



Chapter 5: Network services

DNS - Domain Name System

Lecturer: Nguyễn Thị Thanh Vân – FIT - HCMUTE

NỘI DUNG

- I. Tổng quan về DNS. .
- II. Cách phân bổ dữ liệu quản lý domain name.
- III. Cơ chế phân giải tên. .
- IV. Một số Khái niệm cơ bản
- V. Phân loại Domain Name Server.
- VI. Resource Record (RR).
- VII. Cài đặt và cấu hình dịch vụ DNS.

I. Tổng quan về DNS

- ▶ I.1. Giới thiệu DNS
- ▶ I.2. Sơ đồ tổ chức của DNS
- ▶ I.3 Các thành phần trong dịch vụ DNS
- ▶ I.4. Đặc điểm của DNS trong Windows

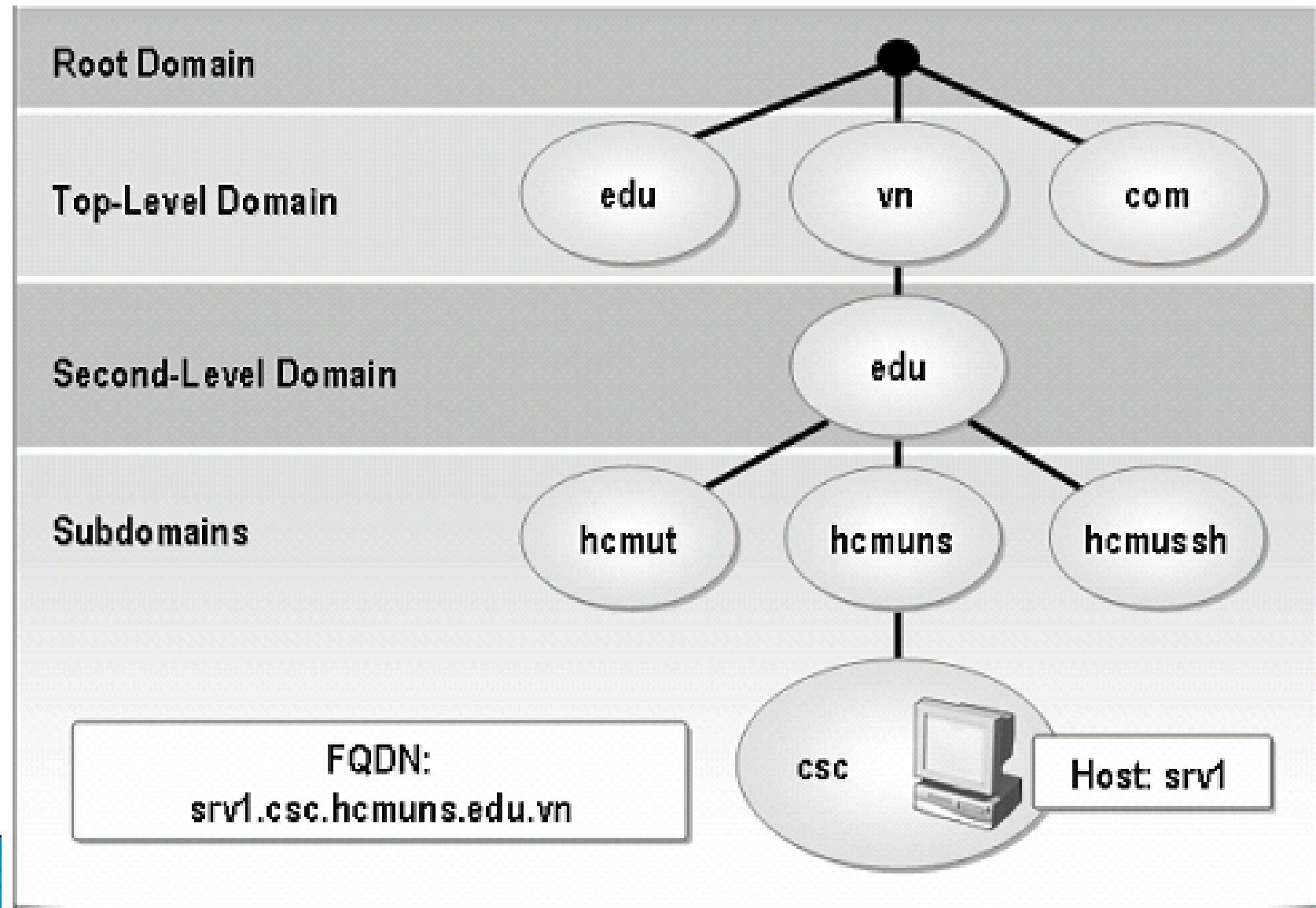
I.1. Giới thiệu DNS

- ❑ Chức năng: Ánh xạ địa chỉ IP – tên miền
- ❑ Lịch sử:
 - host.txt: lưu các ánh xạ tại server -> hạn chế
 - DNS ra đời: (Paul Mockapetris USC's Information Sciences Institute): thiết kế cấu trúc
- ❑ DNS hoạt động theo mô hình Client-Server:
 - Server gọi là máy chủ phục vụ tên hay còn gọi là Name Server: chứa các thông tin CSDL của DNS
 - Client là trình phân giải tên – Resolver: chứa các hàm thư viện dùng để tạo các truy vấn (query) và gửi chúng đến Name Server.
- ❑ Đặc điểm:
 - CSDL được phân tán trên nhiều Name Server.
 - Cơ chế nhân bản (replication) và lưu tạm (caching) => Tăng hiệu suất
 - Thi hành như một giao thức tầng Application trong mạng TCP/IP.

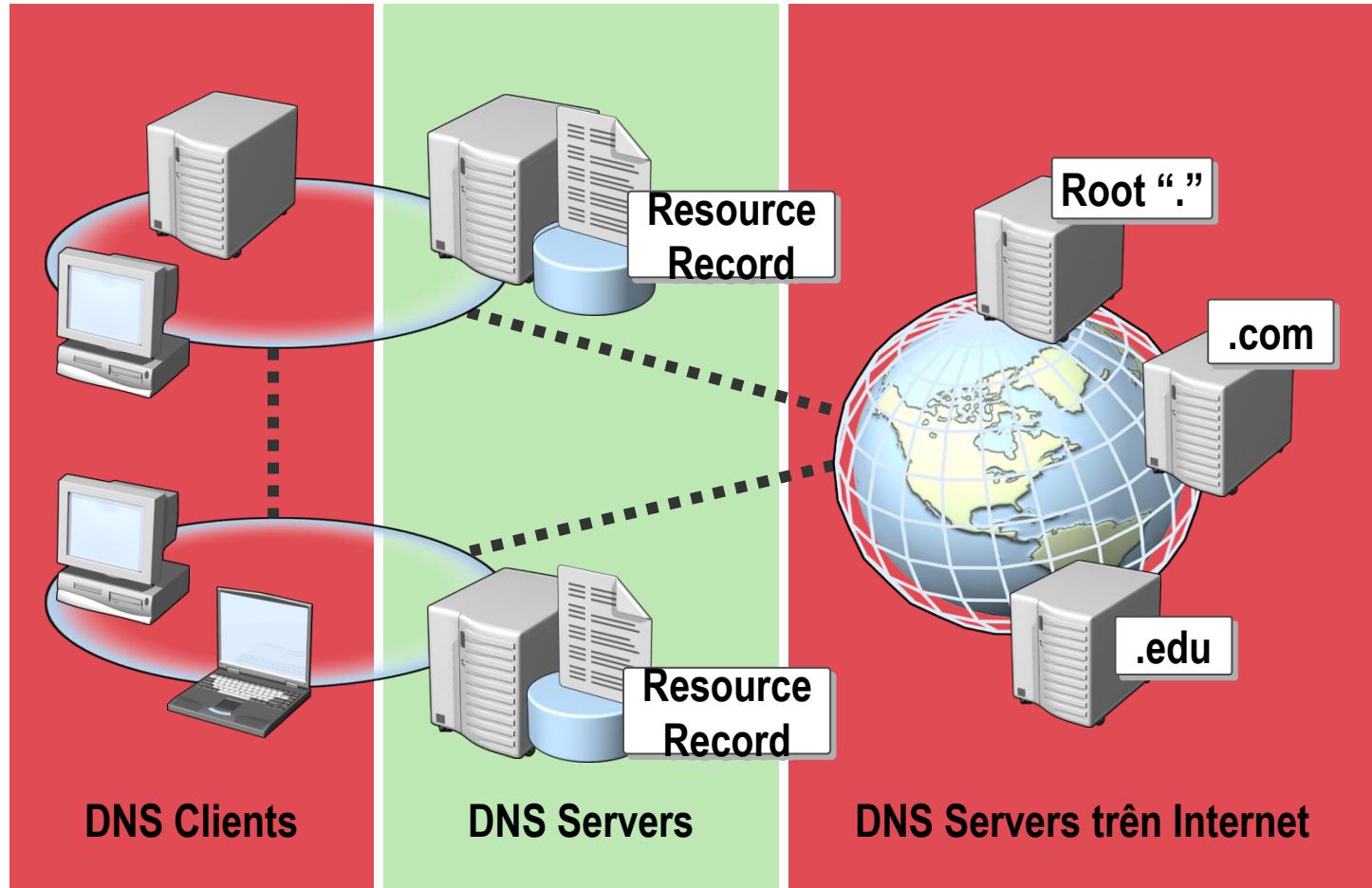
CSDL của DNS

- ▶ CSDL của DNS là một cây đảo ngược:
 - Mỗi nút trên cây cũng lại là gốc của 1 cây con.
 - Mỗi cây con là 1 phân vùng con trong toàn bộ CSDL DNS gọi là 1 miền (domain).
 - Mỗi domain có thể phân chia thành các phân vùng con nhỏ hơn: gọi là subdomain
 - Mỗi domain có 1 tên(domain name): <= 63 ký tự
- ▶ Chiều sâu của cây tối đa là 127 cấp.

I.2. Sơ đồ tổ chức của DNS



I.3. Các thành phần trong dịch vụ DNS:



I.4. Đặc điểm của DNS trong Windows

- ▶ Conditional forwarder:
 - Name Server chuyển các y/c phân giải dựa theo tên domain
- ▶ Stub zone:
 - hỗ trợ cơ chế phân giải hiệu quả hơn.
- ▶ DNS zone replication in Active Directory:
 - Đồng bộ các DNS zone trong Active Directory
- ▶ Security:
 - tốt hơn trong các hệ thống Windows trước đây.
- ▶ Round robin:
 - tất cả các loại RR.
- ▶ DNS Security Extensions (DNSSEC):
 - tính năng bảo mật cho việc lưu trữ và nhân bản (replicate) zone.
- ▶ EDNS0 (Extension Mechanisms for DNS)
 - DNS Requestor quảng bá những zone transfer packet có kích thước lớn hơn 512 byte

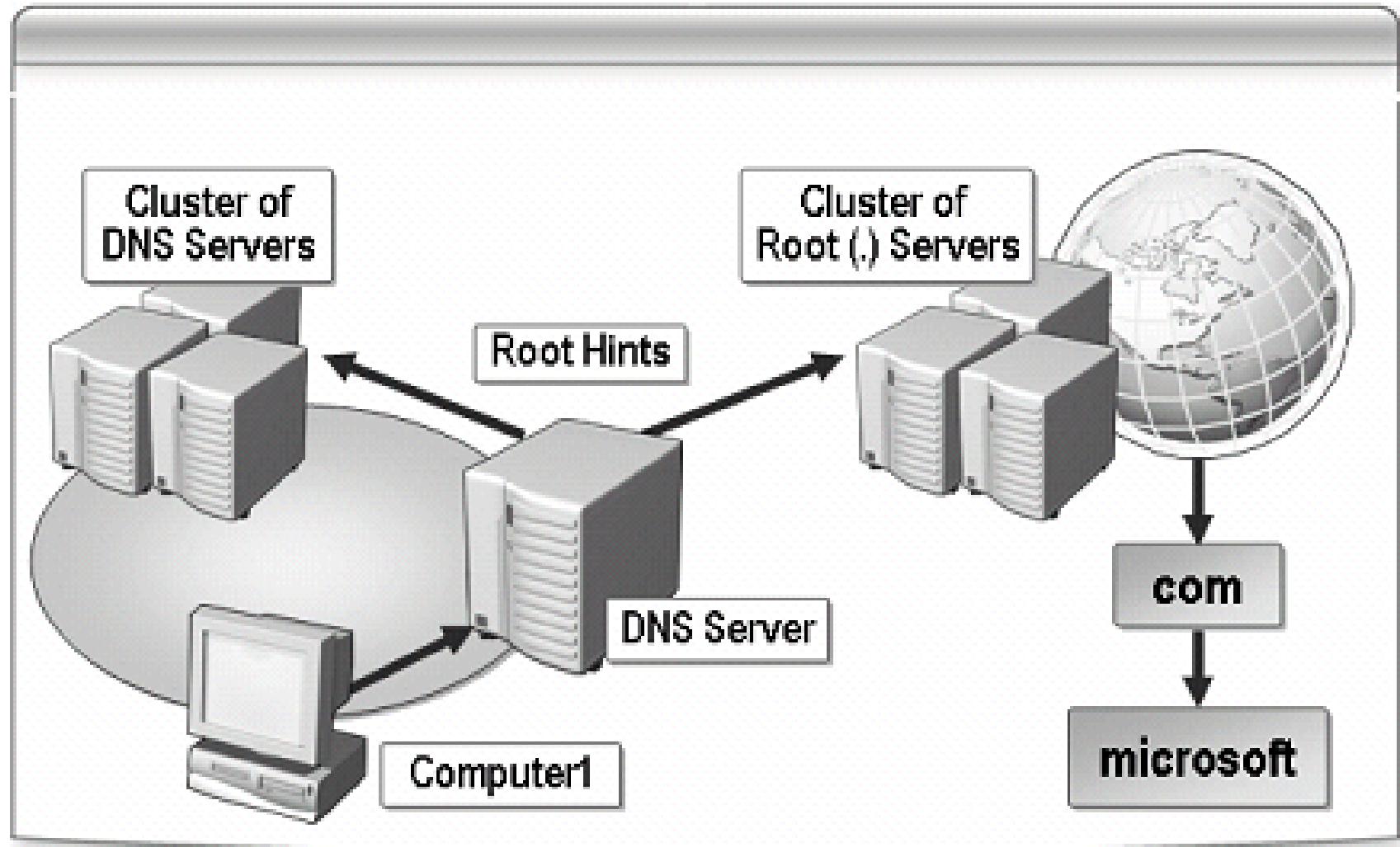
II.Cách phân bổ dữ liệu quản lý domain name.

- ▶ Root name server (.): máy chủ quản lý các name server ở mức top-level domain.
- ▶ Tên máy và địa chỉ IP của root name server này được public
- ▶ Có nhiều Root name server để dự phòng, giảm tải. Có thể đặt chúng khắp nơi trên thế giới và chúng có liên kết với nhau.
=> Đáp ứng kịp thời các yêu cầu phân giải

II.Cách phân bổ dữ liệu quản lý domain name.

| Tên máy tính | Địa chỉ IP |
|--------------------|----------------|
| H.ROOT-SERVERS.NET | 128.63.2.53 |
| B.ROOT-SERVERS.NET | 128.9.0.107 |
| C.ROOT-SERVERS.NET | 192.33.4.12 |
| D.ROOT-SERVERS.NET | 128.8.10.90 |
| E.ROOT-SERVERS.NET | 192.203.230.10 |
| I.ROOT-SERVERS.NET | 192.36.148.17 |
| F.ROOT-SERVERS.NET | 192.5.5.241 |
| F.ROOT-SERVERS.NET | 39.13.229.241 |
| G.ROOT-SERVERS.NET | 192.112.88.4 |
| A.ROOT-SERVERS.NET | 198.41.0.4 |

Mô hình

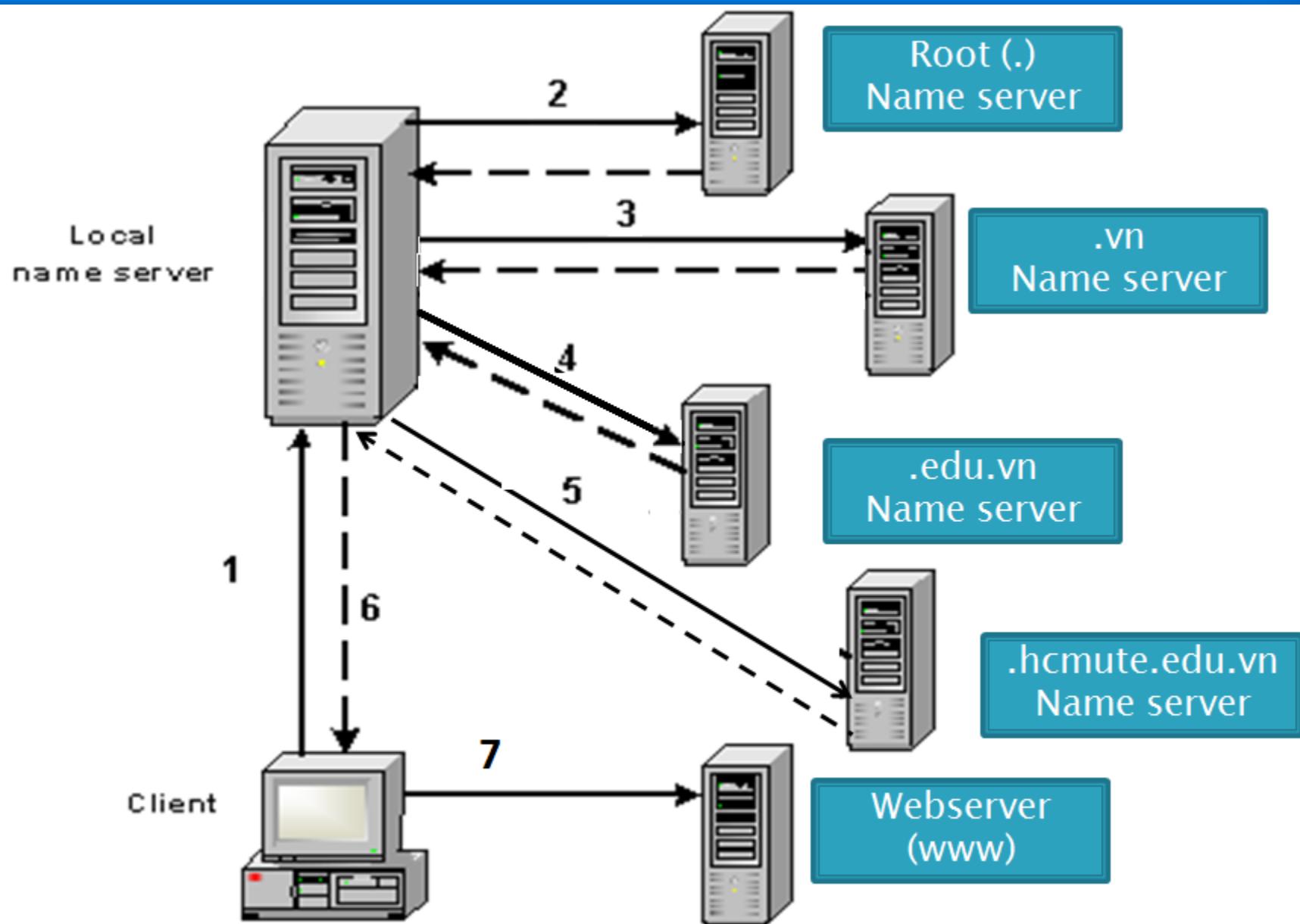


III. Cơ chế phân giải tên.

III.1. Phân giải tên thành IP.

- ▶ Khi có truy vấn về một tên miền nào đó thì Root Name Server phải cung cấp tên và địa chỉ IP của name server quản lý top-level domain
- ▶ Cứ như thế đến khi nào tìm được máy quản lý tên miền cần truy vấn
- ▶ Quá trình tìm kiếm tên miền luôn được bắt đầu bằng các truy vấn gửi cho máy chủ ROOT

Ví dụ: www.hcmute.edu.vn



1. Phân giải tên thành IP.

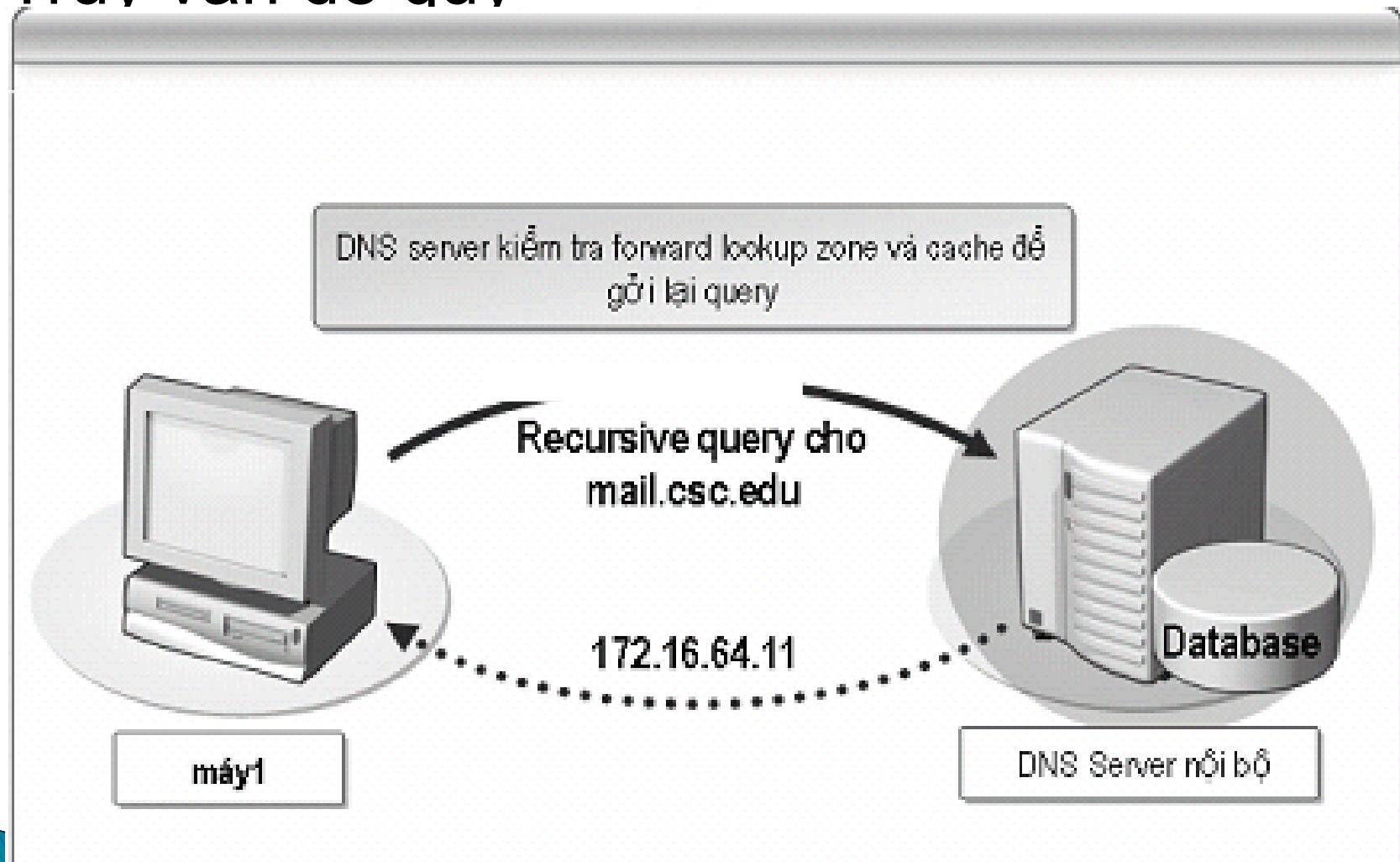
Truy vấn có thể ở 2 dạng :

- ▶ Truy vấn đệ quy (recursive query):

- khi name server nhận được truy vấn dạng này, nó bắt buộc phải trả về kết quả tìm được hoặc thông báo lỗi nếu như truy vấn này không phân giải được.
- Name server có thể gửi truy vấn dạng đệ quy hoặc tương tác đến name server khác nhưng phải thực hiện cho đến khi nào có kết quả mới thôi

1. Phân giải tên thành IP.

▶ Truy vấn đê quy

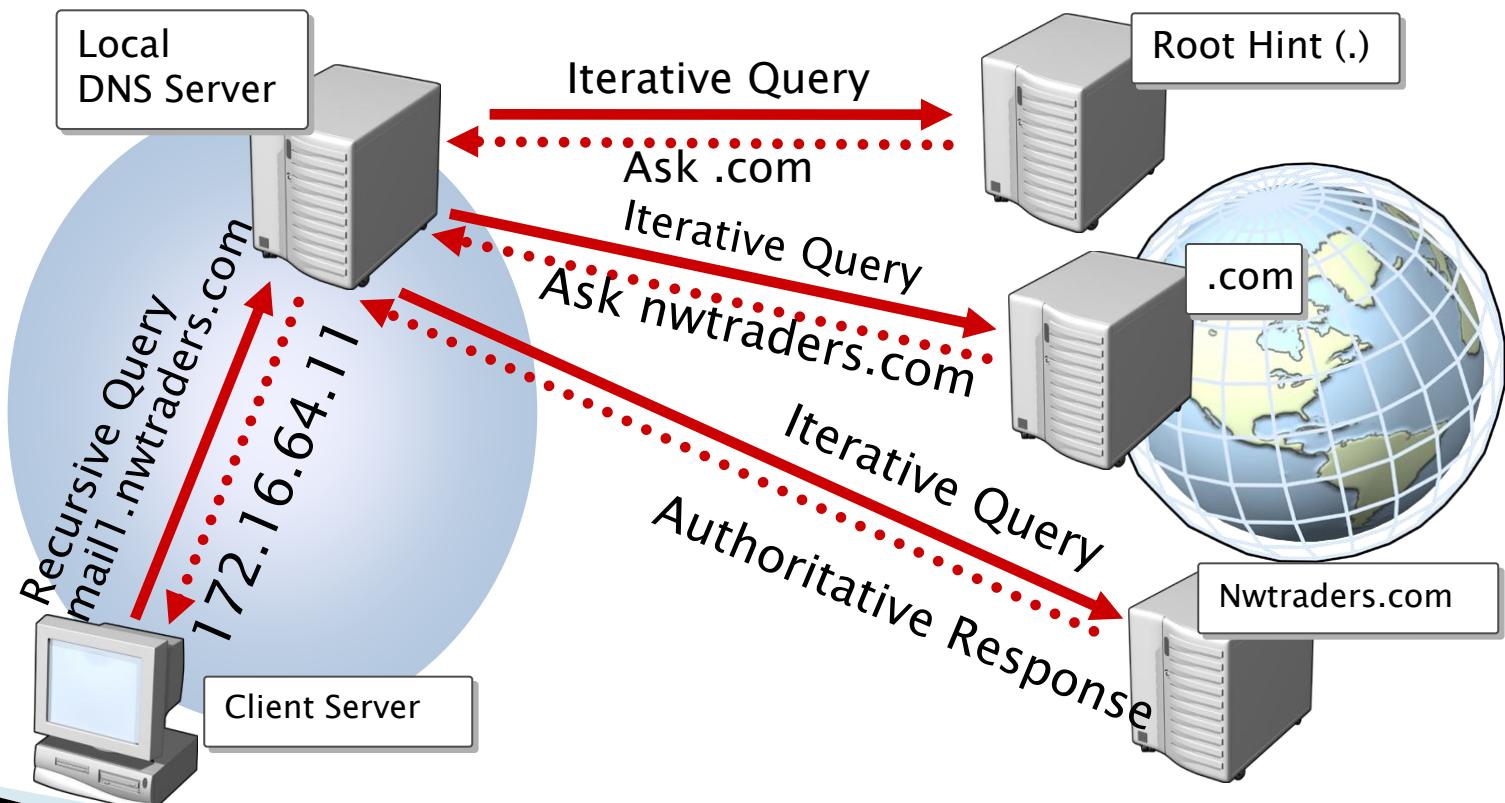


1. Phân giải tên thành IP.

- ▶ Truy vấn tương tác (Interactive query):
 - khi name server nhận được truy vấn dạng này, nó trả lời cho Resolver với thông tin tốt nhất mà nó có được vào thời điểm lúc đó.
 - Thông tin tốt nhất trả về có thể lấy từ dữ liệu cục bộ (kể cả cache). Trong trường hợp name server không tìm thấy trong dữ liệu cục bộ nó sẽ trả về tên miền và địa chỉ IP của name server gần nhất mà nó biết.

1. Phân giải tên thành IP.

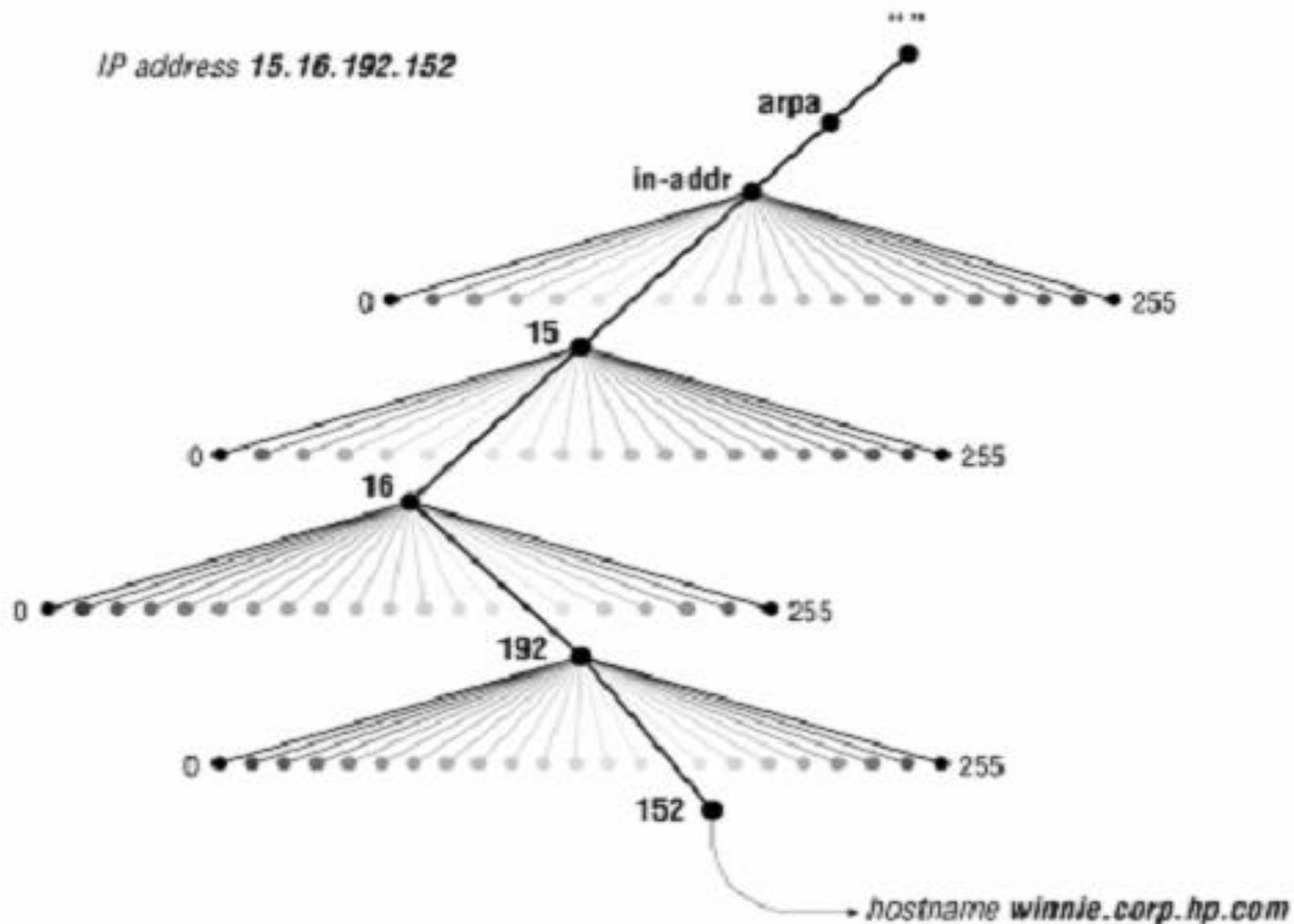
▶ Truy vấn tương tác



2. Phân giải IP thành tên máy

- ▶ Bổ sung thêm một nhánh tên miền mà được lập chỉ mục theo địa chỉ IP.
- ▶ Phần không gian này có tên miền là in-addr.arpa.
- ▶ Tên miền địa chỉ IP sẽ xuất hiện theo thứ tự ngược.
- ▶ Ví dụ: Máy winnie.corp.hp.com có IP là: 15.16.192.152, khi ánh xạ vào miền in-addr.arpa sẽ là 152.192.16.15.in-addr.arpa.

2. Phân giải IP thành tên máy



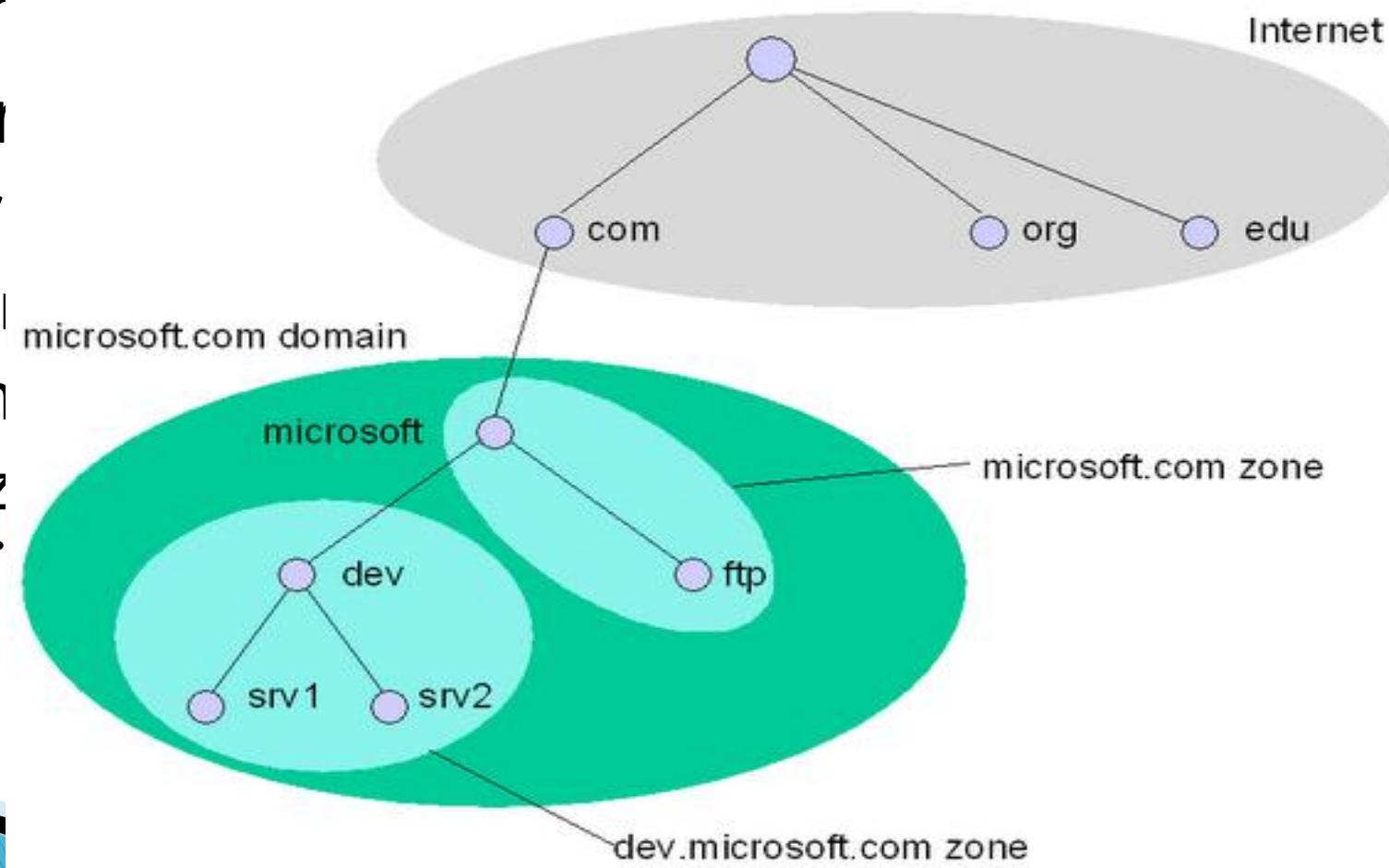
IV. Một số Khái niệm cơ bản

- ▶ IV.1. Domain name và zone
- ▶ IV.2. Fully Qualified Domain Name (FQDN).
- ▶ IV.3. Sự ủy quyền (Delegation). .
- ▶ IV.4. Forwarders.
- ▶ IV.5. Stub zone.
- ▶ IV.6. Dynamic DNS

IV.1. Domain name và zone

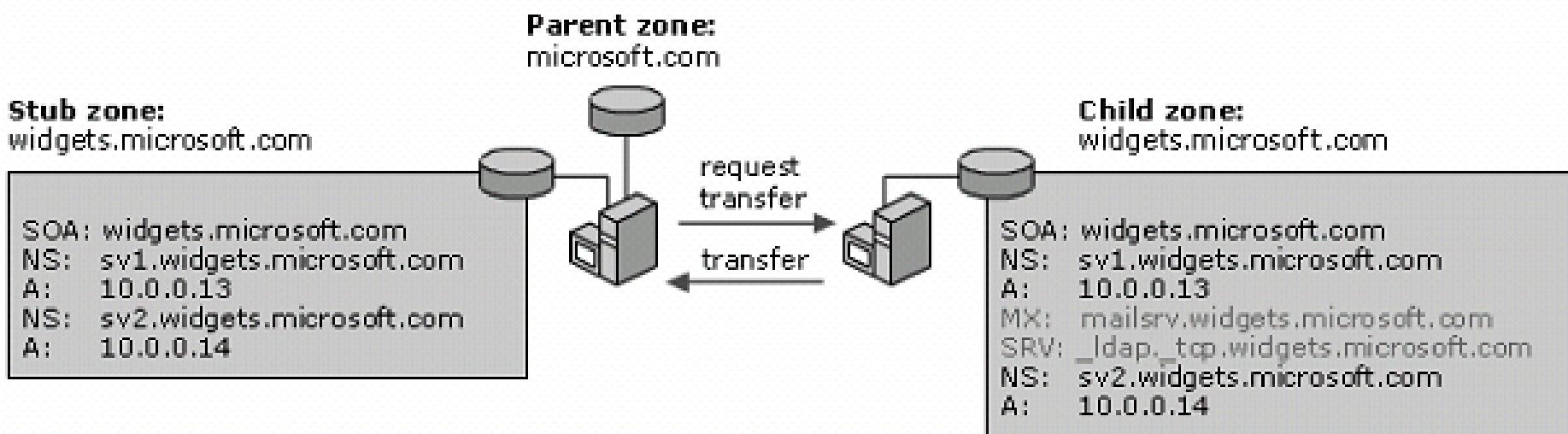
- ▶ Domain name: tên của các máy chủ trên mạng Internet (duy nhất 1) chứa: zones và subdomains

- ▶ Zone:
 - Primary Zone
 - Secondary Zone
 - Stub Zone
 - nó chỉ

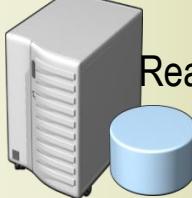
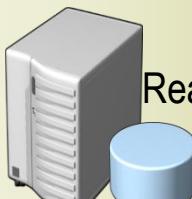
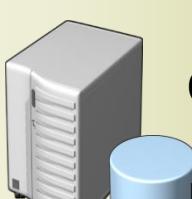


Stub zone

- ▶ Là zone chứa bảng sao CSDL DNS từ master name server, gồm các RR cần thiết như : A, SOA, NS, một hoặc vài địa chỉ của master NS
- ▶ hỗ trợ cơ chế cập nhật Stub zone, chế chứng thực name server trong zone và cung cấp cơ chế phân giải



So sánh

| Zones | Mô tả |
|--|--|
|  Primary Read/Write |  <p>New Zone Wizard</p> <p>Zone Type</p> <p>The DNS server supports various types of zones and storage.</p> |
|  Secondary Read-Only | |
|  Stub Copy of limited records | |

< Back

Next >

Cancel

IV.2. FQDN

Fully Qualified Domain Name (FQDN).

- ▶ Một tên miền đầy đủ của một nút chính:
- ▶ Tên miền có xuất hiện dấu chấm sau cùng được gọi là tên tuyệt đối (absolute)
- ▶ Tên tương đối là tên không kết thúc bằng dấu chấm.
- ▶ Tên tuyệt đối cũng được xem là tên miền đầy đủ đã được chứng nhận (Fully Qualified Domain Name – FQDN)
- ▶ Ex: .abc.com.vn

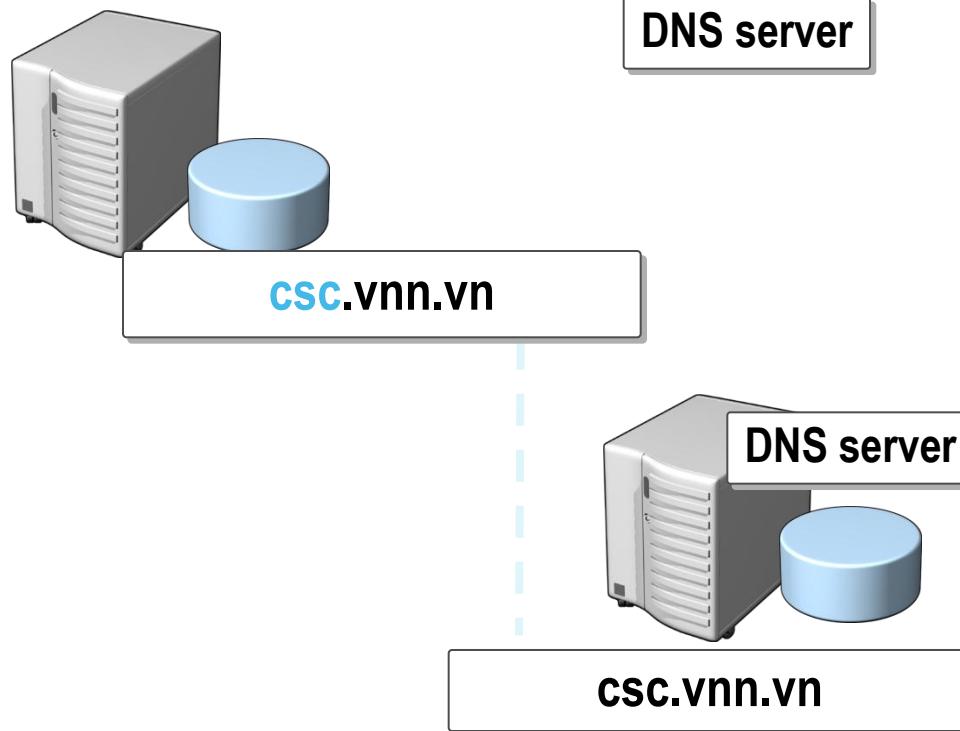
IV.3. Sụ ủy quyền(Delegation).

- ▶ Một miền có thể tổ chức thành nhiều miền con,
- ▶ Miền cha cung cấp các domain cho miền con dưới hình thức ủy quyền cho miền con tự quản lý và tổ chức CSDL cho miền con
- ▶ Khi đó, miền cha chỉ cần một con trỏ trỏ đến miền con này để tham chiếu khi có các truy vấn.
- ▶ Ví dụ miền hcmute.edu.vn có một số miền con:
 - fit.hcmute.edu.vn
 - Spkt.hcmute.edu.vn

nhưng các máy chủ phục vụ cho toàn trường thì vẫn thuộc vào miền hcmute.edu.vn.

Sự ủy quyền (delegation)

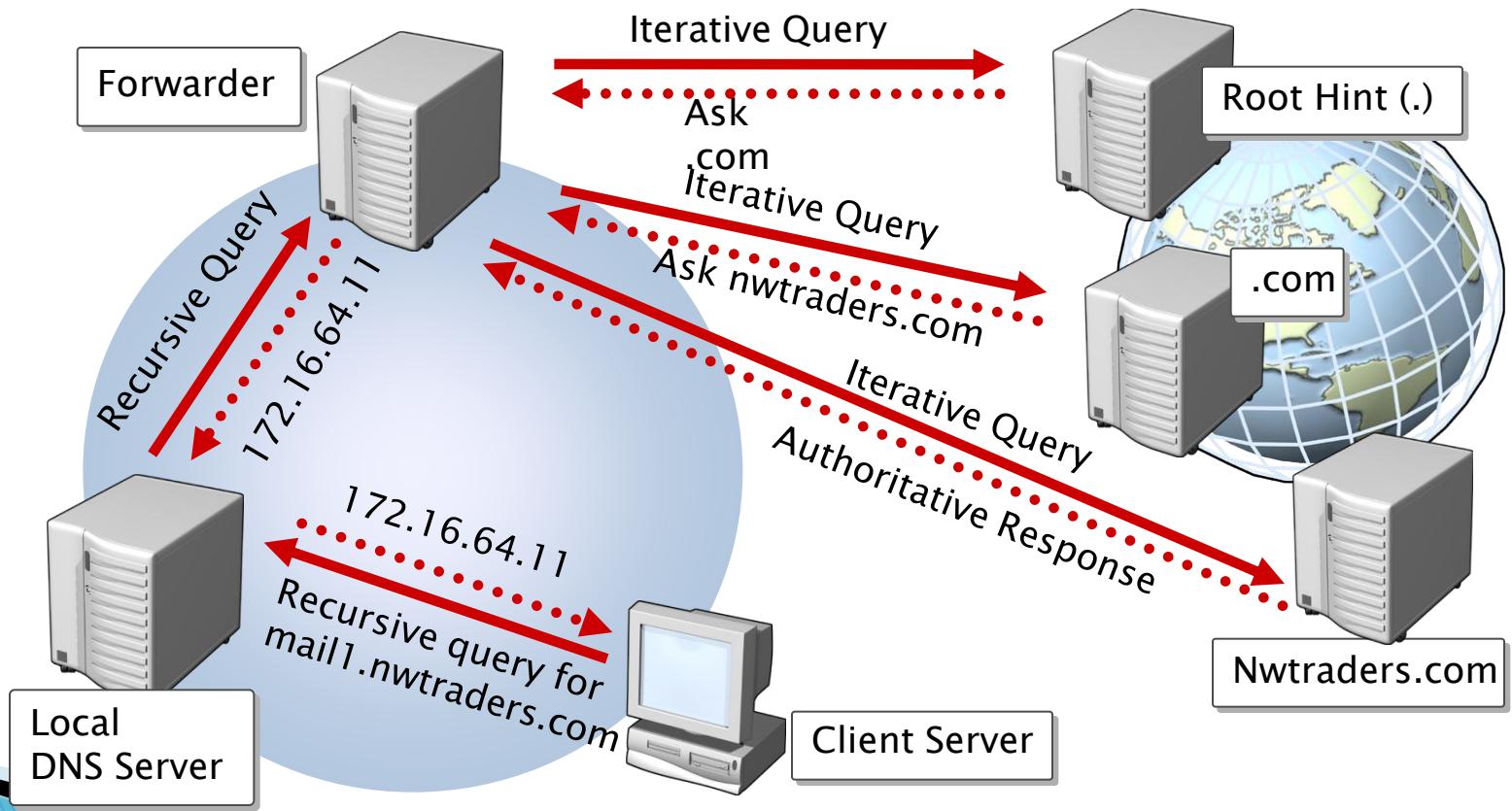
Namespace: csc.vnn.vn



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

IV.4. Forwarder

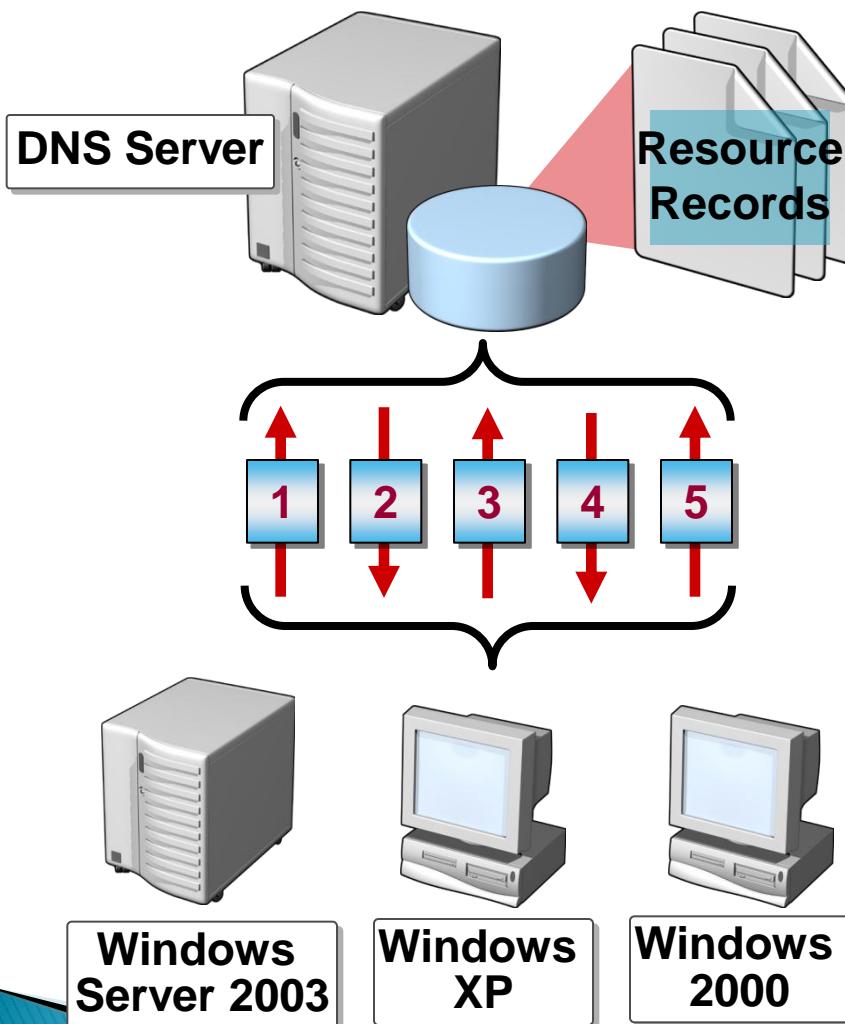
- Là kỹ thuật cho phép Name Server nội bộ chuyển yêu cầu truy vấn cho các Name Server khác để phân giải các miền bên ngoài.



IV.5. Dynamic DNS

- ▶ là phương thức ánh xạ tên miền tới địa chỉ IP có tần xuất thay đổi cao.
- ▶ Dynamic DNS cung cấp một chương trình đặc biệt chạy trên máy tính của NSD là Dynamic Dns Client
(Giám sát sự thay đổi địa chỉ IP tại host và liên hệ với hệ thống DNS mỗi khi địa chỉ IP của host thay đổi và sau đó update thông tin vào CSDL DNS về sự thay đổi địa chỉ đó).
- ▶ DNS Client đăng ký và cập nhật resource record của nó bằng cách gửi dynamic update.

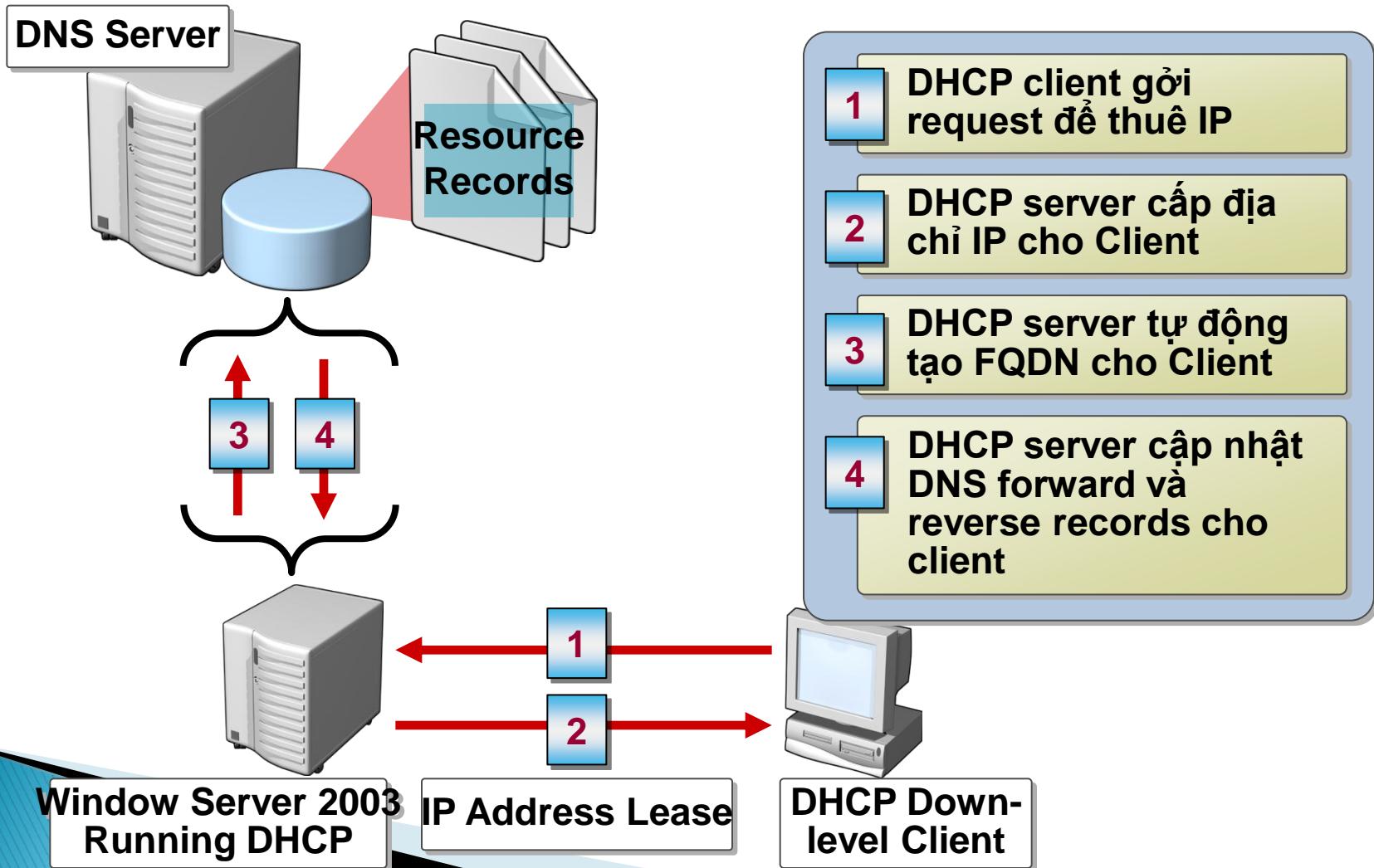
Cập nhật RR tự động từ DNS Client



- 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 server cập nhật dynamic update

- ▶ DHCP Server đăng ký và cập nhật resource record cho Client

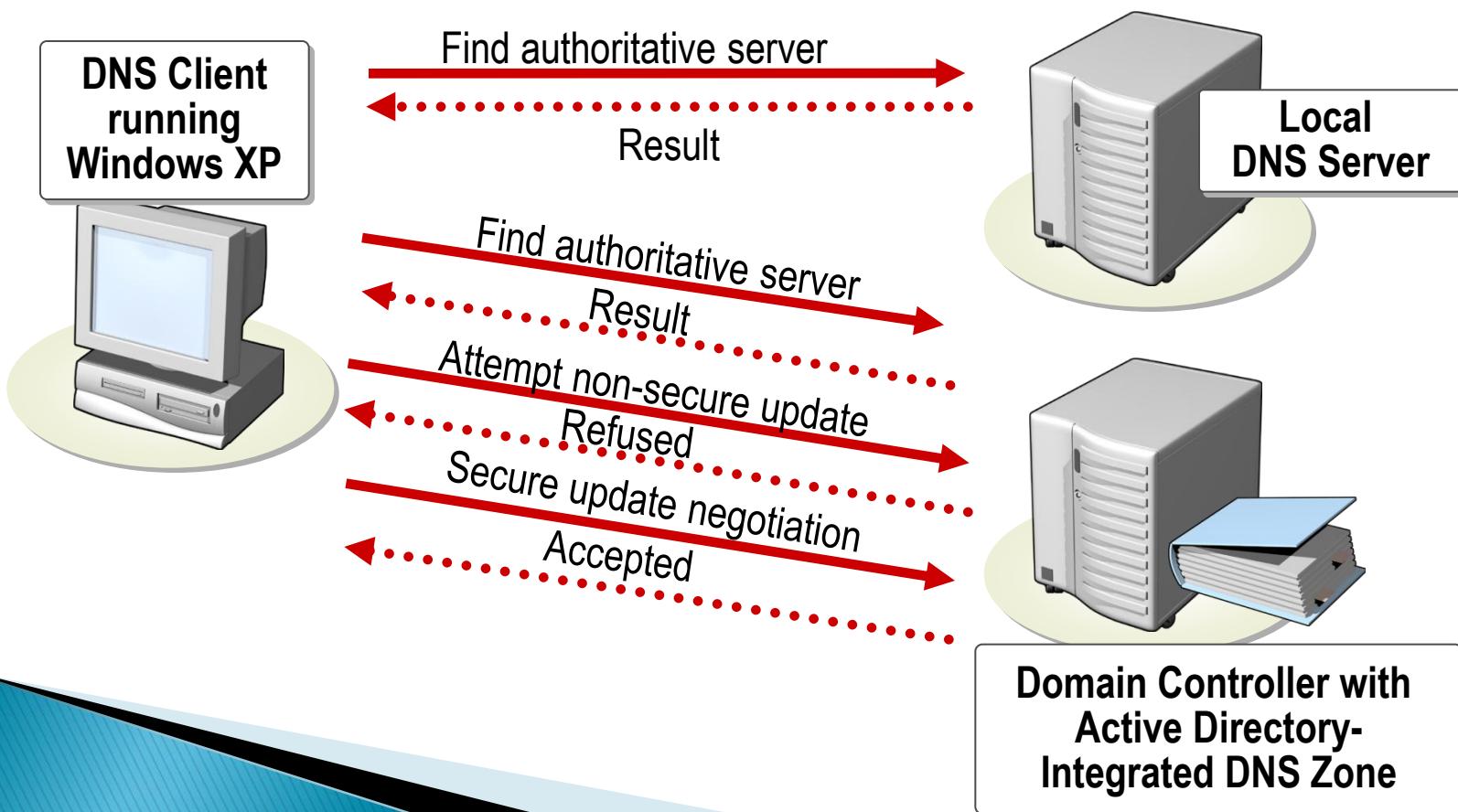


IV.7. Active Directory-integrated zone.

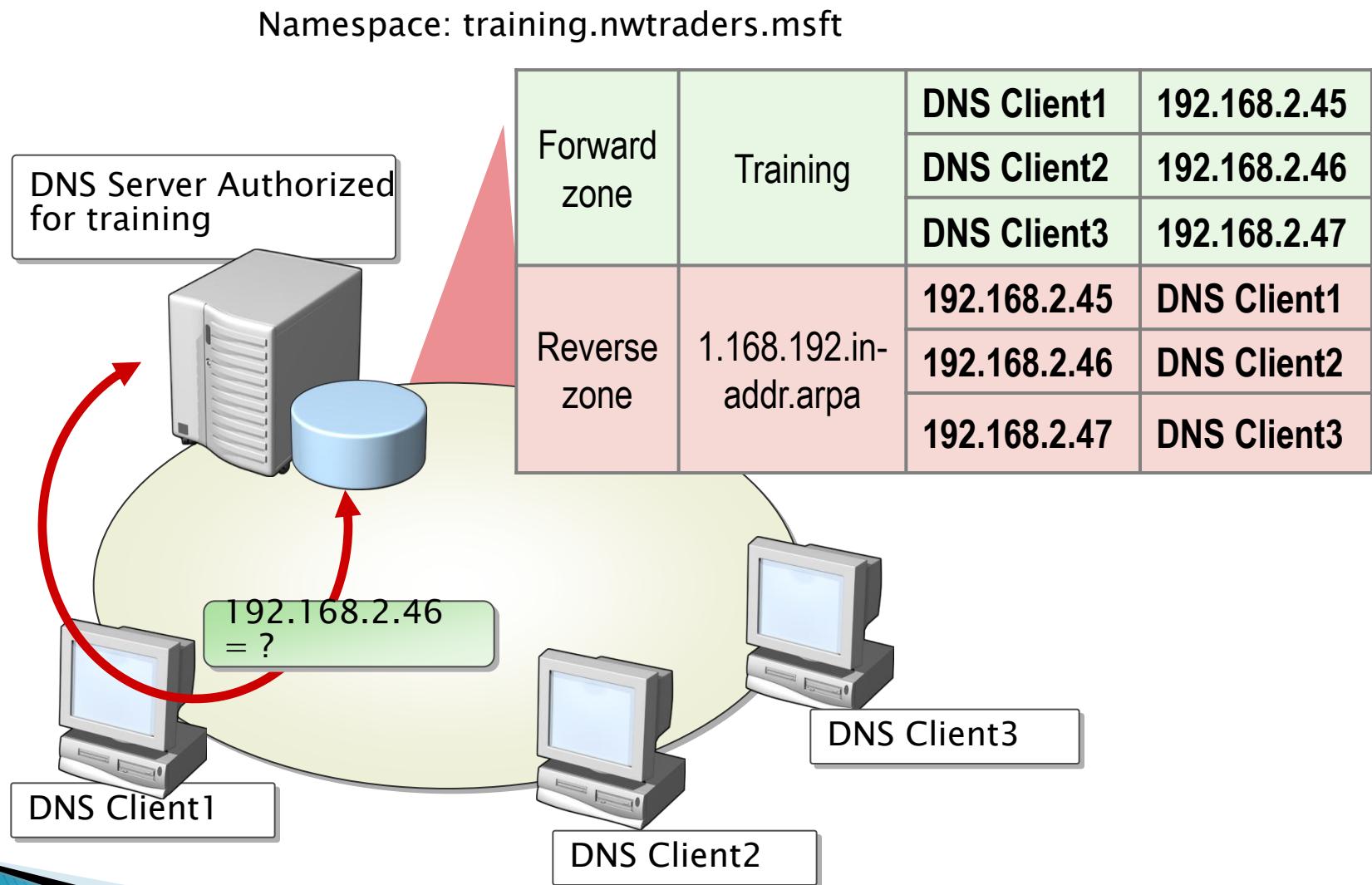
- ▶ Active Directory-integrated zone có một số thuận lợi sau:
 - DNS zone lưu trữ trong trong Active Directory, nhờ cơ chế này mà dữ liệu được bảo mật hơn.
 - Sử dụng cơ chế nhân bản của Active Directory để cập nhận và sao chép cơ sở dữ liệu DNS.
 - Sử dụng secure dynamic update.
 - Sử dụng nhiều master name server để quản lý tên miền thay vì sử dụng một master name server.
- ▶ Mô hình Active Directory-integrated zone sử dụng secure dynamic update

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



8.What Are Forward and Reverse Lookup Zones?



V. Phân loại Domain Name Server.

- ▶ V.1. Primary Name Server
- ▶ V.2. Secondary Name Server.
- ▶ V.3. Caching Name Server.

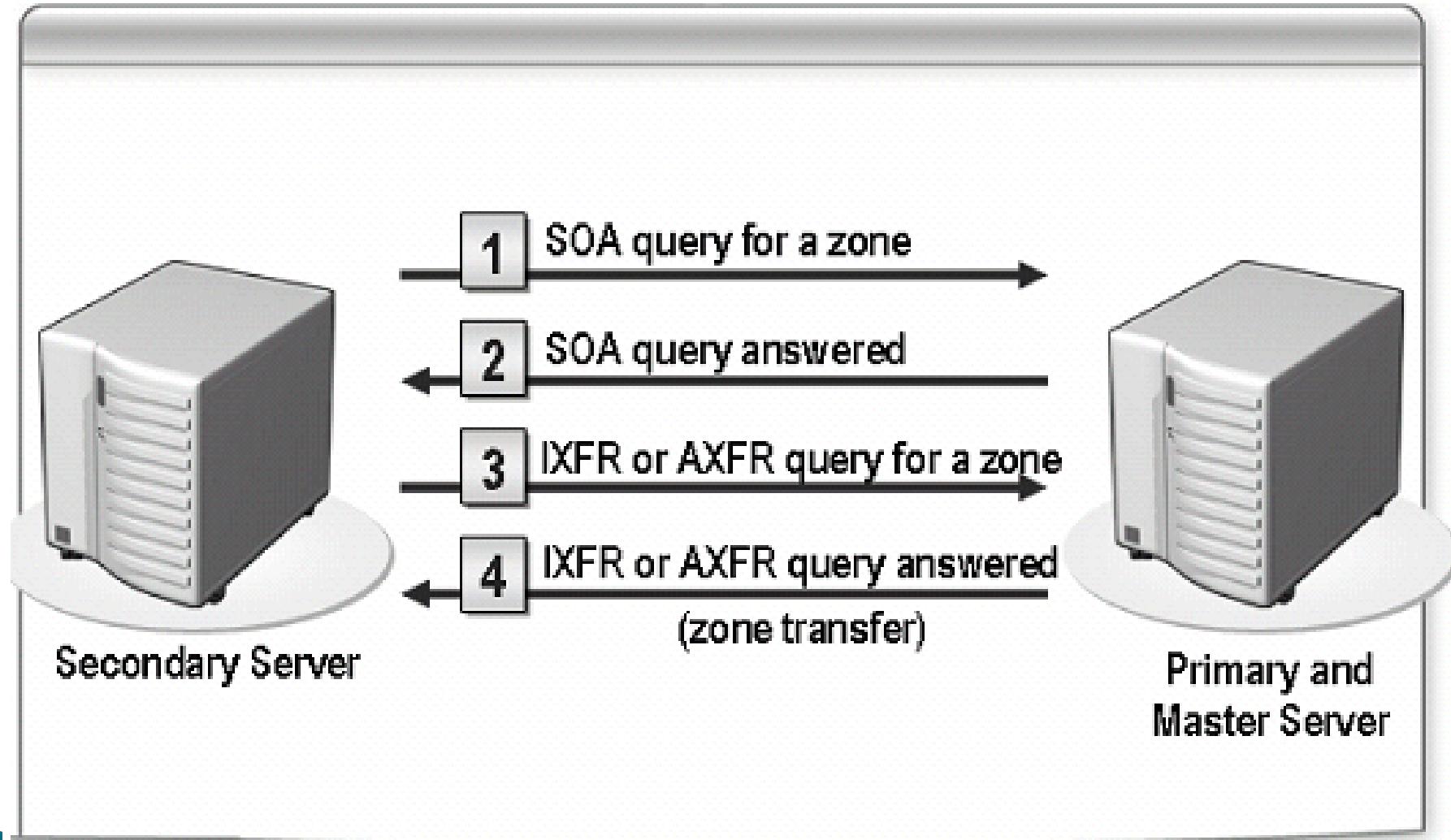
V.1. Primary Name Server

- ▶ Mỗi miền phải có một Primary Name Server để lưu trữ CSDL của DNS.
- ▶ Server này được đăng kí trên Internet để quản lý miền. (public tên và IP)
- ▶ Server này có nhiệm vụ phân giải tất cả các máy trong miền hay zone.

V.2. Secondary (Slave) Name Server

- ▶ Server này có nhiệm vụ sao lưu tất cả những dữ liệu trên Primary Name Server theo một chu kỳ nào đó
- ▶ Dự phòng khi Primary Name Server bị lỗi
- ▶ Trong một miền có thể có một hay nhiều Secondary Name Server.
- ▶ , Secondary sẽ sao chép và cập nhật CSDL từ Primary
- ▶ Tên và địa chỉ IP của Secondary Name Server cũng được public

Zone transfer

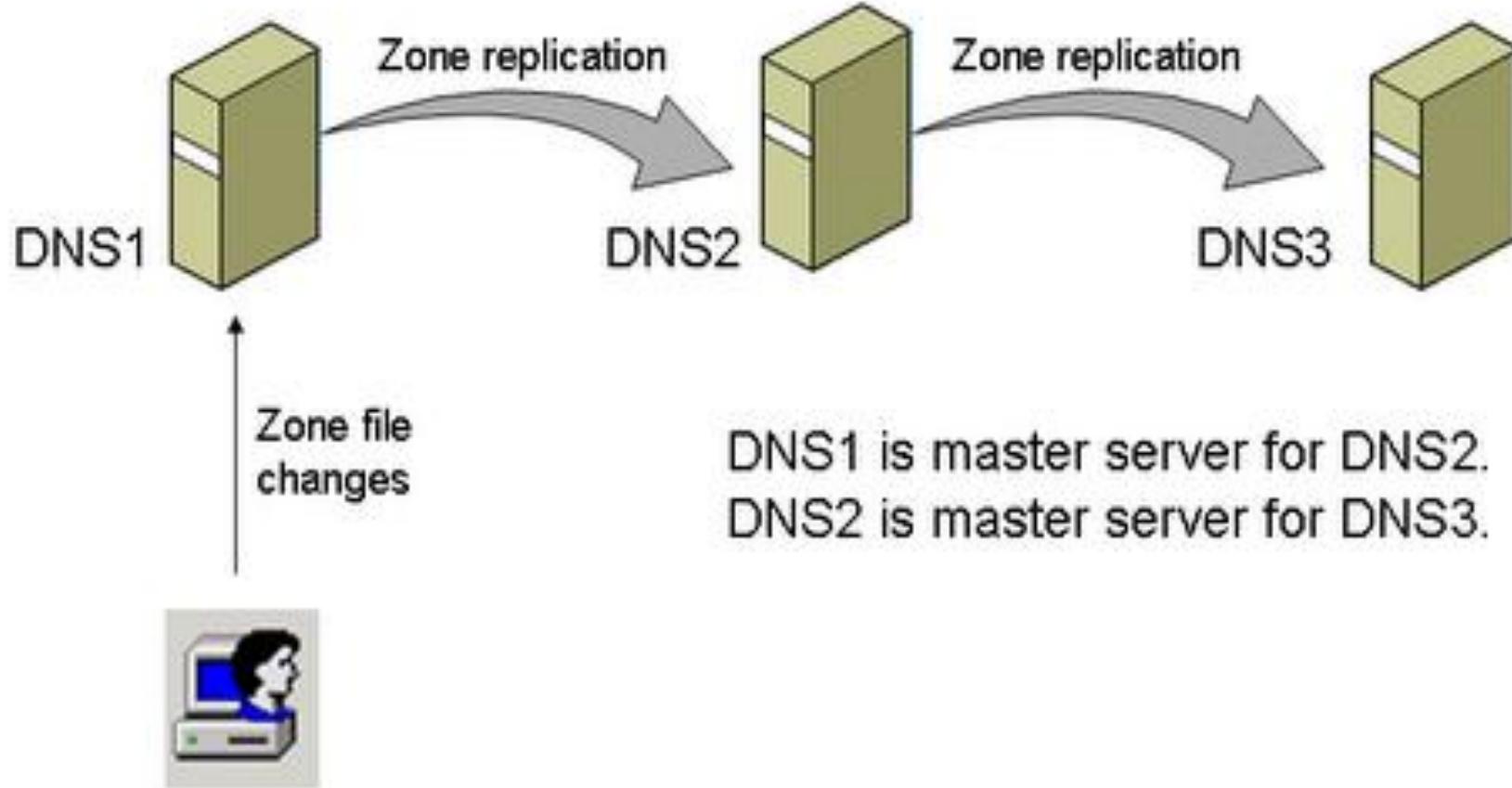


Primary - Secondary

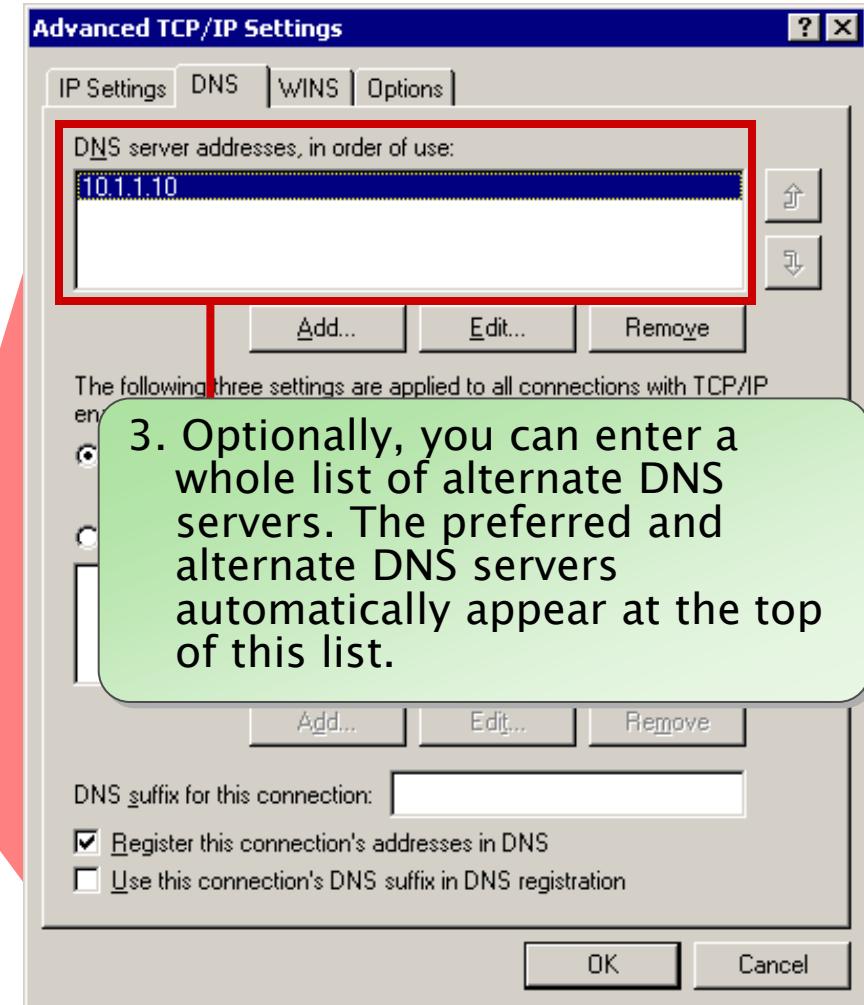
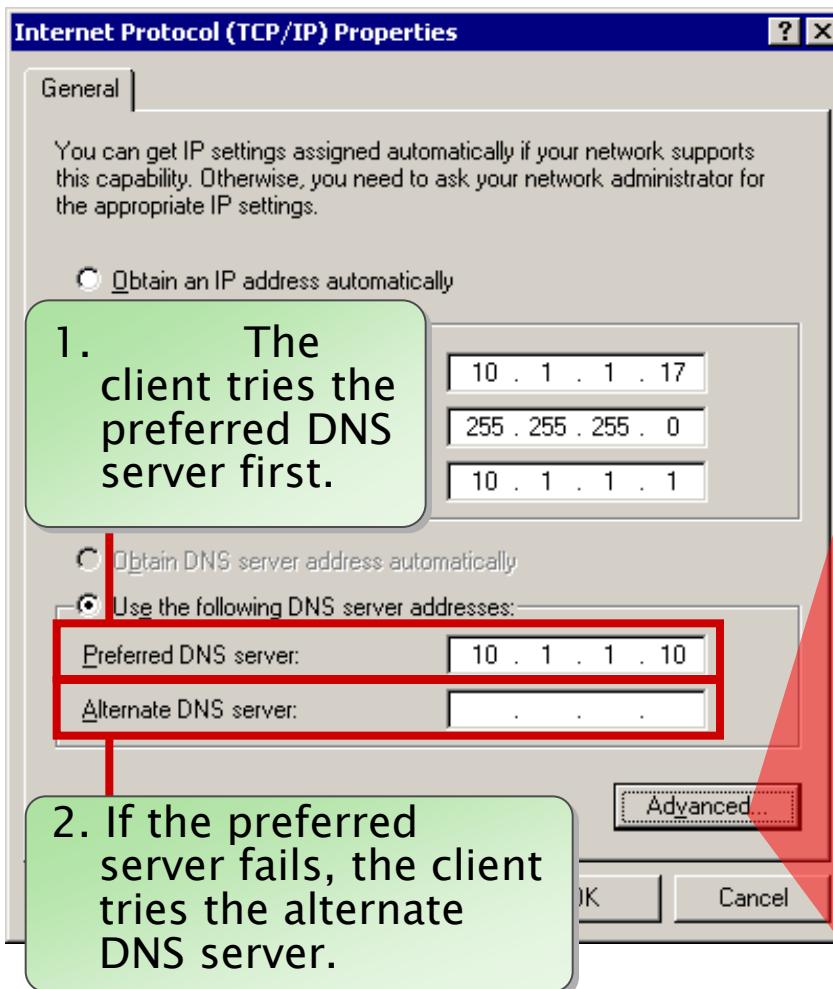
Primary DNS server

Secondary DNS server

Secondary DNS server



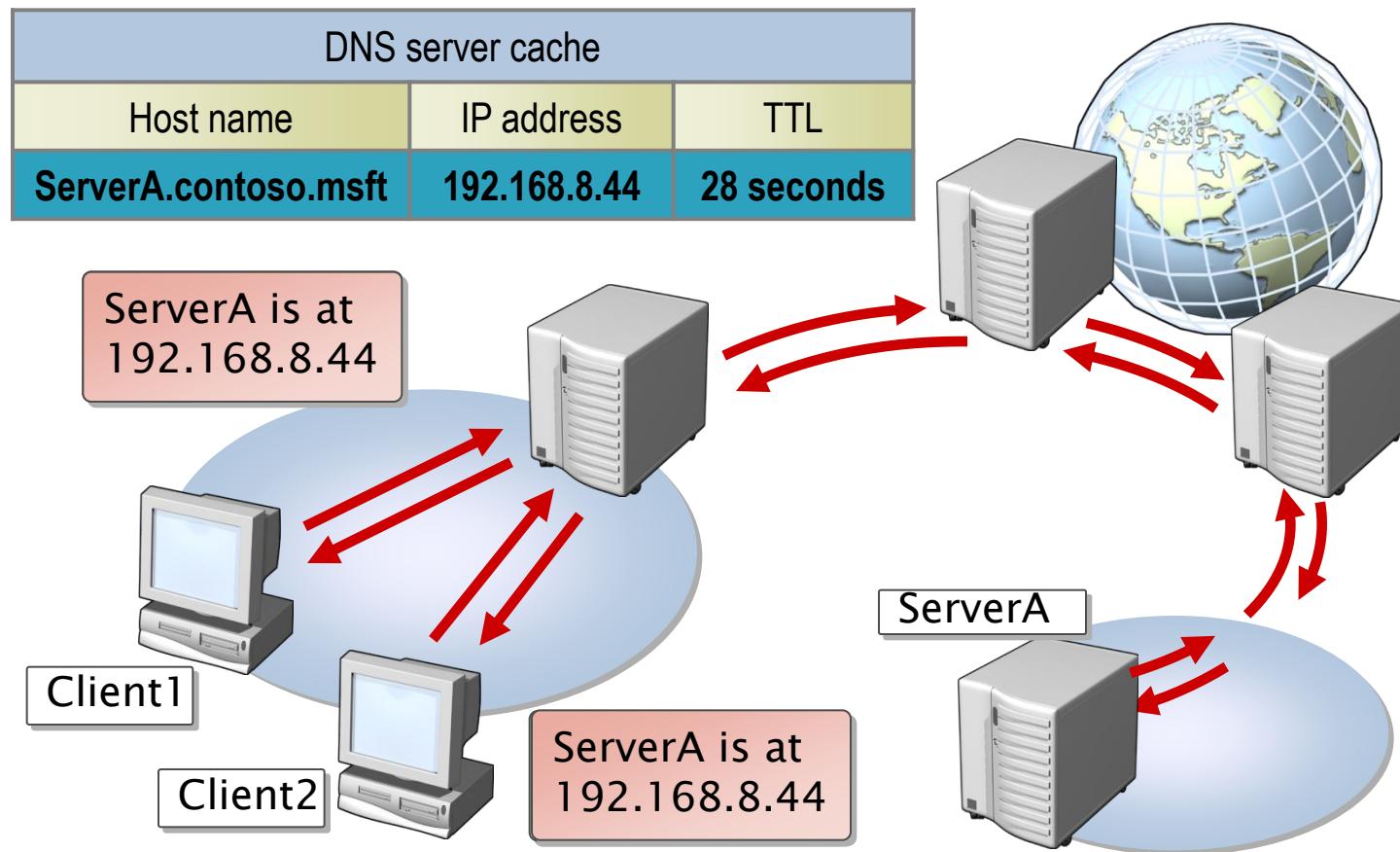
How Preferred and Alternate DNS Servers Work

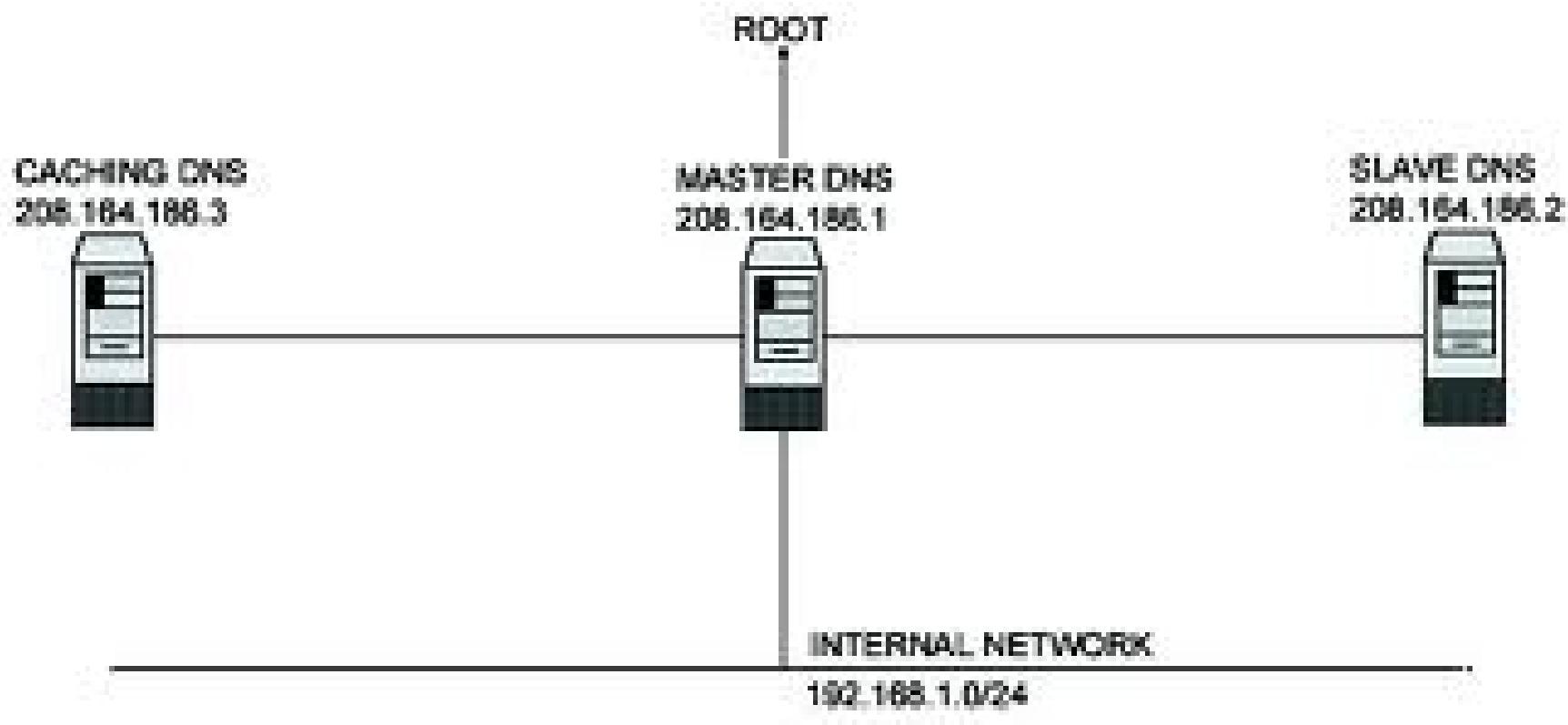


V.3. Caching Name Server

- ▶ Caching Name Server không có bất kỳ tập tin CSDL nào.
- ▶ Nó có chức năng phân giải tên máy trên những mạng ở xa thông qua những Name Server khác.
- ▶ Nó lưu giữ lại những tên máy đã được phân giải trước đó và được sử dụng lại những thông tin này nhằm mục đích:
 - Làm tăng tốc độ phân giải bằng cách sử dụng cache.
 - Giảm bớt gánh nặng phân giải tên máy cho các Name Server.
 - Giảm việc lưu thông trên những mạng lớn.

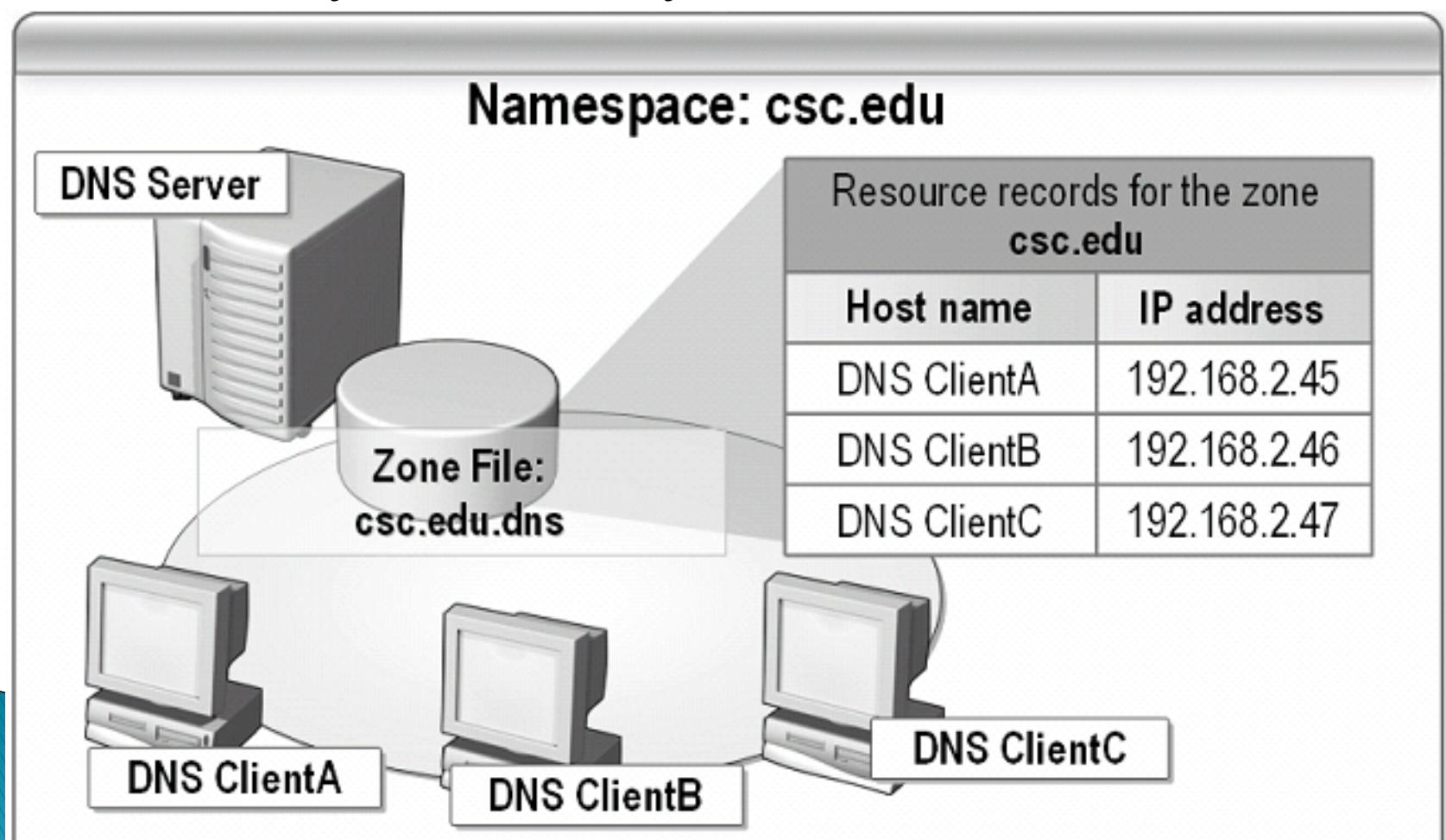
V.3. Caching Name Server





VI. Resource Record (RR).

- RR là mẫu thông tin dùng để mô tả các thông tin về CSDL DNS, được lưu trong các file cơ sở dữ liệu DNS \systemroot\system32\dns



VI. Resource Record (RR).

- VI.1. SOA(Start of Authority).
- VI.2. NS (Name Server).
- VI.3. A (Address) và CNAME (Canonical Name).
- VI.4. AAAA.
- VI.5. SRV.
- VI.6. MX (Mail Exchange).
- VI.7. PTR (Pointer).

What Are Resource Records and Record Types?

The screenshot shows the Windows DNS Management console window titled "dnsmgmt - [DNS\WANNT-DSRHGVLY\Forward Lookup Zones\thanhvan.com]". The left navigation pane shows the tree structure: DNS > WANNT-DSRHGVLY > Forward Lookup Zones > thanhvan.com. The right pane displays the "thanhvan.com 8 record(s)" table:

| Name | Type | Data |
|-------------------------|--------------------------|--|
| DomainDnsZones | | |
| ForestDnsZones | | |
| (same as parent folder) | Start of Authority (SOA) | [9], wannt-dsrhgvlny.thanhvan.com.,... |
| (same as parent folder) | Name Server (NS) | wannt-dsrhgvlny.thanhvan.com. |
| (same as parent folder) | Host (A) | 192.168.90.3 |
| vannt-dsrhgvlny | Host (A) | 192.168.90.3 |
| www | Host (A) | 192.168.90.3 |
| ftp | Host (A) | 192.168.90.3 |

Below the table is a summary table of record types:

| Type | Description |
|-------|--|
| A | Resolves a host name to an IP address |
| PTR | Resolves an IP address to a host name |
| SOA | The first record in any zone file |
| SRV | Resolves names of servers providing services |
| NS | Identifies the DNS server for each zone |
| MX | The mail server |
| CNAME | Resolves an alias to a host name |

VI.1. SOA

- ▶ Trong mỗi tập tin CSDL phải có một và chỉ một record SOA (start of authority).
- ▶ Record SOA chỉ ra máy chủ Name Server là nơi cung cấp thông tin tin cậy từ dữ liệu có trong zone.
- ▶ Cú pháp của record SOA.

[tên-miền] IN SOA [tên-server-dns] [địa-chỉ-email] (

serial number;

refresh number;

retry number;

experi number;

Time-to-live number)

SOA

a) **serial number:** Khi một slave name server kết nối với master server để lấy dữ liệu, trước tiên nó sẽ kiểm tra số serial, nếu số serial của master lớn hơn tức là dữ liệu đã hết hạn sử dụng và nó sẽ load lại dữ liệu mới. Vì vậy khi ta cập nhật dữ liệu trên name server ta nên tăng số serial. Thông thường ta định dạng theo thời gian như sau:

YYYYMMDDNN

Ví dụ: 2012111901

b) **refresh number:** Khoảng Thời gian (giây) mà slave biết phải kiểm tra lại dữ liệu có còn sử dụng được không.

Ví dụ: 10800 ; Refresh sau 3 giờ.

c) **retry number:** Nếu slave không thể kết nối với master name server sau một khoảng thời gian refresh thì nó sẽ cố gắng kết nối lại sau retry giây. Giá trị này nhỏ hơn giá trị refresh.

Ví dụ: 3600 ; Retry sau 1 giờ

d) **experi number:** Nếu slave không thể kết nối với master server sau khoảng thời gian expire (giây) này, thì slave sẽ không trả lời cho vùng dữ liệu đó khi được truy vấn, vì nó cho rằng dữ liệu này đã quá cũ. Giá trị này phải lớn hơn giá trị refresh và retry.

Ví dụ: 604800 ; Expire sau 1 tuần.

e) **time-to-live number:** Time To Live, giá trị này được dùng cho tất cả các resource record trong file cơ sở dữ liệu. Giá trị này cho phép những server khác cache lại dữ liệu trong 1 khoảng thời gian xác định TTL.

Ví dụ : 86400 ; TTL là 1 ngày

VI.2. NS

- ▶ Mỗi Name Server cho zone sẽ có một NS record.

- ▶ Cú pháp:

[domain_name] IN NS [DNS-Server_name]

- ▶ Ví dụ 2: Record NS sau:

abc.com. IN NS server1.abc.com.

abc.com. IN NS server2.abc.com.

- ▶ chỉ ra 2 name servers cho miền abc.com

VI.3. A và CNAME

- ▶ Record A (Address) ánh xạ tên máy (hostname) vào địa chỉ IP.
- ▶ Record CNAME (canonical name) tạo tên bí danh alias trả vào một tên canonical.
- ▶ Tên canonical là tên host trong record A hoặc lại trả vào 1 tên canonical khác.
- ▶ Cú pháp record A, CNAME:
[tên-máy-tính] IN A [địa-chỉ-IP]
[tên-máy-tính] IN CNAME [tên máy gốc]
- ▶ Ví dụ 1: record A trong tập tin abc.com
server.abc.com. IN A 172.29.14.1
game.abc.com. IN A 172.29.14.4
server1.abc.com IN CNAME game.abc.com
- ▶ // Multi-homed hosts
server.abc.com. IN A 172.29.14.1
server.abc.com. IN A 192.253.253.1

VI.4. AAAA

- ▶ Ánh xạ tên máy (hostname) vào địa chỉ IP version 6
- ▶ Cú pháp:
[tên-máy-tính] IN AAAA [địa-chỉ-IPv6]
- ▶ Ví dụ
Server IN AAAA 1243:123:456:789:1:2:3:456ab

VI.5. SRV.

- ▶ Cung cấp cơ chế định vị dịch vụ, Active Directory sử dụng Resource Record này để xác định domain controllers, global catalog servers, Lightweight Directory Access Protocol - LDAP servers.
- ▶ Các field trong SRV:
 - - Tên dịch vụ service.
 - - Giao thức sử dụng.
 - - Tên miền (domain name).
 - - TTL và class.
 - - Priority.
 - - Weight (hỗ trợ load balancing).
 - - Port của dịch vụ.
 - - Target chỉ định FQDN cho host hỗ trợ dịch vụ.
- ▶ Ví dụ:
_ftp._tcp.abc.com. IN SRV 0 0 21 ftpsvr1.abc.com.
_ftp._tcp.abc.com. IN SRV 10 0 21 ftpsvr2.abc.com.

VI.6. MX (Mail Exchange).

- ▶ DNS dùng record MX trong việc chuyển mail trên mạng Internet.
- ▶ Khi nhận được mail, trình chuyển mail (mailer) sẽ dựa vào record MX để quyết định đường đi của mail.
 - Chuyển đến mailbox cục bộ
 - Chuyển tiếp mail đến một mail server khác (SMTP)
 - Chuyển sang một giao thức chuyển mail khác (UUCP-**Unix-to-Unix Copy**)

VI.6. MX (Mail Exchange).

- ▶ Cú pháp record MX:

[domain_name] IN MX [priority] [mail-host]

[priority]: thứ tự ưu tiên 16-bit (0-65535)

- ▶ Ví dụ record MX sau :

abc.com. IN MX 10 mailserver.abc.com.

abc.com. IN MX 15 backup.abc.com

VI.7. PTR (Pointer)

- ▶ Record PTR (pointer) dùng để ánh xạ địa chỉ IP thành Hostname.

- ▶ Cú pháp:

[Host-ID.{Reverse_Lookup_Zone}] IN PTR
[tên-máy-tính]

- ▶ Ví dụ:

Các record PTR cho các host trong mạng
192.249.249:

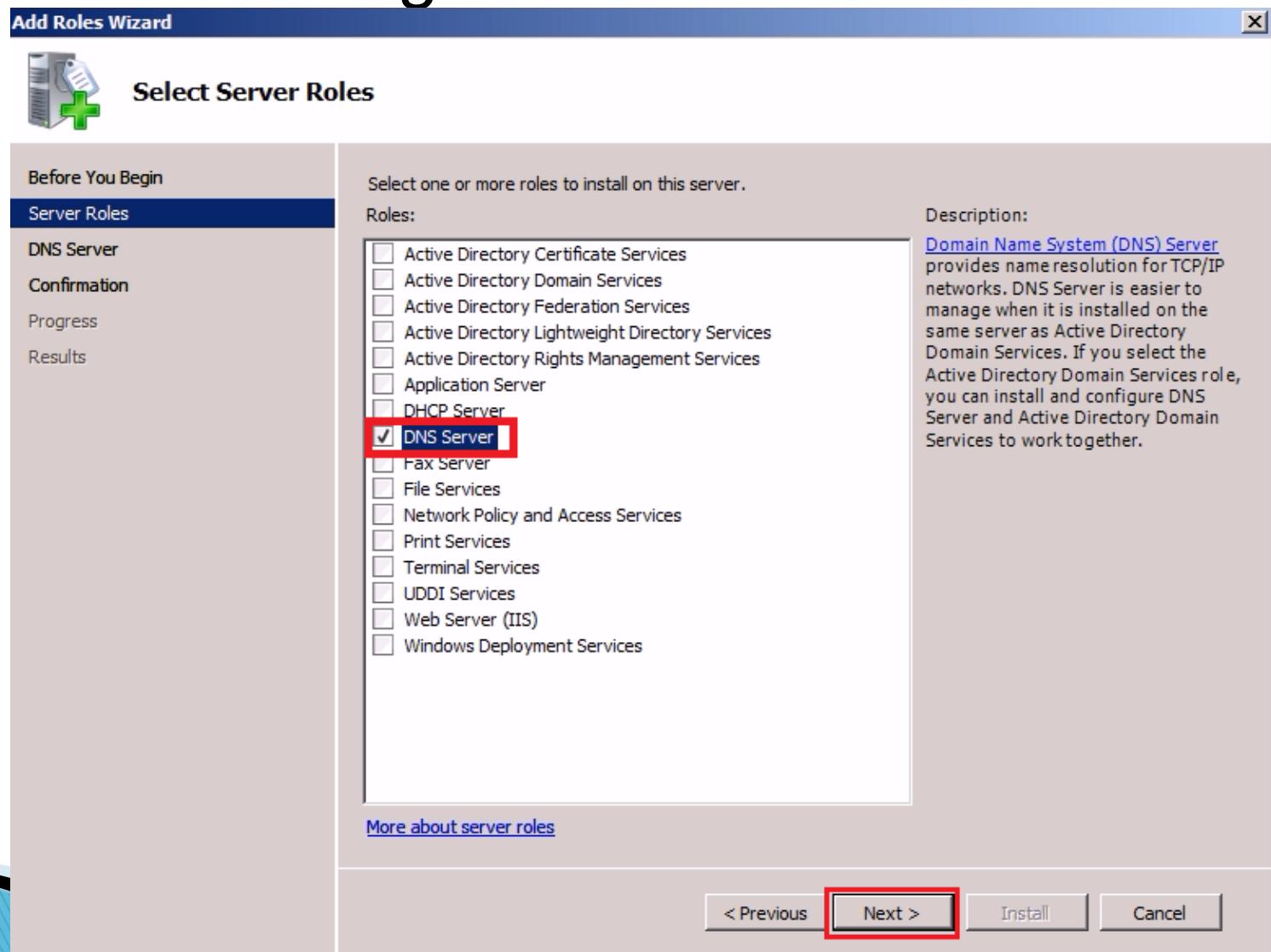
1.14.29.172.in-addr.arpa. IN PTR server.abc.com.

VII. Cài đặt dịch vụ DNS.

- ▶ Yêu cầu: có IP tĩnh
- ▶ Chọn Start | Control Panel | Add/Remove Programs | Add or Remove Windows Components | Windows components.

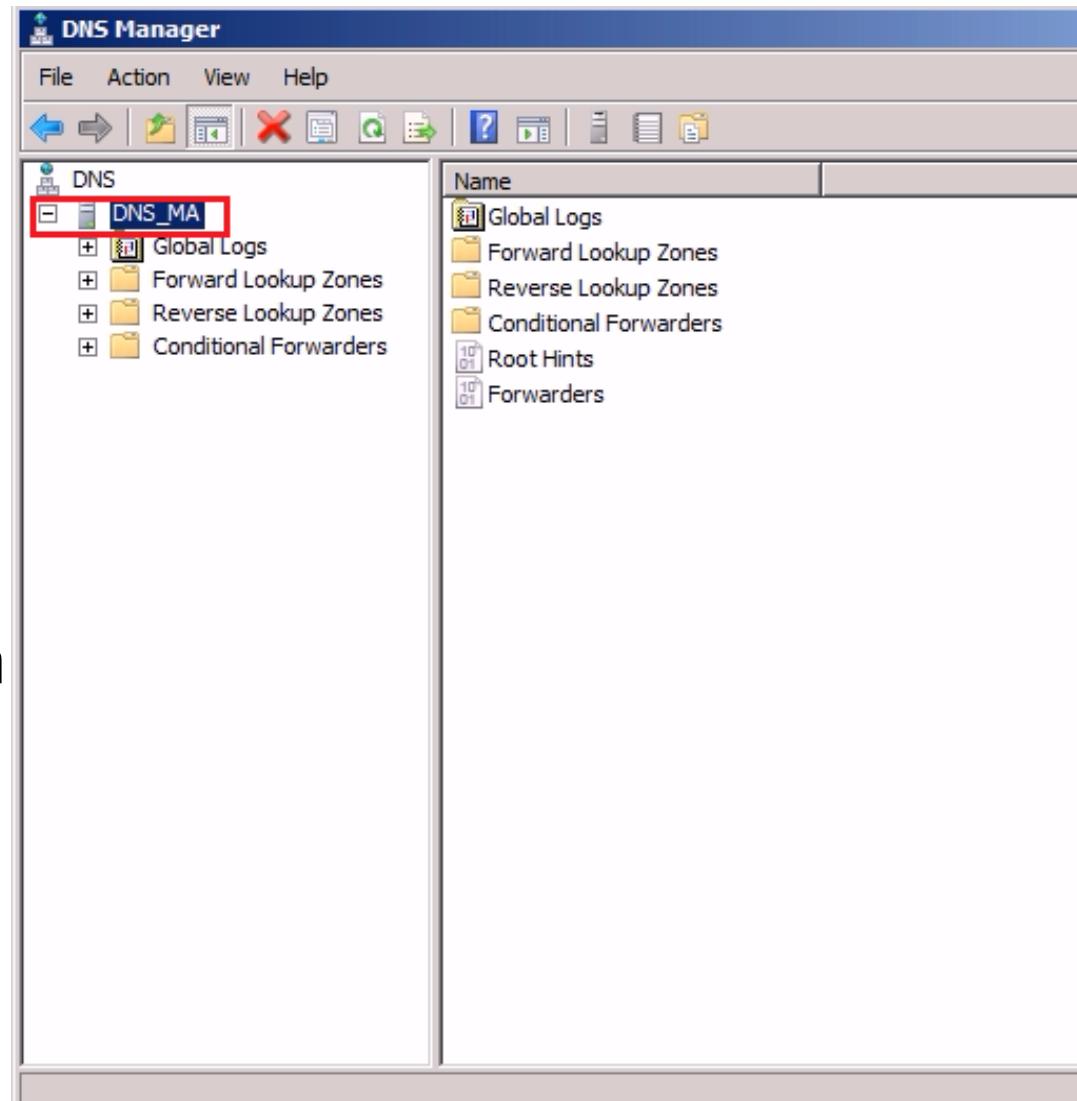
VII. Cài đặt dịch vụ DNS.

▶ Vào Server Manager\Roles



VII. Cài đặt dịch vụ DNS.

- ▶ Start → Programs → Administrative Tools → DNS.
- ▶ Nếu ta không cài DNS cùng với quá trình cài đặt Active Directory thì không có zone nào được cấu hình mặc định. Một số thành phần cần tham khảo trong DNS Console

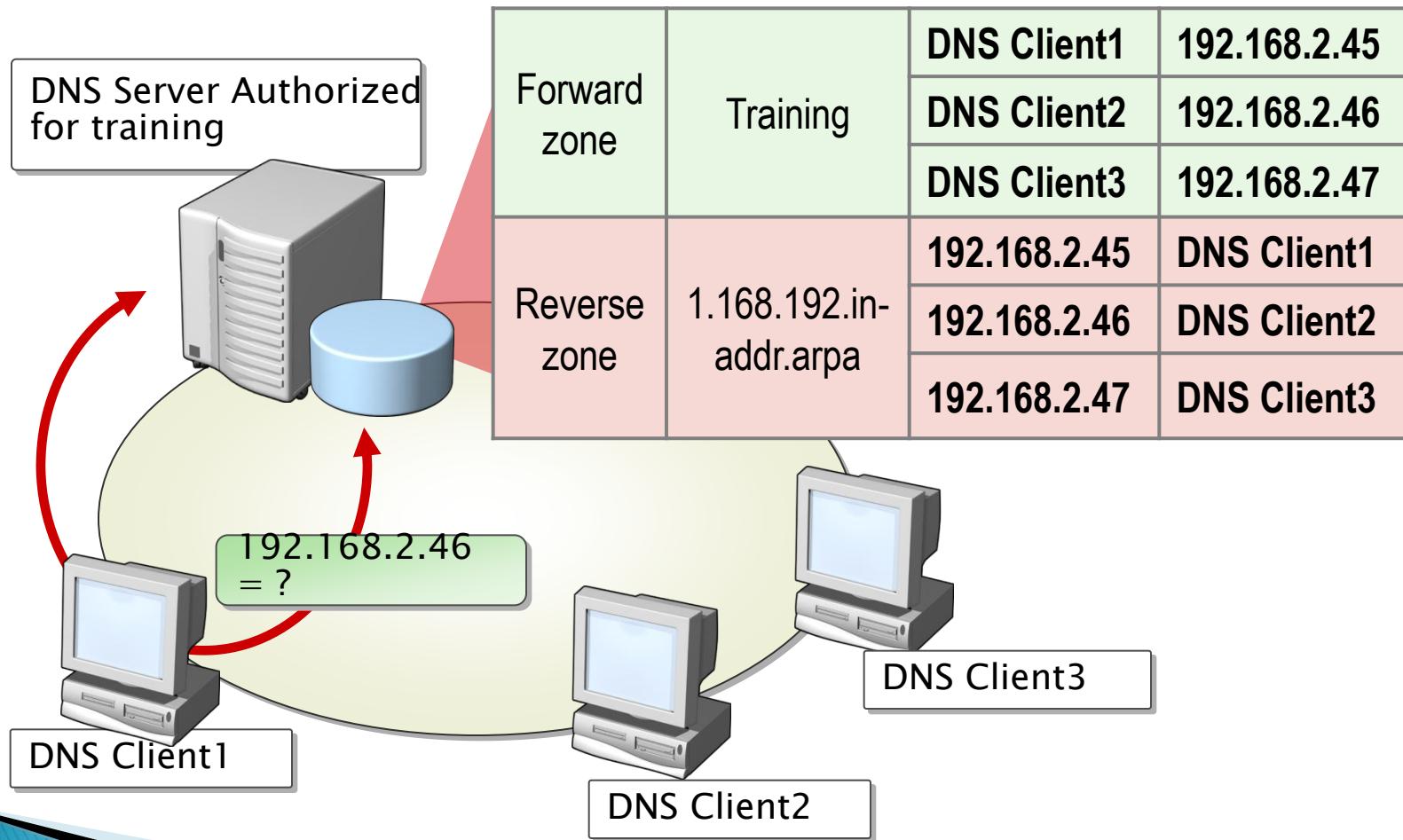


VIII. Cấu hình dịch vụ DNS.

1. Tạo Forward Lookup Zone:
2. Tạo Reverse Lookup Zone.
3. Tạo Resource Record(RR)
4. Kiểm tra hoạt động dịch vụ DNS.
5. Tạo miền con(Subdomain).
6. Ủy quyền cho miền con.
7. Tạo Secondary Zone.
8. Tạo zone tích hợp với Active Directory.
9. Thay đổi một số tùy chọn trên Name Server
10. Theo dõi sự kiện log trong DNS.

What Are Forward and Reverse Lookup Zones?

Namespace: training.nwtraders.msft

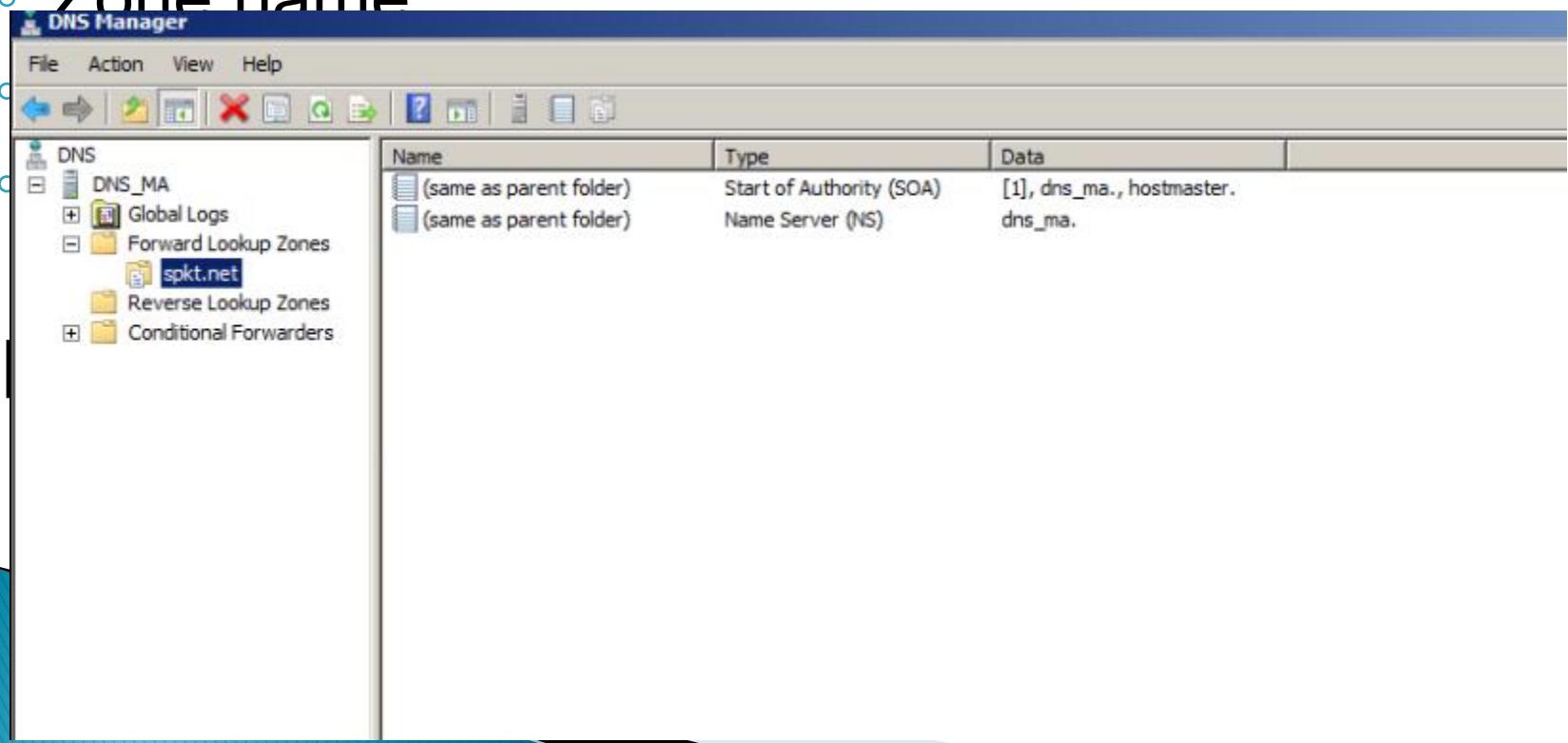


VIII.1. Tạo Forward Lookup Zone

Zone thuận: để phân giải địa chỉ Tên máy (hostname) thành địa chỉ IP

Chú ý chọn:

- Zone Type: Primary, Second, Stub
- Zone name



VIII.2. Tạo Reverse Lookup Zone

Zone nghịch để hỗ trợ cơ chế phân giải địa chỉ IP thành tên máy(hostname).

Sau khi ta tạo zone thuận và zone nghịch, mặc định hệ thống sẽ tạo ra hai resource record NS và SOA. Có thể thay đổi giá trị

VIII.3. Tạo Resource Record(RR)

- ▶ A: để ánh xạ hostname thành tên máy,
Chú ý:
 - New Host: Name, Ip address
 - Create associated pointer (PTR) record để tạo RR PTR trong zone nghịch
- ▶ CNAME
- ▶ MX

VIII.4. Kiểm tra hoạt động dịch vụ DNS.

Khai báo Resolver: tại máy client

- Để chỉ định rõ cho DNS Client biết địa chỉ máy chủ DNS Server hỗ trợ việc phân giải tên miền.

Chỉ định hai thông số .

- Referenced DNS server: PSN
- Alternate DNS server: SSN

Dùng tập lệnh của công cụ nslookup.

>set type=<RR_Type>

Trong đó <RR_Type> là loại RR

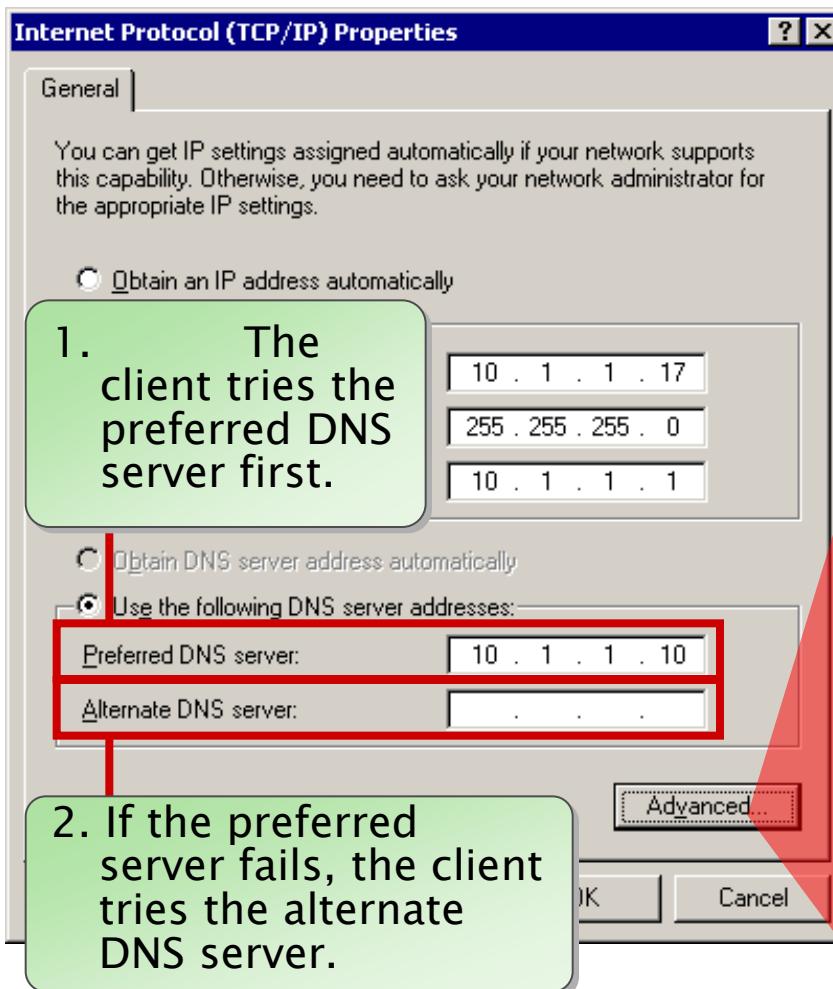
Nhập RR cần kiểm tra

>set type=any: Để xem mọi thông tin về RR trong miền,

Nhập <domain name>

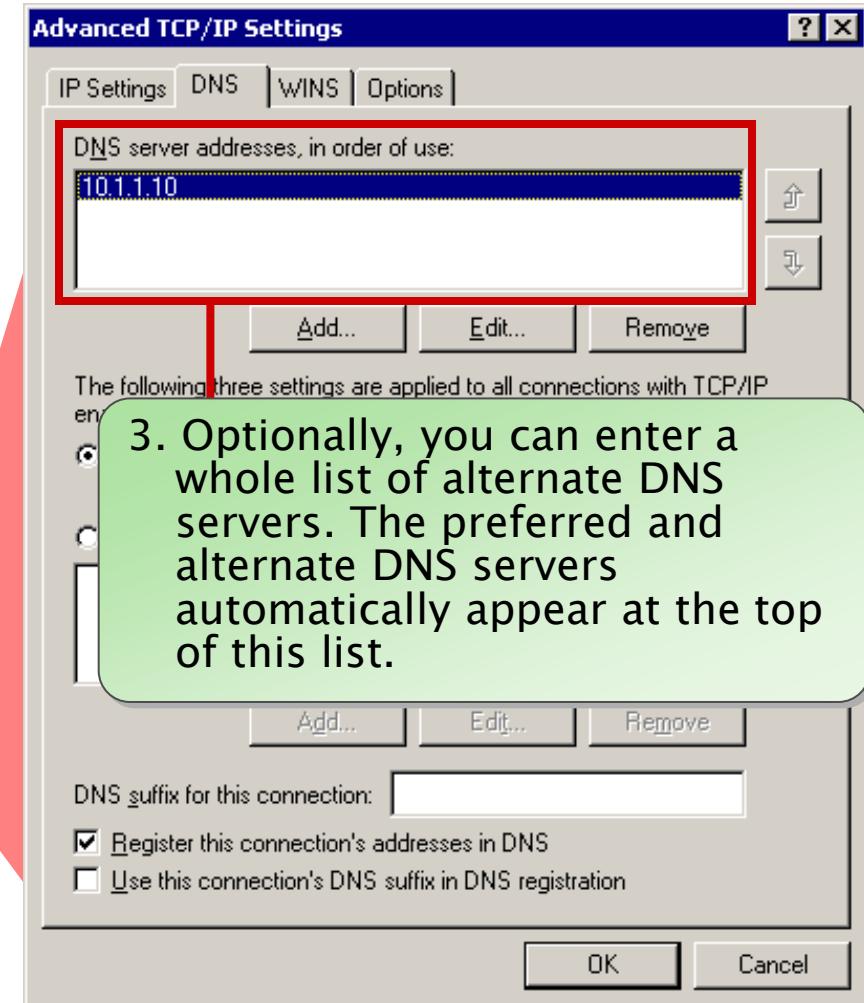
để xem thông tin về các RR như A, NS, SOA, MX của miền này.

How Preferred and Alternate DNS Servers Work



1. The client tries the preferred DNS server first.

2. If the preferred server fails, the client tries the alternate DNS server.



3. Optionally, you can enter a whole list of alternate DNS servers. The preferred and alternate DNS servers automatically appear at the top of this list.

Ex: A

The screenshot shows the Windows DNS Management console and a command-line nslookup session.

DNS Management Console:

- Left pane: Tree view of DNS settings for domain VANNT-DSRHGVLY.
- Right pane: Details for "192.168.90.x Subnet" showing 5 records:

| Name | Type |
|-------------------------|--------------------------|
| (same as parent folder) | Start of Authority (SOA) |
| (same as parent folder) | Name Server (NS) |
| 192.168.90.3 | Pointer (PTR) |
| 192.168.90.3 | Pointer (PTR) |
| 192.168.90.3 | Pointer (PTR) |

nslookup Command-line Session:

```
C:\Users\vannt>nslookup
Default Server: sruad.hcmute.edu.local
Address: 10.0.0.6

> server 192.168.90.3
Default Server: [192.168.90.3]
Address: 192.168.90.3

> 192.168.90.3
Server: [192.168.90.3]
Address: 192.168.90.3

Name: ftp.thanhvan.com
Address: 192.168.90.3

> ftp.thanhvan.com
Server: [192.168.90.3]
Address: 192.168.90.3

Name: ftp.thanhvan.com
Address: 192.168.90.3

> www.thanhvan.com
Server: [192.168.90.3]
Address: 192.168.90.3

Name: www.thanhvan.com
Address: 192.168.90.3
```

Ex: CNAME

dnsmgmt - [DNS\WANNT-DSRHGVLY\Forward Lookup Zones\thanhvan.com]

C:\Windows\system32\cmd.exe

```
C:\Users\wannt>nslookup
Default Server: srvad.hcmute.edu.local
Address: 10.0.0.6

> server 192.168.90.3
Default Server: [192.168.90.3]
Address: 192.168.90.3

> game.thanhvan.com
Server: [192.168.90.3]
Address: 192.168.90.3

Name: thanhvan.com
Address: 192.168.90.3
Aliases: game.thanhvan.com
```

C:\WINDOWS\system32\cmd.exe

```
C:\Documents and Settings\Administrator>ping game.thanhvan.com

Pinging thanhvan.com [192.168.90.3] with 32 bytes of data:
Reply from 192.168.90.3: bytes=32 time<1ms TTL=128

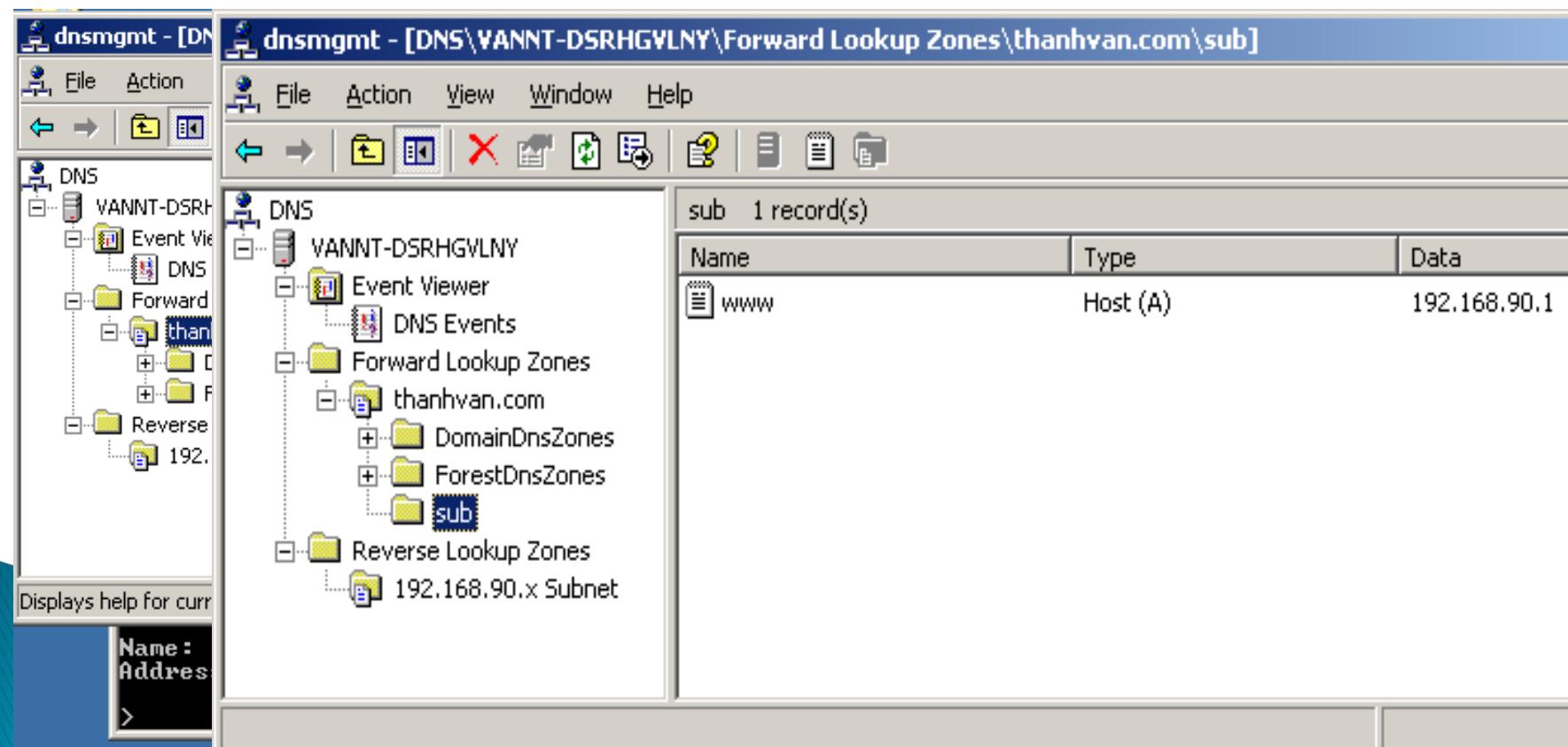
Ping statistics for 192.168.90.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

C:\Documents and Settings\Administrator>

VIII.5. Tạo miền con (Subdomain).

Cung cấp tên miền cho các tổ chức, các bộ phận con trong miền

Có thể phân loại và tổ chức hệ thống dễ dàng hơn.



Ex: subdomain

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>nslookup
Default Server: ftp.thanhvan.com
Address: 192.168.90.3

> server 192.168.90.3
Default Server: www.thanhvan.com
Address: 192.168.90.3

> 192.168.90.3
Server: www.thanhvan.com
Address: 192.168.90.3

Name: thanhvan.com
Address: 192.168.90.3

> 192.168.90.1
Server: www.thanhvan.com
Address: 192.168.90.3

Name: www.sub.thanhvan.com
Address: 192.168.90.1

> exit

C:\Documents and Settings\Administrator>ping www.sub.thanhvan.com

Pinging www.sub.thanhvan.com [192.168.90.1] with 32 bytes of data:
Reply from 192.168.90.1: bytes=32 time<1ms TTL=128
Reply from 192.168.90.1: bytes=32 time<1ms TTL=128
Reply from 192.168.90.1: bytes=32 time<1ms TTL=128
```

VIII. 6. Ủy quyền cho miền con.

Giả sử ta có miền spkt.net, ủy quyền quản lý miền subdomain cntt.spkt.net cho server cntt có địa chỉ IP x.x.x.x quản lý

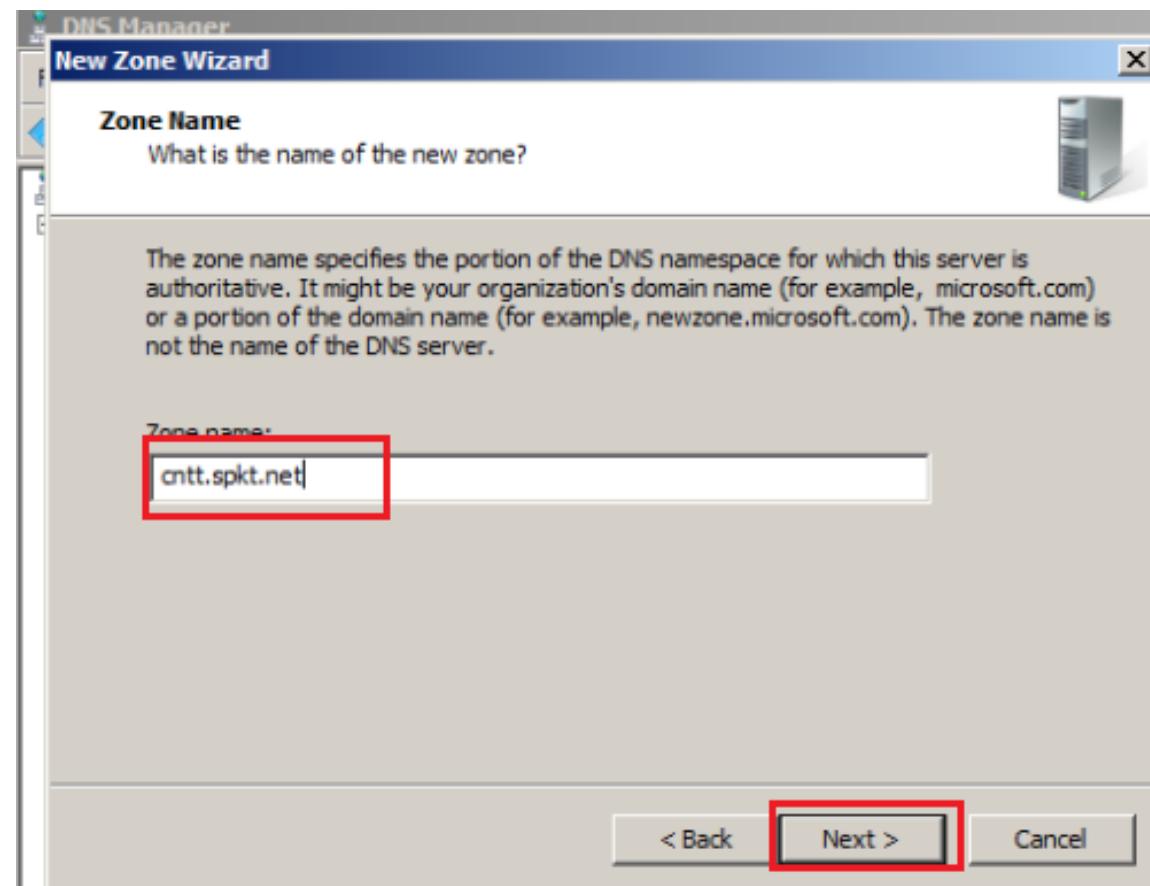
- Tạo resource record A cho cntt trong miền spkt.net
- Chọn Forward Lookup Zone, tên Zone \ chọn **New delegation...**
- Add Name Server quản lý CSDL cho miền con cntt.spkt.net trong hộp thoại Name Server

VIII. 6. Ủy quyền cho miền con.

Dùng server khác kết nối mạng với server DNS Master,

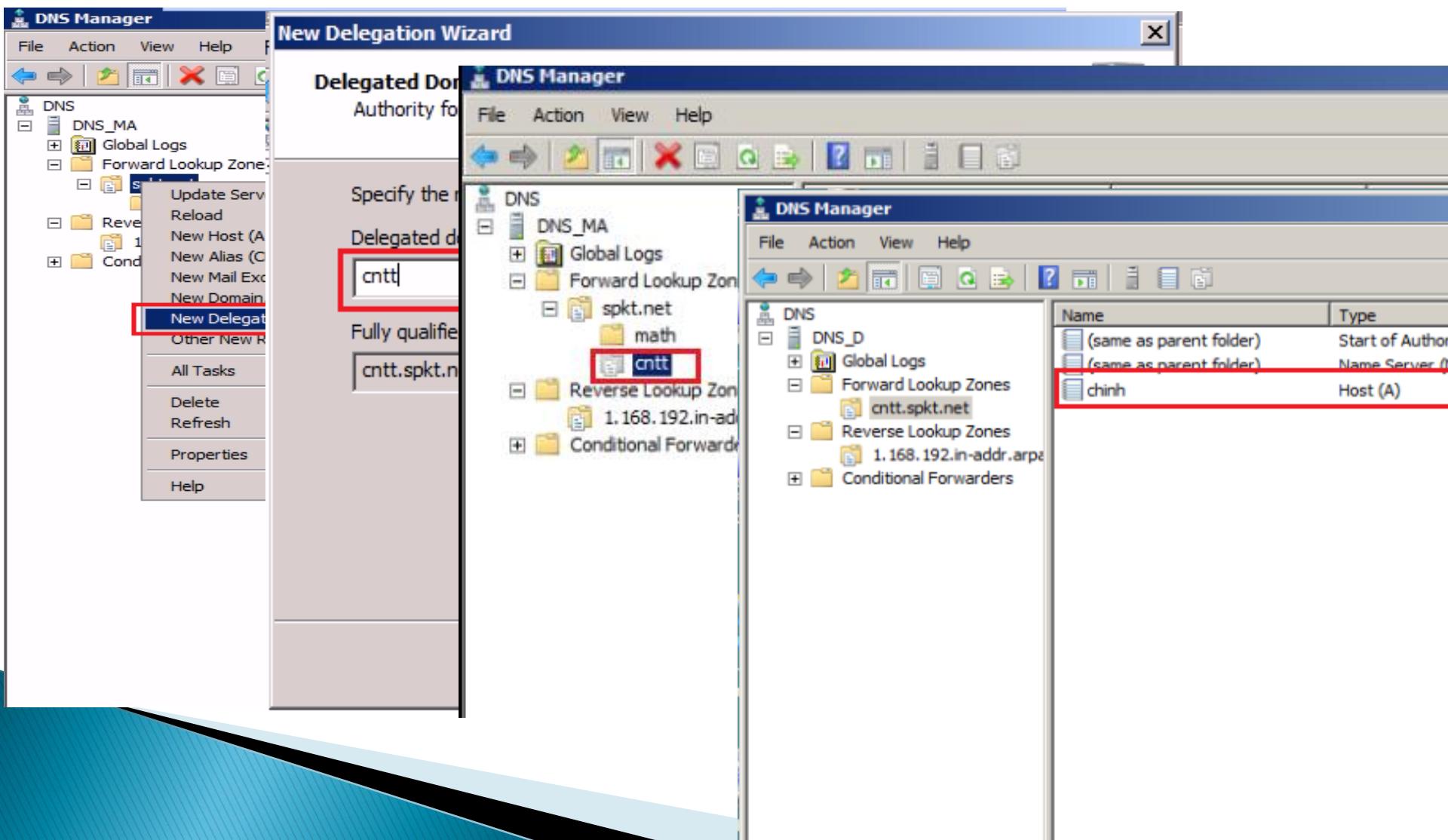
- Đặt IP và cài DNS như server DNS master.
- Tạo **primary zone** (có tên miền là sub của master, ex)
- Các bản ghi A, PTR
- **Forwader** tới Master

(Right Server\Property)



VIII. 6. Ủy quyền cho miền con.

Tại server DNS master



Test

Phân giải miền cha, miền con:

Tại client:

▶ DNS Server miền cha:

- Phân giải miền cha: kết quả bình thường
- phân giải miền con, kết quả là **non-authoritative answer** (kết quả truy vấn lấy được từ) miền con

▶ DNS Server miền con:

- Phân giải miền con: kq bt.
- Không phân giải được miền cha.

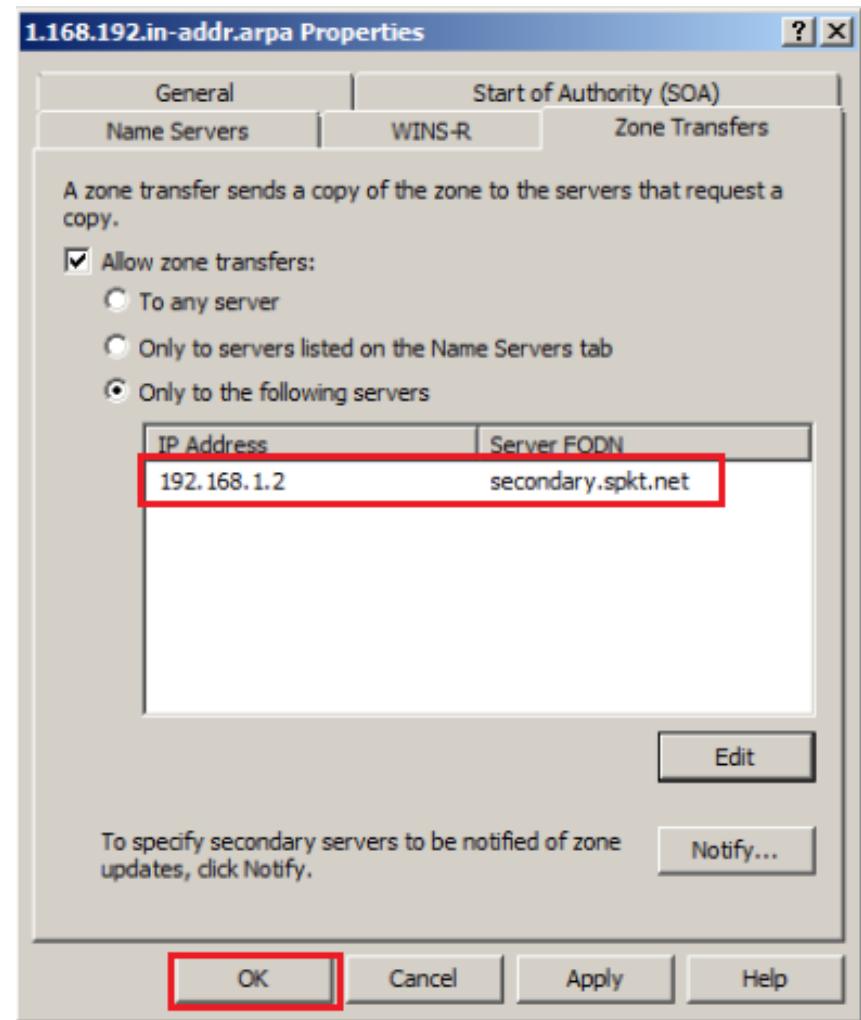
VIII. 7. Tạo Secondary Zone.

Secondary Name Server: là máy dự phòng, nó lưu trữ bảng sao dữ liệu từ máy PNS (CSDL sẽ tự động cập nhập sang SNS)

- ❖ Tại máy Master,
 - Cài đặt DNS
 - Tạo Primary zone, các RR
- ❖ Tại Máy Server DNS Secondary: đặt IP, cài DNS
 - Chọn: **Secondary Zone**
 - Chỉ định Zone Name muốn sao chép (ở master)
 - Chỉ định địa chỉ của máy Master
 - Tạo zone thuận nghịch (giống ở Master)
- ❖ Zone Transfer Reload: tại máy Master:
 - chọn Allow **transfer zone**: chỉ định IP của máy Secondary.
=> Các bản ghi RR từ máy Master sẽ transfer cho Secondary

VIII. 7. Tạo Secondary Zone.

▶ Zone transfer



VIII. 7. Tạo Secondary Zone.

- ▶ Test tại client DNS:

Giả sử PC DNS server primary không hoạt động, Khi sử dụng lệnh nslookup cho DNS server secondary thì vẫn phân giải được

VIII.8. Tạo zone tích hợp với AD

- Thực hiện trong quá trình cài AD:
chỉ tạo một số CSDL cần thiết ban đầu để nó thực hiện một số thao tác truy vấn và quản lý CSDL cho AD
- Hoặc tạo zone sau: có nhiều option
Chọn: Store the zone in AD

9. Thay đổi một số tùy chọn trên Name Server

Thông thường có ba phần chính trong việc thay đổi tùy chọn.

- ▶ Tùy chọn cho Name Server.
- ▶ Tùy chọn cho từng zone name.
- ▶ Tùy chọn cho từng RR trong zone name.

Theo dõi sự kiện log trong DNS.

Trong DNS management console cung cấp
mục Event Viewer

THỰC HÀNH

- ▶ Theo yêu cầu