

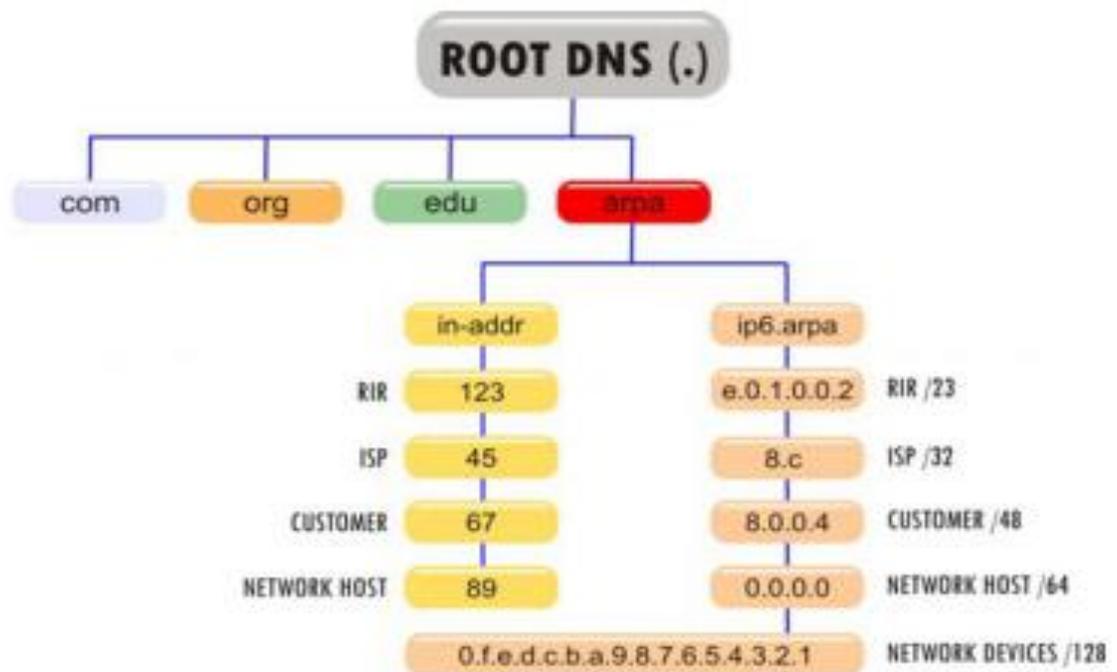
I. Cấu trúc không gian tên miền của bản ghi ngược

Ngoài chức năng chuyển đổi tên miền sang địa chỉ IP, hệ thống DNS còn có chức năng chuyển đổi ngược lại từ địa chỉ IP sang tên miền (reverse lookup). Chức năng reverse lookup cho phép tìm tên miền khi biết địa chỉ IP và được sử dụng trong trường hợp cần kiểm tra tính xác thực của các dịch vụ sử dụng trên Internet.

Ví dụ:

Trong dịch vụ thư điện tử, thư điện tử (email) cần được chuyển qua một loạt các trạm chuyển tiếp thư điện tử (email exchanger) trước khi được chuyển đến người dùng. Khi email được chuyển từ một trạm chuyển tiếp thư điện tử này đến một trạm chuyển tiếp thư điện tử khác, trạm chuyển tiếp thư điện tử nhận thư sẽ dùng chức năng reverse lookup của hệ thống DNS để tìm tên miền của trạm chuyển tiếp thư điện tử chuyển thư đến. Trong trường hợp địa chỉ IP của trạm chuyển tiếp thư điện tử gửi không được khai báo bản ghi ngược, trạm chuyển tiếp thư điện tử nhận sẽ không chấp nhận kết nối này và sẽ loại bỏ thư điện tử.

Không gian tên miền các bản ghi ngược cũng được xây dựng theo cơ chế phân cấp như không gian tên miền của các bản ghi thuận:



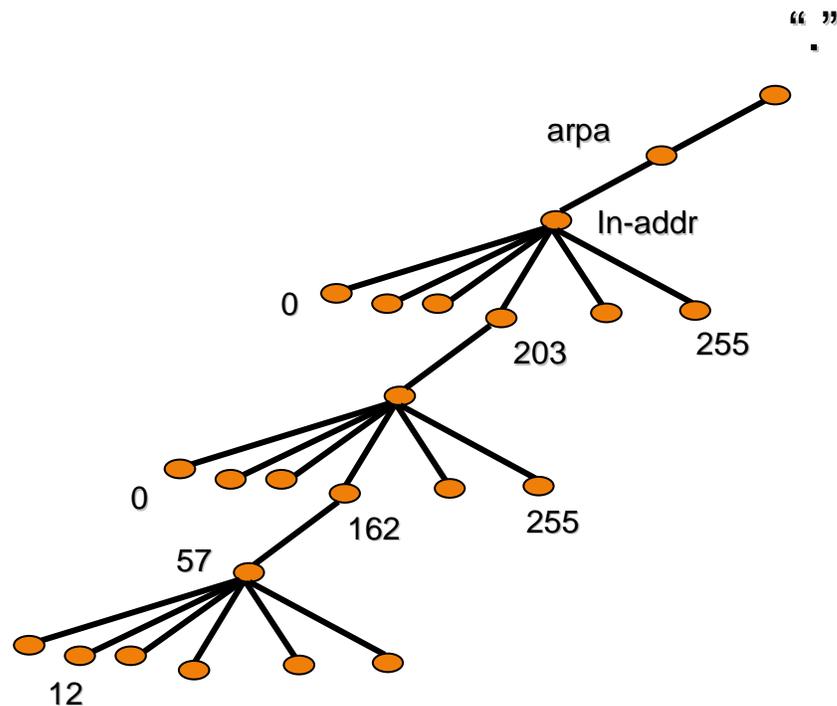
Hình vẽ cấu trúc không gian tên miền ngược của IPv4, IPv6 trong cây tên miền chung

Đối với thế hệ địa chỉ IPv4, cấu trúc của tên miền ngược có dạng như sau: www.zzz.yyy.xxx.in-addr.arpa. Trong đó: xxx, yyy, zzz, www là các số viết trong hệ thập phân biểu diễn giá trị của 4byte cấu thành 1 địa chỉ IPv4.

Ví dụ: Một máy tính trên mạng được gán địa chỉ IPv4 203.162.57.101 thì tên miền ngược tương ứng sẽ là 101.57.162.203.in-addr.arpa.

Máy chủ có tên miền: mail.vnnic.net.vn

Ảnh xạ vào tên miền thuận bằng bản ghi PTR: 12.57.162.203.in-addr.arpa. IN PTR mail.vnnic.net.vn



Hình vẽ minh họa cấu trúc tên miền ngược trong IPv4

Đối với thế hệ địa chỉ Internet mới IPv6, cấu trúc tên miền ngược có khác một chút. Cụ thể:

Không gian các tên miền ngược của các địa chỉ IPv6 không nằm dưới miền in-addr.arpa như của IPv4 mà nằm dưới miền .ip6.arpa.

- Do hoàn toàn không còn khái niệm class (lớp) trong IPv6 và 1 địa chỉ IPv6 được biểu diễn dưới dạng số hexa nên cấu trúc phân cấp tên miền ngược trong IPv6 cũng không chia theo lớp như ở IPv4 mà được phân cấp theo từng biên 4 bit tương ứng với mỗi số hexa cấu thành nên 1 địa chỉ IPv6

- Ví dụ: Một node mạng được gán địa chỉ IPv6
2001:0dc8:0123:1234:abcd:0000:0000:0000 thì tên miền ngược tương ứng sẽ là:
0.0.0.0.0.0.0.0.0.0.0.0.d.c.b.a.4.3.2.1.3.2.1.0.8.c.d.0.1.0.0.2.ip6.arpa

II. Cơ chế khai báo bản ghi ngược hiện tại cho các vùng địa chỉ của Việt Nam :

Hiện tại, các bản ghi ngược dùng cho vùng địa chỉ IP của Việt Nam được khai báo theo cơ chế chuyển giao (delegation classful) thông thường từ máy chủ DNS của APNIC về máy chủ DNS của thành viên. Theo cơ chế này, APNIC sẽ khai báo các bản ghi NS cho các tên miền ngược (classful) xuống các máy chủ DNS của thành viên. Mục đích của việc này là để tăng cường hiệu quả trong việc khai báo tên miền ngược. Cụ thể như sau :

- Các tổ chức sử dụng địa chỉ trực tiếp duy trì các bản ghi tên miền ngược cho địa chỉ sử dụng trong mạng cơ sở hạ tầng và cho khách hàng của tổ chức.
- Các thành viên địa chỉ có thể quản lý linh hoạt việc khai báo tên miền ngược thuộc vùng địa chỉ của mình. Tên miền ngược sẽ được chuyển giao trực tiếp theo không gian lớp (B, C) đối với IPv4 và theo các biên 4 bit (1 số hexa) từ máy chủ DNS của APNIC về DNS của thành viên. Do vậy, các thành viên có thể dễ dàng trong việc quản lý và chuyển giao tên miền ngược tới DNS của khách hàng (trong trường hợp cần thiết hoặc trực tiếp khai báo hỗ trợ khách hàng trên DNS của mình một cách chủ động dễ dàng và hiệu quả).

III. Hướng dẫn thành viên về thủ tục gửi yêu cầu khai báo chuyển giao tên miền ngược:

1. Chuẩn bị:

- Thành viên khai báo sẵn sàng các tên miền ngược tương ứng vùng địa chỉ IP (V4, V6) có nhu cầu chuyển giao về trên hệ thống máy chủ DNS của thành viên.
- Yêu cầu kỹ thuật: Tối thiểu phải có 2 máy chủ DNS phụ trách khai báo cho tên miền (tham khảo hướng dẫn cấu hình khai báo DNS ở phần sau). Các máy chủ phụ trách này phải luôn đảm bảo khả năng có thể truy vấn tên miền từ Internet.

- 2. Gửi yêu cầu qua giao diện web:** Nếu thành viên đã có tài khoản sử dụng hệ thống quản trị IP online tại địa chỉ <http://ipmember.vnnic.vn> thì có thể gửi yêu cầu online tại địa chỉ đó. Trường hợp chưa đăng ký sử dụng hệ thống thì có thể gửi yêu cầu qua email.

3. Gửi yêu cầu qua email:

- Địa chỉ nhận yêu cầu: info@vnnic.net.vn
- Nội dung yêu cầu:
 - + Vùng địa chỉ cần đăng ký chuyển giao tên miền ngược
 - + Tên các máy chủ DNS nhận chuyển giao cho tên miền (tối thiểu 02 tên, chỉ cung cấp tên - không cung cấp địa chỉ IP của máy chủ).

IV. Hướng dẫn thành viên cấu hình máy chủ DNS để khai báo các bản ghi ngược (trong Ipv4):

Theo cơ chế khai báo đang áp dụng, máy chủ DNS của APNIC sẽ chuyển giao classful các subdomain (tương ứng /16, /24) tới các máy chủ DNS của các thành viên. Khi đó, trên máy chủ DNS của các thành viên sẽ phải tạo và quản lý các zone (classful) tương ứng.

1. Cấu hình máy chủ DNS của thành viên

- Tạo trên máy chủ các zone “Z.Y.X.in-addr.arpa.” Trong đó X.Y.Z.0 là các class C địa chỉ mà thành viên nhận được từ VNNIC.
- Tạo các file dữ liệu tương ứng với các zone Z.Y.X.in-addr.arpa.
- Trong file dữ liệu của zone, khai báo các bản ghi ngược (PTR) cho toàn bộ các máy chủ có dịch vụ yêu cầu reverse dns.

Ví dụ:

Giả sử cần khai báo các bản ghi ngược cho tên miền www.abc.com.vn và www.abc1.com.vn trở đến hai địa chỉ 203.162.57.1 và 203.162.57.2 thuộc class C 203.162.57.0/24.

Trên máy chủ DNS của các thành viên sẽ khai báo zone:

57.162.203.in-addr.arpa.

Trong file dữ liệu của zone “57.162.203.in-addr.arpa”, khai báo các bản ghi ngược PTR cho các tên miền ngược như sau:

1.57.162.203.in-addr.arpa. IN PTR www.abc.com.vn.

2.57.162.203.in-addr.arpa. IN PTR www.abc1.com.vn.

Nếu DNS sử dụng phần mềm Bind 9, dữ liệu sẽ được khai báo như sau:

❖ *File named.conf của máy chủ DNS*

- DNS chính (primary) khai báo:

```
Zone "57.162.203.in-addr.arpa" {  
    Type master;  
    File "db.203.162.57";  
};
```

- DNS thứ cấp (secondary) khai báo:

```
Zone "100.162.203.in-addr.arpa" {  
    Type slaver;  
    File "db.203.162.57";  
    Masters { Địa chỉ IP của máy chủ DNS chính;};  
};
```

❖ *File dữ liệu db.203.162.57 khai các bản ghi ngược như sau:*

```
$TTL 86400;  
@ IN SOA tên máy dns primary của ISP địa chỉ email của admin  
(  
    2003091001 ; serial  
    10800 ; refresh (3 hours)  
    3600 ; retry (1 hour)  
    604800 ; expire (1 week)  
    86400 ; minimum (1 day)  
)  
  
    IN NS tên máy dns primary của ISP  
    IN NS tên máy dns secondary của ISP  
  
$ORIGIN 100.162.203.in-addr.arpa.  
1 IN PTR www.abc.com.vn.  
2 IN PTR www.abc1.com.vn.
```

2. Khai báo bản ghi ngược cho khách hàng của ISP

Đối với các bản ghi ngược của khách hàng, tùy theo nhu cầu, các ISP có hai lựa chọn để duy trì các bản ghi ngược cho mạng của khách hàng :

- ISP duy trì toàn bộ các bản ghi ngược trong classful zone trên máy chủ DNS của ISP. Trong trường hợp này, khách hàng của ISP cần gửi các thông tin về máy chủ cần dịch vụ reverse DNS của khách hàng để ISP khai báo trên DNS của ISP.
- ISP chuyển giao subnet (delegate classless) tương ứng vùng địa chỉ của khách hàng tới máy chủ DNS của khách hàng để khách hàng tự khai báo các bản ghi ngược trên máy chủ của khách hàng. Trong trường hợp này, ISP khai báo theo chuẩn rfc 2317 và hướng dẫn khách hàng khai báo trên máy chủ của khách hàng.

3. ISP chuyển giao subnet tương ứng vùng địa chỉ đã cấp cho khách hàng tới máy chủ DNS của khách hàng.

Trong trường hợp này, các ISP cần yêu cầu khách hàng cung cấp thông tin về hai máy chủ mà khách hàng sẽ khai báo bản ghi ngược trên đó. Bao gồm :

- Tên của máy chủ DNS chính (DNS Primary)
- Địa chỉ IP của máy chủ DNS chính (DNS Primary)
- Tên của máy chủ DNS thứ cấp (DNS Secondary)
- Địa chỉ IP của máy chủ DNS thứ cấp (DNS Secondary)

Giả sử trong class C 203.162.57.0/24, ISP cấp cho các khách hàng sau và sẽ chuyển giao subnet đến các khách hàng tương ứng đó như sau:

203.162.57.0/25 cấp cho khách hàng A
203.162.57.128/26 cấp cho khách hàng B
203.162.57.192/26 cấp cho khách hàng C

Class C 203.162.57.0 tương ứng zone mẹ trên máy chủ DNS của ISP là

57.162.203.in-addr.arpa

Các zone con tương ứng sub-domain sẽ chuyển giao được đặt tên bằng cách sử dụng địa chỉ đầu tiên và mặt nạ của subnet như sau:

- Vùng địa chỉ cấp cho A (/25) tương ứng zone
0-25.57.162.203.in-addr.arpa
- Vùng địa chỉ cấp cho B (/26) tương ứng zone
128-26.57.162.203.in-addr.arpa
- Vùng địa chỉ cấp cho C (/26) tương ứng zone
192-26.57.162.203.in-addr.arpa

3.1 Khai báo trên máy chủ DNS của ISP :

Trong file dữ liệu của zone (classful) 57.162.203.in-addr.arpa là db.203.162.57 cần khai như sau:

```
$ORIGIN .
$TTL 86400 ; 1 day
57.162.203.in-addr.arpa IN SOA tên dns primary của ISP email của admin
(
    2003091001 ; serial
    10800 ; refresh (3 hours)
    3600 ; retry (1 hour)
    604800 ; expire (1 week)
    86400 ; minimum (1 day)
)
NS tên miền của máy DNS primary của ISP
NS tên miền của máy DNS Secondary của ISP

$ORIGIN 57.162.203.in-addr.arpa.

; Chuyển giao zone 0-25 cho máy chủ của khách hàng A
0-25 NS tên miền của máy DNS primary của khách hàng A
NS tên miền của máy DNS Secondary của khách hàng A
```

1 CNAME 1.0-25

2 CNAME 2.0-25

; Khai toàn bộ đến địa chỉ 127 thuộc subnet 203.162.57.0/25

; Chuyển giao zone 128-26 cho máy chủ của khách hàng B

128-26 NS tên miền của máy DNS primary của khách hàng B

NS tên miền của máy DNS Secondary của khách hàng B

129 CNAME 129.128-26

130 CNAME 130.128-26

; Khai toàn bộ đến địa chỉ 191 của subnet 203.162.57.128/26

; Chuyển giao zone 192-26 cho máy chủ của khách hàng C

192-26 NS tên miền của máy DNS primary của khách hàng C

NS tên miền của máy DNS Secondary của khách hàng C

193 CNAME 193.192-26

194 CNAME 194.192-26

3.2 Cấu hình máy chủ DNS của khách hàng:

ISP cần hướng dẫn khách hàng cấu hình DNS server và khai báo như sau:

a. Trên máy chủ của khách hàng A

sẽ cấu hình để phụ trách zone “0-25.57.162.203.in-addr.arpa” và khai báo các bản ghi ngược thuộc zone này.

Nếu sử dụng phần mềm Bind 9, dữ liệu được khai báo như sau:

❖ *File named.conf*

* Trên máy chủ Primary khai báo :

```
Zone "0-25.57.162.203.in-addr.arpa" {  
    Type master;  
    File "db.203.162.57";  
};
```

* Trên máy chủ Secondary khai báo:

```
Zone "0-25.57.162.203.in-addr.arpa" {  
    Type slaver;  
    File "db.203.162.57";  
    Master {Địa chỉ IP của máy chủ DNS primary};  
};
```

❖ File dữ liệu db.203.162.57 khai báo như sau:

```
$TTL 86400;
```

```
@ IN SOA      tên dnsprimary của khách hàng A      email của admin
```

```
(
```

```
                2003091001 ; serial
```

```
                10800 ; refresh (3 hours)
```

```
                3600 ; retry (1 hour)
```

```
                604800 ; expire (1 week)
```

```
                86400 ; minimum (1 day)
```

```
)
```

```
IN      NS      tên máy dnsprimary của khách hàng A
```

```
IN      NS      tên máy dnssecondary của khách hàng A
```

```
$ORIGIN 0-25.57.162.203.in-addr.arpa.
```

```
1      IN      PTR      www.a.com.vn.
```

```
2      IN      PTR      www.a1.com.vn.
```

; Khai toàn bộ các bản ghi PTR cho các máy chủ cần đến dịch vụ reverse dns

b. Trên máy chủ khách hàng B

Cấu hình để phụ trách zone “128-26.57.162.203.in-addr.arpa” và khai báo các bản ghi ngược thuộc zone này

Nếu sử dụng phần mềm Bind 9, dữ liệu được khai báo như sau:

❖ *File named.conf*

* Trên máy chủ Primary khai báo :

```
Zone “128-26.57.162.203.in-addr.arpa” {  
    Type master;  
    File “db.203.162.57”;  
};
```

* Trên máy chủ Secondary khai báo:

```
Zone “128-26.57.162.203.in-addr.arpa” {  
    Type slaver;  
    File “db.203.162.57”;  
    Master {Địa chỉ IP của máy chủ DNS primary};  
};
```

❖ *File dữ liệu db.203.162.57 khai báo như sau:*

```
$TTL 86400;
```

```
@ IN SOA      tên dnsprimary của khách hàng B      email của admin (  
                2003090801 ; serial  
                10800 ; refresh (3 hours)  
                3600 ; retry (1 hour)  
                604800 ; expire (1 week)  
                86400 ; minimum (1 day)  
                )  
IN      NS      tên máy dnsprimary của khách hàng B
```

IN NS **tên máy dnssecondary của khách hàng B**

\$ORIGIN 128-26.57.162.203.in-addr.arpa.

129 IN PTR www.b.com.vn.

130 IN PTR www.b1.com.vn.

; Khai toàn bộ các bản ghi PTR cho các máy chủ cần đến dịch vụ reverse dns

c. Trên máy chủ khách hàng C

Cấu hình để phụ trách zone “192-26.57.162.203.in-addr.arpa” và khai báo các bản ghi ngược thuộc zone này

Nếu sử dụng phần mềm Bind 9, dữ liệu được khai báo như sau:

❖ *File named.conf*

* Trên máy chủ Primary khai báo :

```
Zone “192-26.57.162.203.in-addr.arpa” {  
    Type master;  
    File “db.203.162.57”;  
};
```

* Trên máy chủ Secondary khai báo:

```
Zone “192-26.57.162.203.in-addr.arpa” {  
    Type slaver;  
    File “db.203.162.57”;  
    Master {Địa chỉ IP của máy chủ DNS primary};  
};
```

❖ *File dữ liệu db.203.162.57 khai báo như sau:*

\$TTL 86400;

@ IN SOA **tên dnsprimary của khách hàng C** **email của admin**

(

2003091001 ; serial

10800 ; refresh (3 hours)

3600 ; retry (1 hour)

604800 ; expire (1 week)

86400 ; minimum (1 day)

)

IN NS tên máy dnsprimary của khách hàng C

IN NS tên máy dnssecondary của khách hàng C

\$ORIGIN 192-26.57.162.203.in-addr.arpa.

193 IN PTR www.c.com.vn.

194 IN PTR mail.c.com.vn.

; Khai toàn bộ các bản ghi PTR cho các máy chủ cần đến dịch vụ reverse dns