DNS/DNSSEC

3 August 2015

Whoami

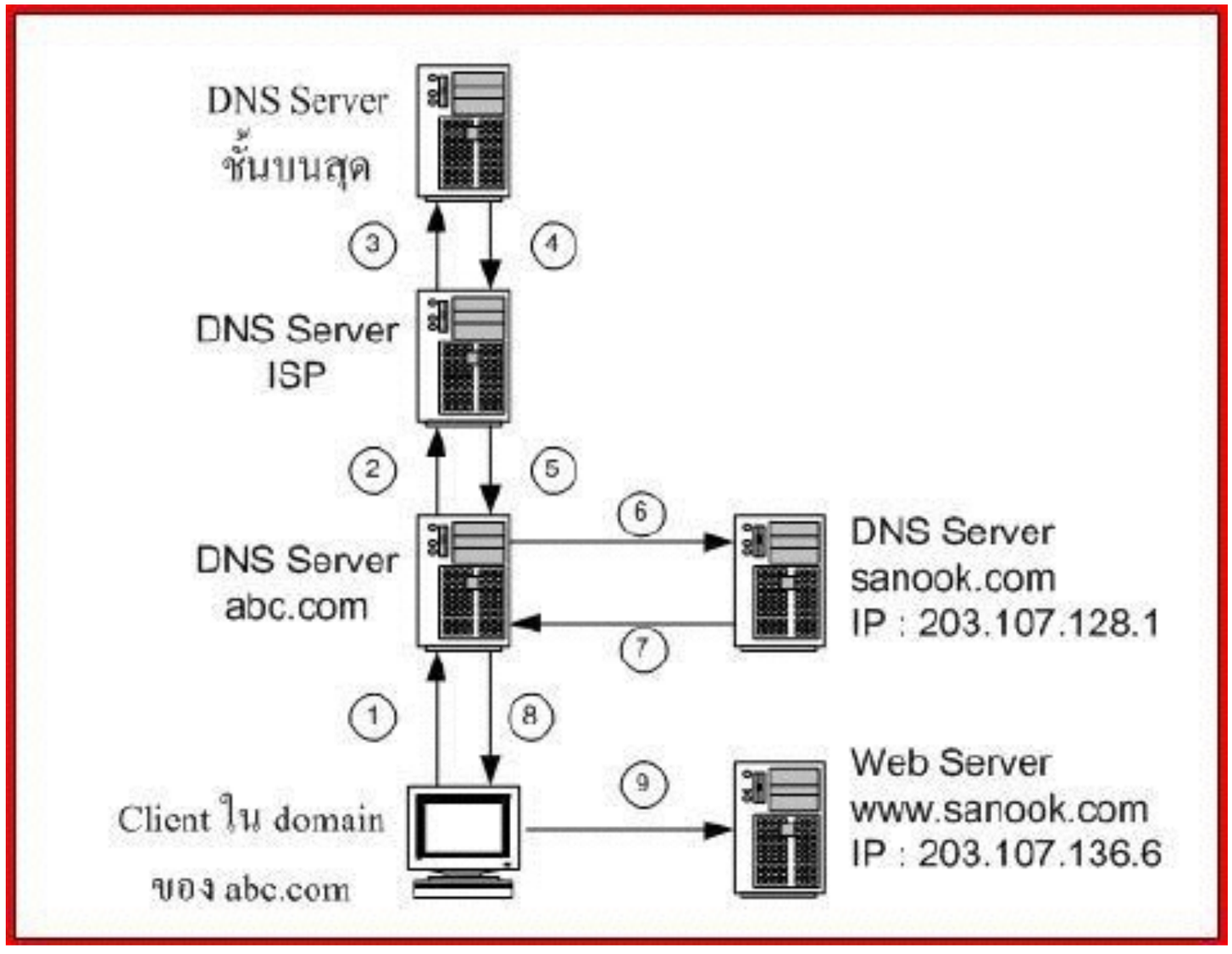
- ธงไชย จารุสุรุเกษม (เบิร์ด)
  - วิศวกรความมั่นคงปลอดภัยสารสนเทศ 2
  - Tongchai@ega.or.th
  - 02-612-6000 Ext. 4307

Agenda

- DNS Concepts
- BIND Installation & Configuration (Labs)
- Domains Configuration (Labs)
- Master(Primary) and Slave(Secondary) (Labs)

DNS Concepts

- DNS ย่อมาจาก Domain Name System
- ระบบจัดการแปลงชื่อไปเป็น IP Address โดยมีหลักการทำงาน ดังนี้



DNS Types

- DNS แบ่งออกได้เป็น 2 ประเภท ได้แก่
  - Master Name Server (Primary)
    - เป็นฐานข้อมูลหลักของโดเมน การเพิ่ม/แก้ไข/ลบ ข้อมูลทำที่ Master อย่างเดียว
  - Slave Name Server (Secondary)
    - ทำหน้าที่สำเนาข้อมูลมาจาก Master ตามเวลาที่กำหนดโดยอัตโนมัติ

ทั้ง 2 ประเภทข้างต้นในแต่ละประเภทก็จะแบ่งย่อยไปอีก 2 ประเภทคือ

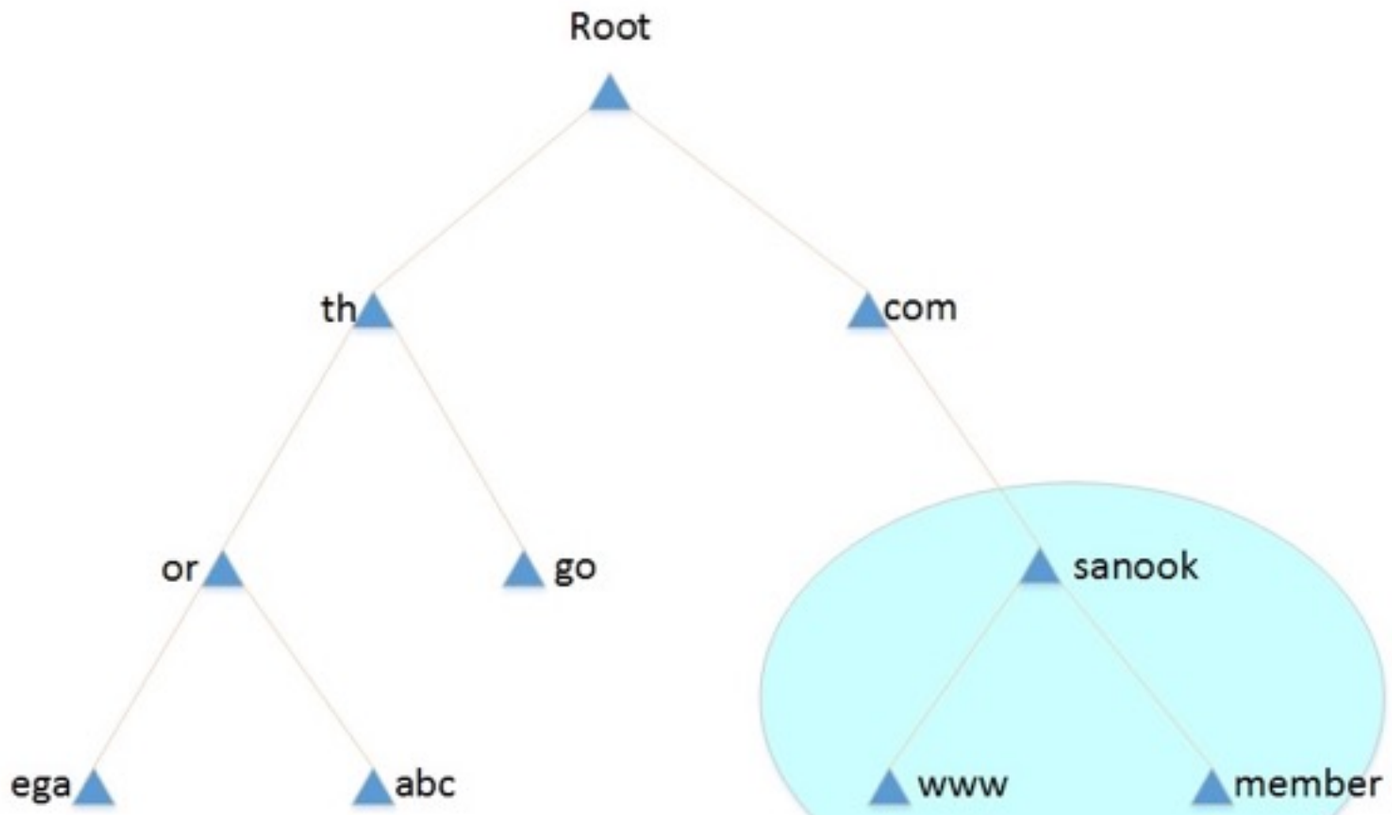
- Forward Lookup Zone
  - ทำหน้าที่แปลง Domain Name หรือ Host Name ให้เป็น IP Address
- Reverse Lookup Zone
  - ทำหน้าที่แปลงค่า IP Address ให้เป็น Host Name

Name Space

- Name Space - บน Internet จะมีการควบคุมการตั้งชื่อต่างๆ และ IP Address ซึ่งจะต้องมีชื่อที่ไม่ซ้ำกัน แบ่งออกเป็น 2 แบบ คือ
  - Flat Name Space - การตั้งชื่อ Name Space ไม่มีโครงสร้าง เช่น 123.testx, asdf.12
  - Hierarchical Name space - การตั้งชื่อ Name Space แบบมีโครงสร้างเป็นลำดับชั้น เช่น .th , .or.th , ega.or.th

Domain Name Space

- Domain Name Space - มีโครงสร้างแบบลำดับชั้น เป็น Tree โดยมี Root อยู่ด้านบนสุด
  - Label - ในแต่ละ node จะมี Label กำกับอยู่ และ label ของ root จะเป็น null string หรือ ไม่มีชื่อ โดย node ลูกที่แตกออกมาจาก node แม่จะต้องมี label ไม่ซ้ำกับ node แม่
  - Domain Name – เป็นลำดับของ label โดยใช้จุด (.) เป็นตัวแยก domain name และจะอ่านจากข้างล่างขึ้นด้านบนไปยัง root



DNS Server and Zone

- DNS Server - เครื่องคอมพิวเตอร์ หรือ โปรแกรมที่เก็บฐานข้อมูลเกี่ยวกับ Domain Name และ IP Address และ ให้บริการแปลง Domain Name ไปเป็น IP Address เมื่อมีการร้องขอ เพื่อใช้อ้างอิงถึงที่อยู่ของเครื่องคอมพิวเตอร์ที่มี IP Address ตรงกับ Domain ที่ร้องขอ

- Zone - หรือ Domain คือ สิ่งเดียวกัน โดย DNS Server จะสร้างฐานข้อมูลที่เรียกว่า Zone file เพื่อเก็บข้อมูลของทุกๆ node ภายใต้ domain นั้นๆ โดยที่
  - Primary Server - ทำหน้าที่เก็บ Zone file ปรับปรุง/แก้ไข/ดูแล Zone file นั้นๆ
  - Secondary Server – ทำหน้าที่ถ่ายโอนข้อมูลเกี่ยวกับ Zone file มาจาก DNS Server อื่นๆ (ได้ทั้ง Primary และ Secondary)

Zone file คือ file ที่ใช้เก็บข้อมูลเกี่ยวกับ Domain โดยจะมี Resource Record เป็นตัวบ่งบอกชนิดของ Record ที่บันทึกไว้ใน zone file ดังนี้

Resource Record (Zone File)

- A - Address record คือ record ที่ใช้สำหรับ map Host name เป็น IP Address

```
<host>   IN     A     <IP-address>
```

- AAAA - Address record คือ record ที่ใช้สำหรับ map Host name เป็น IPv6 Address

```
<host>     IN     AAAA     <IP-address-IPv6>
```

- CNAME - Canonical name record คือ record ที่ใช้ map ไปอีกชื่อ

```
<alias-name>     IN     CNAME <real-name>
```

- MX - Mail Exchange record คือ record ที่ใช้เกี่ยวกับระบบ email

```
IN     MX   <preference-value>   <email-server-name>
```

Resource Record (Zone File)

- NS - Name Server record คือ record ที่แจ้ง name server ที่เป็น Authorize server ของ domain นั้นๆ

```
IN    NS    <nameserver-name>
```

- PTR - Pointer record คือ record ที่ใช้สำหรับ map IP Address ไปเป็น Host name

```
<IP-address>  IN    PTR  <host-name>
```

Resource Record (Zone File)

- SOA - Start Of Authority resource record คือ record ที่เก็บรายละเอียดว่า DNS Server ตัวไหนทำหน้าที่เป็น Primary server ของโดเมนนั้นรวมทั้งกระบวนการเก็บความถี่ในการ update ข้อมูลของ Secondary server

```
@    IN    SOA    <primary-name-server>    <hostmaster-email> (
                  <serial-number>
                  <time-to-refresh>
                  <time-to-retry>
                  <time-to-expire>
                  <minimum-TTL> )
```

Forward Zone File (Example)

```
$TTL 86400
@       IN      SOA     dns1.example.com.     root.example.com. (
                        2015080301 ; serial
                        21600      ; refresh after 6 hours
                        3600       ; retry after 1 hour
                        604800     ; expire after 1 week
                        86400      ; minimum TTL of 1 day    )
        IN      NS      dns1.example.com.
        IN      NS      dns2.example.com.
        IN      MX      10      mail.example.com.
        IN      MX      20      mail2.example.com.
        IN      A       10.0.1.5
server1         IN      A       10.0.1.5
server2         IN      A       10.0.1.7
dns1    IN      A       10.0.1.2
dns2    IN      A       10.0.1.3
ftp     IN      CNAME   server1
mail    IN      CNAME   server1
mail2   IN      CNAME   server2
www     IN      CNAME   server2
```

Reverse Zone File (Example)

```
$TTL 86400
@       IN    SOA    dns1.example.com.     hostmaster.example.com. (
                2015080301   ; serial
                21600        ; refresh after 6 hours
                3600         ; retry after 1 hour
                604800       ; expire after 1 week
                86400        ; minimum TTL of 1 day )
        IN    NS     dns1.example.com.
        IN    NS     dns2.example.com.
20      IN    PTR    alice.example.com.
21      IN    PTR    betty.example.com.
22      IN    PTR    charlie.example.com.
23      IN    PTR    doug.example.com.
24      IN    PTR    ernest.example.com.
25      IN    PTR    fanny.example.com.
```

DNS Server Installation (BIND)

- ติดตั้ง BIND

  [root@master ~]# yum install bind bind-utils –y

- Config ให้ Service BIND run โดยอัตโนมัติ หากมีการ Restart Server

  [root@master ~]# chkconfig named on

- สั่งให้ Service BIND Start

  [root@master ~]# service named start

  Generating /etc/rndc.key: [OK]

  Starting named: [OK]

ตรวจสอบ service

- คำสั่งในการตรวจสอบว่า Service ทำงานอยู่หรือไม่

```
[root@master ~]# netstat -natup | grep named
tcp  0      0 127.0.0.1:53    0.0.0.0:*           LISTEN      1284/named
tcp  0      0 127.0.0.1:953   0.0.0.0:*           LISTEN      1284/named
tcp  0      0 ::1:53          :::*                LISTEN      1284/named
tcp  0      0 ::1:953         :::*                LISTEN      1284/named
udp 0       0 127.0.0.1:53    0.0.0.0:*                       1284/named
udp 0       0 ::1:53          :::*                            1284/named
```

Iptables Configuration

- เพิ่ม Policy firewall สำหรับให้ Service DNS

```
[root@master ~]# vi /etc/sysconfig/iptables
# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 53 -j ACCEPT
-A INPUT -m state --state NEW -m udp -p udp --dport 53 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

DNS Configuration

❖ แก้ไข Config โดยใช้ text editor ไปที่ /etc/named.conf

```
[root@master ~]# vi /etc/named.conf
options {
        listen-on port 53 { any; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { any; };
        recursion yes;
        ……
};
```

DNS Configuration

- BIND Configuration

```
options {
        .....
        dnssec-enable yes;
        dnssec-validation yes;
        dnssec-lookaside auto;

    /* Path to ISC DLV key */
        bindkeys-file "/etc/named.iscdlv.key";

        managed-keys-directory "/var/named/dynamic";
};
```

Domains Configuration (Create)

- แก้ไขที่ file config

```
[root@master ~]# vi /etc/named.conf
        .....
      zone "labs.test" IN {
                        type master;
                        file "labs.test.db";
                        allow-update { none; };
      };
      zone "250.168.192.in-addr.arpa" IN {
                        type master;
                        file "250.168.192.in-addr.arpa.db";
                        allow-update { none; };
      };
```

สร้าง Forward Zone File

❖สร้าง Zone file ใหม่โดยสร้างไว้ที่ folder /var/named/

[root@master ~]# vi /var/named/labs.test.db

```
$TTL 86400
@                   IN      SOA     ns.labs.test.      root.labs.test. (
                            2015080301     ; serial
                            21600                ; refresh after 6 hours
                            3600                 ; retry after 1 hour
                            604800               ; expire after 1 week
                            86400 )              ; minimum TTL of 1 day
                    IN      NS      ns.labs.test.
                    IN      MX      10      mail.labs.test.
                    IN      MX      20      mail2.labs.test.
                    IN      A       192.168.250.250
server1             IN      A       192.168.250.10
server2             IN      A       192.168.250.20
ns                  IN      A       192.168.250.250
ftp                 IN      CNAME   server1
mail                IN      CNAME   server1
mail2               IN      CNAME   server2
www                 IN      CNAME   server2
```

สร้าง Reverse Zone File

❖สร้าง Reverse Zone File

```
[root@master ~]# vi /var/named/250.168.192.in-addr.arpa.db
$TTL 86400
@       IN      SOA     ns.labs.test.   root.labs.test. (
                2015080301          ; serial
                21600               ; refresh after 6 hours
                3600                ; retry after 1 hour
                604800              ; expire after 1 week
                86400    )          ; minimum TTL of 1 day
        IN      NS      ns.labs.test.
10      IN      PTR     server1.labs.test.
20      IN      PTR     server2.labs.test.
```

Master Server Configuration

❖ Config เพิ่มเติมในส่วนของ Zone ที่อนุญาตให้สามารถ transfer zone file ไปยัง Slave ได้ (Config ที่ Master Server)

```
[root@master ~]# vi /etc/named.conf
zone "labs.test" IN {
        type master;
        file "labs.test.db";
        allow-update { none; };
        allow-transfer { 192.168.250.251; };
};
```

Slave Server Configuration

- Config ให้ Slave transfer zone จาก Master (Config ที่ Slave Server)

```
[root@master ~]# vi /etc/named.conf
        zone "labs.test" IN {
                type slave;
                masters { 192.168.250.250; };
                file "labs.test.db";
                allow-update{ none; };
};
```

Q & A