Bind DNS 雲端同步設定

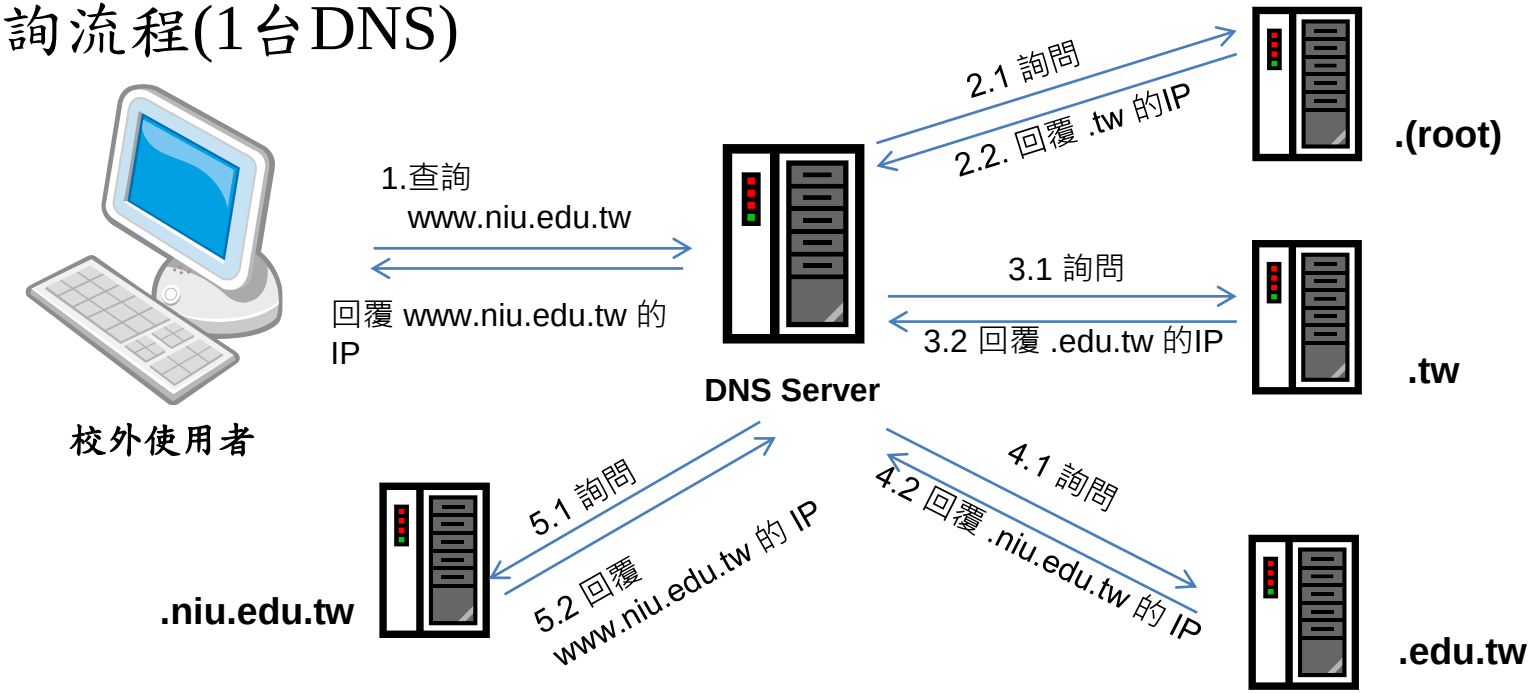
宜蘭區網中心　施衣喬

11/21/2014

目標

- 提供學校的DNS外部查詢主機
  - 學校端的學術網路因故斷線
  - 學校DNS無法提供服務
  - 減少校內DNS被攻擊的情形 (DNS 放大(反射)攻擊)
  - 降低學校DNS流量
- Master & Slave DNS 同步資料
  - Linux & Windows

- 查詢流程(1台DNS)


校外使用者
1.查詢
www.niu.edu.tw
回覆 www.niu.edu.tw 的IP
DNS Server
2.1 詢問
2.2. 回覆 .tw 的IP
.(root)
3.1 詢問
3.2 回覆 .edu.tw 的IP
.tw
4.1 詢問
4.2 回覆 .niu.edu.tw 的 IP
.edu.tw
5.1 詢問
5.2 回覆
www.niu.edu.tw 的 IP
.niu.edu.tw

查詢流程(多台DNS)

校外使用者

1.查詢 www.niu.ilc.edu.tw

回覆 www.niu.edu.tw 的 IP

DNS Server

round robin

2.1 詢問

2.2. 回覆 .tw 的IP

.(root)

3.1 詢問

3.2 回覆 .edu.tw 的IP

.tw

4.1 詢問

4.2 回覆 .niu.edu.tw 的 IP

.edu.tw

5.2 回覆 IP

5.1 詢問

.niu.edu.tw

5.2 回覆 IP

5.1 詢問

.niu.edu.tw

5.2 回覆IP

5.1 詢問

.niu.edu.tw

```
nameserver = ns2.niu.edu.tw
nameserver = niudns.niu.edu.tw
nameserver = ns1.niu.edu.tw
```

Bind基本架構

3大常用設定

named.conf

- 路徑
  /etc/named.conf
- Options
- Logging
- zone

Logging Files

- 路徑
  /var/named/chroot/var/log
- default
- security
- query

Zone Files

- 路徑
  /var/named/chroot/var/named
- 正解檔案
- 反解檔案

named.conf 設定

- /etc/named.conf
  - Bind 的主要設定檔，可從此檔案得知Bind其它相關設定
- options
  - Bind的基本設定
- logging
  - 設定Bind要記錄的資訊、內容及檔案位置
- zone
  - 設定網域正反解的檔案名稱

named.conf 設定

- **options**
  - **allow-query { any;}; (學校DNS可設定為校內 IP)**
    - 任何使用者都可以透過此DNS伺服器查詢 IP
  - **recursion no; (學校DNS需設定為Yes)**
    - 是否可代為查詢非本機擁有的Domain name
  - **allow-transfer { 163.28.192.15; 163.28.192.16; } ; (需在Master DNS設定)**
    - 只有這些 IP 可以跟本機取得最新設定檔
  - **also-notify { 163.28.192.15; 163.28.192.16;}; (需在Master DNS設定)**
    - 是否通知其它DNS伺服器，有更新zone的資料
  - **version**
    - 自行設定DNS版本的資訊，避免顯示太多資訊

named.conf 設定(Logging)

- logging
  {
    channel default-log {
      file “/var/log/default.log” versions 10 size 200m;
      (在/var/named/chroot/var/log/目錄下，最多保留10個檔案，每個檔案最多200M)
      severity info;
      print-time yes;}; (在Log中顯示查詢的時間)
      category default { default-log;};
  };
- 常用種類
  - default：記錄BIND啟動及 zone transfer 的狀態
  - security：記錄被拒絕存取的IP及Domain nam
  - query：記錄 client 透過此 DNS 查詢 IP 的所有紀錄

named.conf 設定(Zone)

- **Master Bind Zone (學校)**

```
zone “niu.edu.tw” in {
        type master;
        file “niu.hosts”;
        };
```

- 這個zone是主要的DNS主機
- 檔案名稱設定為 niu.hosts

- **Slave Bind Zone(區網)**

```
zone “niu.edu.tw” in {
        type slave;
        file “niu.hosts”;
        masters {120.101.0.1;};
        };
```

- 這個zone是次要的DNS主機
- 到120.101.0.1取得檔案內容
- 將取得的檔案寫入niu.hosts中

zone基本設定

- 正解

```
$ORIGIN .
niu.edu.tw          IN SOA      mrtg.niu.du.tw. root.niu.edu.tw. (
                    201411051  ; serial    (序號：Slave判斷是否需更新檔案)
                    1H         ; refresh (1 小時)  (Slave自動來取得檔案的時間)
                    30M        ; retry (30分) (若refresh失敗，再度取得檔案的時間)
                    2W         ; expire (2 weeks) (若refresh失敗，保留該網域的時間)
                    1D         ; minimum (1 天) (別台DNS 伺服器保留cache的時間)
                    )
                    NS          ns1.niu.edu.tw.
                    NS          ns2.niu.edu.tw.

$ORIGIN niu.edu.tw.
ns1                 A           120.101.0.1
ns2                 A           120.101.0.2
abc                 A           120.101.0.3
```

zone基本設定

- 反解

```
$ORIGIN .
101.120.in-addr.arpa        IN SOA      mrtg.niu.du.tw. root.niu.edu.tw. (
                            201411051  ; serial
                            3600       ; refresh (1 hour)
                            3600       ; retry (1 hour)
                            1209600    ; expire (2 weeks)
                            3600       ; minimum (1 hour)
                            )
                            NS          ns1.niu.edu.tw.
                            NS          ns2.niu.edu.tw.

$ORIGIN 0.101.120.in-addr.arpa.
1                           A           ns1.niu.edu.tw.
2                           A           ns2.niu.edu.tw.
3                           A           abc.niu.edu.tw.
```

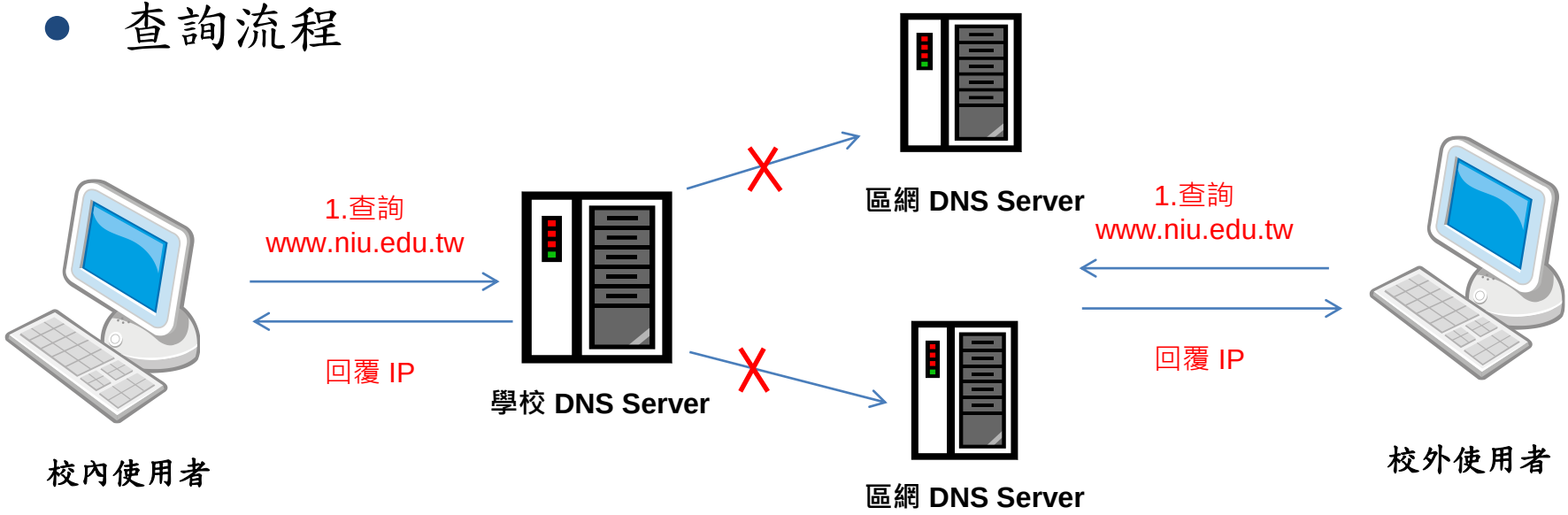
修改DNS記錄流程

1. 填寫區網雲端DNS服務申請表
   http://goo.gl/u1Ep0j
2. 設定學校 DNS 主機（包含named.conf、正反解檔的NS Record）
3. 確認可透過 163.28.192.15及163.28.192.16查詢學校的domain name
4. 與DNS上層單位聯繫，修改NS記錄
   正解 => 宜蘭縣網或教育部
   反解 => 教育部

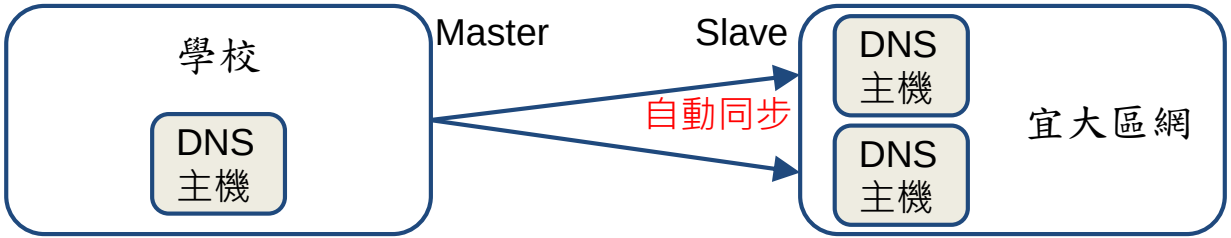
區網DNS主機

- 宜大區網DNS
  - 提供2台DNS主機，每台規格如下
    - 4個CPU
    - 2G RAM
    - 100G HD
  - 作業系統：CentOS 6.6
  - DNS版本：Bind 9

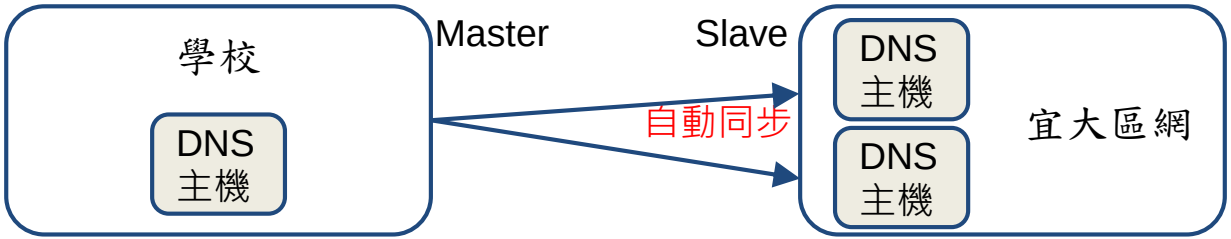
- 查詢流程


1.查詢
www.niu.edu.tw
回覆 IP
學校 DNS Server
區網 DNS Server
區網 DNS Server
1.查詢
www.niu.edu.tw
回覆 IP
校內使用者
校外使用者

- Linux 環境



- Windows環境

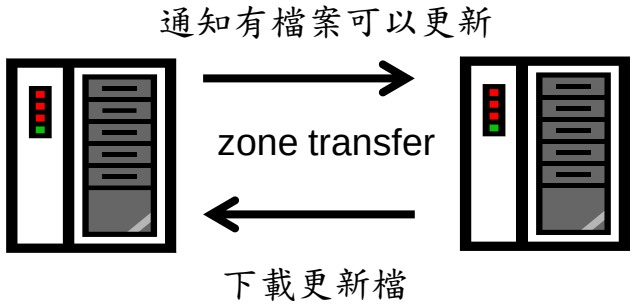


同步架構

Master DNS
（學校）

Slaver DNS
(區網)

1. 新增1筆 正/反解記錄
2. 修改 Serial 序號
3. Restart / reload DNS服務



1. 檢查 zone 的序號
2. 若版本序號較大，更新Zone檔
3. 到達Retry時間，自動檢查是否有新Zone檔

Bind同步設定

學校DNS伺服器

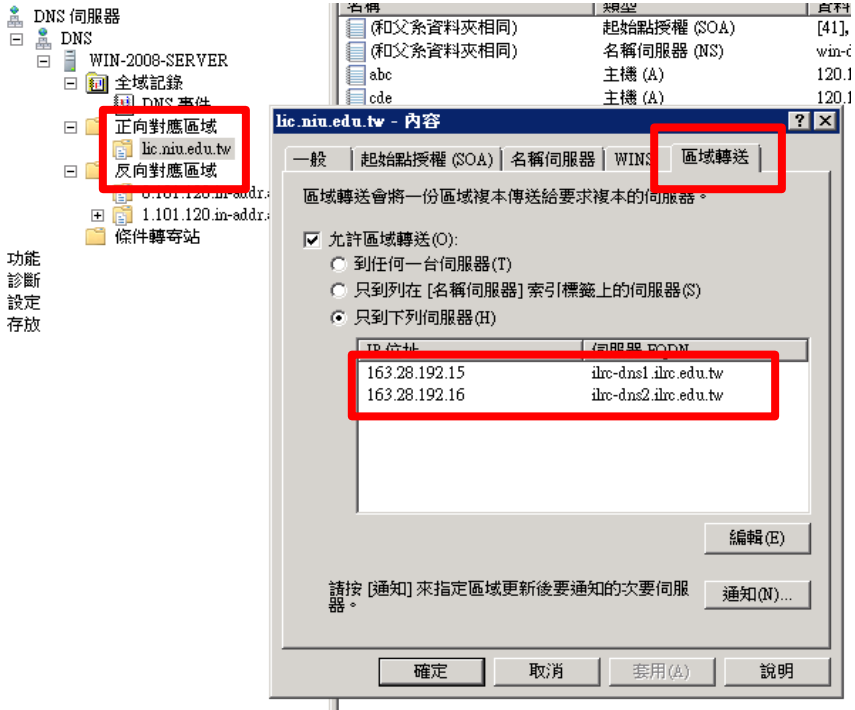
```
options {
   directory      "/var/named";
   allow-query      { 校內IP; };
   allow-recursion { 校內IP; };
   also-notify      { 163.28.192.15;
                      163.28.192.16; };
   allow-transfer   { 163.28.192.15; ;
                      163.28.192.16; };
};
zone "test.niu.edu.tw" {
      type master;
      file "host.test";
};
```

區網DNS伺服器

```
options {
   directory      "/var/named";
   allow-query      { any; };
   allow-recursion { none; };
   allow-transfer    { none; };
};

zone "test.niu.edu.tw" {
      type slave;
      file "host.test";
      master “學校DNS IP” ;
};
```

Windows同步設定

學校DNS伺服器



區網DNS伺服器

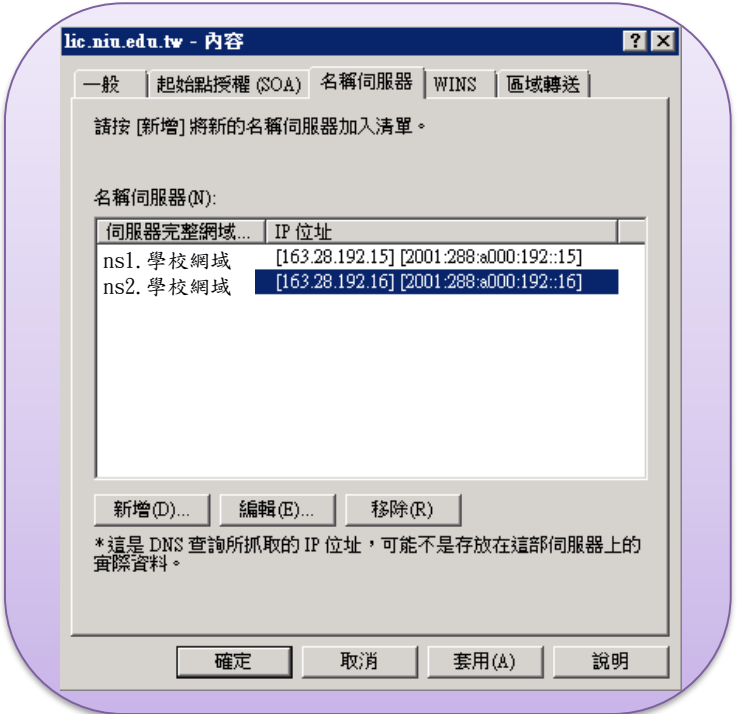
```
options {
    directory      "/var/named";
    allow-query      { any; };
    allow-recursion { none; };
    allow-transfer    { none; };
};

zone "test.niu.edu.tw" {
        type slave;
        file "host.test";
        master “學校DNS IP” ;
};
```

學校zone 設定

Bind

```
$ORIGIN .
$TTL 600        ; 10 minutes
niu.edu.tw      …… (
                201411051  ; serial
                    .
                    .
                )
                NS   ns1.學校網域
                NS   ns2.學校網域
$ORIGIN niu.edu.tw.
ns1             A       163.28.192.15
                AAAA  2001:288:a000:192::15
ns2             A       163.28.192.15
                AAAA  2001:288:a000:192::15
```

Windows



相關指令

- nslookup

  server 163.28.192.15 **(切換DNS伺服器)**

  www.lic.niu.edu.tw **(查詢IP)**

  ls -d lic.niu.edu.tw **(列出該網域下所有的DNS紀錄)**

- dig

  dig www.lic.niu.edu.tw @163.28.192.15 **(透過特定DNS伺服器查詢IP)**

  dig www.niu.edu.tw @168.95.1.1 +trace **(追蹤DNS查詢所經過的DNS伺服器)**

  dig chaos txt version.bind @ns1.niu.edu.tw **(查詢DNS的版本)**