

## Nội dung

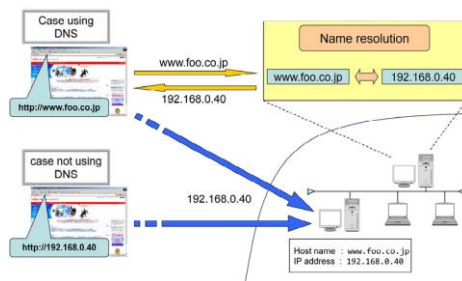
- Vai trò của DNS
- Hệ thống tên miền
- Các thành phần của hệ thống tên miền
- Cơ chế giải tên miền
- Các vấn đề về bảo mật
- Các loại server DNS
- Cài đặt và cấu hình DNS

## Dịch vụ tên miền

1

2

## Vai trò của DNS



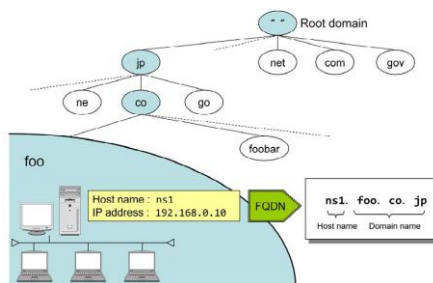
3

## Vai trò của DNS

- Phân giải tên miền thành IP
- Là dịch vụ cần thiết cho các dịch vụ mạng khác
- Có nhiều giải pháp
  - WINNS, NIS, DNS, host file
- Giải pháp tập trung
- Giải pháp phân tán
  - Chức năng, dữ liệu, quản lý

4

## Hệ thống các tên miền-cấu trúc



5

## Hệ thống tên miền-cấu trúc

- Gốc “.”
- Tên miền cấp 1
  - Chức năng (gTLD), quốc gia (ccTLD), tài trợ (sTLD)
- Tên miền cấp 2
  - Chức năng-quốc gia, tỉnh-quốc gia, khác
- FQDN-tên miền đầy đủ
  - www.hut.edu.vn.

6

## Hệ thống tên miền-quản lý

- ICANN (Internet Corporation for Assigned Numbers and Names)
- [Root Servers Systems Advisory Committee \(RSSAC\)](#)
- Ủy quyền cho
  - Các ủy ban của các nước (ccTLD)
  - Các nhà đăng ký (gTLD, sTLD)
  - Các nhà đăng ký phạm vi từng nước
- Ủy quyền hoàn toàn

7

## Các thành phần của hệ thống tên miền

- Root Server
- Top Lever Domain (TLD) server
- Các server khác
- DNS resolver
- Dữ liệu trên các server
  - Cấu hình của các server
  - Dữ liệu được phân bố trên server (zone file)
  - Dữ liệu bộ nhớ đệm

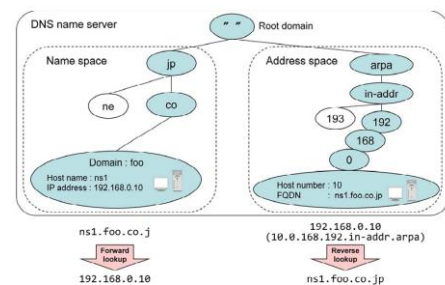
8

## Dữ liệu phân bố trên server

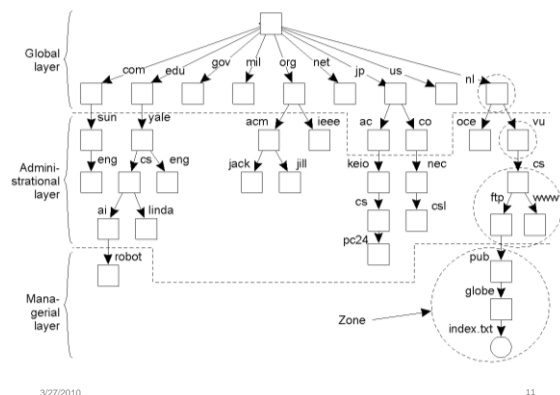
- Zone file: lưu trữ các thông tin về một zone
- Các bản ghi trong zone file
  - Thông tin chung về zone
  - Thông tin về các host trong zone (A, AAAA, CNAME)
  - Thông tin về các dịch vụ trong zone (MX, SRV, ....)
  - Thông tin về các subdomain trong zone (NS)

9

## Không gian tên và không gian địa chỉ



10



3/27/2010

11

## Quản lý không gian tên

Tính chất	Mức toàn cầu	Mức hành chính (administrational)	Mức vận hành (managerial)
Qui mô địa lý	Toàn cầu	Quốc gia/tổ chức lớn	Tổ chức nhỏ
Số lượng server tương tác	Một vài (16)	Nhiều	Lớn
Thời gian đáp ứng	Giây	10 <sup>-3</sup> giây	Ngay
Tốc độ cập nhật	Ít cập nhật	Liên tục	Liên tục
Số lượng sao lưu	Nhiều	Rất ít	Không có
Bộ nhớ đệm trên client	Có	Có	Có

12

11

## Cơ chế giải tên miền không đệ quy

- Client gửi yêu cầu dạng không đệ quy đến server
  - Server thỏa thuận với client có hỗ trợ hay không
- Nếu không
  - Nếu tồn tại host, gửi thông báo trả lời về cho client
  - Nếu không có trả lời là không có host nào như vậy
  - Nếu server đang bận báo lỗi
- Nếu có
  - Server tìm trong dữ liệu cục bộ (không thấy)
  - Server gửi cho client địa chỉ của các **root server**
  - Client tự hỏi** các root server về tên miền
  - Các root server trả lại địa chỉ của các DNS
  - Client tiếp tục hỏi các server khác

13

## Cơ chế giải tên miền đệ quy

- Server có thể hỏi các server khác
- Client gửi thông báo đệ quy đến server
  - Server thỏa thuận với client có hỗ trợ hay không
- Nếu không hỗ trợ:
  - Nếu tồn tại host, gửi thông báo trả lời về cho client
  - Nếu không có trả lời là không có host nào như vậy
  - Hoặc trả lời là host đang bận
- Nếu có hỗ trợ:
  - Server tìm trong dữ liệu cục bộ (không thấy)
  - Server gửi** cho các root server
  - Các root server gửi IP các NS TLD
  - Server hỏi các server khác về tên miền
  - Trả lời lại client

14

## Diễn giải ngược tên miền

- Gửi thông báo yêu cầu diễn giải ngược
  - Không có nhiều DNS server hỗ trợ
- Dùng zone ngược để lưu trữ các thông tin giải địa chỉ ngược
- 142.47.202.in-addr.arpa.zone
- Các bản ghi PTR

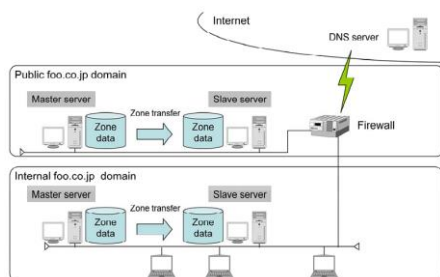
15

## Các loại server DNS

Master	Slave	Cache	Các thao tác giữa các server
<ul style="list-style-type: none"> <li>Quản lý các thông tin liên quan đến một hoặc nhiều tên miền</li> <li>Trả lời các yêu cầu liên quan đến tên miền</li> <li>Chuyển tiếp các yêu cầu nếu không có thông tin</li> <li>Các thông tin trả lời được lấy cục bộ từ server</li> <li>Các thông báo trả lời được đặt là Authoritative</li> </ul>	<ul style="list-style-type: none"> <li>Quản lý các thông tin về một miền đã được Master quản lý</li> <li>Nhận thông tin về miền thông qua thao tác chuyển miền</li> </ul>	<ul style="list-style-type: none"> <li>Không tham gia vào quá trình quản lý thông tin của domain</li> <li>Chỉ lưu trữ các thông tin bảng bộ nhớ đệm</li> </ul>	<ul style="list-style-type: none"> <li>Cập nhật đầy đủ zone</li> <li>Cập nhật tăng dần</li> <li>Thông báo về sự thay đổi</li> <li>Cập nhật động</li> </ul>

16

## Các loại server DNS



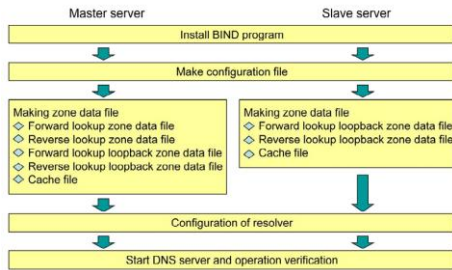
17

## Cài đặt DNS dưới linux

- Cấu hình mạng với IP cố định
- Cài đặt các gói
  - bind9
  - bind9utils
  - dnstools

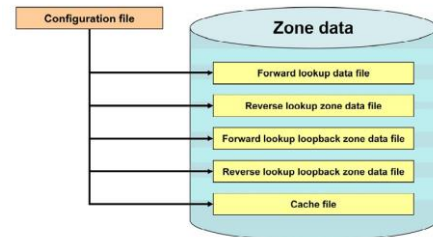
18

## Quy trình cài đặt



19

## Cấu hình bind



20

## Cấu hình bind daemon

```

/etc/named.conf file

options {
    directory "/etc/namedb";
};

zone "localhost" IN {
    type master;
    file "localhost.db";
};

zone "0.0.127.in-addr.arpa" IN {
    type master;
    file "localhost.rev";
};

zone "foo.co.jp" IN {
    type slave;
    file "foo.db:slave";
    masters {
        192.168.0.10 ;
    };
};

zone "0.168.192.in-addr.arpa" IN {
    type slave;
    file "foo.rev:slave";
    masters {
        192.168.0.10 ;
    };
};

zone "." IN {
    type hint;
    file "named.root";
};
  
```

21

## Forward lookup

```

/etc/namedb/foo.db' file

$TTL 86400
foo.co.jp. IN SOA ns1.foo.co.jp. root.foo.co.jp. (
    2004072201 ; serial
    10800 ; refresh
    3600 ; retry
    3600000 ; expiry
    86400 ) ; minimum

foo.co.jp. IN NS ns1.foo.co.jp.
foo.co.jp. IN NS ns2.foo.co.jp.

ns1.foo.co.jp. IN A 192.168.0.10
ns2.foo.co.jp. IN A 192.168.0.20
  
```

22

## Loopback zone file

```

$TTL 86400
localhost. IN SOA localhost. root.localhost. (
    2004072201 ; serial
    10800 ; refresh
    3600 ; retry
    3600000 ; expiry
    86400 ) ; minimum

localhost. IN NS localhost.
localhost. IN A 127.0.0.1
  
```

23

## Reverse lookup

```

/etc/namedb/foo.rev' file

$TTL 86400
0.168.192.in-addr.arpa. IN SOA ns1.foo.co.jp. root.foo.co.jp. (
    2004072201 ; serial
    10800 ; refresh
    3600 ; retry
    3600000 ; expiry
    86400 ) ; minimum

0.168.192.in-addr.arpa. IN NS ns1.foo.co.jp.
0.168.192.in-addr.arpa. IN NS ns2.foo.co.jp.

10.0.168.192.in-addr.arpa. IN PTR ns1.foo.co.jp.
20.0.168.192.in-addr.arpa. IN PTR ns2.foo.co.jp.
  
```

24

## Reverse lookup zone file

```

/etc/namedb/localhost.rev file

$TTL      86400
0.0.127.in-addr.arpa.  IN  SOA  localhost.  root.localhost. (
                        2004072201 ; serial
                        10800      ; refresh
                        3600       ; retry
                        3600000    ; expiry
                        86400     ; minimum
0.0.127.in-addr.arpa.  IN  NS   localhost.
1.0.0.127.in-addr.arpa. IN  PTR  localhost.

```

25

## Cache file

```

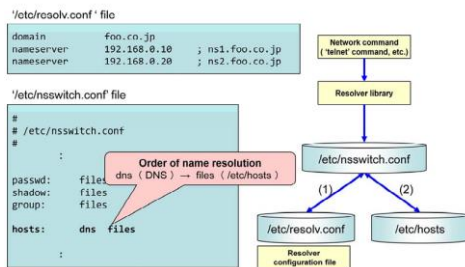
/etc/namedb/named.root file

;
;
; formerly NS.INTERNIC.NET
;
; A.ROOT-SERVERS.NET. 3600000 IN NS A.ROOT-SERVERS.NET.
; 198.41.0.4
;
; formerly NS1.ISI.EDU
;
; B.ROOT-SERVERS.NET. 3600000 IN NS B.ROOT-SERVERS.NET.
; 128.9.0.107
;
;
; operated by NIDE
;
; M.ROOT-SERVERS.NET. 3600000 IN NS M.ROOT-SERVERS.NET.
; 202.12.27.33
; End of File

```

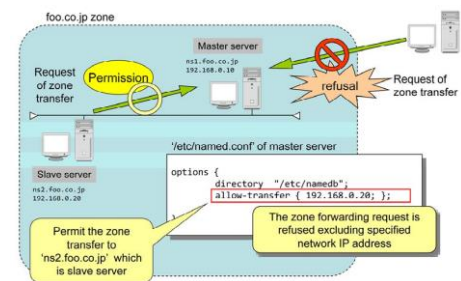
26

## resolver



27

## Hạn chế trao đổi zone

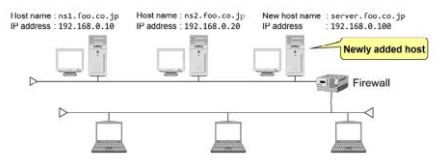


28

## Cập nhật thông tin trên DNS

Change procedure of zone data file when a host is added

- (1) Add 'A' record to the forward lookup zone data file and **update the serial number**
- (2) Add 'PTR' record addition to the reverse lookup zone data file and **update the serial number**
- (3) Restart the DNS server
- (4) Verify by the 'host' command, etc



29

## Bài tập

- Cài đặt bind9
- Xác định các tệp cấu hình
- Xác định các tệp dữ liệu cho localhost và cho hint
- Cấu hình master server quản lý domain với 12.hedspi
- Cấu hình các máy may1, may2, may3 trong domain nói trên ánh xạ sang địa chỉ IP của máy
- Cấu hình /etc/resolv.conf để sử dụng máy cục bộ như DNS server.
- Cấu hình server để sử dụng được Internet như bình thường.
- Dùng CNAME để cấu hình may2 may3

30