Bài 6. DỊCH VỤ TÊN MIỀN

1. Giới thiệu

- Máy tính và các thiết bị kết nối mạng, cụ thể là các giao diện mạng (network interfaces) của chúng, sử dụng địa chỉ IP làm định danh. Con người sử dụng tên miền thay cho IP để dễ nhớ. Vì vậy, cần phân giải/ánh xạ từ tên miền sang địa chỉ IP và ngược lại.
- DNS (Domain Name System) là một hệ cơ sở dữ liệu phân tán dùng để ánh xạ giữa các tên miền về các địa chỉ IP.
- DNS Client: Chạy trên thiết bị của người dùng, nhận tên miền do người dùng cung cấp, ví dụ người dùng nhập địa chỉ trang web trên trình duyệt, hỏi DNS để biết địa chỉ IP của máy đích.
- DNS Server: Hệ thống phân cấp các DNS servers.

2. DNS Client

2.1. Cấu hình DNS Client

Xem Mục "1.3 Phân giải tên" trong "Bài 5. Kết nối mạng."

2.2. Các phương pháp cơ bản kiểm tra DNS

DNS phân giải tên miền đầy đủ (FQDN - Fully Qualified Domain Name), ví dụ như vnu.edu.vn, tới một địa chỉ IP. Việc này được gọi là phân giải xuôi. Phân giải từ địa chỉ IP ra tên miền đầy đủ được gọi là phân giải ngược.

Nhiều tên miền có thể ánh xạ tới một địa chỉ IP duy nhất, nhưng ngược lại thì không đúng, một địa chỉ IP chỉ có thể ánh xạ tới duy nhất một tên miền. Điều này có nghĩa việc phân giải xuôi và ngược có thể không cho kết quả giống nhau. Các trường trong DNS dùng cho phân giải ngược thường thuộc trách nhiệm của nhà cung cấp dịch vụ (ISP), như vậy là khá phổ biến cho việc phân giải ngược tới tên miền của ISP. Đây không phải là yếu tố quan trọng đối với các trang web nhỏ, nhưng với một số ứng dụng thương mại điện tử thường yêu cầu việc phân giải xuôi và ngược phải phù hợp với nhau. Ta có thể yêu cầu ISP thay đổi DNS cho phù hợp với yêu cầu này.

Dưới đây là một số lệnh ta có thể dùng để tra cứu tên miền.

2.2.1. Lệnh host

Lệnh **host** chấp nhận các tham số là tên miền đầy đủ hoặc địa chỉ IP. Để tìm phân giải xuôi (tìm địa chỉ IP của tên miền đầy đủ), ta sử dụng cú pháp như sau:

```
[root@localhost ~]# host www.linuxhomenetworking.com
www.linuxhomenetworking.com has address 65.115.71.34
```

Còn để tìm phân giải ngược (tìm tên miền đầy đủ từ địa chỉ IP)

```
[root@localhost ~]# host 65.115.71.34
34.71.115.65.in-addr.arpa domain name pointer 65-115-71-34.myisp.net.
```

2.2.2. Lệnh nslookup

Lệnh nslookup dùng để tìm kiếm địa chỉ IP từ tên miền

```
[root@localhost ~]# nslookup www.linuxhomenetworking.com
Server:  192-168-1-200.my-site.com
Address:  192.168.1.200

Non-authoritative answer:
Name:    www.linuxhomenetworking.com
Address:  65.115.71.34
```

Để thực hiện tìm kiếm tên miền từ địa chỉ IP:

```
[root@localhost ~]# nslookup 65.115.71.34
Server:  192-168-1-200.my-site.com
Address: 192.168.1.200

Name:    65-115-71-34.my-isp.com
Address: 65.115.71.34
```

3. DNS Server

DNS Server có thể cung cấp các thông tin do DNS client yêu cầu, hoặc chuyển đến một DNS Server khác để nhờ phân giải hộ trong trường hợp nó không thể trả lời được các truy vấn về những tên miền không thuộc quyền quản lý, đồng thời cũng luôn sẵn sàng trả lời các DNS server khác về các tên miền mà nó quản lý. DNS server cấp cao nhất là Root Server do tổ chức ICANN quản lý.

- Phân loại:
  - Primary DNS server
  - Secondary DNS server
  - Caching DNS server

Khuyến nghị nên sử dụng ít nhất là hai DNS Server để lưu cho mỗi một zone. Primary DNS Server quản lý các zone và Secondary Server lưu trữ dự phòng cho Primary Server. Secondary DNS Server được khuyến nghị dùng nhưng không nhất thiết phải có.

Caching DNS server chỉ sử dụng cho việc truy vấn, lưu giữ câu trả lời dựa trên thông tin có trên cache của máy và cho kết quả truy vấn. Chúng không hề quản lý một domain nào và thông tin mà nó chỉ giới hạn những gì được lưu trên cache của Server.

3.1. Cài đặt DNS Server BIND

BIND (Berkeley Internet Name Distributed) là phần mềm DNS Server được sử dụng nhiều nhất hiện nay trên thế giới. Một chương trình phục vụ DNS trên nền các hệ thống AIX/BSD/HP-UX/Unix/Linux..., Bind chạy nhanh, hiệu suất cao, đáp ứng được số lượng user lớn, cấu hình linh hoạt, ...

Chạy lệnh sau để cài đặt BIND

```
sudo apt install bind9 dsnutils
```

3.2. Cấu hình BIND

Thư mục chứa các tệp cấu hình là /etc/bind/. Tệp cấu hình chính là /etc/bind/named.conf. Các dòng include bao hàm các tệp chứa các tùy chọn.

3.2.1. Cấu hình Caching nameserver

Nếu chỉ sử dụng bind như caching nameserver, đơn giản chỉ cần thêm các địa chỉ IP của các nameservers khác (ví dụ của các ISP). Chỉnh sửa tệp /etc/bind/named.conf.options, bỏ chú thích (#) và chỉnh sửa nội dung forwarders tương tự sau:

```
forwarders {
        8.8.8.8;
        8.8.4.4;
};
```

Để cấu hình mới có tác dụng, hãy khởi động lại bind bằng cách chạy lệnh sau:

```
sudo systemctl restart bind9.service
```

3.2.2. Cấu hình nameserver chính

Phần này trình bày ví dụ cấu hình phân giải tên cho tên miền example.com. Cấu hình cho các tên miền khác tương tự.

DNS cho phép chia hệ thống tên miền thành các zones phân cấp, và phân quyền cho các DNS Server quản lý các zones.

Resource Records (RR) là các bản ghi trong cơ sở dữ liệu DNS, được sử dụng để trả lời cho các truy vấn từ DNS Client. Có những loại RR sau:

Loại RR	**Mô tả**
A	Host – Phân giải tên thành địa chỉ IPv4
AAAA	Host – Phân giải tên thành địa chỉ IPv6
MX	Mail exchange – Chỉ đến Email Server trong domain.
CNAME (Alias)	Canonical name – Cho phép một host có thể có nhiều tên.
NS	Name Server – Chứa địa chỉ IP của DNS Server cùng với các thông tin về domain đó.
SOA	Start of Authority – Bao gồm các thông tin về domain trên DNS Server.
SRV	Service – Được sử dụng bởi Active Directory để lưu thông tin về vị trí của Domain Controllers
PTR	Pointer – Phân giải địa chỉ IP thành tên máy.

Cấu trúc bản ghi SOA:

```
Name Class Type Nameserver.  Email-address. (
```

Serial Refresh Retry Expire Negative-Cache-TTL

)

trong đó,

Name	Tên của zone. Có thể sử dụng "@" là tham chiếu đến zone gốc hiện tại trong tệp /etc/bind/named.conf.
Class	Lớp DNS. Trong bản ghi này là IN (Internet).
Type	DNS RR Type. Trong bản ghi này là SOA.
Nameserver	Tên đầy đủ của nameserver. Theo sau là dấu chấm (.)
Email-address	Địa chỉ email của quản trị viên quản trị nameserver. Ký tự @ trong email phải được thay bằng dấu chấm. Theo sau email cũng là dấu chấm.
Serial-no	Số tuần tự của cấu hình hiện tại.
Refresh	Chu kỳ các secondary DNS server phải đồng bộ với primary DNS server.
Retry	Chu kỳ các secondary DNS server phải thử kết nội lại để thực hiện đồng bộ nếu có lỗi kết nối.
Expire	Thời gian hết hạn của các bản ghi trên secondary DNS server nếu chúng chưa được đồng bộ từ primary DNS server.
Negative-Cache-TTL	Thời gian DNS client/DSN server thứ cấp được lưu đệm các trả lời tên miền không tồn tại (negative answer). Lưu đệm các trả lời này giúp không phải hỏi lại một cách lãng phí.

Cấu trúc các bản ghi NS, MX, A, AAA, CNAME, SRV và PTR:

Name Class Type Data

trong đó, giá trị của các trường phụ thuộc Type, được mô tả như sau.

Type	Name	Class	Data
NS	Thường để trống. Có thể sử dụng @ để chỉ tên zone hiện tại.	IN	Địa chỉ IP hoặc tên của nameserver. Tên có dấu chấm ở cuối.
MX	Domain được dùng cho email, thường trùng với domain của zone.	IN	Tên của mail server với dấu chấm ở cuối.
A	Tên của một máy trong domain	IN	Địa chỉ IPv4
AAAA	Tên của một máy trong domain	IN	Địa chỉ IPv6
CNAME	Bí danh	IN	Tên của bản ghi "A"
PTR	Octet cuối của địa chỉ IP của máy	IN	Tên đầy đủ của máy với dấu chấm ở cuối.

Phân giải xuôi

Để bắt đầu cấu hình phân giải xuôi cho miền example.com, thêm zone xuôi mới như sau vào tệp /etc/bind/named.conf.local:

```
zone "example.com" {
        type master;
        file "/etc/bind/db.example.com";
};
```

Bây giờ, tạo tệp /etc/bind/db.example.com và đưa các bản ghi DNS vào tệp này như ví dụ sau:

```
$TTL    604800
@       IN      SOA     ns.example.com. root.example.com. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
        IN      A       192.168.1.10
;
@       IN      NS      ns.example.com.
@       IN      A       192.168.1.10
@       IN      AAAA    ::1
ns      IN      A       192.168.1.10
printer IN A 192.168.1.11
hoapc IN A 192.168.1.12
ftp IN CNAME hoapc.example.com
```

Để cấu hình mới có tác dụng, hãy khởi động lại bind bằng cách chạy lệnh sau:

```
sudo systemctl restart bind9.service
```

Phân giải ngược

Để bắt đầu cấu hình phân giải ngược cho miền example.com, thêm zone ngược mới như sau vào tệp /etc/bind/named.conf.local:

```
zone "1.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.192";
};
```

Thay 1.168.192 bằng ba octet đầu của mạng (viết ngược). Đồng thời đặt tên tệp của zone là /etc/bind/db.192 với số là octet đầu của mạng.

Bây giờ tạo tệp /etc/bind/db.192 và đưa các bản ghi DNS vào tệp này như ví dụ sau:

```
$TTL    604800
@       IN      SOA     ns.example.com. root.example.com. (
                              2         ; Serial
                         604800         ; Refresh
```

```
                        86400       ; Retry
                       2419200       ; Expire
                        604800 )     ; Negative Cache TTL
;
@       IN      NS      ns.
10      IN      PTR     ns.example.com.
11      IN      PTR     printer.example.com.
12      IN      PTR     hoapc.example.com.
```

Mỗi bản ghi 'A' trong /etc/bind/db.example.com cần có một bản ghi 'PTR' trong /etc/bind/db.192.

Để cấu hình mới có tác dụng, hãy khởi động lại bind bằng cách chạy lệnh sau:

```
sudo systemctl restart bind9.service
```

3.2.3. Cấu hình nameserver thứ cấp

Secondary DNS Server nên được thiết lập để đảm bảo tính sẵn sàng của dịch vụ DNS. Để thiết lập DNS server thứ cấp, trước hết cần cấu hình DNS server chính để nó được phép chuyển zone. Thêm tùy chọn allow-transfer vào cả zone xuôi và zone ngược như sau:

```
zone "example.com" {
        type master;
          file "/etc/bind/db.example.com";
        allow-transfer { 192.168.1.13; };
};
zone "1.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.192";
          allow-transfer { 192.168.1.13; };
};
```

Trong ví dụ này, DNS server thứ cấp sẽ có địa chỉ IP là 192.168.1.13.

Khởi động lại DNS server chính để cấu hình mới có tác dụng.

Tiếp theo, trên DNS server thứ cấp, cài đặt BIND như bình thường, sau đó chỉnh sửa tệp /etc/bind/named.conf.local và thêm cả zone xuôi và zone ngược như sau:

```
zone "example.com" {
          type slave;
        file "db.example.com";
        masters { 192.168.1.10; };
};
```

```
zone "1.168.192.in-addr.arpa" {
        type slave;
    file "db.192";
    masters { 192.168.1.10; };
};
```

Lưu ý 192.168.1.10 là địa chỉ IP của nameserver chính.

Khởi động lại bind để cấu hình mới có tác dụng.

4. Thực hành

Cấu hình DNS phân giải tên miền "mydomain.com.vn", có các server sau:

- DNS Server: mydns.mydomain.com.vn; IP: 192.168.20.10/24
- Web Server: myweb.mydomain.com.vn; IP: 192.168.20.20/24
- Samba Server: samba.mydomain.com.vn; IP: 192.168.30.30/24