

# **WINDOWS SERVER 2012**

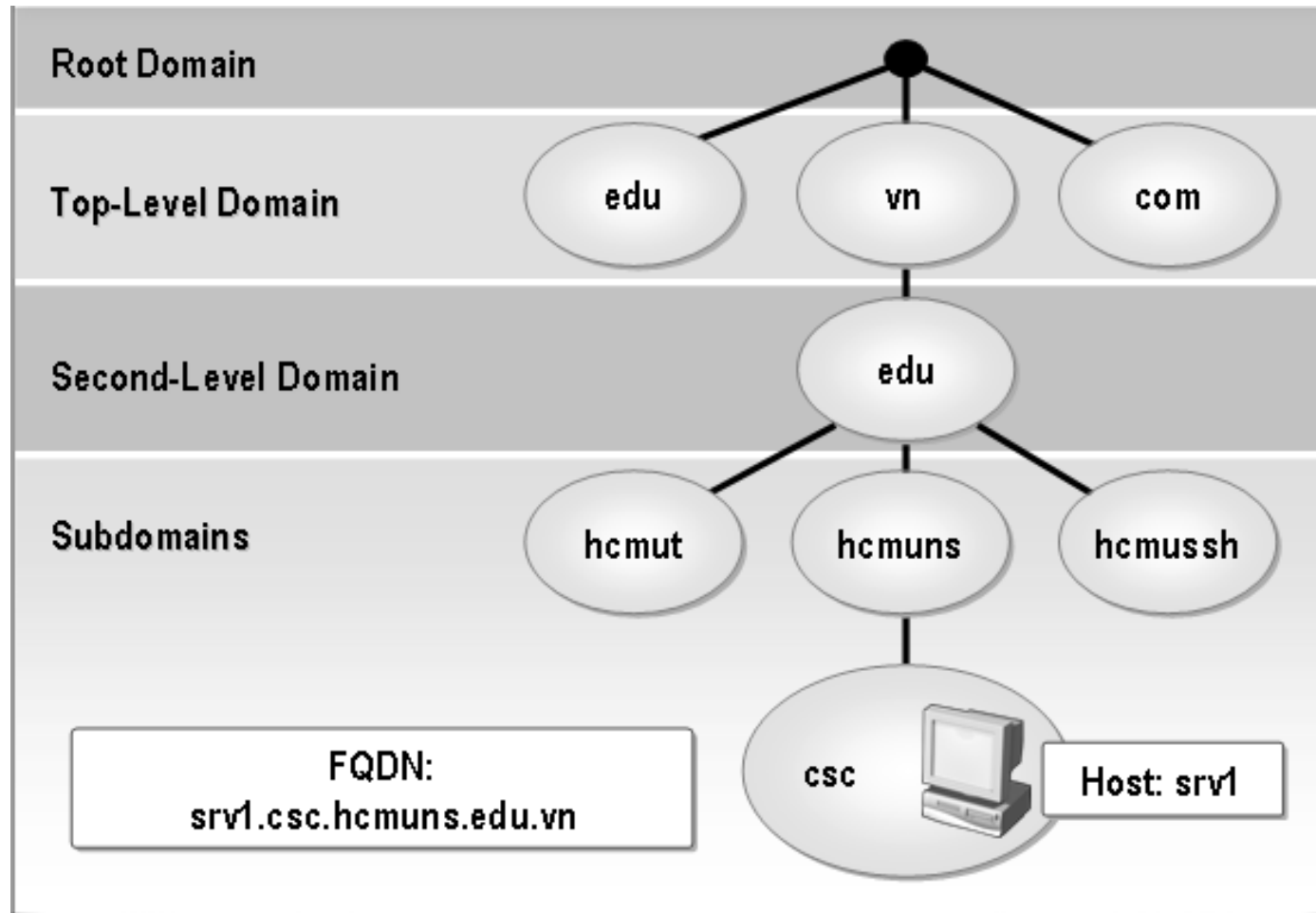
## **Bài 5**

### **DOMAIN NAME SYSTEM (DNS)**

# Giới thiệu dịch vụ DNS

- DNS là dịch vụ quản lý tên miền.
- Dịch vụ DNS do Paul Mockapetris - USC's Information Sciences Institute thiết kế,
- Hoạt động theo mô hình Client-Server.
- Cơ sở dữ liệu DNS được phân tán trên nhiều Name Server.
- Hiệu suất sử dụng tăng nhờ cơ chế nhân bản(replication) và lưu tạm(caching).
- Domain được phân bổ theo cơ chế phân cấp tương tự như sự phân bổ trong hệ thống UNIX.

# Giới thiệu dịch vụ DNS(t.t.)



Sơ đồ tổ chức DNS

# Giới thiệu dịch vụ DNS(t.t.)

## Các Top-Level Domain:

**.com**

**.org**

**.net**

**.edu**

**.gov**

**.mil**

**.int**

**.arts**

**.nom**

**.rec**

**...**

**.vn**

**.us**

**.ca**

**.jp**

**.cn**

**uk**

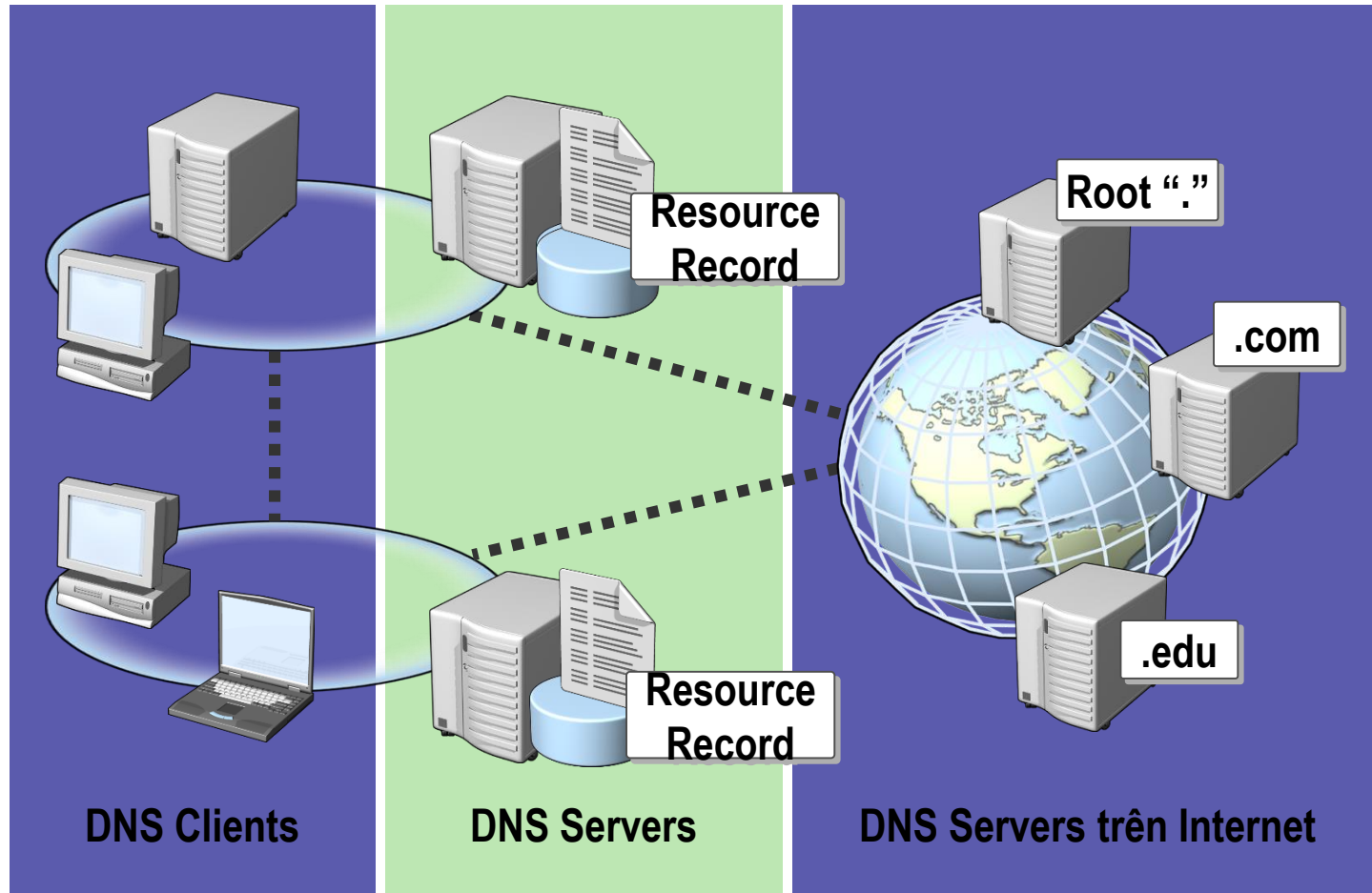
**us**

**tw**

**...**

# Giới thiệu dịch vụ DNS(t.t.)

## Các thành phần trong dịch vụ DNS:



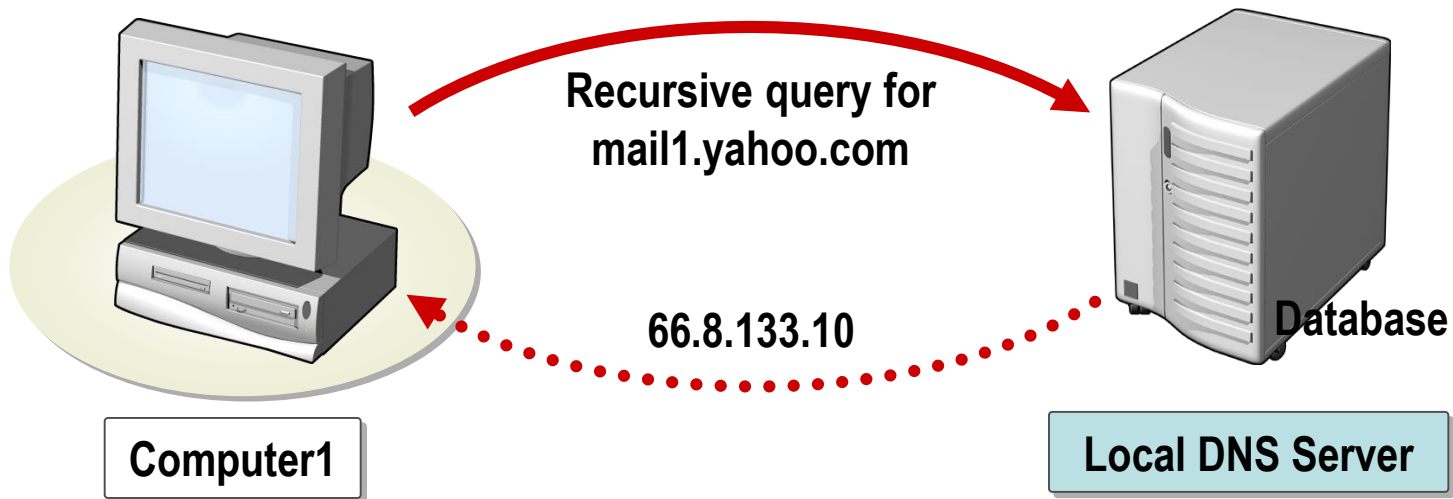
# Truy vấn thông tin

- Truy vấn là quá trình gửi yêu cầu phân giải tên miền tới DNS Server, có hai loại truy vấn : truy vấn đệ quy (recursive query) và truy vấn tương tác (Iteractive query).
- DNS Client và DNS Server Khởi tạo Truy Vấn cho việc phân giải tên miền.
- Authoritative DNS server sẽ thực hiện:
  - Kiểm tra cache, kiểm tra zone, gửi IP address cho truy vấn.
- Non-authoritative DNS server sẽ thực hiện:
  - Chuyển yêu cầu truy vấn không thể phân giải đến Forwarder server.
  - Sử dụng root hints server để trả lời cho truy vấn.

# Recursive query

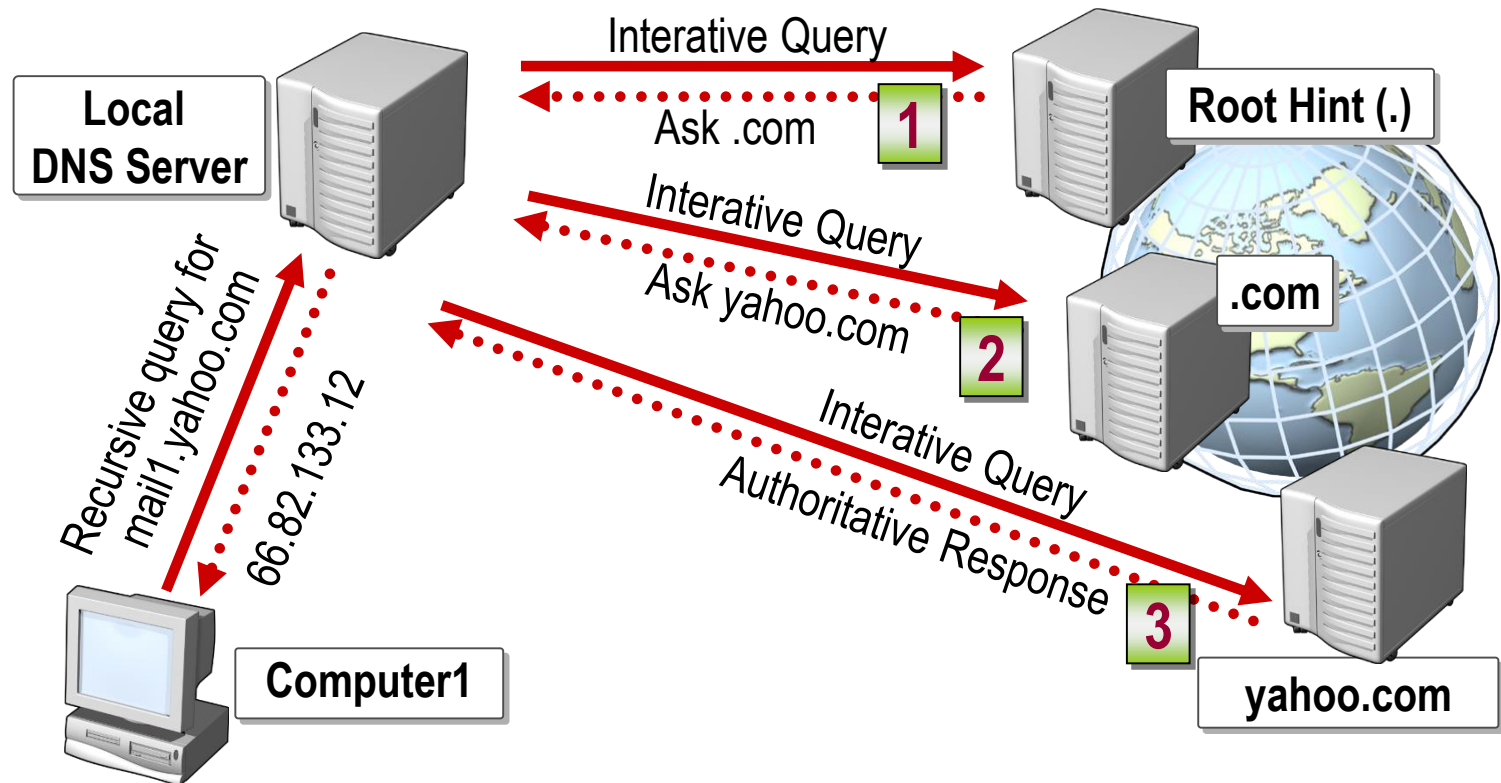
*recursive query* được gửi tới DNS server, trong đó DNS client yêu cầu DNS server cung cấp đầy đủ thông tin cho truy vấn.

DNS server kiểm tra forward lookup zone và cache để trả lời truy vấn



# Interactive query

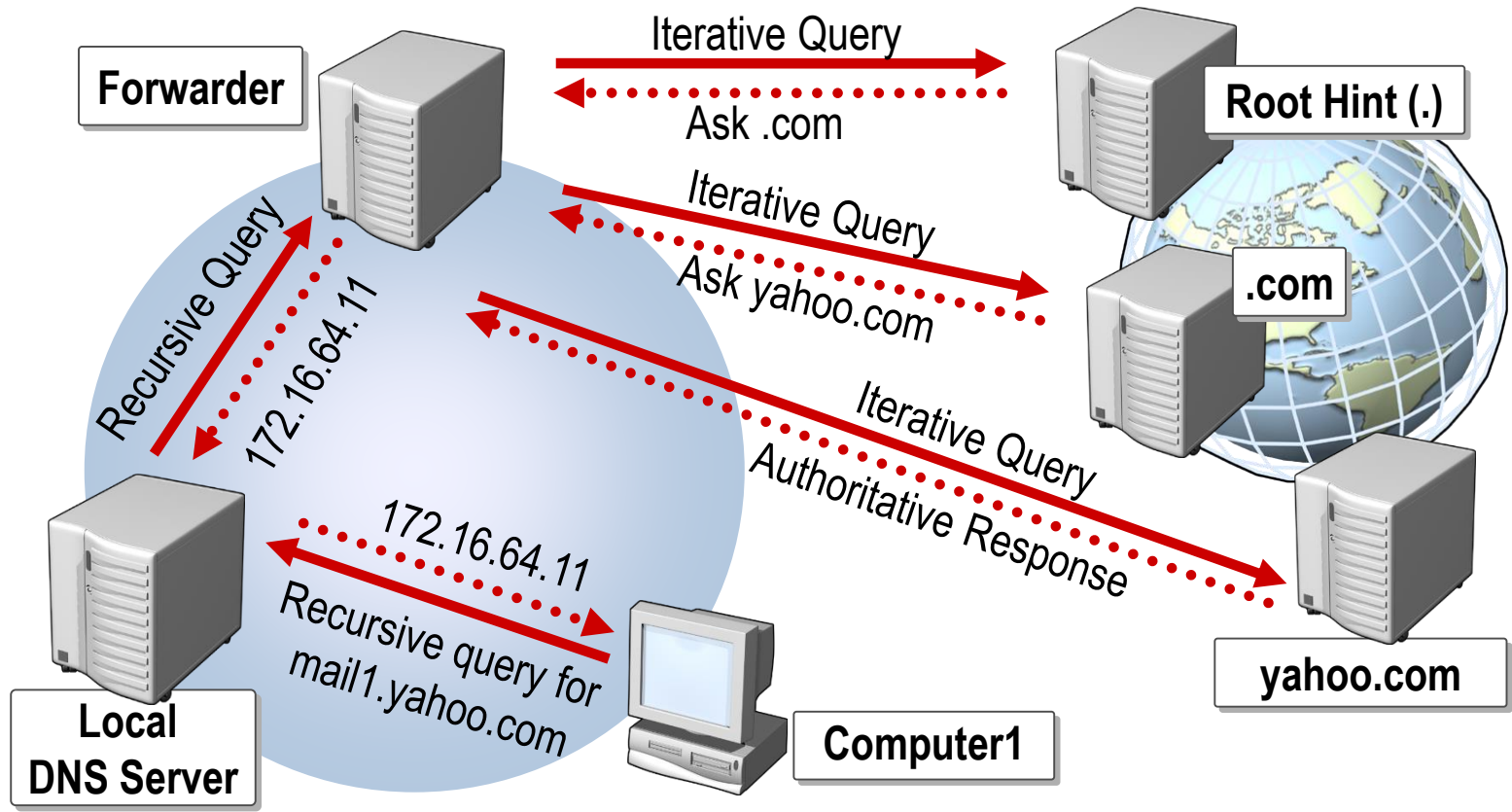
*interactive query* là truy vấn được gửi tới DNS server trong đó DNS client yêu cầu DNS server cung cấp thông tin tốt nhất mà nó có chứ không tìm sự trợ giúp từ Name server khác. ACK của interactive query thường tham chiếu đến DNS server con trong DNS tree.





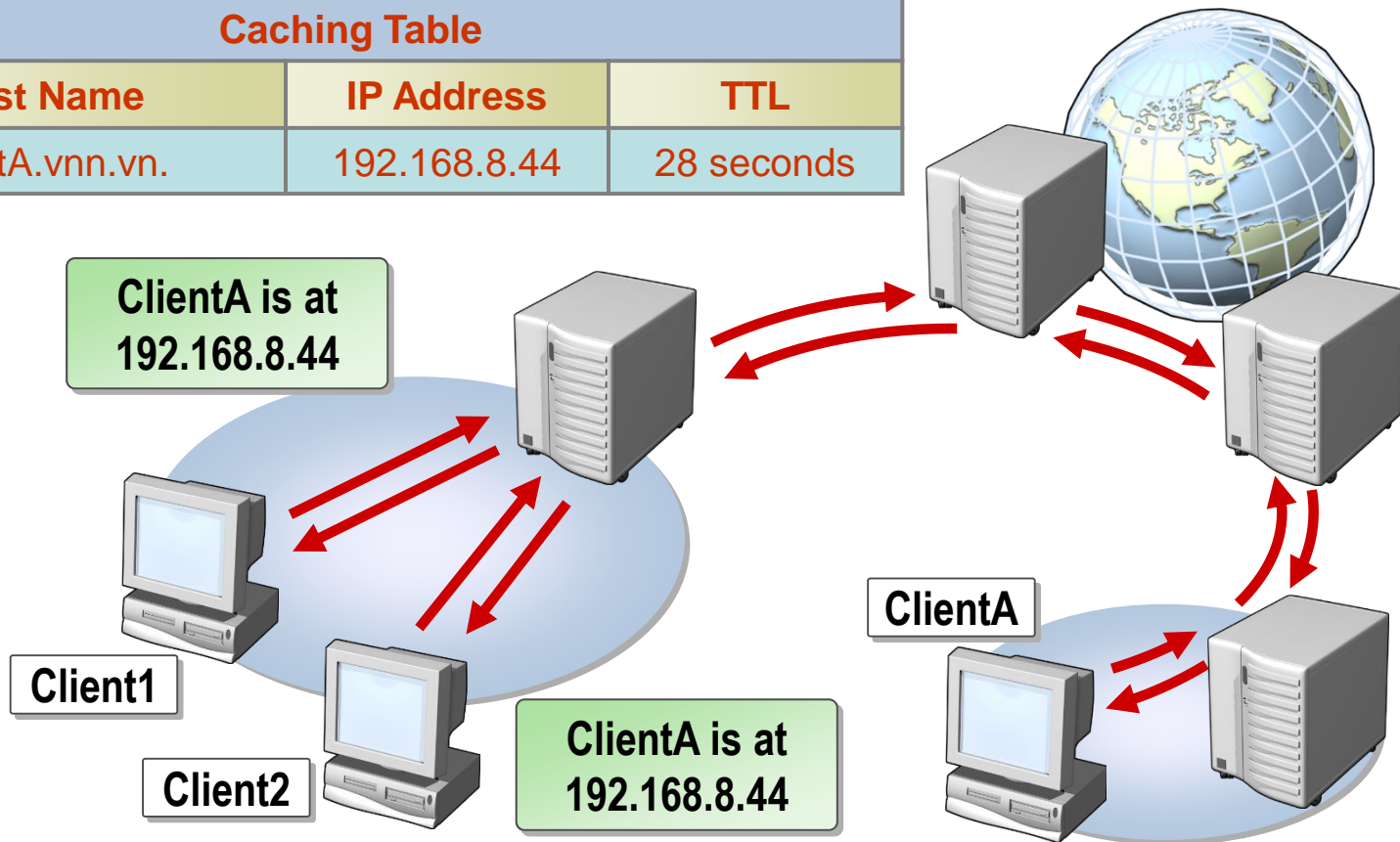
# Forwarder

*forwarder* cung cấp cơ chế chuyển yêu cầu truy vấn cho internal DNS servers ra ngoài external DNS server



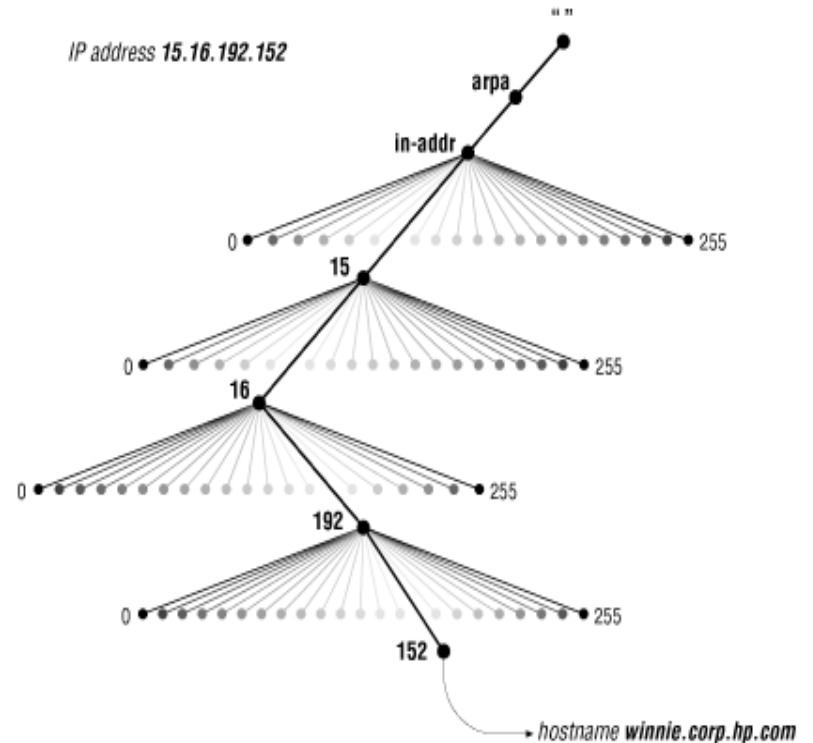
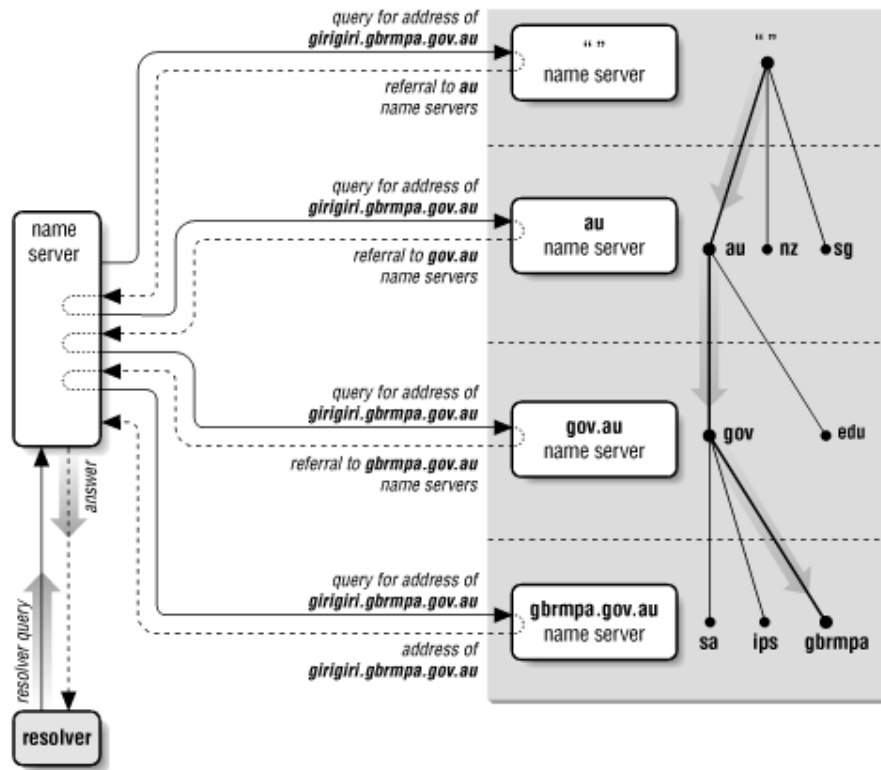
# Caching DNS Server

Caching Table		
Host Name	IP Address	TTL
clientA.vnn.vn.	192.168.8.44	28 seconds



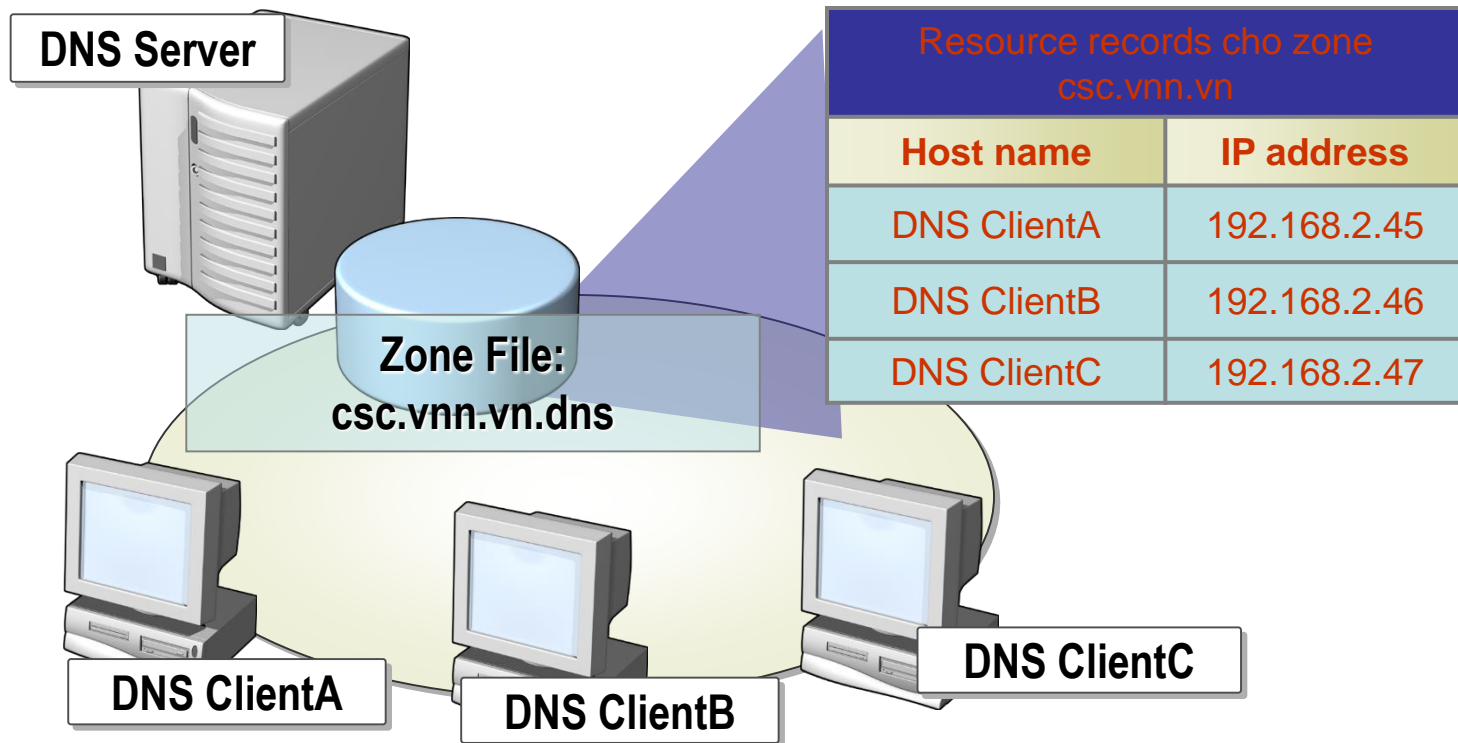
**Caching** là tiến trình lưu trữ tạm một số thông tin phân giải trước để cung cấp cho các lần phân giải sau này nhằm làm tăng tốc quá trình phân giải tên miền

# Phân giải địa chỉ



# Cơ chế lưu trữ và duy trì CSDL

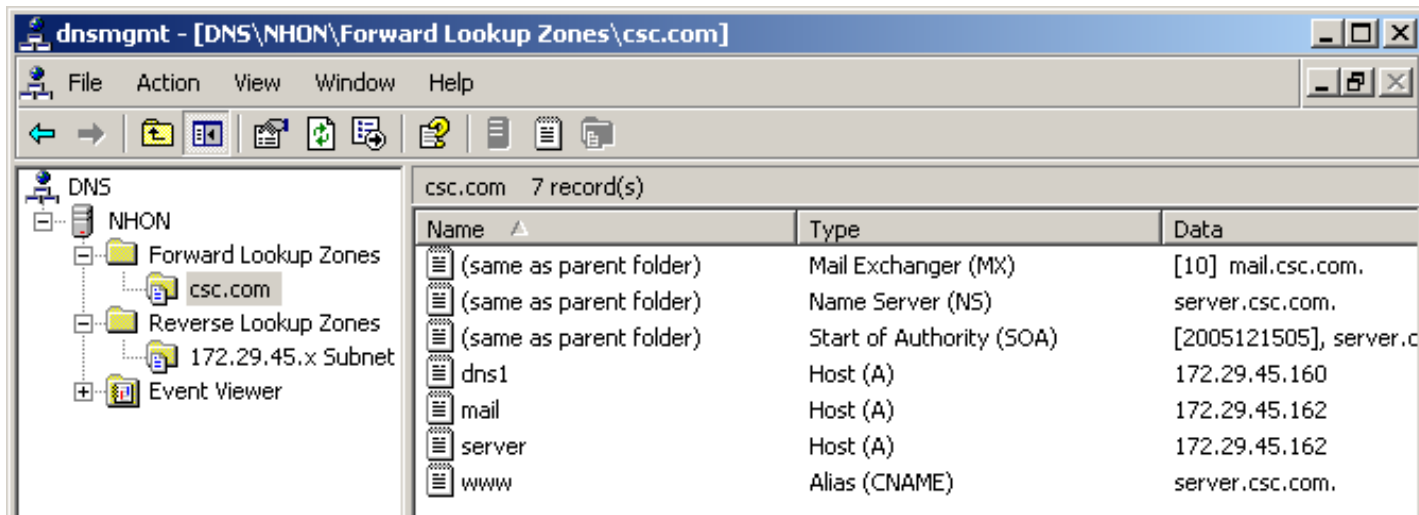
Namespace: csc.vnn.vn



**resource record (RR)** là chuẩn cấu trúc của DNS database chứa thông tin cần thiết cung cấp cho các yêu cầu truy vấn DNS

**zone file** là thành phần của DNS database chứa các resource records

# Resource record và record type



The screenshot shows the dnsmgmt console window titled "dnsmgmt - [DNS\NHON\Forward Lookup Zones\csc.com]". The left pane shows a tree view with "DNS" expanded, then "NHON", then "Forward Lookup Zones", and finally "csc.com" selected. The right pane shows a list of 7 records for the "csc.com" zone. The records are as follows:

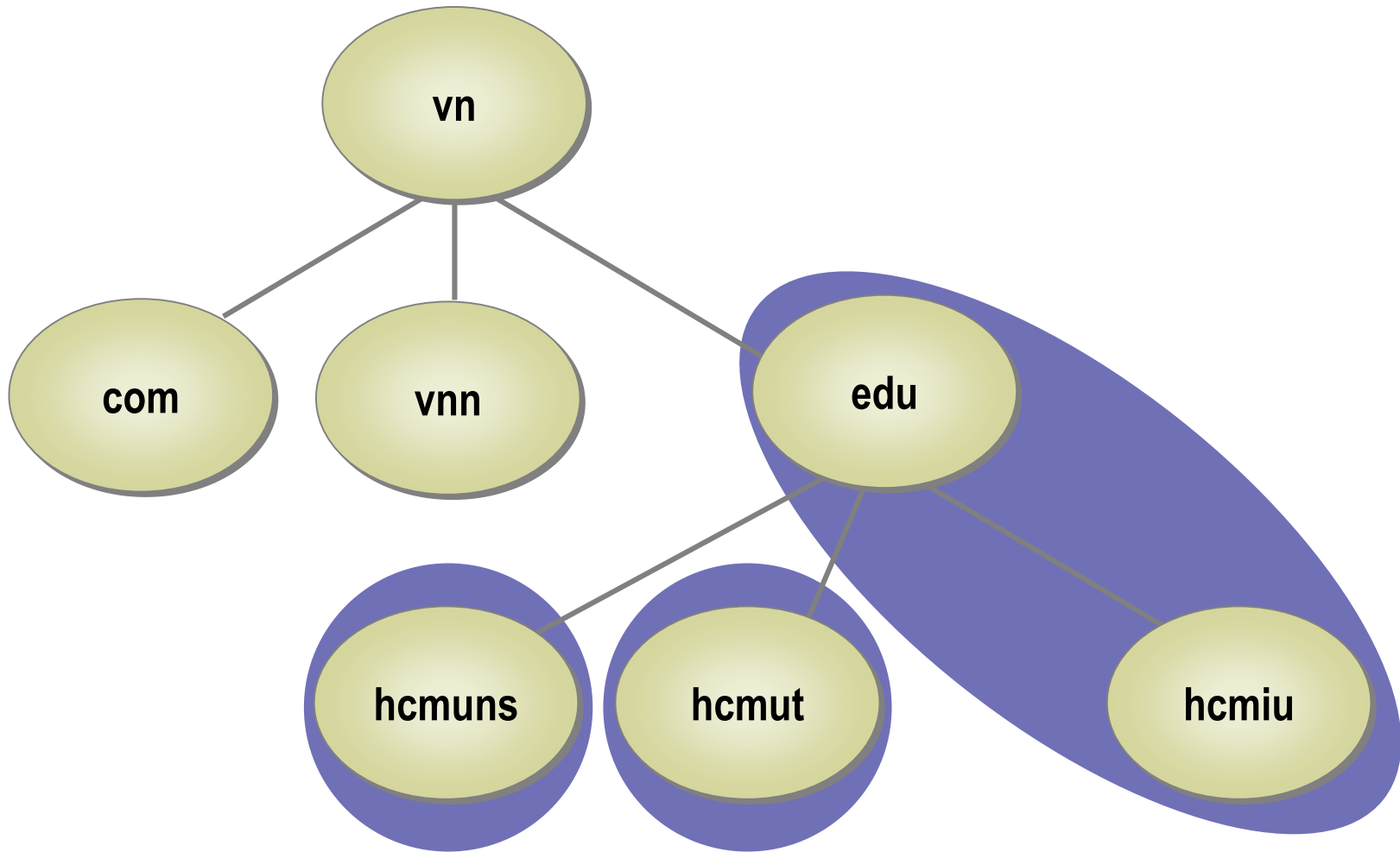
Name	Type	Data
(same as parent folder)	Mail Exchanger (MX)	[10] mail.csc.com.
(same as parent folder)	Name Server (NS)	server.csc.com.
(same as parent folder)	Start of Authority (SOA)	[2005121505], server.c
dns1	Host (A)	172.29.45.160
mail	Host (A)	172.29.45.162
server	Host (A)	172.29.45.162
www	Alias (CNAME)	server.csc.com.

Loại Record	Mục đích
A	Phân giải tên thành địa chỉ IP
PTR	Phân giải địa chỉ IP thành tên host name
SOA	Chứng thực cơ sở dữ liệu cho zone
SRV	Phân giải tên của cung cấp dịch vụ AD
NS	Chỉ định DNS server cho zone
MX	Chỉ định mail server cho zone
CNAME	Phân giải hostname thành hostname

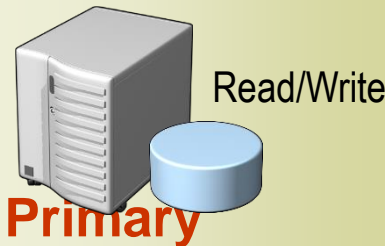
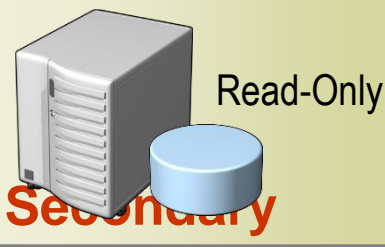
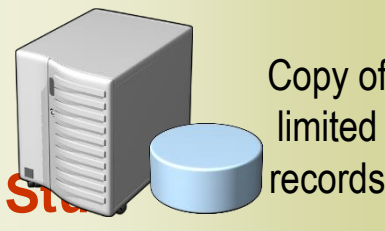
# Tạo cơ sở dữ liệu cho Zone

- Tạo record A : ánh xạ host name -> ip address
- Tạo record CNAME: : ánh xạ host name -> host name
- Tạo record NS: : ánh xạ host name -> host name
- Tạo record MX:: chỉ định mail server quản lý mail cho miền.

# DNS Zone



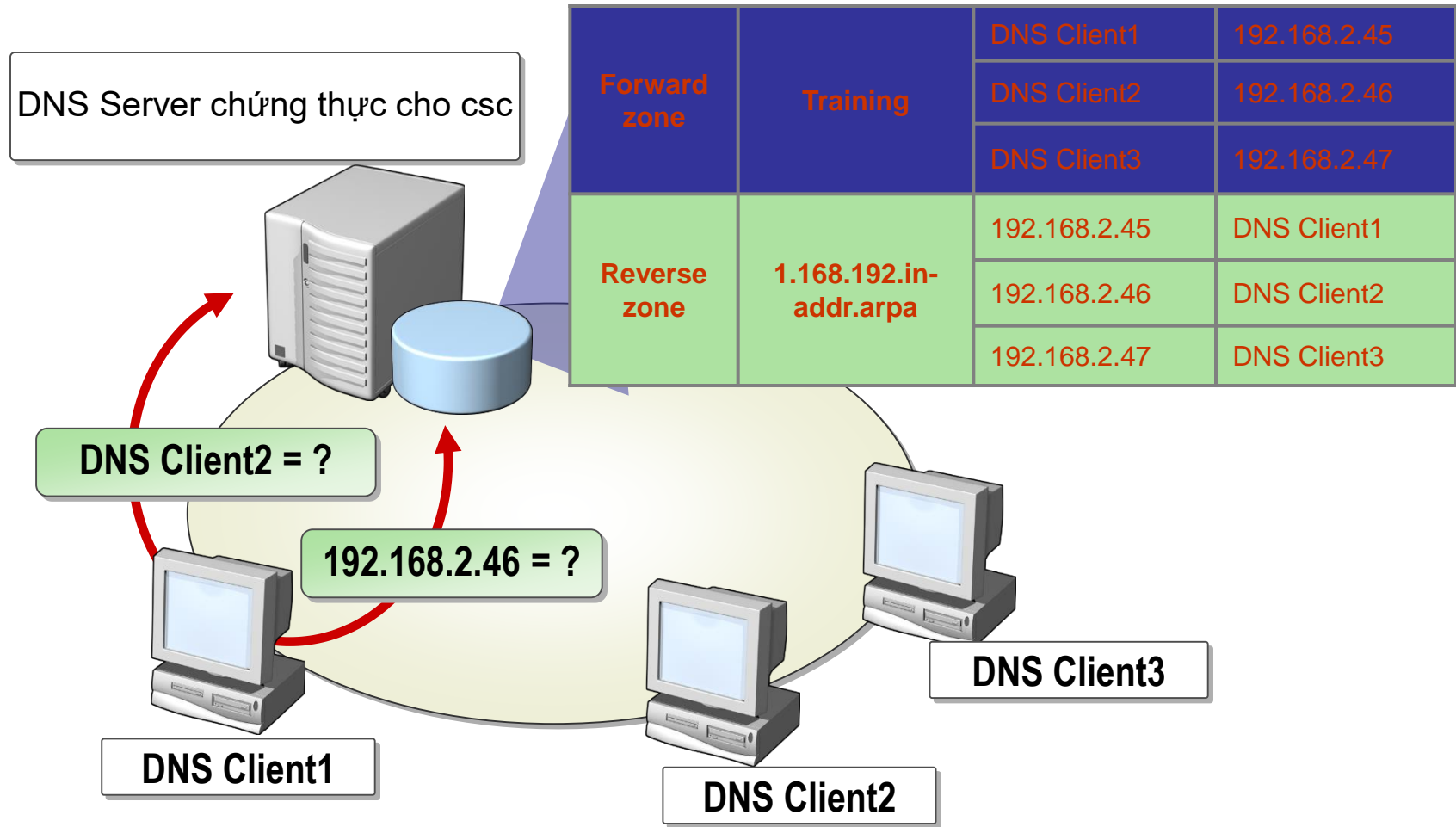
# Phân loại DNS Zone

Zones	Mô tả
 <b>Primary</b>	Read/write DNS database
 <b>Secondary</b>	Read-only DNS database
 <b>Stub</b>	Bảng sao của zone chứa một số RR



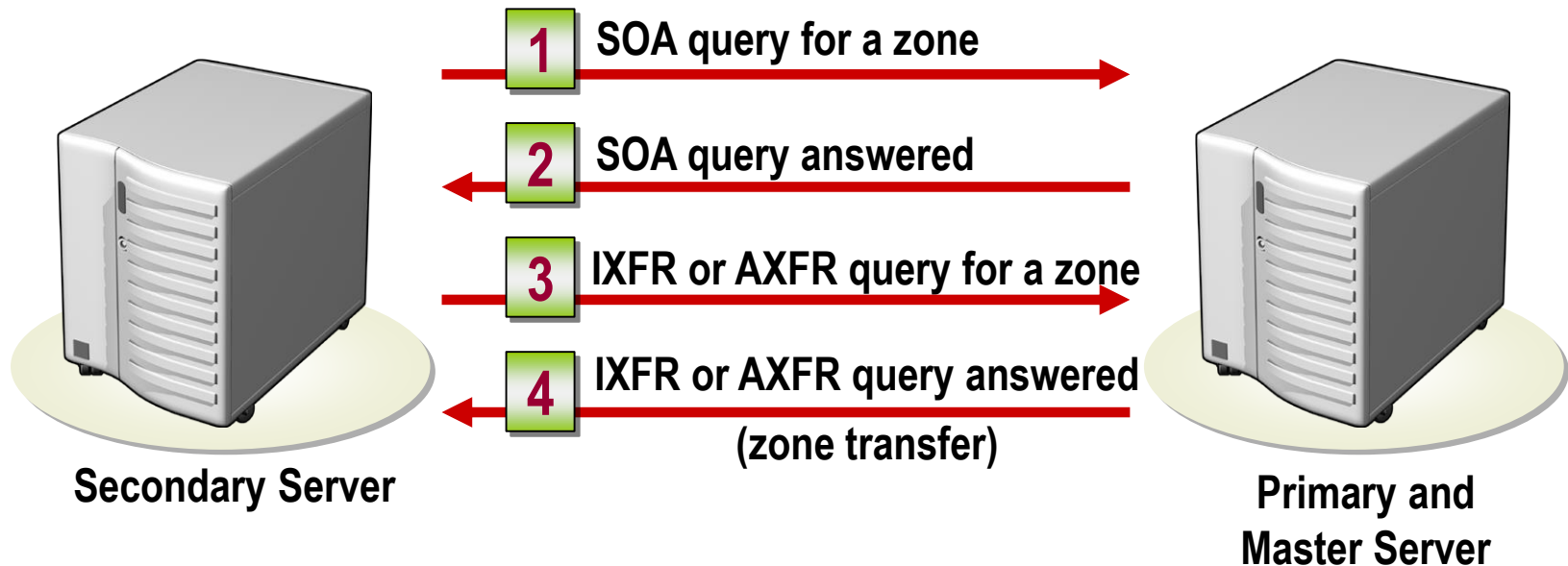
# Forward Lookup Zone và Reverse Lookup Zone

Namespace: csc.vnn.vn.



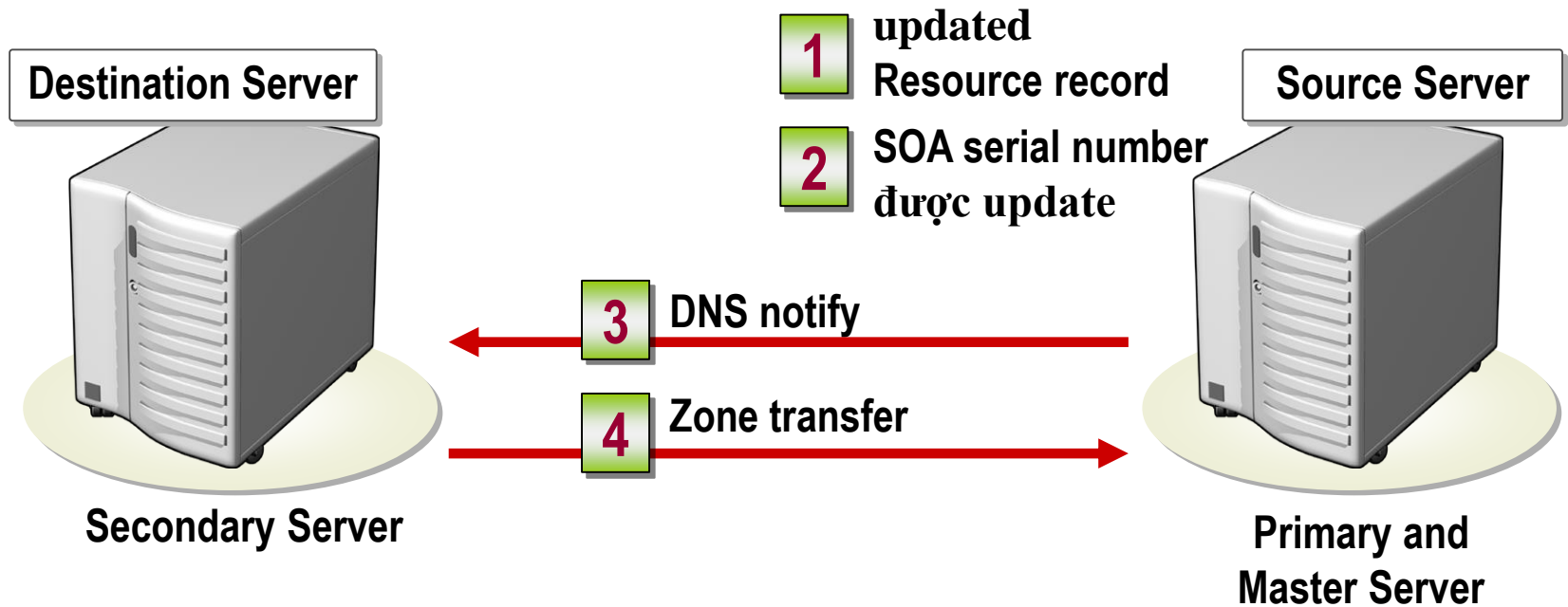
# DNS Zone transfer

*DNS zone transfer* là quá trình đồng bộ cơ sở dữ liệu DNS zone data giữa các DNS servers



# DNS Notify

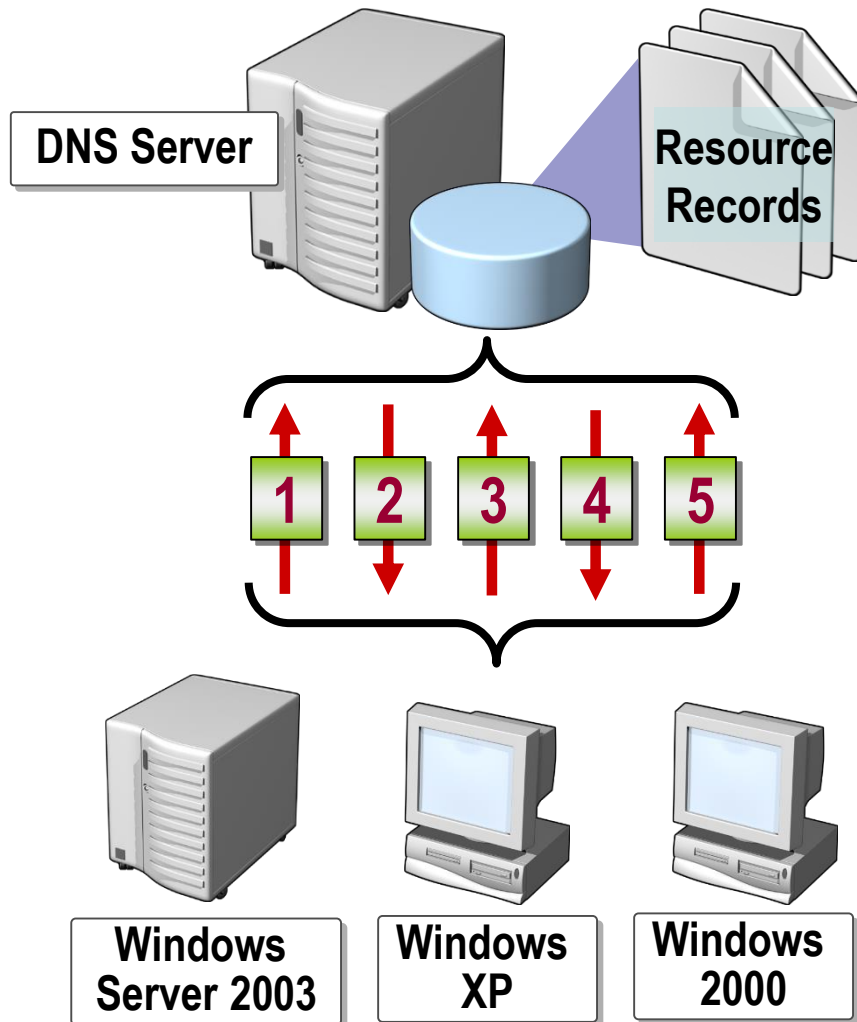
**DNS notify** là một cơ chế thông báo sự thay đổi cơ sở dữ liệu DNS cho secondary name server khi có sự thay đổi cơ sở dữ liệu trong zone



# Giới thiệu Dynamic DNS

- 1. *Dynamic update*** là tiến trình mà DNS client tự động tạo, đăng ký hoặc cập nhật RR trong zone.
- 2. *Manual update*** là tiến trình mà người quản trị phải tạo, đăng ký hoặc cập nhật resource record

# Cập nhật RR tự động từ DNS Client



**1** Client gửi SOA query

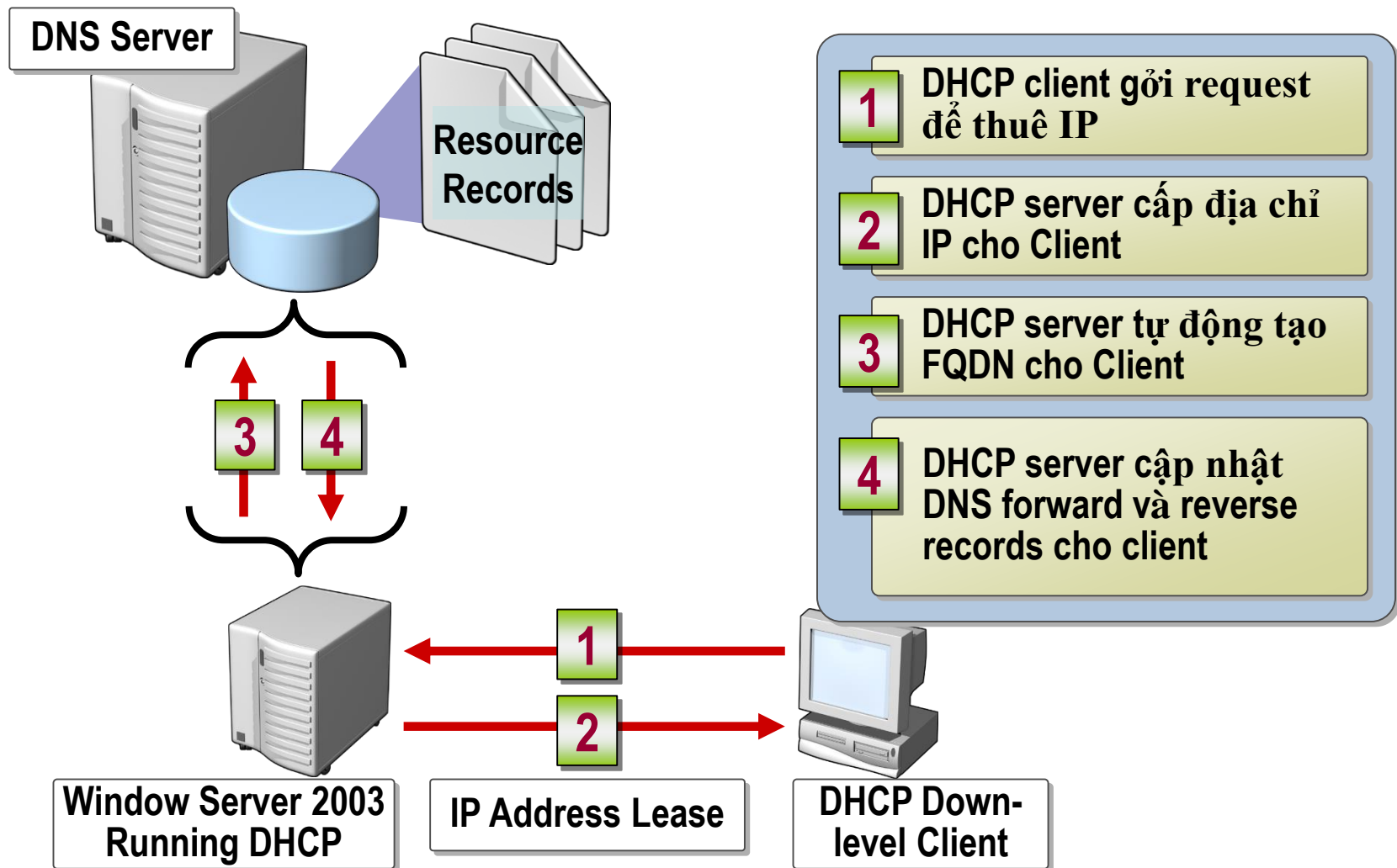
**2** DNS server gửi zone name và server IP address

**3** Client kiểm tra đã đăng ký chưa

**4** DNS server trả lời trạng thái chưa đăng ký

**5** Client gửi dynamic update tới DNS server

# DHCP đăng ký và cập nhật RR cho DNS Client



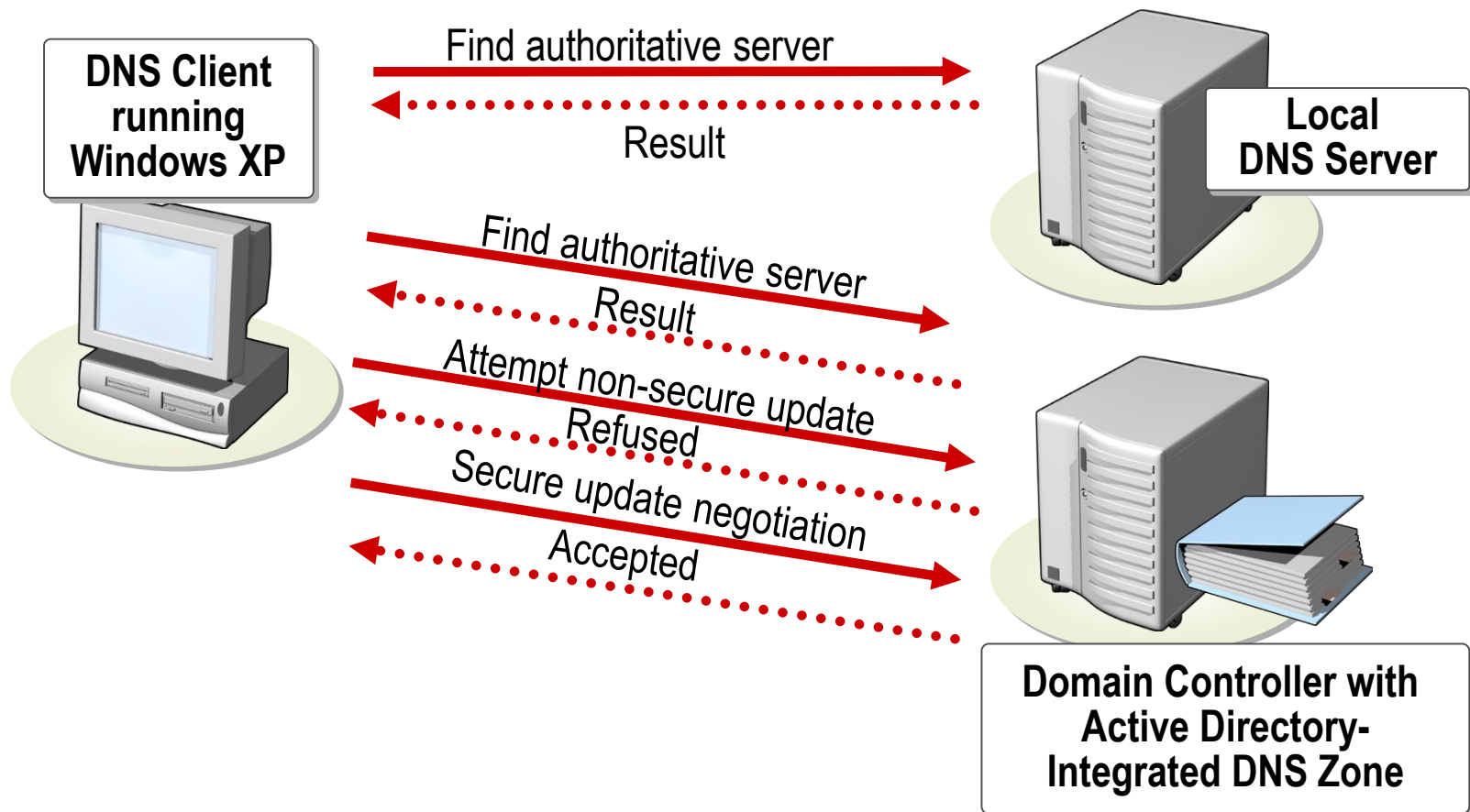
# Active Directory - Integrated Zone

Loại DNS zone	Thuận lợi
Non Active Directory-integrated zone	<ul style="list-style-type: none"><li>• Không yêu cầu dịch vụ Active Directory</li></ul>
Active Directory-integrated zone	<ul style="list-style-type: none"><li>• Lưu DNS zone data trong Active Directory cung cấp nhiều tính năng bảo mật</li><li>• sử dụng Active Directory replication thay vì zone transfers</li><li>• Cho phép chỉ secure dynamic updates</li><li>• sử dụng cấu trúc multi-master thay vì single master</li></ul>

***Active Directory-integrated DNS zone là DNS zone lưu trong Active Directory***

# Secure Dynamic Update với Active Directory - Integrated Zone

***secure dynamic update*** là tiến trình trong đó DNS Client cập nhật RR chỉ khi nào Client thực sự đăng nhập vào DNS Server





# Cấu hình Preferred và Alternate DNS Server cho Client

**Internet Protocol (TCP/IP) Properties**

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

**1. Preferred DNS server**

10 . 1 . 1 . 17  
255 . 255 . 255 . 0  
10 . 1 . 1 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: 10 . 1 . 1 . 10

Alternate DNS server: . . .

Advanced...

Cancel

**2. Nếu preferred server lỗi thì client truy vấn tới alternate DNS server**

**3. Chỉ định các alternate DNS servers**

**Advanced TCP/IP Settings**

IP Settings DNS WINS Options

DNS server addresses, in order of use:

10.1.1.10

Add... Edit... Remove

The following three settings are applied to all connections with TCP/IP enabled. For resolution of unqualified names:

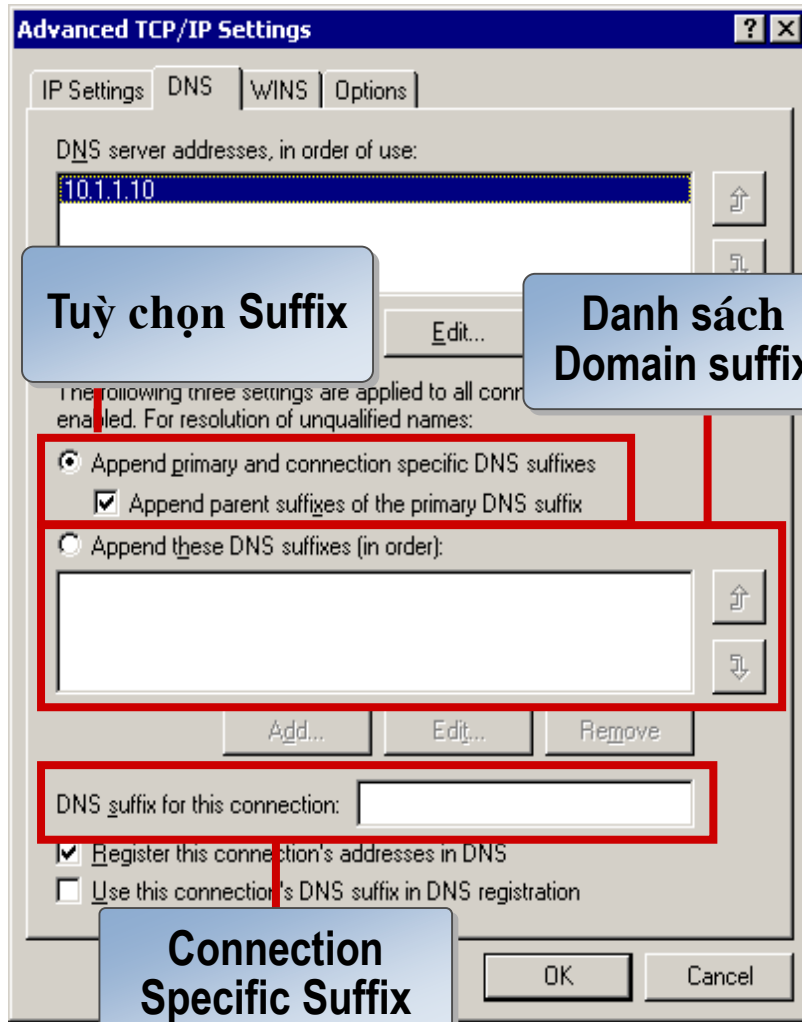
☒ Register this connection's addresses in DNS

☐ Use this connection's DNS suffix in DNS registration

OK Cancel

**4. Preferred và alternate DNS servers tự động xuất hiện trong list này**

# Cấu hình domain suffix



Name query = server1

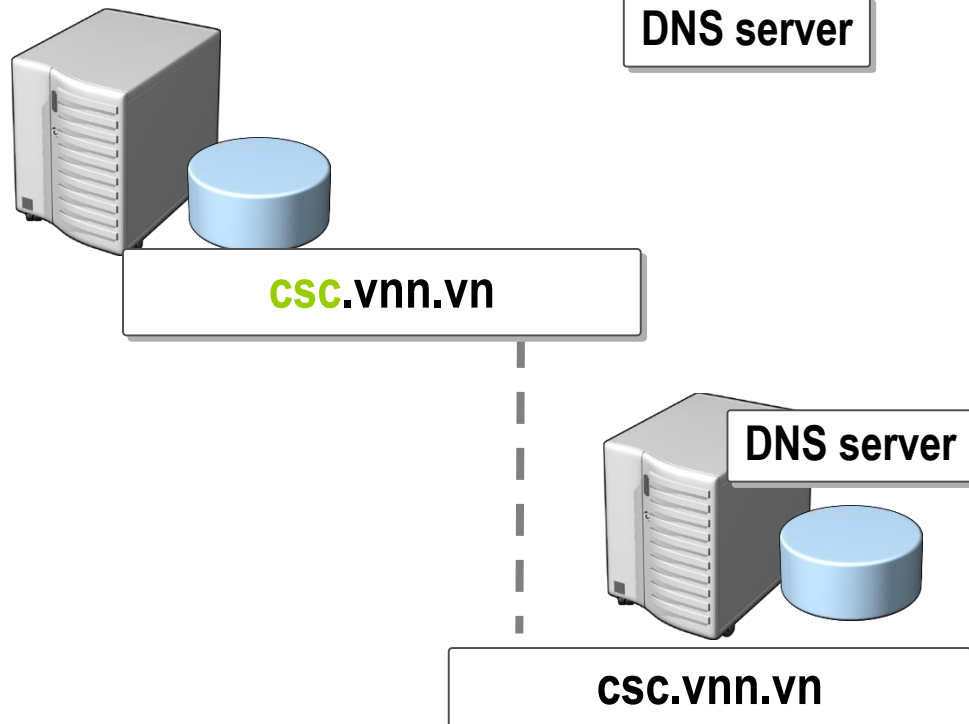
server1.tm.csc.vnn.vn

server1.csc.vnn.vn

server1.vnn.vn

# Sự ủy quyền (delegation)

Namespace: csc.vnn.vn



**Delegation là quá trình gán toàn quyền subdomain cho một name server khác quản lý.**

# Cấu hình DNS

## ➤ Lab DNS

# Câu hỏi và giải đáp

