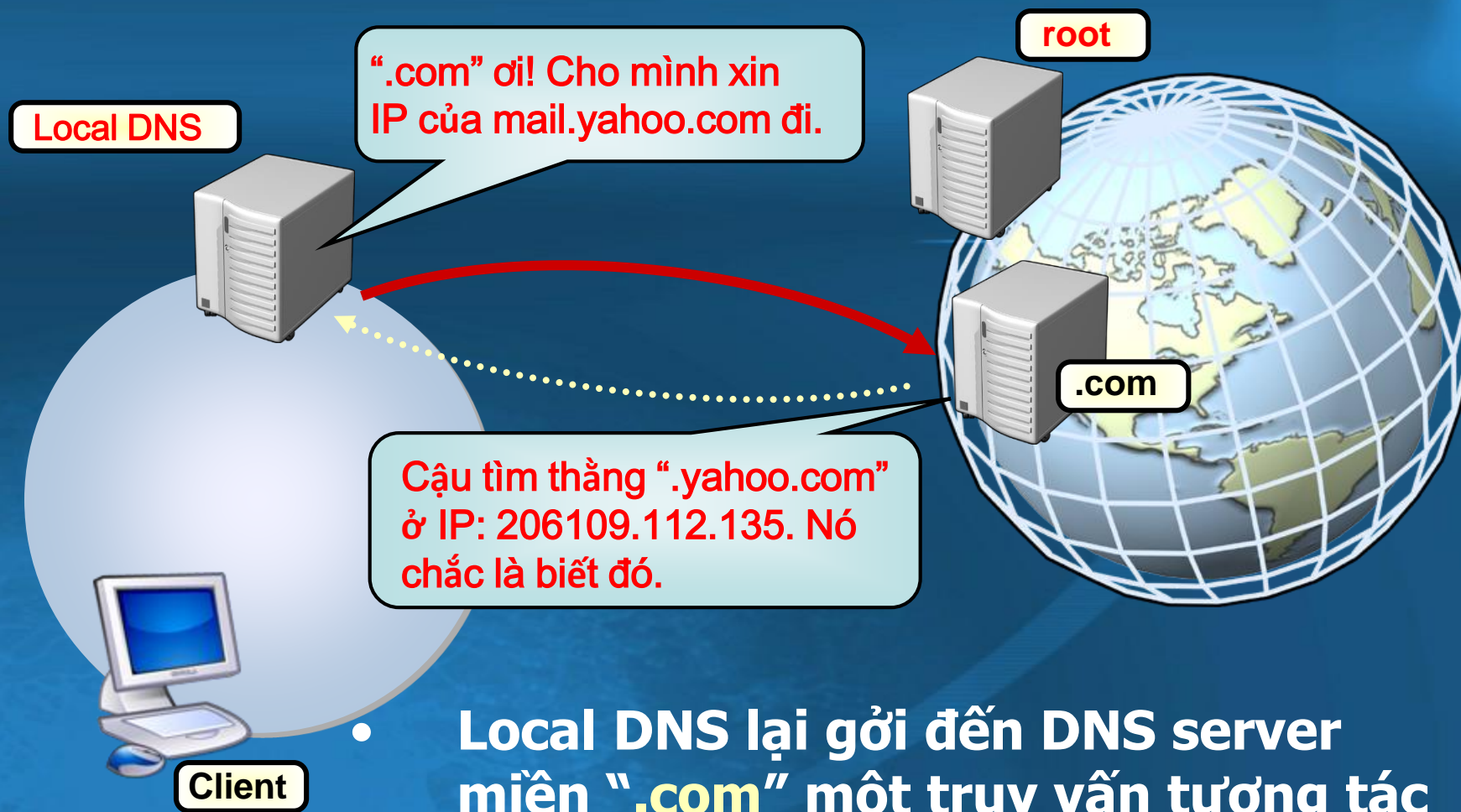


- Local Server sẽ gửi 1 truy vấn tương tác (Iterative Queries\*) lên Root Hints, hỏi địa chỉ của mail.yahoo.com

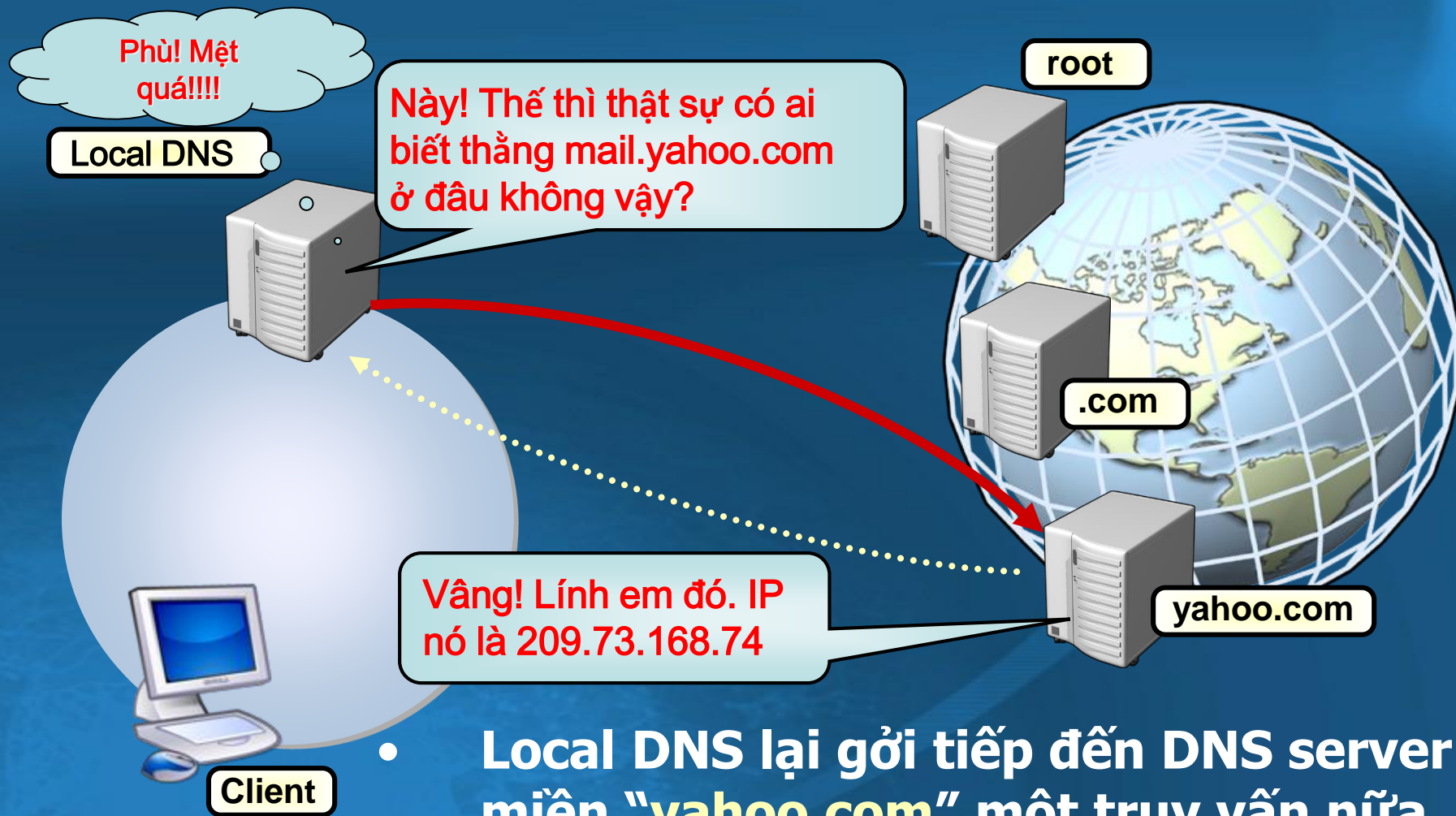


- Trong FQDN đó root chỉ giải đáp được tên miền cấp 1, là miền nó quản lý. Đó là kết quả tốt nhất mà nó biết.





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



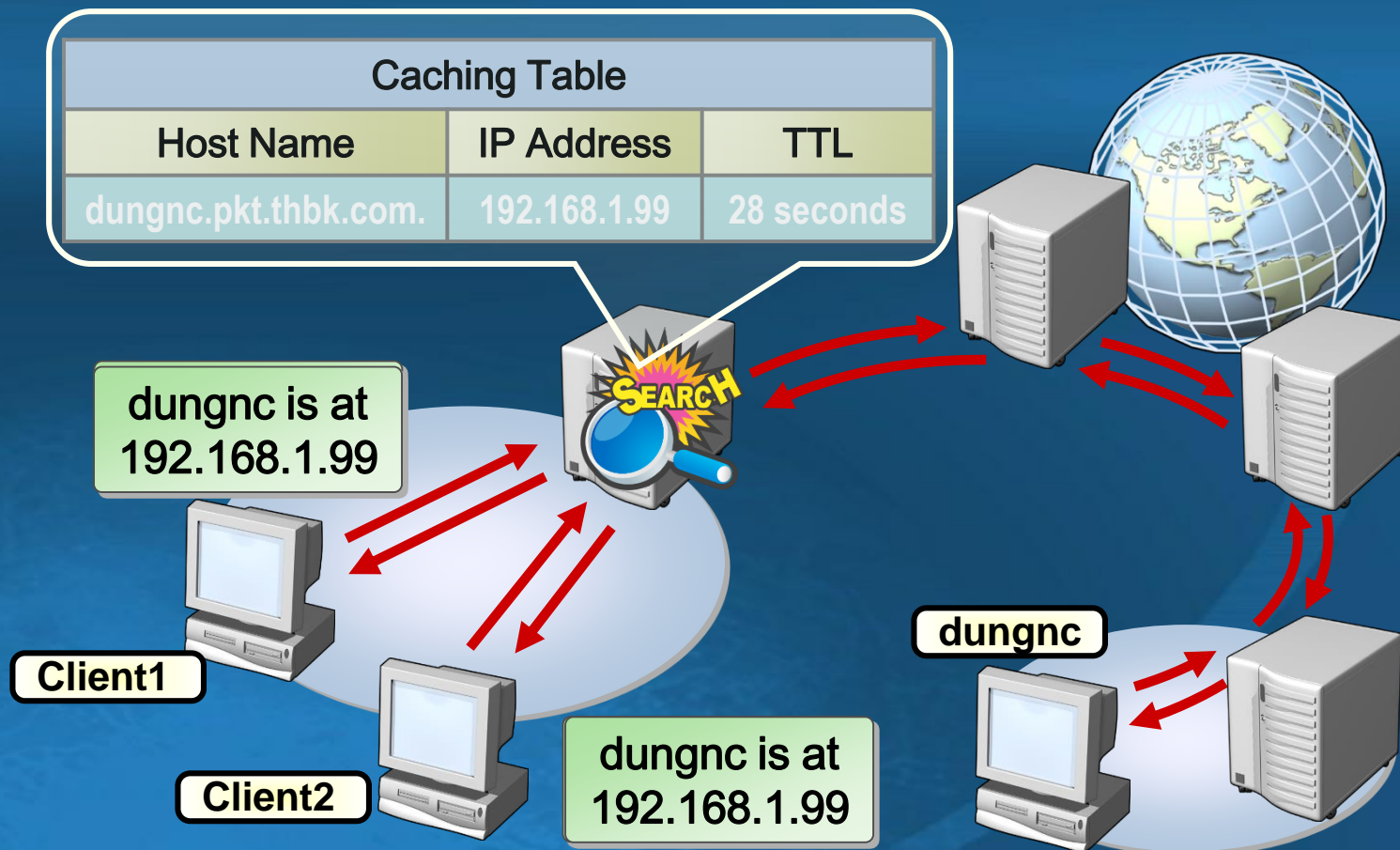
- Local DNS lại gửi tiếp đến DNS server miền "**yahoo.com**" một truy vấn nữa.
- Zone này do nó quản lý, nên Name Server này trả lời chính xác được truy vấn đó.



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



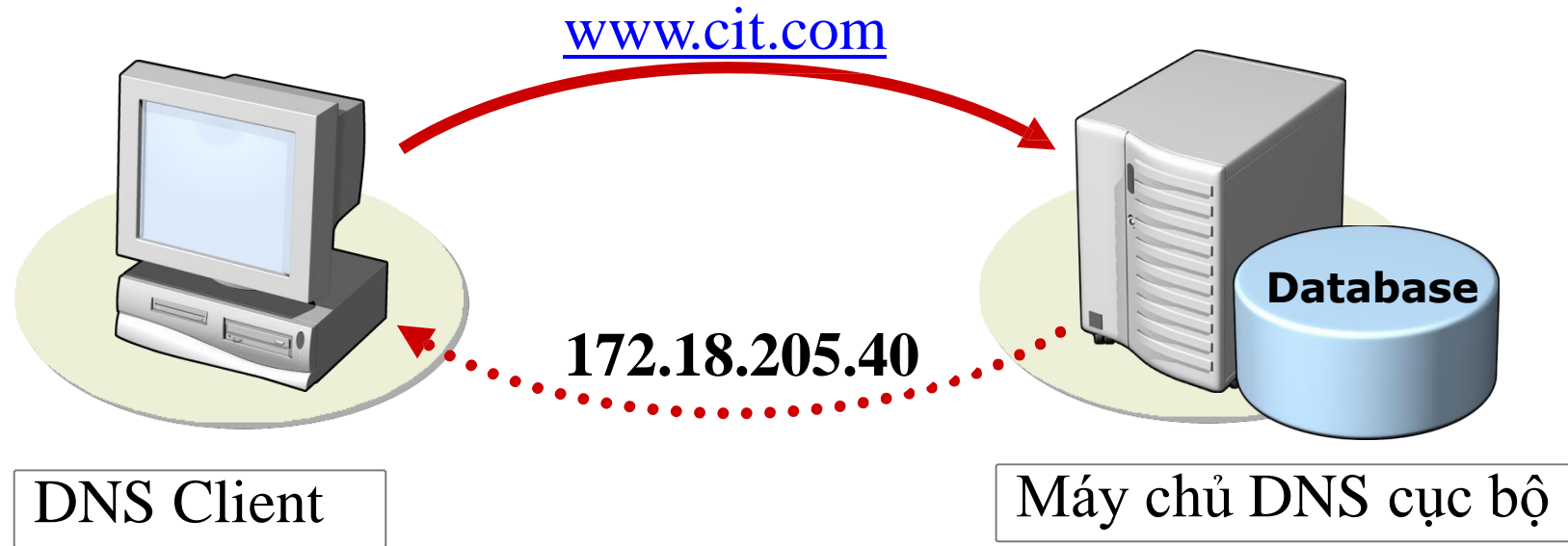
# \* caching.



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?

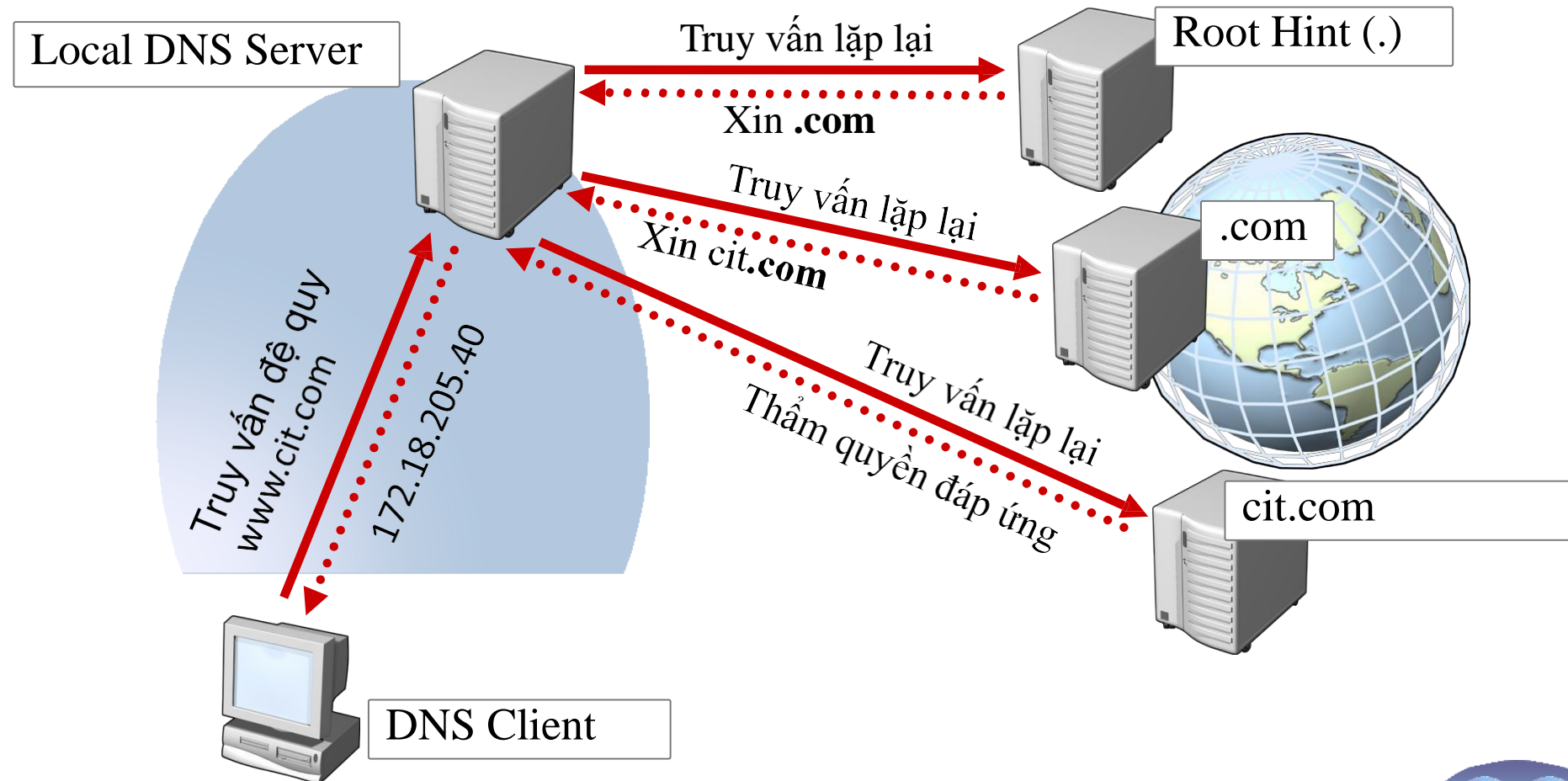
Một câu truy vấn đệ quy được gửi tới một máy chủ DNS và yêu cầu một câu trả lời hoàn chỉnh





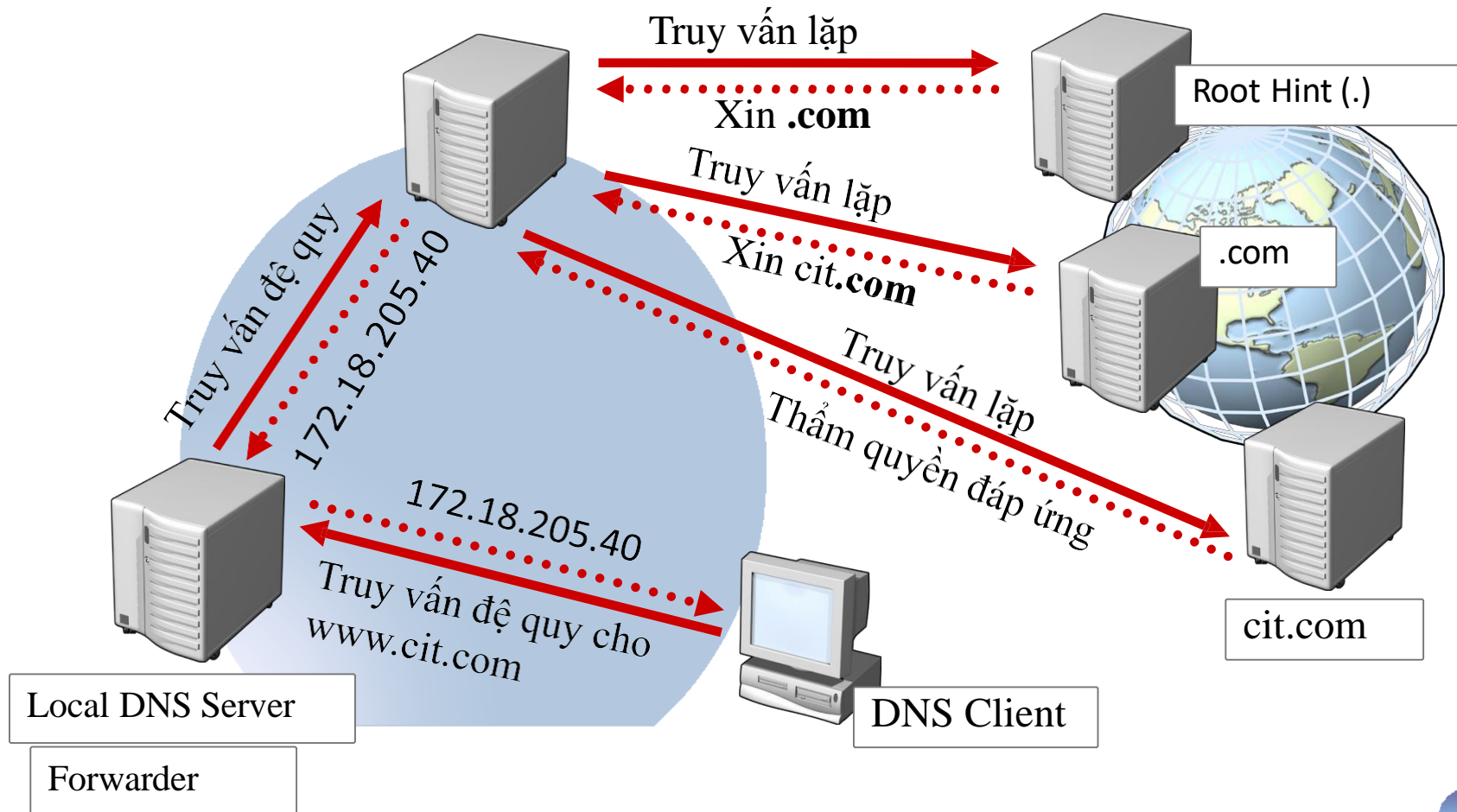
# Truy vấn lặp là gì?

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



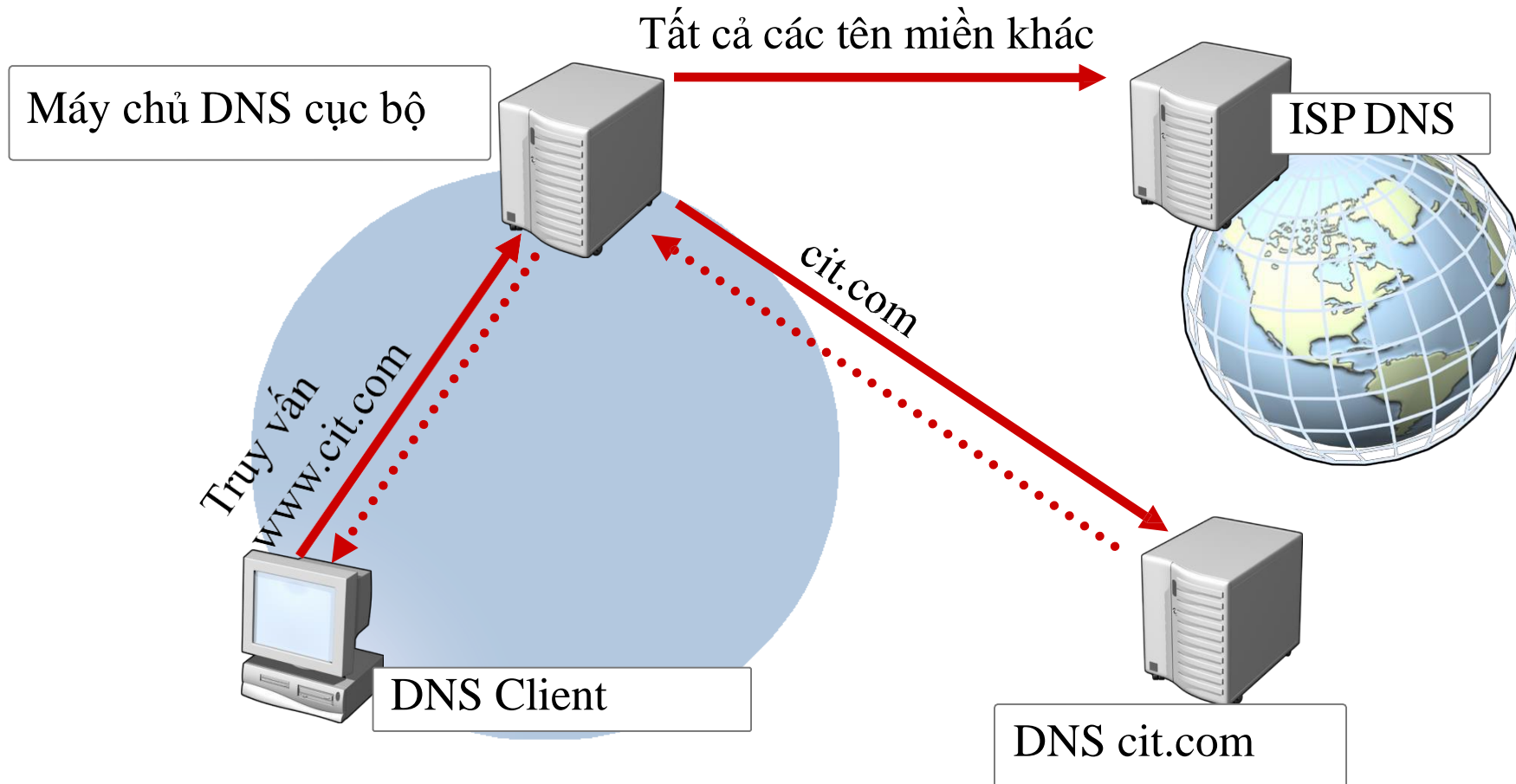
# Chuyển tiếp là gì?

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?

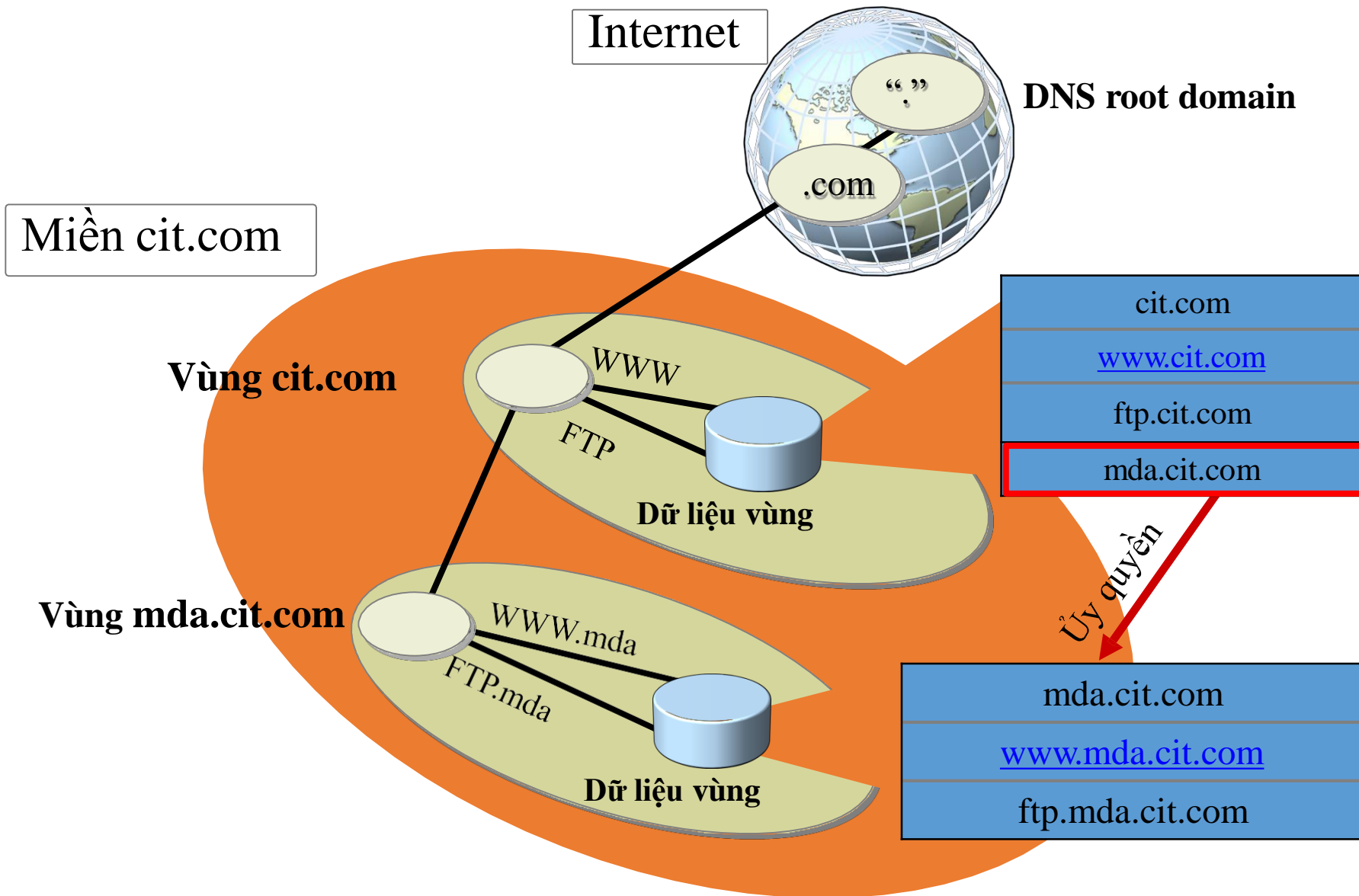
Chuyển tiếp có điều kiện cho phép DNS cục bộ chuyển tiếp các yêu cầu phân giải theo tên miền trong truy vấn yêu cầu



# 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

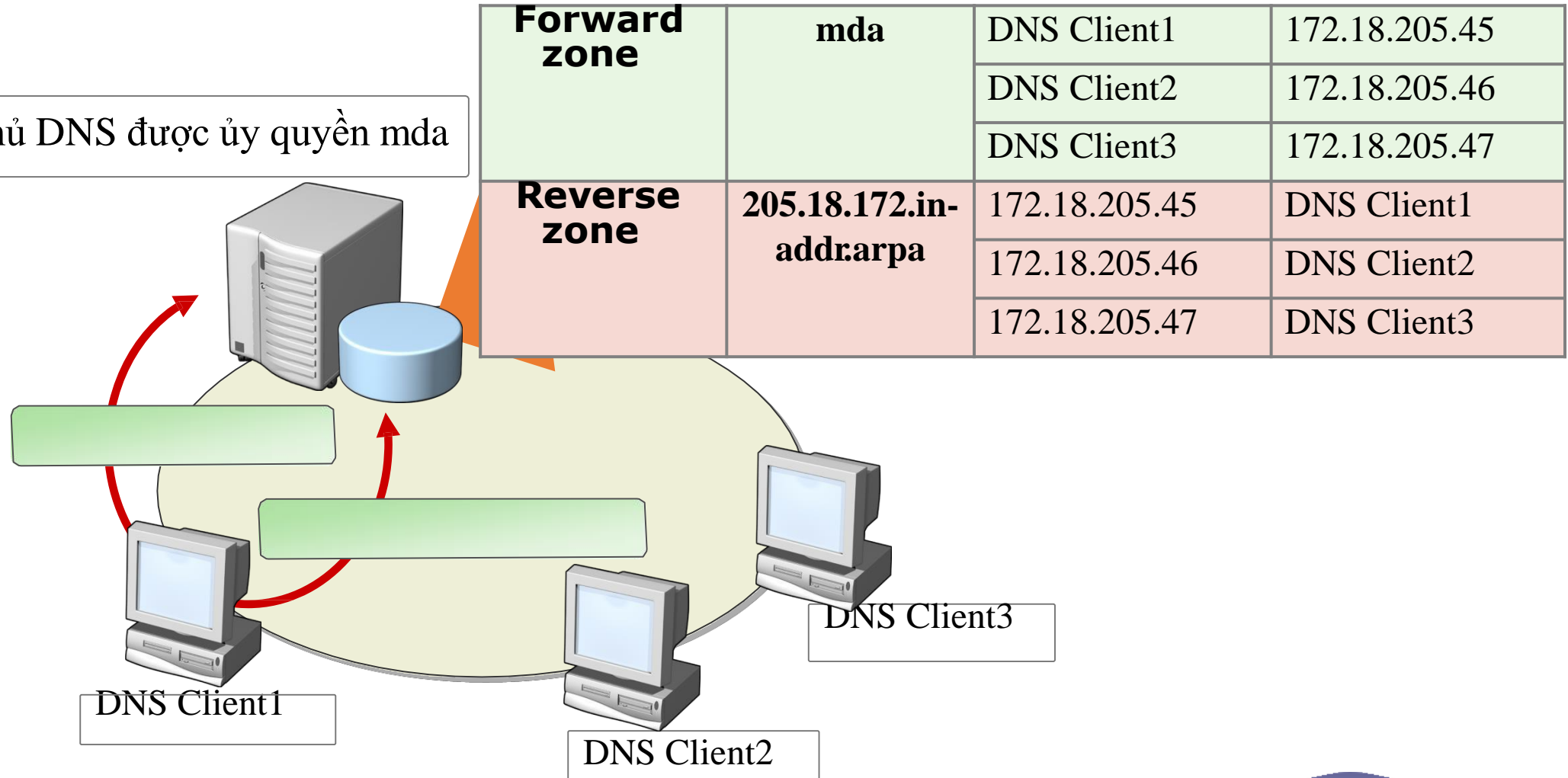
# Name Server trên Internet

- ❖ 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 một hoặc nhiều miền con
- ❖ Một Name Server có thể phụ trách một hoặc nhiều ZOA

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

Không gian: mda.cit.com

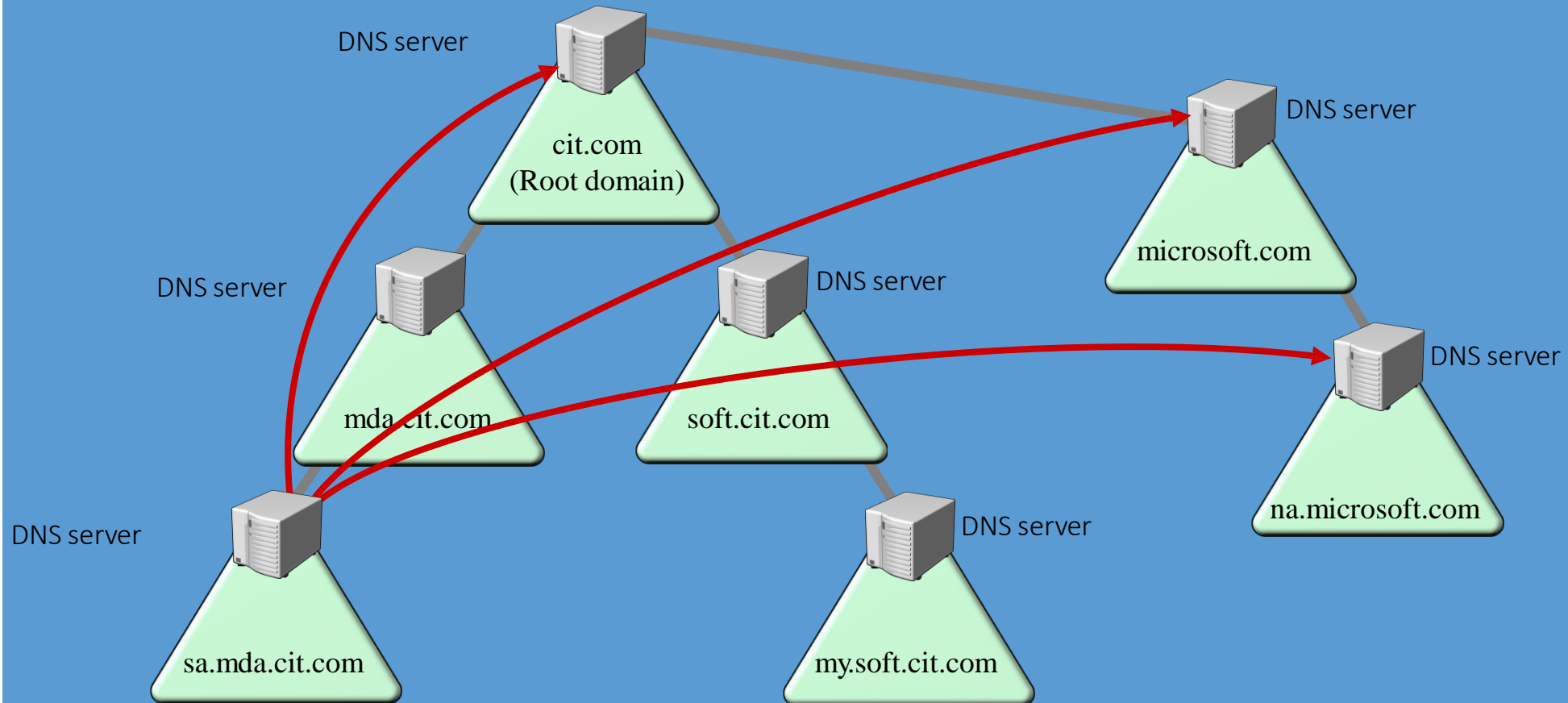
Máy chủ DNS được ủy quyền mda





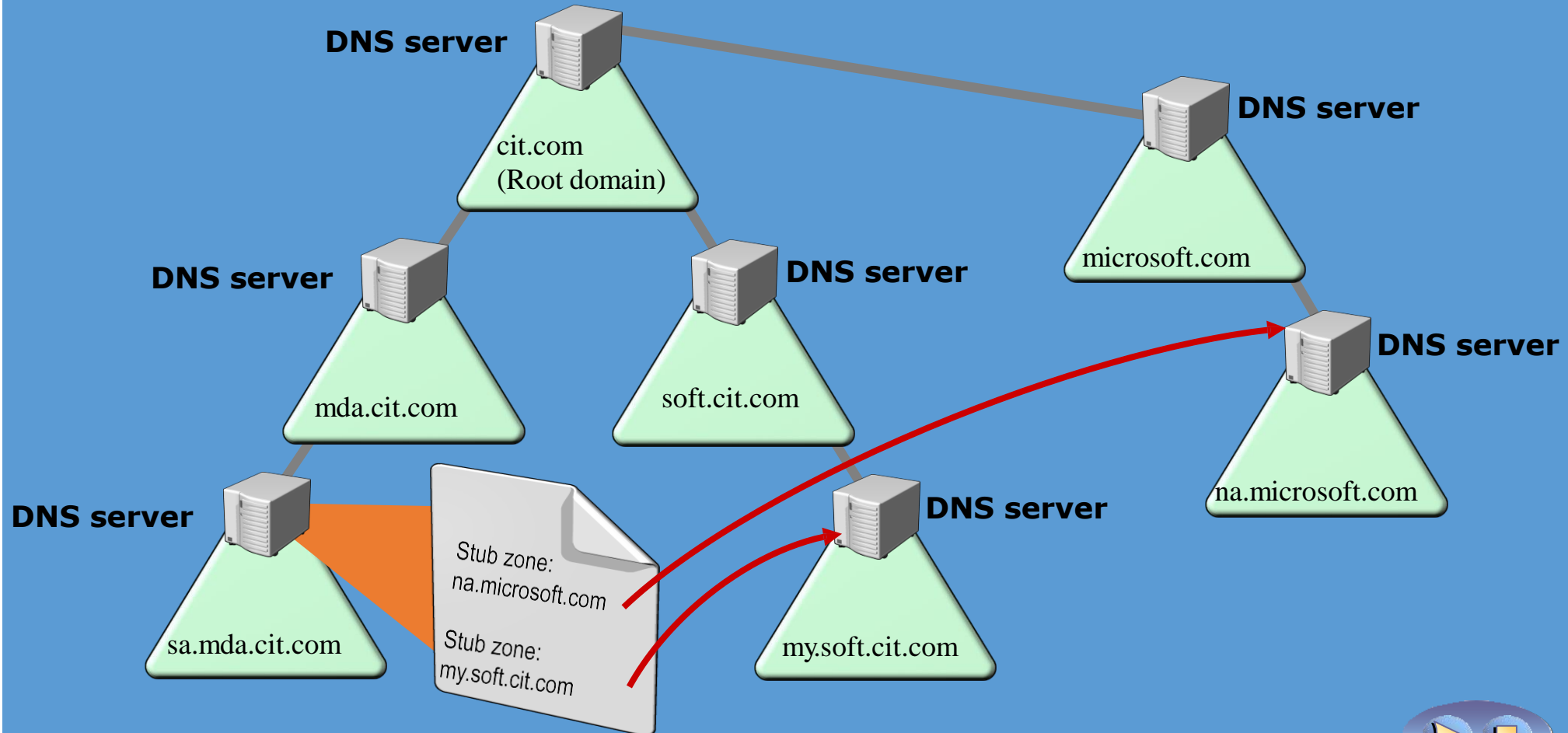
# Stub Zones là gì?

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

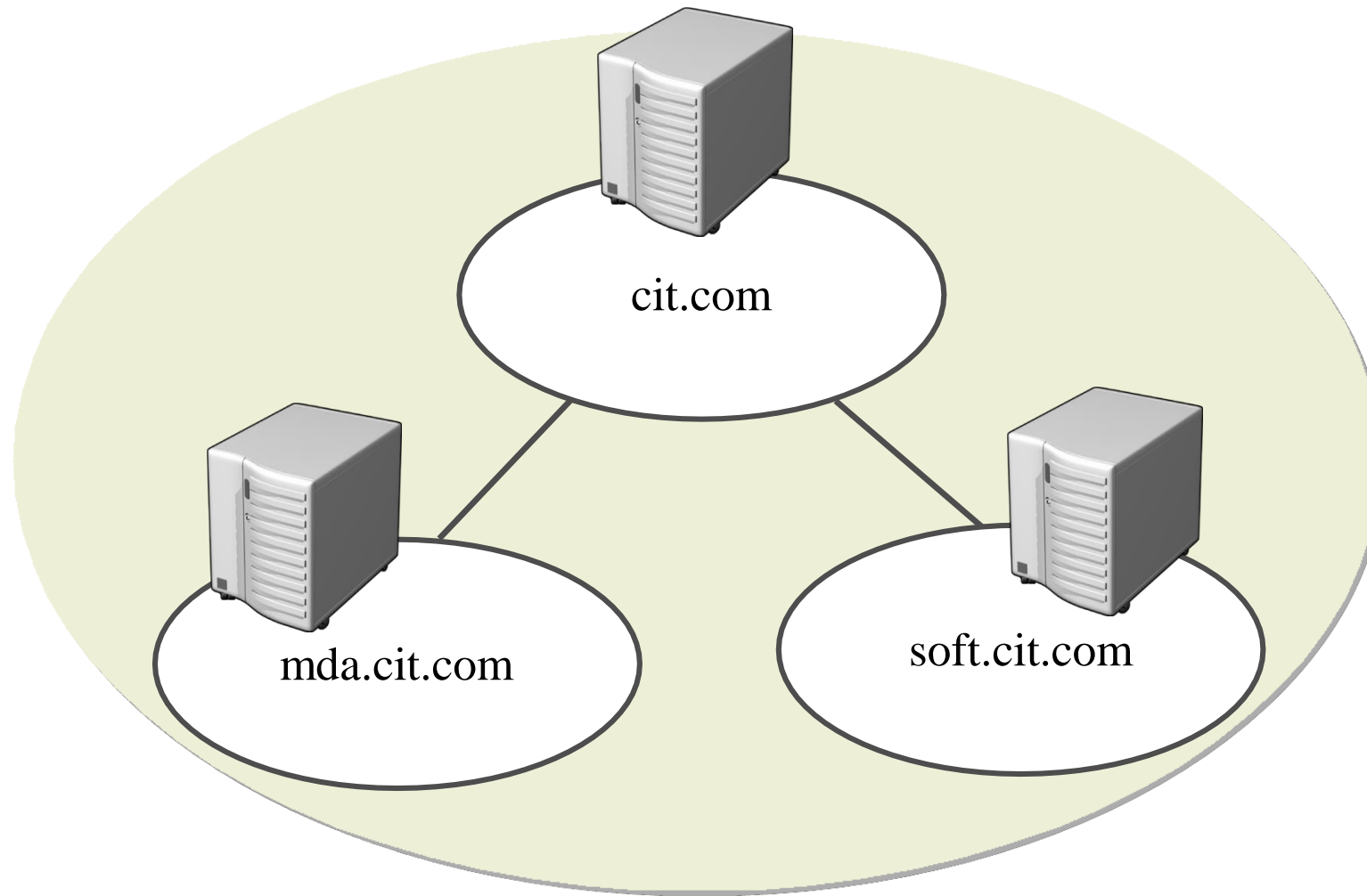


# Stub Zones là gì?

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](http://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
- ☐ AAAA: IPv6 DNS Record

The screenshot shows the 'domain41.com Properties' dialog box with the 'Start of Authority (SOA)' tab selected. The fields are as follows:

Field	Value	Unit
Serial number	52	
Primary server	server41.domain41.com	
Responsible person	hostmaster.domain41.com	
Refresh interval	15	minutes
Retry interval	10	minutes
Expires after	1	days
Minimum (default) TTL	1	hours
TTL for this record	0	:1:0:0 (DDDD:HH.MM.SS)

# 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 nó

➤(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)

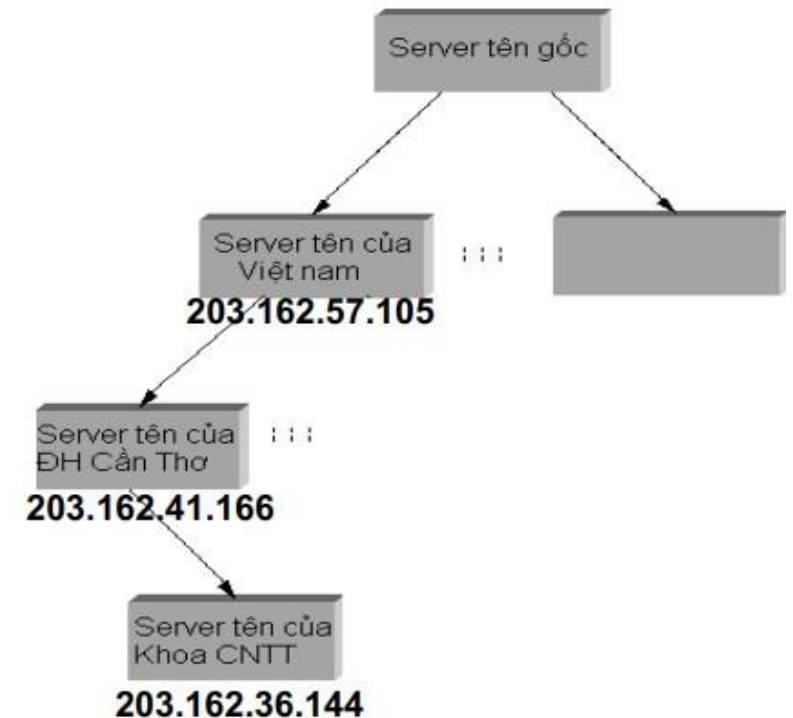
# Cơ sở dữ liệu của DNS

## ❖ 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)





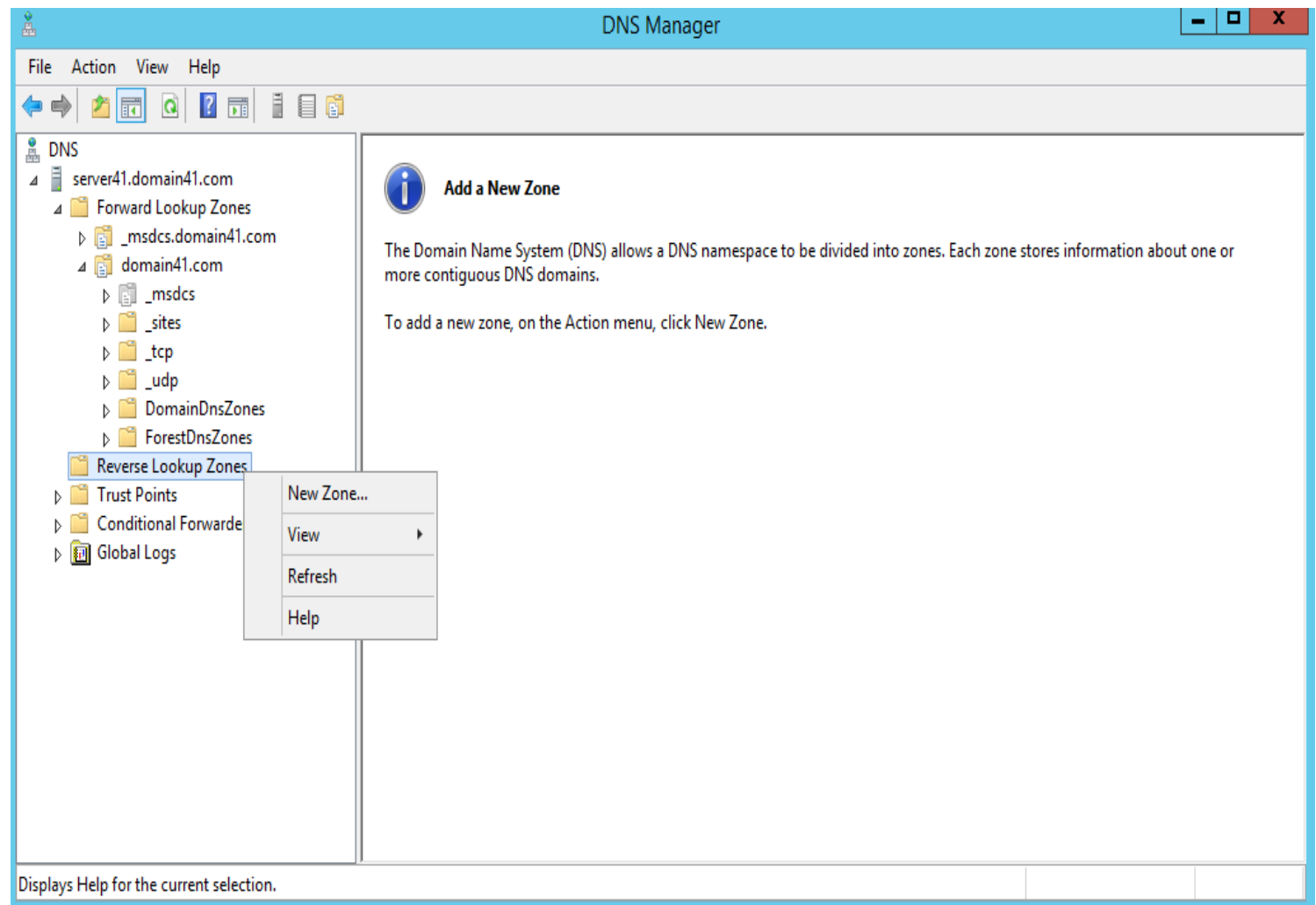
# Tiến trình phân tích tên

- ❖ 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)



# Cài đặt và Cấu hình DNS

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



# Cài đặt và Cấu hình DNS

**New Zone Wizard** [X]

**Zone Type**  
The DNS server supports various types of zones and storage.

Select the type of zone you want to create:

- ☒ **Primary zone**  
Creates a copy of a zone that can be updated directly on this server.
- ☐ **Secondary zone**  
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.
- ☐ **Stub zone**  
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.

☒ **Store the zone in Active Directory** (available only if DNS server is a writeable domain controller)

< Back   Next >   Cancel

**New Zone Wizard** [X]

**Active Directory Zone Replication Scope**  
You can select how you want DNS data replicated throughout your network.

Select how you want zone data replicated:

- ☐ To all DNS servers running on domain controllers in this forest: domain41.com
- ☒ To all DNS servers running on domain controllers in this domain: domain41.com
- ☐ To all domain controllers in this domain (for Windows 2000 compatibility): domain41.com
- ☐ To all domain controllers specified in the scope of this directory partition:

< Back   Next >   Cancel

# Cài đặt và Cấu hình DNS

New Zone Wizard

**Reverse Lookup Zone Name**  
A reverse lookup zone translates IP addresses into DNS names.

Choose whether you want to create a reverse lookup zone for IPv4 addresses or IPv6 addresses.

☒ IPv4 Reverse Lookup Zone  
☐ IPv6 Reverse Lookup Zone

< Back   Next >   Cancel

New Zone Wizard

**Reverse Lookup Zone Name**  
A reverse lookup zone translates IP addresses into DNS names.

To identify the reverse lookup zone, type the network ID or the name of the zone.

☒ Network ID:  
192 .168 .2

The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.

If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.

☐ Reverse lookup zone name:  
2.168.192.in-addr.arpa

< Back   Next >   Cancel



# Cài đặt và Cấu hình DNS


**New Zone Wizard**

**Dynamic Update**

You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.

Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur.

Select the type of dynamic updates you want to allow:

- ☒ Allow only secure dynamic updates (recommended for Active Directory)  
This option is available only for Active Directory-integrated zones.
- ☐ Allow both nonsecure and secure dynamic updates  
Dynamic updates of resource records are accepted from any client.  
 This option is a significant security vulnerability because updates can be accepted from untrusted sources.
- ☐ Do not allow dynamic updates  
Dynamic updates of resource records are not accepted by this zone. You must update these records manually.

< Back   Next >   Cancel

**New Zone Wizard**

**Completing the New Zone Wizard**

You have successfully completed the New Zone Wizard. You specified the following settings:

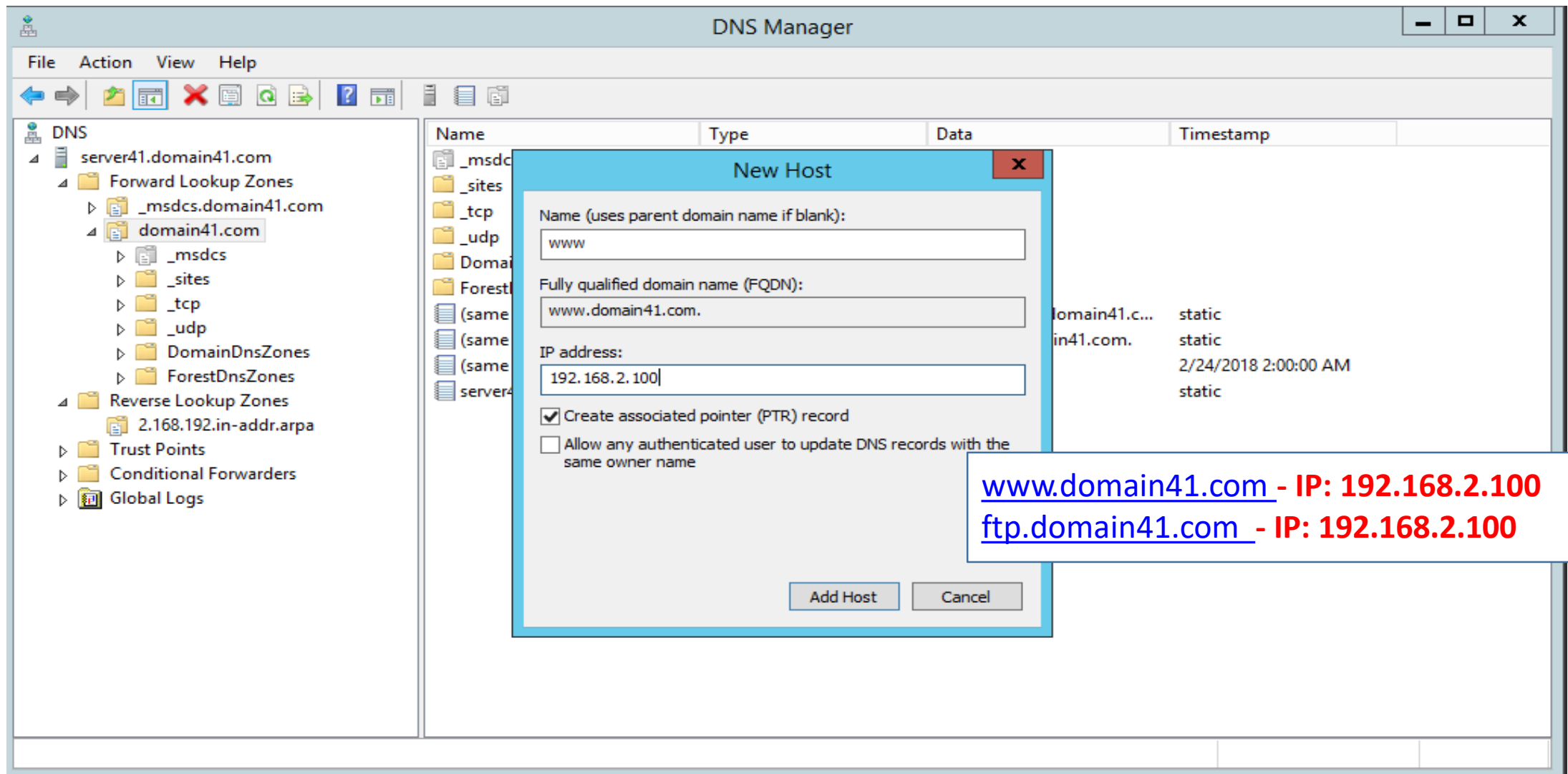
Name:	2.168.192.in-addr.arpa
Type:	Active Directory-Integrated Primary
Lookup type:	Reverse

Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup.

To close this wizard and create the new zone, click Finish.

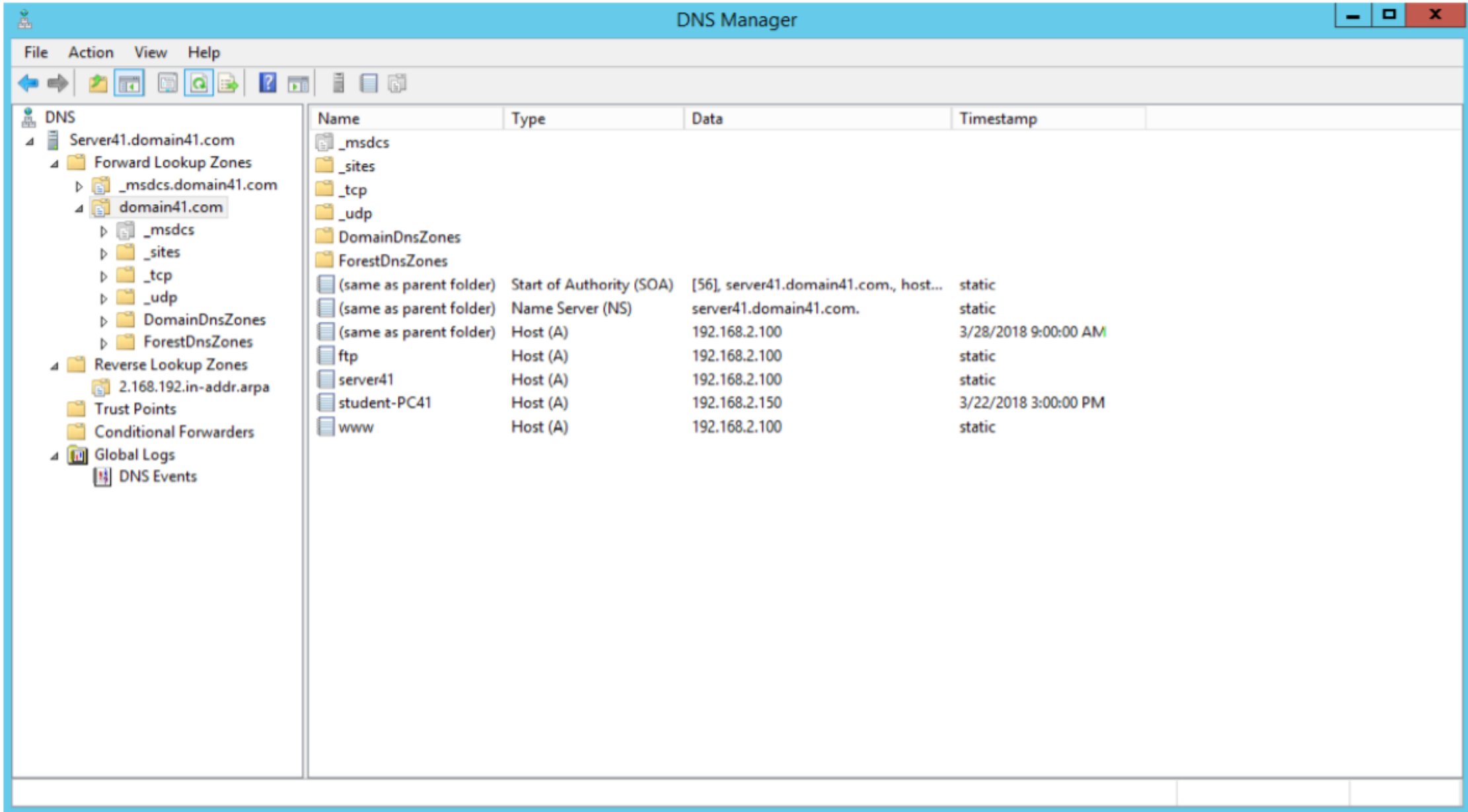
< Back   Finish   Cancel

# Cài đặt và Cấu hình DNS



[www.domain41.com](http://www.domain41.com) - IP: 192.168.2.100  
[ftp.domain41.com](http://ftp.domain41.com) - IP: 192.168.2.100

# Forward Lookup Zones

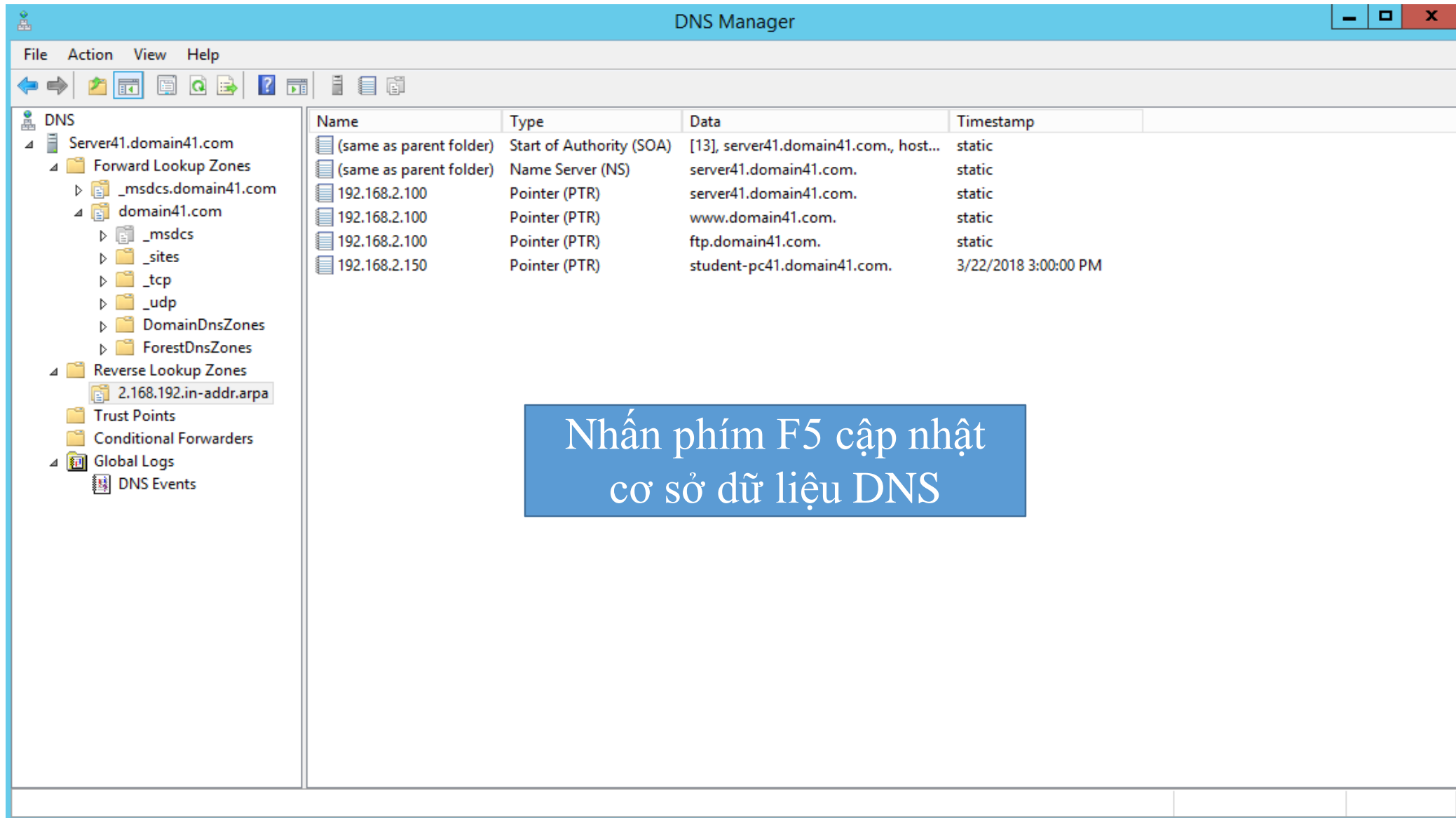


The screenshot displays the DNS Manager application window. The left pane shows the tree structure of the DNS hierarchy, with 'domain41.com' selected under 'Forward Lookup Zones'. The right pane shows a list of DNS records for this zone.

Name	Type	Data	Timestamp
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(same as parent folder)	Start of Authority (SOA)	[56], server41.domain41.com., host...	static
(same as parent folder)	Name Server (NS)	server41.domain41.com.	static
(same as parent folder)	Host (A)	192.168.2.100	3/28/2018 9:00:00 AM
ftp	Host (A)	192.168.2.100	static
server41	Host (A)	192.168.2.100	static
student-PC41	Host (A)	192.168.2.150	3/22/2018 3:00:00 PM
www	Host (A)	192.168.2.100	static



# Reverse Lookup Zones



The screenshot shows the DNS Manager application window. The left pane displays the tree structure of the DNS configuration for Server41.domain41.com. The right pane shows the details of the selected Reverse Lookup Zone, 2.168.192.in-addr.arpa, which contains several PTR records.

Name	Type	Data	Timestamp
(same as parent folder)	Start of Authority (SOA)	[13], server41.domain41.com., host...	static
(same as parent folder)	Name Server (NS)	server41.domain41.com.	static
192.168.2.100	Pointer (PTR)	server41.domain41.com.	static
192.168.2.100	Pointer (PTR)	www.domain41.com.	static
192.168.2.100	Pointer (PTR)	ftp.domain41.com.	static
192.168.2.150	Pointer (PTR)	student-pc41.domain41.com.	3/22/2018 3:00:00 PM

Trong ảnh chụp màn hình, giao diện DNS Manager hiển thị cấu hình DNS cho Server41.domain41.com. Bên trái là cây thư mục, bên phải là danh sách các bản ghi. Một hộp thoại thông báo màu xanh dương ở trung tâm màn hình khuyến nghị nhấn phím F5 để cập nhật cơ sở dữ liệu DNS.

Nhấn phím F5 cập nhật  
cơ sở dữ liệu DNS

# Kiểm tra DNS

```
C:\> 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>
```