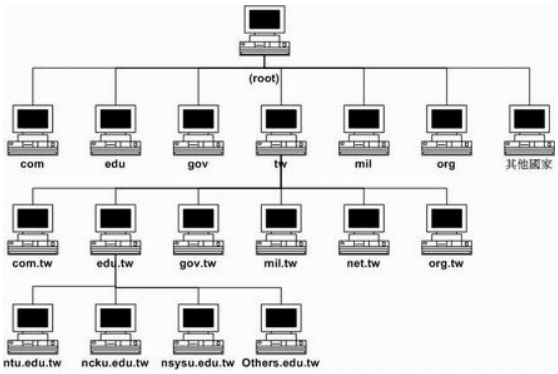
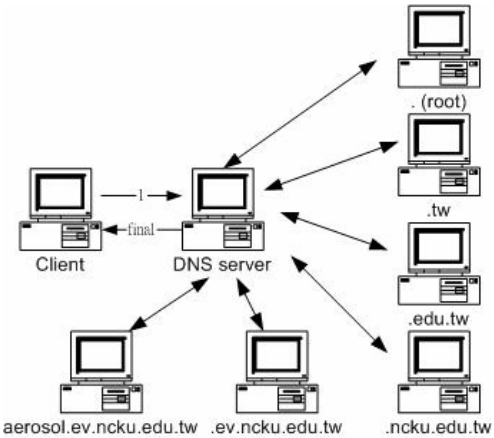
Unit 4　　DNS 系統(Organizing Networked Systems)

2008/01/09 建立 by VBird

1. 課前重點分析：
   a. TCP/IP 在 Internet 上面應用的困擾：妳必須要『背誦』 32bits 的 IP 嗎？
   b. 主機名稱的應用：透過主機名稱來取代 IP 的背誦，比較好記憶的方法：
      A. /etc/hosts　　：早期的作法，麻煩的是，每增加一部 Internet 主機，該檔案必須同步更新
      B. DNS system　　：由加州柏克萊大學開發，具有分散式資料庫的功能，管理簡單方便！
   c. DNS 的功能：
      A. 正解：由主機名稱找到 IP　　(最常使用的功能)
      B. 反解：由 IP 找到主機名稱　　(目前由於 spam 郵件的關係，越來越重要)
   d. DNS 的架構：



      A. 最頂層爲 root(.)，全球約有 13 部主機負責管理，底下僅記錄 TLD(Top Level Domain)
         1. 一般最上層領域名稱 (Generic TLDs)：例如 .com, .org, .gov 等等；
         2. 國碼最上層領域名稱 (Country code TLDs)：例如 .tw, .uk, .jp 等
   e. 主機名稱的分辨：FQDN (Fully Qualified Domain Name)
      A. 領域名稱(domain name)：每個資料庫所管理的名稱
      B. 主機名稱(Host name)　：在該資料庫中所記錄的名稱
   f. DNS 領域的查詢流程：(請在右側寫下查詢的程序喔！)



   g. 一部『合法』的 DNS 主機，重點在於『授權』！所謂的『授權』是上層 DNS server 將『該下游資料庫的查詢權交代給下層』的動作，並且從此後不再管理該下游資料庫的維護！
   h. 資料庫所記錄的內容方面，主要記錄的資源爲 Resource Record (RR)，分別有：
      A. domain (ttl) IN type rdata
         1. NS　　：該資料庫需要向哪一部主機查詢的標誌
         2. SOA　　：master/slave DNS 主機之間，作爲資料庫交換的重要參數
         3. A　　：找 IP
         4. PRT　　：pointer 的縮寫，由 IP 找主機名稱
         5. MX　　：與 Male eXchange 有關，
         6. CNAME　　：別名，可以指向某一部主機名稱，避免修改過多的 IP 資源。

2. 主機名稱解析器的相關設定資源：

   a. 主要提供主機名稱解析的服務有：

      A. file　　/etc/hosts
      B. DNS　　/etc/resolv.conf
      C. NIS　　透過 NIS 服務來處理 (setup 看一下！)

   b. 主機名稱解析重要的設定檔：　　/etc/nsswitch.conf 裡面的 hosts: 設定資源！

   c. 用戶端(client)常用的解析指令：

      A. host [-a] hostname　：僅會針對/etc/resolv.conf 的設定來處理名稱解析，不會讀取/etc/nsswitch.conf
      B. dig [-t type] hostname：同 host 的相關功能，不過輸出的資訊要詳細很多！非常重要！
      C. nslookup hostname　：會越來越少使用！

   d. 練習：利用『 dig +trace redhat.com 』來查詢整體的 DNS 搜尋流程！並對照前一頁的查詢流程！

      A. 仔細分析每個查詢流程
      B. 由每個流程的 domain ttl IN type rdata 講解 page 110 內的各項 RR 資源喔！

3. 用戶端利用 dig 進行正解(forward lookups)與反解(reverse lookups)的方式：(page 111-page 117)

   a. dig redhat.com　　：察看一下四個 section 的內容分別在講 question, answer, authority, additional
   b. dig -x 209.132.177.50：重點在看 domain name 卻是『 in-addr.arpa. 』！非常重要！
   c. dig -t mx redhat.com：具有 mail gateway 的功能！對 mail server 有用！
   d. dig -t soa redhat.com：有五個數字，與 Master/Slave DNS server 有關，參考 115 頁的詳細說明

4. Linux 上面的 DNS 伺服器軟體相關資訊：

   a. Package　：bind, bind-utils, bind-chroot, caching-nameserver
   b. daemon　：/usr/sbin/named, /usr/sbin/rndc
   c. Port　：port 53, port 953
   d. configure　：/var/named/chroot/目錄爲其根目錄，底下的/etc/named.conf, /var/named/*..
      請注意， why chroot？

5. 與 SELinux 有關的議題：

   a. 所有的設定檔都在 /var/named/chroot 內，因此有更動過該檔案後，確認 rwx 後，可進行：
      A. restorecon -R /var/named/chroot
   b. 可利用『getsebool -a | grep named』找出相關的 SELinux 之規則設定！
   c. 可利用類似『setsebool -P named_write_master_zones on』來將設定值寫入
      A. /etc/selinux/targeted/modules/active/booleans.local

6. 與 DNS 設定檔有關的議題：

   a. 是否需要 chroot 與 bind-chroot 套件有關，其設定檔主要在/etc/sysconfig/named 當中，請查閱！

      A. ROOTDIR=/var/named/chroot (每一家 distributions 可能都不相同)

      B. 可以使用 ps -ef | grep named 來察看是否有啓動 chroot 喔！ (named -t /var/named/chroot)

   b. 如果使用 DHCP 取得 IP 時，可能需要指定讓 DHCP 不要更動/etc/resolv.conf，可指定：

      A. PEERDNS=no (在 ifcfg-eth* 當中！)

   c. 所有的 zone file 設定檔其實是在 caching-nameserver 套件所提供的！所以請務必安裝！

7. 與 /etc/named.conf 有關的設定資料：主要在設定整個大環境，以及 zone (domain) 的指定！

```
acl "mynetwork"  { 192.168.5.0/24; };
options {
        directory  "/var/named" ;
        allow-query { any; };
        allow-transfer { mynetwork; };
        forwarders { 168.95.1.1; };
};
zone "." IN {
        type hint;
        file "named.ca";
};
```

1. 注意每一行的後面都有分號
2. 設定值也需要分號
3. acl 可以用來指定範圍
4. 某些沒有指定的項目使用預設值

8. 指定一個正反解的範例：

   a. 正解：stationXX.lccnet 爲你的 zone，且爲 master 類型

   b. 反解：192.168.5.0/24 爲你的 zone ，且爲 slave 類型，主要來自 192.168.5.100 那部主機

9. 正解的設定檔

```
$TTL    600
@               IN      SOA     @       root (
                        42              ; serial (d. adams)
                        3H              ; refresh
                        15M             ; retry
                        1W              ; expiry
                        1D )            ; minimum
                IN      NS      @
                IN      A       192.168.5.XX
www             IN      A       192.168.5.XX
ftp             IN      CNAME   www.stationXX.lccnet.     // ←注意到最後面那個 . 喔！
```

10. 反解的設定檔：

```
$TTL    86400
@       IN      SOA     stationXX.lccnet. root.stationXX.lccnet.  (
                            1997022700 ; Serial
                            28800      ; Refresh
                            14400      ; Retry
                            3600000    ; Expire
                            86400 )    ; Minimum
@       IN      NS      stationXX.lccnet.
200     IN      PTR     stationXX.lccnet.       //←務必使用 FQDN 喔！
```

11. 啓動與測試：

   a. 先測試語法有沒有錯誤　　：/etc/init.d/named configtest

      A. named-checkconf -t /var/named/chroot
      B. named-checkzone stationXX.lccnet /var/named/chroot/var/named/正確的檔名

   b. 啓動看看能否執行　　：/etc/init.d/named start

   c. 查閱一下登錄檔內是否 OK　：tail -n 30 /var/log/messages

12. 練習：利用剛剛上課的資料新增一些額外的 zone 與防火牆的機制來處理：

   a. 如何確認你有沒有啓動 chroot 呢？_____

   b. 確認防火牆有打開 port 53 讓人家可以來查詢：_____

   c. 如何讓你的 /etc/resolv.conf 不會被 DHCP 所修改：_____

   d. 檢查有沒有 . 這個 zone file 的存在？_____

   e. 增加一個名爲 nodeXX.test 的正解 zone ，對應到你的 IP，則 /etc/named.conf 該如何設定？_____

      _____

   f. 假設我需要 MX 標誌，那麼那個 zone file 的內容應該如何撰寫？

   g. 檢查一下，上述新增的檔案之 SELinux 是否正確？_____

   h. 檢查一下妳設定檔的語法正確否？_____

   i. 啓動並觀察登錄檔內的資訊是否正確無誤？_____

   j. 該如何測試你的設定是否正確(利用 dig)_____

   k. 如何讓你的 DNS 每次開機都啓動？_____