

壹、DNS 概念：

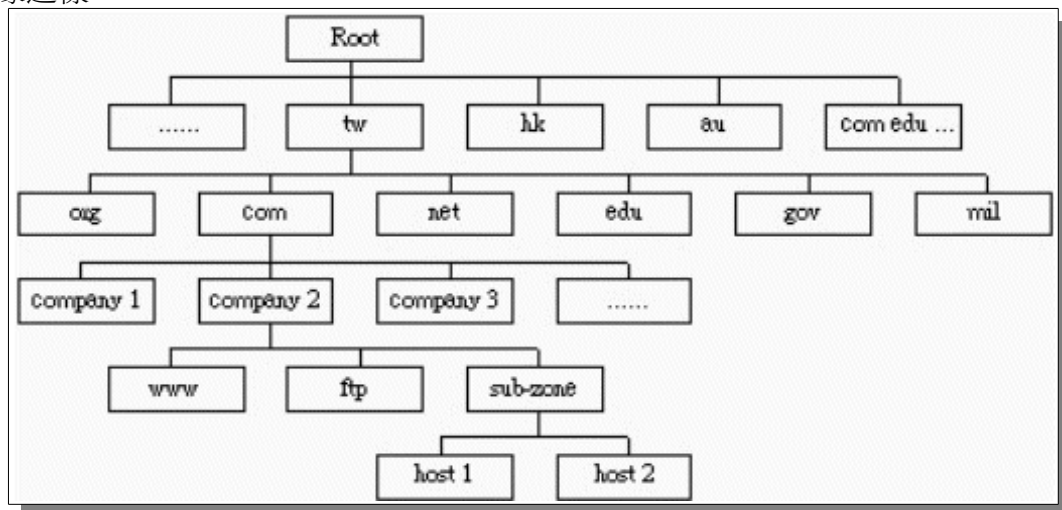
DNS 的結構

DNS 是一個分層級的分散式名稱對應系統，有點像電腦的目錄樹結構：在最頂端的是一個“root”，然後其下分為好幾個基本類別名稱，如：com、org、edu 等；再下面是組織名稱，如：sony、toshiba、intel 等；繼而是主機名稱，如：www、mail、ftp 等。因為當初 internet 是從美國發起的，所以當時並沒有國域名稱，但隨著後來 internet 的蓬勃發展，DNS 也加進了諸如 tw、hk、au 等國域名稱。所以一個完整的 dns 名稱就好像是這樣的：www.xyz.com.tw，而整個名稱對應的就是一個 IP 地址了。

在開始的時候，root 下面只有六個組織類別：

edu 教育、學術單位
org 組織、機構
net 網路、通訊單位
com 公司、企業
gov 政府機關
mil 軍事單位

不過，自從組織類別名稱開放以後，各種各樣五花八門的名稱也相繼涌現出來了，但無論如何，取名的規則最好盡量適合網站性質。除了原來的類別資料由美國本土的 NIC(Network Information Center)管理之外，其它在國域以下的類別分別由該國的 NIC 管理。這樣的結構看起來就像這樣



DNS 的運作

在我們設定 IP 網路環境的時候，通常都要告訴每台主機關於 DNS 伺服器的地址，下面讓我們看看 DNS 是怎樣運作的：

1. 當被詢問到有關本域名之內的主機名稱的時候，DNS 伺服器會直接做出回答；
2. 如果所查詢的主機名稱屬於其它域名的話，會檢查記憶體，看看有沒有相關資料；

3. 如果沒有發現，則會轉向 root 伺服器查詢；
4. 然後 root 伺服器會將該域名之授權(authoritative)伺服器(可能會超過一台)的地址告知；
5. 本地伺服器然後會向其中的一台伺服器查詢，並將這些伺服器名單存到記憶體中，以備將來之需(省卻再向 root 查詢的步驟)；
6. 遠方伺服器回應查詢；
7. 將查詢結果回應給客戶，並同時將結果儲存一個備份在自己的快取記憶體裡面；
8. 如果在存放時間尚未過時之前再接到相同的查詢，則以存放於快取記憶體裡面的資料來做回應。

從這個過程我們可以看出，沒有任何一台 DNS 主機會包含所有域名的 DNS 資料，資料都是分散在全部的 DNS 伺服器中，而 NIC 只需知道各 DNS 伺服器地址就可以了。

分擔 DNS 工作

Primary(master) DNS 伺服器是架設在某一個網域下被主要授權並控制所有名稱記錄的主控制伺服器，管轄著所有該網域的記錄資料，這些記錄資料只有 primary(master)可以修改。

但如果一個比較大型的網路中，DNS 伺服器就會變得很繁忙了，所以您可以設定多個 DNS 來分擔 master 的工作，但您或許不願意到每一個 DNS 伺服器去更新資料吧？而且就算您願意這樣做，也容易出現錯誤或資料不同步的情形。這樣您可以設定其它的伺服器為 secondary (slave) DNS 來複製 master 上面的記錄資料，這樣，其它的電腦可以被指定到不同的 DNS 做查詢，既可以分擔 master 的工作，而且資料也可以自動進行同步工作。您可以設定 DNS 資料同步的時間間隔，在 dns 檔案中的 Refresh 設定就是了。同時您還會看到 Serial，當 slave 的上面的 serial 數字少於它，資料就會被複製，否則會被忽略。

若您沒有被授權或指定管理某個 domain 的 DNS，但您所管理的電腦數實在太多，您可在您管理的區域內，架一個 Cache name server，以減輕對外網路的負擔。

驗證 DNS 工作

當您建立好一個 DNS 伺服器之後，除了可以直接使用命令 ping (這個會在後面章節說明)直接 ping 一下上面的記錄之外，最好還是使用 “nslookup”這個命令進行檢測或除錯，(Windows9x 系統並不包含此命令)。

貳、DNS Server 的相關套件及檔案：

在 Linux 上面，執行 DNS 程式是叫 BIND，但我們一般稱它的服務程式為：named。

您可到 <http://www.isc.org/> 尋找最新版 BIND Version 9.10.1-P1，目前在 CentOS6 上的最新版本為 9.8.2-0.30.rc1。

CentOS 6 套件上的相關檔案：

bind-9.8.2-0.30.rc1.el6.x86_64.rpm
bind-chroot-9.8.2-0.30.rc1.el6.x86_64.rpm
bind-devel-9.8.2-0.30.rc1.el6.i686.rpm
bind-devel-9.8.2-0.30.rc1.el6.x86_64.rpm
bind-dyndb-ldap-2.3-5.el6.x86_64.rpm
bind-libs-9.8.2-0.30.rc1.el6.i686.rpm
bind-libs-9.8.2-0.30.rc1.el6.x86_64.rpm
bind-sdb-9.8.2-0.30.rc1.el6.x86_64.rpm
bind-utils-9.8.2-0.30.rc1.el6.x86_64.rpm

您可由 CentOS 6 安裝光碟及到

<ftp://ftp.kh.edu.tw/pub/Linux/Caosity/centos/6/os/i386/CentOS/>

ftp://ftp.kh.edu.tw/pub/Linux/Caosity/centos/6/os/x86_64/CentOS/

中取得最新檔。

Bind 相關的設定檔：

1.一般執行模式：(安全性較差，Redhat 9.x 之前版本適用)

/etc/named.conf.....主設定檔
/var/named/named.ca..... root zone 資料表
/var/named/localhost.zone.....localhost 正解資料表
/var/named/named.local.....localhost 反解資料表
/var/named/named.[domain].....domain 正解資料表
/var/named/named.[Network No.]....domain 反解資料表

2.chroot 執行模式：(安全性較佳，Fedora Core 1 以後版本建議使用)

/var/named/chroot/etc/named.conf.....主設定檔
/var/named/chroot/var/named/named.ca..... root zone 資料表
/var/named/chroot/var/named/localhost.zone.....localhost 正解資料表
/var/named/chroot/var/named/named.local.....localhost 反解資料表
/var/named/chroot/var/named/named.[domain].....domain 正解資料表
/var/named/chroot/var/named/named.[Network No.]....domain 反解資料表

bind 常用命令：

/etc/rc.d/init.d/named {start|stop|status|restart|condrestart|reload|probe}
service named {start|stop|status|restart|condrestart|reload|probe}
/usr/sbin/named-checkconf
/usr/sbin/named-checkzone
/usr/sbin/rndc
/usr/bin/dig

/usr/bin/host
/usr/bin/nslookup
/usr/bin/nsupdate

參、DNS Server 的安裝

有關 bind9.8 系列之設定手冊在 <http://www.isc.org/downloads/bind/doc/bind-9-8/>

可取得英文之電子文件檔案，可提供您進一步的詳細資料。

為了系統安全考量，以下安裝之舉例，均以 chroot 執行模式為主，不以 chroot 執行模式進行者，請自行變換相對之目錄。

1. 檢查 bind 是否安裝至系統中：

```
rpm -qa | grep bind
rpm -qa | grep caching-nameserver
```

2. 安裝 bind 相關套件：(以 CentOS 6 為例)

```
yum install bind bind-chroot bind-libs bind-utils
```

3. 升級 bind 相關套件：(以 CentOS 6 為例)

```
yum update bind bind-chroot bind-libs bind-utils
```

4. 檢查設定檔是否有更新，若有更新，請刪除原設定檔，並將.rpmnew 的設定檔，改回原檔名(以/etc/sysconfig/named 為例)：

```
# ls -al /etc/sysconfig/named.rpmnew
若有該檔名則
# rm -f named ; mv named.rpmnew named
```

5. 檢查系統預定 bind 的執行方式：

在這裡我們比較建議安全性較高的 chroot 執行模式！

請檢查/etc/sysconfig/named 的內容是否有

```
ROOTDIR=/var/named/chroot
```

若無上述之描述，請在最後一行加上該描述！

6. 預設安裝的設備定檔，僅供本機使用的caching only設定，這些設定檔均在原本的目錄中，在執行狀況，它們會全部remount到/var/named/chroot相關目錄中，以便以chroot模式執行之：

```
ls -al /etc/
```

```
-rw-r--r--. 1 root root 774 2014-12-09 21:48 localtime
drwxr-x---. 2 root named 4096 2014-10-15 21:28 named
-rw-r-----. 1 root named 1008 2010-07-19 21:34 named.conf
-rw-r--r--. 1 root named 2389 2014-10-15 21:28 named.iscdlv.key
-rw-r-----. 1 root named 931 2007-06-21 18:09 named.rfc1912.zones
-rw-r--r--. 1 root named 487 2010-07-19 21:28 named.root.key
drwxr-x---. 3 root named 4096 2014-12-10 11:24 pki
-rw-r-----. 1 root named 77 2014-12-10 11:32 rndc.key
```

```
ls -al /var/named/
```

```
drwxr-x---. 6 root named 4096 2014-12-10 11:24 chroot
drwxrwx---. 2 named named 4096 2014-12-10 11:32 data
drwxrwx---. 2 named named 4096 2014-12-10 11:33 dynamic
-rw-r-----. 1 root named 2075 2014-04-23 20:57 named.ca
-rw-r-----. 1 root named 152 2009-12-15 20:27 named.empty
-rw-r-----. 1 root named 152 2007-06-21 18:09 named.localhost
-rw-r-----. 1 root named 168 2009-12-15 20:27 named.loopback
drwxrwx---. 2 named named 4096 2014-10-15 21:28 slaves
```

肆、DNS Server 安全性設定檔說明

DNS Server 在網際網路的服務，是必須存在的服務；就安全性而言，就相當重要。為了讓學校的 DNS Server 可以正常的服務，不會被入侵、竄改紀錄或偽裝紀錄，我們參考了系統的 sample 檔，再加上安全性的考量，終於完成了比較安全的 DNS 設定檔。由於設定檔很長很繁雜，分別先說明如下：

1. DNS 相關的設定範例檔案，系統是放在/usr/share/doc/bind-9.3.6/sample/目錄底，可以直接 copy 相對應的目錄中，再來修改設定值。

```
# find /usr/share/doc/bind-9.8.2/sample/  
/usr/share/doc/bind-9.8.2/sample/  
/usr/share/doc/bind-9.8.2/sample/var  
/usr/share/doc/bind-9.8.2/sample/var/named  
/usr/share/doc/bind-9.8.2/sample/var/named/my.external.zone.db  
/usr/share/doc/bind-9.8.2/sample/var/named/named.localhost  
/usr/share/doc/bind-9.8.2/sample/var/named/slaves  
/usr/share/doc/bind-9.8.2/sample/var/named/slaves/my.slave.internal.zone.db  
/usr/share/doc/bind-9.8.2/sample/var/named/slaves/my.ddns.internal.zone.db  
/usr/share/doc/bind-9.8.2/sample/var/named/named.empty  
/usr/share/doc/bind-9.8.2/sample/var/named/named.loopback  
/usr/share/doc/bind-9.8.2/sample/var/named/named.ca  
/usr/share/doc/bind-9.8.2/sample/var/named/data  
/usr/share/doc/bind-9.8.2/sample/var/named/my.internal.zone.db  
/usr/share/doc/bind-9.8.2/sample/etc  
/usr/share/doc/bind-9.8.2/sample/etc/named.conf  
/usr/share/doc/bind-9.8.2/sample/etc/named.rfc1912.zones
```

2. 您可以至高雄市網 FTP 站去下載已經設計好的 config 檔：
若您只是設定單純的 master 或 slave DNS Server，請下載
<http://ftp.kh.edu.tw/APPL/dns-config/dns-conf.tar.bz2>
若您想要設定內外網不同 DNS 解析(回應)的功能，請下載
<http://ftp.kh.edu.tw/APPL/dns-config/dualview-dns-conf.tar.bz2>
下載回來後，只要將壓縮檔解壓縮至/var/named/chroot/目錄下即可。
注意：本設定檔僅適用於 bind 9.8.2 版以上。
3. 為了瞭解日益複雜的 DNS 主設定檔，我們將 named.conf 拆成幾個部份，以方便解說及日後的維護。
 - (1) named.conf 主設定檔：主要的設定保留在這個檔案內
 - (2) named.root.hints：將 DNS 的 13 個 root 的設定值，獨立成一個檔案，以方便每個 view 引入使用。
 - (3) named.rfc1912.zones：將原來設定檔中，有關 local 的幾項設定，因為每個 view 都會用到，為了減少重覆的設定，將這些設定獨立成一個檔案。
 - (4) named.zones.in：放置內部網段使用的正反解表的設定檔。
 - (5) named.zones：放置外部網段(或只有一個網段)使用的正反解表的設定檔。
 - (6) named.zones.master.*：設定成 Master DNS Server 主機的設定檔。
 - (7) named.zone.slave.*：設定成 Slave DNS Server 主機的設定檔。
 - (8) malice.zones：DNS 正反解黑名單，最主要是用來防治教育部公告之惡意網站。
 - (9) named.caching-nameserver.conf：cache only DNS 設定檔。

4. 設定 named.conf：

- (1) acl 描述：因應內、外部網段不同的環境，增加 acl 控制功能，以便控制內外部網段

名單，供後面的 view 描述使用；同時其他網段名單(如 forwarderss)，也改用 acl 方便處理。

```
// secondaries (slave) dns server的IP設定，將自己及市網的五台DNS IP設在這個acl之中
acl secondaries {
    localhost;
    163.28.136.10;
    2001:288:8201:1::10;
    163.28.136.2;
    2001:288:8201:1::2;
    163.28.136.14;
    2001:288:8201:1::14;
    163.16.1.12;
    2001:288:8401::2;
    163.16.1.23;
    2001:288:8401::3;
};

// 內部網段的宣告，將內部使用的網段逐條列在這個acl中。
acl trusted {
    localnets;
    163.32.xxx.0/24;
    2001:288:82xx:1::/64;
};

// 黑名單網段的宣告，將黑名單網段逐條列在這個acl中。
acl drop {
    244.0.0.0/24;
};
```

(2) option 描述：DNS 中大部份的主要功能，都放這個描述中。

```
//
// See the BIND Administrator's Reference Manual (ARM) for details, in:
//   file:///usr/share/doc/bind-*/arm/Bv9ARM.html
// Also see the BIND Configuration GUI : /usr/bin/system-config-bind and
// its manual.
//
options
{
    // Those options should be used carefully because they disable port
    // randomization
    // query-source    port 53;
    // query-source-v6 port 53;
    listen-on        { any; }; //開啟IPv4服務
    listen-on-v6     { any; }; //開啟IPv6服務

    // Put files that named is allowed to write in the data/ directory:
    directory "/var/named"; // the default
    dump-file        "data/cache_dump.db";
    statistics-file   "data/named_stats.txt";
    memstatistics-file "data/named_mem_stats.txt";
    transfer-format    many-answers;
    max-transfer-time-in 60;
    interface-interval 0;

    // 開放給secondaries DNS Server做全table的dump
    allow-transfer {
        secondaries;
    };

    // 若記憶體內找不到的正反解表，直接到市網的三台IP去查詢。
    forwarders {
        163.28.136.10;
```

```

        2001:288:8201:1::10;
        163.28.136.2;
        2001:288:8201:1::2;
        163.28.136.14;
        2001:288:8201:1::14;
        163.16.1.12;
        2001:288:8401::2;
        163.16.1.23;
        2001:288:8401::3;
    };

    // 將查詢預設值設定為僅開放給內部的IP查詢，至於外部查詢，再從外部的view去設定。
    allow-query {
        trusted;
    };

    // 黑名單一律不做任何回應
    blackhole {
        drop;
    };
};

dnssec-validation yes;

/* Enable DLV by default, use built-in ISC DLV key. */
dnssec-lookaside auto;

/* In RHEL-7 we use /run/named instead of default /var/run/named
   so we have to configure paths properly. */
pid-file "/run/named/named.pid";
session-keyfile "/run/named/session.key";

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

```

(3) logging 描述：設定 DNS log 的方式。

```

logging
{
    /*      If you want to enable debugging, eg. using the 'rndc trace' command,
    *      named will try to write the 'named.run' file in the $directory (/var/named).
    *      By default, SELinux policy does not allow named to modify the /var/named
    directory,
    *      so put the default debug log file in data/ :
    */
    channel default_debug {
        file "data/named.run";
        severity dynamic;
    };
    category lame-servers { null; };
};

```

(4) view 描述：設定每個不同的區域，給予不同的名稱解析。

view 描述架構大致如下：

```

view "area-name(區域名稱)" in {
    match-clients { acl-name; };
    match-destinations { acl-name; };
    recursion yes; //or no
    additional-from-auth yes; //or no
    additional-from-cache yes; //or no
    allow-query { acl-name; };

    include "/etc/named.zone.area-name";
}

```



```
};
```

在此我們的設定，共設計了三個 view：localhost_resolver、internal、external。

Localhost resolver：給本機使用。

internal：給校內網段使用。可提供 recursion 查詢。

external：給 internet 網段使用。不可 recursion 查詢，僅提供本網域正反解查詢。

```
//
// All BIND 9 zones are in a "view", which allow different zones to be served
// to different types of client addresses, and for options to be set for groups
// of zones.
//
// By default, if named.conf contains no "view" clauses, all zones are in the
// "default" view, which matches all clients.
//
// If named.conf contains any "view" clause, then all zones MUST be in a view;
// so it is recommended to start off using views to avoid having to restructure
// your configuration files in the future.
//
view "localhost_resolver"
{
/* This view sets up named to be a localhost resolver ( caching only nameserver ).
 * If all you want is a caching-only nameserver, then you need only define this view:
 */
    match-clients          { localhost; };
    match-destinations     { localhost; };
    recursion yes;
    # all views must contain the root hints zone:
    include "/etc/named.root.hints";

    /* these are zones that contain definitions for all the localhost
     * names and addresses, as recommended in RFC1912 - these names should
     * ONLY be served to localhost clients:
     */
    include "/etc/named.rfc1912.zones";
};

view "internal"
{
/* This view will contain zones you want to serve only to "internal" clients
   that connect via your directly attached LAN interfaces - "localnets" .
 */
    match-clients          { trusted; };
    match-destinations     { trusted; };
    recursion yes;
    additional-from-auth   yes;
    additional-from-cache  yes;
    // all views must contain the root hints zone:
    include "/etc/named.root.hints";

    // include "named.rfc1912.zones";
    // you should not serve your rfc1912 names to non-localhost clients.

    // These are your "authoritative" internal zones, and would probably
    // also be included in the "localhost_resolver" view above :

    //內部正反解表設定檔引入
    include "/etc/named.zones";

    // 教育部公告中繼站列表
    include "/etc/malice.zones";

    // 以下為系統預設值，本範例不採用
    /*
    zone "my.internal.zone" {
```

```

        type master;
        file "my.internal.zone.db";
    };
    zone "my.slave.internal.zone" {
        type slave;
        file "slaves/my.slave.internal.zone.db";
        masters { /* put master nameserver IPs here */ 127.0.0.1; } ;
        // put slave zones in the slaves/ directory so named can update them
    };
    zone "my.ddns.internal.zone" {
        type master;
        allow-update { key ddns_key; };
        file "slaves/my.ddns.internal.zone.db";
        // put dynamically updateable zones in the slaves/ directory so named can
update them
        */
    };
};

/*
key ddns_key
{
    algorithm hmac-md5;
    secret "use /usr/sbin/dns-keygen to generate TSIG keys";
};
*/

view "external"
{
/* This view will contain zones you want to serve only to "external" clients
* that have addresses that are not on your directly attached LAN interface subnets:
*/
    match-clients          { any; };
    match-destinations     { any; };
    recursion no;
    additional-from-auth no;
    additional-from-cache no;
    allow-query { any; };

    recursion no;
    // you'd probably want to deny recursion to external clients, so you don't
    // end up providing free DNS service to all takers

    allow-query-cache { none; };
    // Disable lookups for any cached data and root hints

    // all views must contain the root hints zone:
    include "/etc/named.root.hints";

    // These are your "authoritative" external zones, and would probably
    // contain entries for just your web and mail servers:

    //外部正反解表設定檔引入
    include "/etc/named.zones";

    // 以下為系統預設值，本範例不採用
    /*
    zone "my.external.zone" {
        type master;
        file "my.external.zone.db";
    };
    */
};

```

- (5) 以上做好結構化設定檔後，靠著 internal、external 兩個 view 描述中引入的正反解表設定檔，就可做不同的 DNS 主機型態變化。
- a.單純、簡單的 DNS Server，只要將 internal、external 兩個 view 引入正反解表設定檔，設成同一個檔案(/etc/named.zones)即可。
 - b.若要設定 master 或 slave DNS Server，只要改正反解表設定檔(/etc/named.zones)即可。
 - c.若要設定校內外不同正反解表，只要將 internal、external 兩個 view 引入正反解表設定檔，設成不同設定檔即可(/etc/named.zones.in 及/etc/named.zones.out)。

5. named.root.hints:內含 DNS 13 個 root 的主機資料設定檔。

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

named.ca:

```
; <<>> DiG 9.5.0b2 <<>> +bufsize=1200 +norec NS . @a.root-servers.net
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7033
;; flags: qr aa; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 20

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;.                IN      NS

;; ANSWER SECTION:
.                518400    IN      NS      D.ROOT-SERVERS.NET.
.                518400    IN      NS      E.ROOT-SERVERS.NET.
.                518400    IN      NS      F.ROOT-SERVERS.NET.
.                518400    IN      NS      G.ROOT-SERVERS.NET.
.                518400    IN      NS      H.ROOT-SERVERS.NET.
.                518400    IN      NS      I.ROOT-SERVERS.NET.
.                518400    IN      NS      J.ROOT-SERVERS.NET.
.                518400    IN      NS      K.ROOT-SERVERS.NET.
.                518400    IN      NS      L.ROOT-SERVERS.NET.
.                518400    IN      NS      M.ROOT-SERVERS.NET.
.                518400    IN      NS      A.ROOT-SERVERS.NET.
.                518400    IN      NS      B.ROOT-SERVERS.NET.
.                518400    IN      NS      C.ROOT-SERVERS.NET.

;; ADDITIONAL SECTION:
A.ROOT-SERVERS.NET. 3600000    IN      A        198.41.0.4
A.ROOT-SERVERS.NET. 3600000    IN      AAAA     2001:503:ba3e::2:30
B.ROOT-SERVERS.NET. 3600000    IN      A        192.228.79.201
C.ROOT-SERVERS.NET. 3600000    IN      A        192.33.4.12
D.ROOT-SERVERS.NET. 3600000    IN      A        128.8.10.90
E.ROOT-SERVERS.NET. 3600000    IN      A        192.203.230.10
F.ROOT-SERVERS.NET. 3600000    IN      A        192.5.5.241
F.ROOT-SERVERS.NET. 3600000    IN      AAAA     2001:500:2f::f
G.ROOT-SERVERS.NET. 3600000    IN      A        192.112.36.4
H.ROOT-SERVERS.NET. 3600000    IN      A        128.63.2.53
H.ROOT-SERVERS.NET. 3600000    IN      AAAA     2001:500:1::803f:235
I.ROOT-SERVERS.NET. 3600000    IN      A        192.36.148.17
J.ROOT-SERVERS.NET. 3600000    IN      A        192.58.128.30
J.ROOT-SERVERS.NET. 3600000    IN      AAAA     2001:503:c27::2:30
K.ROOT-SERVERS.NET. 3600000    IN      A        193.0.14.129
K.ROOT-SERVERS.NET. 3600000    IN      AAAA     2001:7fd::1
L.ROOT-SERVERS.NET. 3600000    IN      A        199.7.83.42
M.ROOT-SERVERS.NET. 3600000    IN      A        202.12.27.33
M.ROOT-SERVERS.NET. 3600000    IN      AAAA     2001:dc3::35

;; Query time: 110 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Tue Feb 26 15:05:57 2008
```

```
;; MSG SIZE rcvd: 615
```

6. `named.rfc1912.zones`: 內含 `localhost` 的各項主機資料設定檔。

```
// named.rfc1912.zones:
//
// ISC BIND named zone configuration for zones recommended by
// RFC 1912 section 4.1 : localhost TLDs and address zones
//
zone "localdomain" IN {
    type master;
    file "localdomain.zone";
    allow-update { none; };
};

zone "localhost" IN {
    type master;
    file "localhost.zone";
    allow-update { none; };
};

zone "0.0.127.in-addr.arpa" IN {
    type master;
    file "named.local";
    allow-update { none; };
};

zone "0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa" IN {
    type master;
    file "named.ip6.local";
    allow-update { none; };
};

zone "255.in-addr.arpa" IN {
    type master;
    file "named.broadcast";
    allow-update { none; };
};

zone "0.in-addr.arpa" IN {
    type master;
    file "named.zero";
    allow-update { none; };
};
```

localdomain.zone

```
$TTL 86400
@      IN SOA      localhost root (
                                42      ; serial (d. adams)
                                3H      ; refresh
                                15M     ; retry
                                1W      ; expiry
                                1D      ; minimum
                                )
localhost IN NS      localhost
localhost IN A       127.0.0.1
```

localhost.zone

```
$TTL 86400
@           IN SOA      @           root (
                                42      ; serial (d. adams)
                                3H      ; refresh
                                15M     ; retry
                                1W      ; expiry
                                1D )    ; minimum

           IN NS        @
           IN A          127.0.0.1
           IN AAAA       ::1
```

named.local

```

$TTL 86400
@      IN      SOA      localhost. root.localhost. (
                                1997022700 ; Serial
                                28800      ; Refresh
                                14400      ; Retry
                                3600000    ; Expire
                                86400 )    ; Minimum

1      IN      NS       localhost.
1      IN      PTR      localhost.

```

named.ip6.local

```

$TTL 86400
@      IN      SOA      localhost. root.localhost. (
                                1997022700 ; Serial
                                28800      ; Refresh
                                14400      ; Retry
                                3600000    ; Expire
                                86400 )    ; Minimum

1      IN      NS       localhost.
1      IN      PTR      localhost.

```

named.broadcast

```

$TTL      86400
@          IN      SOA      localhost.      root.localhost. (
                                42            ; serial (d. adams)
                                3H            ; refresh
                                15M           ; retry
                                1W            ; expiry
                                1D )           ; minimum

          IN      NS       localhost.

```

named.zero

```

$TTL      86400
@          IN      SOA      localhost.      root.localhost. (
                                42            ; serial (d. adams)
                                3H            ; refresh
                                15M           ; retry
                                1W            ; expiry
                                1D )           ; minimum

          IN      NS       localhost.

```

7. DNS 黑名單設定：用於將教育部公告的中繼站放入 DNS 黑名單，以防止電腦遭惡意入侵及中斷殭屍網路的形成。

malice.zones

<pre> zone "1416job.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "2288.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "2mydns.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "2myip.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "3322.org" IN { type master; </pre>	<pre> zone "is-a-geek.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "istme.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "itsAOL.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "j2ee.us" IN { type master; file "malice.host"; allow-update { none; }; }; zone "jazzhigh.com" IN { type master; </pre>	<pre> zone "yamn.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "yi.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "yj93837.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "zackel.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "zapto.org" IN { type master; </pre>
--	---	--

<pre> file "malice.host"; allow-update { none; }; }; zone "3721.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "3d-game.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "45z.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "51.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "512j.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "6600.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "672k.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "7766.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "8800.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "8866.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "9966.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "achteins.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "adslDNS.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "aiopsxi.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "apgong.com" IN { type master; file "malice.host"; allow-update { none; }; }; </pre>	<pre> file "malice.host"; allow-update { none; }; }; zone "Jetos.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "Jkub.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "jpubzone.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "justdied.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "jw991.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "kicks-ass.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "kicks-ass.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "kimoo.com.tw" IN { type master; file "malice.host"; allow-update { none; }; }; zone "kmip.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "kneel369.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "kpubzone.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "leaphare.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "lovebaritone.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "loveminim.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "lovequartet.com" IN { type master; file "malice.host"; allow-update { none; }; }; </pre>	<pre> file "malice.host"; allow-update { none; }; }; zone "zyns.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "163info.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "dialerDNS.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "freedns.us" IN { type master; file "malice.host"; allow-update { none; }; }; zone "izony.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "jyintl.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "myz.info" IN { type master; file "malice.host"; allow-update { none; }; }; zone "th-fish.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "9asales.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "opointcn.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "afz.biz" IN { type master; file "malice.host"; allow-update { none; }; }; zone "bounceme.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "changeip.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "chatnook.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "cnread.net" IN { type master; file "malice.host"; allow-update { none; }; }; </pre>
--	--	--

<pre> }; zone "apubzone.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "ath.cx" IN { type master; file "malice.host"; allow-update { none; }; }; zone "au2000.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "b0ne.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "bi-apple.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "blogdns.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "blogdns.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "blogdns.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "bpubzone.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "bsd.st" IN { type master; file "malice.host"; allow-update { none; }; }; zone "car.llev.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "coom.in" IN { type master; file "malice.host"; allow-update { none; }; }; zone "cpubzone.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "c-zz.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "darktech.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "dd.blueline.be" IN { </pre>	<pre> }; zone "lovequaver.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "lovequintet.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "lovesolo.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "lovetrio.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "lpubzone.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "lycosgame.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "maoti.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "mefound.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "memoryfree.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "merseine.nu" IN { type master; file "malice.host"; allow-update { none; }; }; zone "milstone.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "mine.nu" IN { type master; file "malice.host"; allow-update { none; }; }; zone "mmtcat.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "m-music.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "mpubzone.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "mrbasic.com" IN { </pre>	<pre> }; zone "fh689.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "gamanies.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "gamemuster.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "hawaiianwatershots.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "iseekcool.hk" IN { type master; file "malice.host"; allow-update { none; }; }; zone "longmusic.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "newtouring.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "ns01.us" IN { type master; file "malice.host"; allow-update { none; }; }; zone "palms-us.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "roadutter.cd" IN { type master; file "malice.host"; allow-update { none; }; }; zone "sendpath.hk" IN { type master; file "malice.host"; allow-update { none; }; }; zone "support-microsoft.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "ttvtimes.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "weedns.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "wikaba.com" IN { type master; file "malice.host"; allow-update { none; }; }; </pre>
---	---	---

<pre> type master; file "malice.host"; allow-update { none; }; }; zone "dd.bluelinecomputers.be" IN { type master; file "malice.host"; allow-update { none; }; }; zone "ddumm.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "diyserver.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "dnsalias.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "dnsalias.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "dnyp.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "dondon555.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "dpubzone.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "dumbl.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "dvrdns.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "dynalias.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "dynalias.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "dynalias.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "dyndns.biz" IN { type master; file "malice.host"; allow-update { none; }; }; zone "dyndns.info" IN { type master; </pre>	<pre> type master; file "malice.host"; allow-update { none; }; }; zone "mrbonus.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "MrFace.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "MrLove.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "MrsLove.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "my03.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "myftp.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "myphotos.cc" IN { type master; file "malice.host"; allow-update { none; }; }; zone "nease.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "netfirms.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "ninth.biz" IN { type master; file "malice.host"; allow-update { none; }; }; zone "nod99.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "npubzone.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "ns0.it" IN { type master; file "malice.host"; allow-update { none; }; }; zone "ods.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "oicp.net" IN { type master; file "malice.host"; </pre>	<pre> }; zone "wordcasts.cd" IN { type master; file "malice.host"; allow-update { none; }; }; zone "xxuz.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "yourtrap.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "airbridge.info" IN { type master; file "malice.host"; allow-update { none; }; }; zone "bluewinnt.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "deaftone.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "dns0755.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "dnsrd.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "ggsddup.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "googleadnews.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "mydyn.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "pigeonsky.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "servebeer.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "serveblog.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "tw7890.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "webhop.info" IN { </pre>
--	--	--

<pre> file "malice.host"; allow-update { none; }; }; zone "dyndns.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "dyndns.tv" IN { type master; file "malice.host"; allow-update { none; }; }; zone "dyndns.ws" IN { type master; file "malice.host"; allow-update { none; }; }; zone "dyndsl.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "dynserv.ca" IN { type master; file "malice.host"; allow-update { none; }; }; zone "dynserv.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "dynserv.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "dynserv.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "dynu.ca" IN { type master; file "malice.host"; allow-update { none; }; }; zone "dynu.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "easydns.us" IN { type master; file "malice.host"; allow-update { none; }; }; zone "effers.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "ezua.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "faqserv.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "fetftp.nu" IN { type master; file "malice.host"; allow-update { none; }; </pre>	<pre> allow-update { none; }; }; zone "opubzone.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "ostabil.nu" IN { type master; file "malice.host"; allow-update { none; }; }; zone "page.us" IN { type master; file "malice.host"; allow-update { none; }; }; zone "panasonics.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "patchwindows.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "pcanywhere.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "podzone.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "podzone.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "ppubzone.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "prout.be" IN { type master; file "malice.host"; allow-update { none; }; }; zone "ringiii.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "rlogin.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "scieron.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "selfip.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "servebbs.org" IN { type master; file "malice.host"; allow-update { none; }; }; </pre>	<pre> type master; file "malice.host"; allow-update { none; }; }; zone "windowupdates.hk" IN { type master; file "malice.host"; allow-update { none; }; }; zone "yeah.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "3322.org.cn" IN { type master; file "malice.host"; allow-update { none; }; }; zone "chsniper.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "ddns.info" IN { type master; file "malice.host"; allow-update { none; }; }; zone "dontexist.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "ibmunion.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "imwork.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "kabsersky.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "loneswim.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "myvnc.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "ServeUser.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "windowupdata.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "25u.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "4irc.com" IN { type master; file "malice.host"; </pre>
---	---	---

<pre> }; zone "fileuk0410.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "fjxmasp.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "flnet.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "fpubzone.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "freens.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "game-host.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "game-server.cc" IN { type master; file "malice.host"; allow-update { none; }; }; zone "gmx.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "gotdns.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "gotdns.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "gpubzone.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "ham-radio-op.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "homedns.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "homeftp.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "homeftp.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "homeip.net" IN { </pre>	<pre> zone "serveftp.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "serveftp.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "servegame.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "server.us" IN { type master; file "malice.host"; allow-update { none; }; }; zone "sextracker.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "sexxy.biz" IN { type master; file "malice.host"; allow-update { none; }; }; zone "shacknet.nu" IN { type master; file "malice.host"; allow-update { none; }; }; zone "sinamoil.com.tw" IN { type master; file "malice.host"; allow-update { none; }; }; zone "slyip.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "smallblack.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "snusk.nu" IN { type master; file "malice.host"; allow-update { none; }; }; zone "solaris.nu" IN { type master; file "malice.host"; allow-update { none; }; }; zone "squirly.info" IN { type master; file "malice.host"; allow-update { none; }; }; zone "stabilit.se" IN { type master; file "malice.host"; allow-update { none; }; }; zone "staticcling.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "stockfound.com" IN { type master; </pre>	<pre> allow-update { none; }; }; zone "bbsindex.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "changeip.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "checalla.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "cndns.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "coloreagle.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "cute86.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "dns2.us" IN { type master; file "malice.host"; allow-update { none; }; }; zone "dnsupdating.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "docomnews.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "etowns.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "fartit.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "feiloglobe.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "flower-show.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "iaSolution.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "jaqan.cn" IN { type master; file "malice.host"; allow-update { none; }; }; }; </pre>
--	---	--

<pre> type master; file "malice.host"; allow-update { none; }; }; zone "homelinux.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "homelinux.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "homelinux.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "homelu.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "homepc.it" IN { type master; file "malice.host"; allow-update { none; }; }; zone "homeunix.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "homeunix.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "homeunix.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "hpubzone.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "hyfitech.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "icpcn.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "ifulme.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "iglus.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "ipread.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "ipubzone.com" IN { type master; file "malice.host"; </pre>	<pre> file "malice.host"; allow-update { none; }; }; zone "suroot.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "systemupdate.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "tophi.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "tophi.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "touchxfeel.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "trickip.Net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "uni.cc" IN { type master; file "malice.host"; allow-update { none; }; }; zone "uptyou.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "usagameplay.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "vicp.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "westcowboy.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "windowupdates.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "winupdate.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "wmdshr.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "www1.biz" IN { type master; file "malice.host"; allow-update { none; }; }; </pre>	<pre> zone "jeiyuang.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "kickgick.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "macfeeresponse.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "mathcamp.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "miccrasoft.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "nationcar.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "nsl.name" IN { type master; file "malice.host"; allow-update { none; }; }; zone "ntimobile.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "onedumb.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "oray2008.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "pc-officer.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "phoniexco.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "qpoe.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "selfip.info" IN { type master; file "malice.host"; allow-update { none; }; }; zone "sendsmtp.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "servebbs.com" IN { type master; </pre>
--	--	--

<pre> allow-update { none; }; }; zone "isa-geek.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "is-a-geek.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "isa-geek.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "is-a-geek.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "isa-geek.org" IN { type master; file "malice.host"; allow-update { none; }; }; </pre>	<pre> }; zone "wwwcrazy.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "xicp.net" IN { type master; file "malice.host"; allow-update { none; }; }; zone "xtycoon.org" IN { type master; file "malice.host"; allow-update { none; }; }; zone "xxxy.info" IN { type master; file "malice.host"; allow-update { none; }; }; zone "xygong.com" IN { type master; file "malice.host"; allow-update { none; }; }; </pre>	<pre> file "malice.host"; allow-update { none; }; }; zone "servemp3.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "sportsmacaca.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "toh.info" IN { type master; file "malice.host"; allow-update { none; }; }; zone "wahju.com" IN { type master; file "malice.host"; allow-update { none; }; }; zone "westsaga.com" IN { type master; file "malice.host"; allow-update { none; }; }; </pre>
--	--	---

8. 接下來，就依您的需求，去變動 internal、external 兩個 view 的正反解設定檔引入。再去設定您的正反解表就可以了！

伍、Primary DNS Server 的設定

Primary DNS Server 適用於 DNS 由學校自己維護管理的單位；在架構上，以學校 DNS 做為 Primary Server，上層(市網中心)DNS 做為學校的 Secondary Server，來備份學校 DNS 內的 DNS table，當學校端斷線或 DNS Server 故障時，外界還能找到學校的機器。

1. 請下載 <http://ftp.kh.edu.tw/APPL/dns-config/dns-conf.tar.bz2>，並解壓縮至/var/named/chroot

```
# wget http://ftp.kh.edu.tw/APPL/dns-config/dns-conf.tar.bz2
--2014-12-11 08:47:04-- http://ftp.kh.edu.tw/APPL/dns-config/dns-conf.tar.bz2
正在查找主機 ftp.kh.edu.tw... 163.28.136.5
正在連接 ftp.kh.edu.tw[163.28.136.5]:80... 連上了。
已送出 HTTP 要求，正在等候回應... 200 OK
長度: 7894 (7.7K) [application/x-bzip2]
Saving to: `dns-conf.tar.bz2'

100%[=====>] 7,894      --.-K/s   in 0s

2014-12-11 08:47:04 (225 MB/s) - `dns-conf.tar.bz2' saved [7894/7894]

# tar jxvf dns-conf.tar.bz2 -C /var/named/chroot/
./
./etc/
./etc/named.root.hints
./etc/named.zones.master
./etc/named.rfc1912.zones
./etc/named.conf
./etc/malice.zones
./etc/named.zones.slave
./etc/named.caching-nameserver.conf
./etc/named.zones
./var/
./var/named/
./var/named/localhost.zone
./var/named/malice.host
./var/named/named.broadcast
./var/named/named.ca
./var/named/localhostdomain.zone
./var/named/named.ip6.local
./var/named/named.local
./var/named/named.zero
./var/named/data/
./var/named/master/
./var/named/master/named.host
./var/named/master/named.rev.ipv6
./var/named/master/named.rev
./var/named/slaves/

# restorcon -R /var/named/chroot
```

2. 檢查一下/var/named/chroot/etc/named.conf 中 internal、external 兩個 view 引入的正反解設定檔，是否都是/etc/named.zones

```
view "internal"
{
    //內部正反解表設定檔引入
    include "/etc/named.zones";
};
view "external"
{
    //外部正反解表設定檔引入
    include "/etc/named.zones";
};
```

3. 修改/var/named/chroot/etc/named.zones 檔案，修改貴校正反解的設定：

```
//貴單位網域之正查資料設定([domain]字串請換成貴校核定之 Domain Name)
zone "[domain].kh.edu.tw">{
```

```

    type master;
    file "master/named.host";
};

//貴單位 IPv4 反查資料設定(xxx 字串請換成貴校核定網段之第三碼，如核定網段為 163.32.36.0，則須表示成 36.32.163.in-addr.arpa)
zone "xxx.32.163.in-addr.arpa"{
    type master;
    file "master/named.rev";
};

//貴單位 IPv6 反查資料設定(xx 字串請換成貴校核定 IPv6 /48 之最末兩碼，如核定網段為 2001:288:8234::/48，則須表示成 4.3.2.8.8.8.2.0.1.0.0.2.ip6.arpa)
zone "x.x.2.8.8.8.2.0.1.0.0.2.ip6.arpa" {
    type master;
    file "master/named.rev.ipv6";
};

```

4. 增加貴單位正查之資料表：(/var/named/chroot/var/named/master/named.host)

```

$TTL 86400
@      IN      SOA      [domain].kh.edu.tw. root.[domain].kh.edu.tw. (
                        2010101201 ; serial
                        1H ; refresh
                        15 ; retry
                        14D ; expire
                        12H ; Minimum
                        )

@      IN      MX       5      mail.[domain].kh.edu.tw.
@      IN      NS       [domain].kh.edu.tw.
@      IN      NS       dns.[domain].kh.edu.tw.
@      IN      A        163.32.xxx.1
dns     IN      CNAME    [domain].kh.edu.tw.
proxy  IN      A        163.32.xxx.2
mail   IN      A        163.32.xxx.3
       IN      AAAA     2001:288:82xx:1::3
       IN      MX       0      mail.[domain].kh.edu.tw.
www    IN      A        163.32.xxx.4
ftp    IN      CNAME    www

;; Windows 7/Vista KMS register record
;; Windows 7/Vista KMS 啟動方式之服務紀錄，有了這筆紀錄，全市授權之 Windows 7/Vista 企業版便可
找到這筆紀錄後，自動向中心登錄主機啟用 Windows 7/Vitsa 及 office 2010
vlmcs._tcp      IN      SRV       0 0 1688      ap24.kh.edu.tw.

```

5. 增加貴單位 IPv4 反查之資料表：(/var/named/chroot/var/named/master/named.host.rev)

```

$TTL 86400
@      IN      SOA      [domain].kh.edu.tw. root.[domain].kh.edu.tw. (
                        2001101201 ; serial
                        1H ; refresh
                        15 ; retry
                        14D ; expire
                        12H ; Minimum
                        )

@      IN      NS       [domain].kh.edu.tw.
@      IN      NS       dns.[domain].kh.edu.tw.
1      IN      PTR      [domain].kh.edu.tw.
2      IN      PTR      proxy.[domain].kh.edu.tw.
3      IN      PTR      mail.[domain].kh.edu.tw.
4      IN      PTR      www.[domain].kh.edu.tw.
; 使用變數作大範圍反解
$GENERATE 100-150 $      PTR      pc$.[domain].kh.edu.tw.

```

6. 增加貴單位 IPv6 反查之資料表：(/var/named/chroot/var/named/master/named.rev.ipv6)

```

; IPv6 reverse lookup zone for 2001:288:82xx::/48
$TTL 86400
@      IN      SOA      dns.[domain].kh.edu.tw. root.[domain].kh.edu.tw. (
                        2010102101 ; serial
                        28800 ; refresh
                        7200 ; retry

```



```
dns_rdata_fromtext: named.host:6: near eol: unexpected end of input
zone test.kh.edu.tw/IN: loading master file named.test.zone: unexpected end of input
```

9. 啟動 DNS Server :

```
/etc/rc.d/init.d/named start
```

10.查看系統之 log 檔：
vi /etc/log/messages

vi /etc/log/messages

```
Dec 11 08:36:54 cent6x64 named: zone localdomain/IN: loaded serial 42
Dec 11 08:36:54 cent6x64 named: zone localhost/IN: loaded serial 42
Dec 11 08:36:54 cent6x64 named: zone 0.0.127.in-addr.arpa/IN: loaded serial 1997022700
Dec 11 08:36:54 cent6x64 named: zone
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa/IN: loaded serial 1997022700
Dec 11 08:36:54 cent6x64 named: zone 255.in-addr.arpa/IN: loaded serial 42
Dec 11 08:36:54 cent6x64 named: zone 0.in-addr.arpa/IN: loaded serial 42
Dec 11 08:36:54 cent6x64 named: dns_rdata_fromtext: master/named.host:17: near '2001:288:82xx:1::3': bad IPv6 address
Dec 11 08:36:54 cent6x64 named: zone test.kh.edu.tw/IN: loading from master file master/named.host failed: bad IPv6 address
Dec 11 08:36:54 cent6x64 named: zone test.kh.edu.tw/IN: not loaded due to errors.
Dec 11 08:36:54 cent6x64 named: internal/test.kh.edu.tw/IN: bad IPv6 address
Dec 11 08:36:54 cent6x64 named: zone 119.32.163.in-addr.arpa/IN: loaded serial 2001101201
Dec 11 08:36:54 cent6x64 named: zone 1.0.2.8.8.8.2.0.1.0.2.ip6.arpa/IN: loaded serial 2010102101
Dec 11 08:36:54 cent6x64 named: zone 1416job.com/IN: loaded serial 2008080501
Dec 11 08:36:54 cent6x64 named: zone 2288.org/IN: loaded serial 2008080501
Dec 11 08:36:54 cent6x64 named: zone 2mydns.com/IN: loaded serial 2008080501
Dec 11 08:36:54 cent6x64 named: zone 2myip.com/IN: loaded serial 2008080501
Dec 11 08:36:54 cent6x64 named: zone 3322.org/IN: loaded serial 2008080501
Dec 11 08:36:54 cent6x64 named: zone 3721.com/IN: loaded serial 2008080501
```

設定檔有問題須改正。

```
Dec 11 08:53:59 cent6x64 named[8017]: starting BIND 9.8.2rc1-RedHat-9.8.2-0.30.rc1.el6 -u named -t
/var/named/chroot
Dec 11 08:53:59 cent6x64 named[8017]: built with '--build=x86_64-redhat-linux-gnu' '--host=x86_64-redhat-
linux-gnu' '--target=x86_64-redhat-linux-gnu' '--program-prefix=' '--prefix=/usr' '--exec-prefix=/usr' '--
bindir=/usr/bin' '--sbindir=/usr/sbin' '--sysconfdir=/etc' '--datadir=/usr/share' '--includedir=/usr/include'
'--libdir=/usr/lib64' '--libexecdir=/usr/libexec' '--sharedstatedir=/var/lib' '--mandir=/usr/share/man' '--
infodir=/usr/share/info' '--with-libtool' '--localstatedir=/var' '--enable-threads' '--enable-ipv6' '--enable-
filter-aaaa' '--with-pic' '--disable-static' '--disable-openssl-version-check' '--with-dlopen=yes' '--with-
dlz-ldap=yes' '--with-dlz-postgres=yes' '--with-dlz-mysql=yes' '--with-dlz-filesystem=yes' '--with-gssapi=yes'
'--disable-isc-spnego' '--with-docbook-xsl=/usr/share/sgml/docbook/xsl-stylesheets' '--enable-fixed-rreset'
'build alias=x86_64-redhat-linux-gnu' 'host alias=x86_64-redhat-linux-gnu' 'target alias=x86_64-redhat-linux-
gnu' 'CFLAGS=-O2 -g -pipe -Wall -Wp,-D_FORTIFY_SOURCE=2 -fexceptions -fstack-protector --param=ssp-buffer-
size=4 -m64 -mtune=generic' 'CPPFLAGS=-DDIG_SIGCHASE'
Dec 11 08:53:59 cent6x64 named[8017]: -----
Dec 11 08:53:59 cent6x64 named[8017]: BIND 9 is maintained by Internet Systems Consortium,
Dec 11 08:53:59 cent6x64 named[8017]: Inc. (ISC), a non-profit 501(c)(3) public-benefit
Dec 11 08:53:59 cent6x64 named[8017]: corporation. Support and training for BIND 9 are
Dec 11 08:53:59 cent6x64 named[8017]: available at https://www.isc.org/support
Dec 11 08:53:59 cent6x64 named[8017]: -----
Dec 11 08:53:59 cent6x64 named[8017]: adjusted limit on open files from 4096 to 1048576
Dec 11 08:53:59 cent6x64 named[8017]: found 2 CPUs, using 2 worker threads
Dec 11 08:53:59 cent6x64 named[8017]: using up to 4096 sockets
Dec 11 08:53:59 cent6x64 named[8017]: loading configuration from '/etc/named.conf'
Dec 11 08:53:59 cent6x64 named[8017]: using default UDP/IPv4 port range: [1024, 65535]
Dec 11 08:53:59 cent6x64 named[8017]: using default UDP/IPv6 port range: [1024, 65535]
Dec 11 08:53:59 cent6x64 named[8017]: listening on IPv6 interfaces, port 53
Dec 11 08:53:59 cent6x64 named[8017]: listening on IPv4 interface lo, 127.0.0.1#53
Dec 11 08:53:59 cent6x64 named[8017]: listening on IPv4 interface eth0, 163.32.119.175#53
Dec 11 08:53:59 cent6x64 named[8017]: generating session key for dynamic DNS
Dec 11 08:53:59 cent6x64 named[8017]: sizing zone task pool based on 321 zones
Dec 11 08:53:59 cent6x64 named[8017]: set up managed keys zone for view localhost_resolver, file
'dynamic/03641f096ea0ceb02e407a63ea6d9e42d7ceafab8d156336551aeae23ee060ed.mkeys'
Dec 11 08:53:59 cent6x64 named[8017]: Warning: view localhost_resolver: 'empty-zones-enable/disable-empty-
zone' not set; disabling RFC 1918 empty zones
Dec 11 08:53:59 cent6x64 named[8017]: automatic empty zone: view localhost_resolver: 127.IN-ADDR.ARPA
Dec 11 08:53:59 cent6x64 named[8017]: automatic empty zone: view localhost_resolver: 254.169.IN-ADDR.ARPA
Dec 11 08:53:59 cent6x64 named[8017]: automatic empty zone: view localhost_resolver: 2.0.192.IN-ADDR.ARPA
Dec 11 08:53:59 cent6x64 named[8017]: automatic empty zone: view localhost_resolver: 100.51.198.IN-ADDR.ARPA
Dec 11 08:53:59 cent6x64 named[8017]: automatic empty zone: view localhost_resolver: 113.0.203.IN-ADDR.ARPA
Dec 11 08:53:59 cent6x64 named[8017]: automatic empty zone: view localhost_resolver: 255.255.255.255.IN-
ADDR.ARPA
Dec 11 08:53:59 cent6x64 named[8017]: automatic empty zone: view localhost_resolver:
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.IP6.ARPA
Dec 11 08:53:59 cent6x64 named[8017]: automatic empty zone: view localhost_resolver:
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.IP6.ARPA
Dec 11 08:53:59 cent6x64 named[8017]: automatic empty zone: view localhost_resolver: D.F.IP6.ARPA
Dec 11 08:53:59 cent6x64 named[8017]: automatic empty zone: view localhost_resolver: 8.E.F.IP6.ARPA
Dec 11 08:53:59 cent6x64 named[8017]: automatic empty zone: view localhost_resolver: 9.E.F.IP6.ARPA
Dec 11 08:53:59 cent6x64 named[8017]: automatic empty zone: view localhost_resolver: A.E.F.IP6.ARPA
Dec 11 08:53:59 cent6x64 named[8017]: automatic empty zone: view localhost_resolver: B.E.F.IP6.ARPA
```



```
Dec 11 08:53:59 cent6x64 named[8017]: automatic empty zone: view localhost_resolver: 8.B.D.0.1.0.0.2.IP6.ARPA
Dec 11 08:53:59 cent6x64 named[8017]: set up managed keys zone for view internal, file
'dynamic/3bed2cb3a3acf7b6ba8ef408420cc682d5520e26976d354254f528c965612954f.mkeys'
Dec 11 08:53:59 cent6x64 named[8017]: Warning: view internal: 'empty-zones-enable/disable-empty-zone' not set:
disabling RFC 1918 empty zones
Dec 11 08:53:59 cent6x64 named[8017]: automatic empty zone: view internal: 0.IN-ADDR.ARPA
Dec 11 08:53:59 cent6x64 named[8017]: automatic empty zone: view internal: 127.IN-ADDR.ARPA
Dec 11 08:53:59 cent6x64 named[8017]: automatic empty zone: view internal: 254.169.IN-ADDR.ARPA
Dec 11 08:53:59 cent6x64 named[8017]: automatic empty zone: view internal: 2.0.192.IN-ADDR.ARPA
Dec 11 08:53:59 cent6x64 named[8017]: automatic empty zone: view internal: 100.51.198.IN-ADDR.ARPA
Dec 11 08:53:59 cent6x64 named[8017]: automatic empty zone: view internal: 113.0.203.IN-ADDR.ARPA
Dec 11 08:53:59 cent6x64 named[8017]: automatic empty zone: view internal: 255.255.255.255.IN-ADDR.ARPA
Dec 11 08:53:59 cent6x64 named[8017]: automatic empty zone: view internal:
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.IP6.ARPA
Dec 11 08:53:59 cent6x64 named[8017]: automatic empty zone: view internal:
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.IP6.ARPA
Dec 11 08:53:59 cent6x64 named[8017]: automatic empty zone: view internal: D.F.IP6.ARPA
Dec 11 08:53:59 cent6x64 named[8017]: automatic empty zone: view internal: 8.E.F.IP6.ARPA
Dec 11 08:53:59 cent6x64 named[8017]: automatic empty zone: view internal: 9.E.F.IP6.ARPA
Dec 11 08:53:59 cent6x64 named[8017]: automatic empty zone: view internal: A.E.F.IP6.ARPA
Dec 11 08:53:59 cent6x64 named[8017]: automatic empty zone: view internal: B.E.F.IP6.ARPA
Dec 11 08:53:59 cent6x64 named[8017]: automatic empty zone: view internal: 8.B.D.0.1.0.0.2.IP6.ARPA
Dec 11 08:53:59 cent6x64 named[8017]: set up managed keys zone for view external, file
'dynamic/3c4623849a49a53911c4a3e48d8cead8a1858960bccdea7a1b978d73ec2f06d7.mkeys'
Dec 11 08:53:59 cent6x64 named[8017]: command channel listening on 127.0.0.1#953
Dec 11 08:53:59 cent6x64 named[8017]: command channel listening on ::1#953
Dec 11 08:53:59 cent6x64 named[8017]: zone 0.in-addr.arpa/IN/localhost_resolver: loaded serial 42
Dec 11 08:53:59 cent6x64 named[8017]: zone 0.0.127.in-addr.arpa/IN/localhost_resolver: loaded serial
1997022700
Dec 11 08:53:59 cent6x64 named[8017]: zone 255.in-addr.arpa/IN/localhost_resolver: loaded serial 42
Dec 11 08:53:59 cent6x64 named[8017]: zone
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa/IN/localhost_resolver: loaded serial
1997022700
Dec 11 08:53:59 cent6x64 named[8017]: zone localdomain/IN/localhost_resolver: loaded serial 42
Dec 11 08:53:59 cent6x64 named[8017]: zone localhost/IN/localhost_resolver: loaded serial 42
Dec 11 08:53:59 cent6x64 named[8017]: managed-keys-zone ./IN/localhost_resolver: loaded serial 0
Dec 11 08:53:59 cent6x64 named[8017]: zone 119.32.163.in-addr.arpa/IN/internal: loaded serial 2001101201
Dec 11 08:53:59 cent6x64 named[8017]: zone 1.0.2.8.8.8.2.0.1.0.0.2.ip6.arpa/IN/internal: loaded serial
2010102101
Dec 11 08:53:59 cent6x64 named[8017]: zone dd.blueline.be/IN/internal: loaded serial 2008080501
Dec 11 08:53:59 cent6x64 named[8017]: zone dd.bluelinecomputers.be/IN/internal: loaded serial 2008080501
Dec 11 08:53:59 cent6x64 named[8017]: zone prout.be/IN/internal: loaded serial 2008080501
Dec 11 08:53:59 cent6x64 named[8017]: zone afz.biz/IN/internal: loaded serial 2008080501
```

DNS Server 成功啟動。

伍、Secondary DNS Server 的設定

Secondary DNS Server適用於以下兩種情況：(1)學校的DNS由市網中心代管，必須在校內架一台DNS Server做備份，以增加DNS查詢效率；如此，學校就可以直接使用校內的DNS Server，而要修改DNS記錄就直接上DNS代管網頁去設定，Secondary Server會自動去更新並同步DNS Table；(2)DNS由學校自行維護，想在校內架設第二台DNS Server以做為備份。

1. 請下載 <http://ftp.kh.edu.tw/APPL/dns-config/dns-conf.tar.bz2>，並解壓縮至/var/named/chroot

```
# wget http://ftp.kh.edu.tw/APPL/dns-config/dns-conf.tar.bz2
--2014-12-11 08:47:04-- http://ftp.kh.edu.tw/APPL/dns-config/dns-conf.tar.bz2
正在查找主機 ftp.kh.edu.tw... 163.28.136.5
正在連接 ftp.kh.edu.tw|163.28.136.5|:80... 連上了。
已送出 HTTP 要求，正在等候回應... 200 OK
長度: 7894 (7.7K) [application/x-bzip2]
Saving to: `dns-conf.tar.bz2'

100%[=====>] 7,894      --.-K/s   in 0s

2014-12-11 08:47:04 (225 MB/s) - `dns-conf.tar.bz2' saved [7894/7894]

# tar jxvf dns-conf.tar.bz2 -C /var/named/chroot/
./
./etc/
./etc/named.root.hints
./etc/named.zones.master
./etc/named.rfc1912.zones
./etc/named.conf
./etc/malice.zones
./etc/named.zones.slave
./etc/named.caching-nameserver.conf
./etc/named.zones
./var/
./var/named/
./var/named/localhost.zone
./var/named/malice.host
./var/named/named.broadcast
./var/named/named.ca
./var/named/localhost.zone
./var/named/named.ip6.local
./var/named/named.local
./var/named/named.zero
./var/named/data/
./var/named/master/
./var/named/master/named.host
./var/named/master/named.rev.ipv6
./var/named/master/named.rev
./var/named/slaves/

# restorcon -R /var/named/chroot
```

2. 檢查一下/var/named/chroot/etc/named.conf中 internal、external 兩個 view 引入的正反解設定檔，是否都是/etc/named.zones.slave

```
view "internal"
{
    //內部正反解表設定檔引入
    include "/etc/named.zones.slave";
};
view "external"
{
    //外部正反解表設定檔引入
    include "/etc/named.zones.slave";
};
```

3. 修改/var/named/chroot/etc/named.zones.slave 檔案，修改貴校正反解的設定：

```
// masters IP: 163.28.136.14 為 DNS 代管主機，若 DNS 自建者，請將 IP 改為校內 DNS IP
//貴單位網域之正查資料設定([domain]字串請換成貴校核定之 Domain Name)
zone "[domain].kh.edu.tw"{
    type slave;
    file "slave/named.host";
    masters{
        163.28.136.14;
    };
};

//貴單位 IPv4 反查資料設定(xxx 字串請換成貴校核定網段之第三碼，如核定網段為 163.32.36.0，則須表示成 36.32.163.in-addr.arpa)
zone "xxx.32.163.in-addr.arpa"{
    type slave;
    file "slave/named.rev";
    masters{
        163.28.136.14;
    };
};

//貴單位 IPv6 反查資料設定(xx 字串請換成貴校核定 IPv6 /48 之最末兩碼，如核定網段為 2001:288:8234::/48，則須表示成 4.3.2.8.8.8.2.0.1.0.0.2.ip6.arpa)
zone "x.x.2.8.8.8.2.0.1.0.0.2.ip6.arpa" {
    type slave;
    file "slave/named.rev.ipv6";
    masters{
        163.28.136.14;
    };
};
```

4. 檢查設定是否正確：

named-checkconf是用來檢查 named.conf 設定是否正確，若設定正確，則不會有任何訊息

```
# named-checkconf -t /var/named/chroot etc/named.conf
```

5. 啟動 DNS 服務：

```
# /etc/rc.d/init.d/named start
```

6. 檢查系統之 log 檔，看看 DNS 是否正常執行：

vi /etc/log/messages

```
Dec 11 13:02:50 cent6x64 named[32227]: starting BIND 9.8.2rc1-RedHat-9.8.2-0.30.rc1.el6 -u named -t /var/named/chroot
Dec 11 13:02:50 cent6x64 named[32227]: built with '--build=x86_64-redhat-linux-gnu' '--host=x86_64-redhat-linux-gnu' '--target=x86_64-redhat-linux-gnu' '--program-prefix=' '--prefix=/usr' '--exec-prefix=/usr' '--bindir=/usr/bin' '--sbindir=/usr/sbin' '--sysconfdir=/etc' '--datadir=/usr/share' '--includedir=/usr/include' '--libdir=/usr/lib64' '--libexecdir=/usr/libexec' '--sharedstatedir=/var/lib' '--mandir=/usr/share/man' '--infodir=/usr/share/info' '--with-libtool' '--localstatedir=/var' '--enable-threads' '--enable-ipv6' '--enable-filter-aaaa' '--with-pic' '--disable-static' '--disable-openssl-version-check' '--with-dlopen=yes' '--with-dlz-ldap=yes' '--with-dlz-postgres=yes' '--with-dlz-mysql=yes' '--with-dlz-filesystem=yes' '--with-gssapi=yes' '--disable-isc-spnego' '--with-docbook-xsl=/usr/share/sgml/docbook/xsl-stylesheets' '--enable-fixed-rreset' 'build_alias=x86_64-redhat-linux-gnu' 'host_alias=x86_64-redhat-linux-gnu' 'target_alias=x86_64-redhat-linux-gnu' 'CFLAGS=-O2 -g -pipe -Wall -Wp,-D_FORTIFY_SOURCE=2 -fexceptions -fstack-protector --param=ssp-buffer-size=4 -m64 -mtune=generic' 'CPPFLAGS= -DDIG_SIGCHASE'
Dec 11 13:02:50 cent6x64 named[32227]: -----
Dec 11 13:02:50 cent6x64 named[32227]: BIND 9 is maintained by Internet Systems Consortium,
Dec 11 13:02:50 cent6x64 named[32227]: Inc. (ISC), a non-profit 501(c)(3) public-benefit
Dec 11 13:02:50 cent6x64 named[32227]: corporation. Support and training for BIND 9 are
Dec 11 13:02:50 cent6x64 named[32227]: available at https://www.isc.org/support
Dec 11 13:02:50 cent6x64 named[32227]: -----
Dec 11 13:02:50 cent6x64 named[32227]: adjusted limit on open files from 4096 to 1048576
Dec 11 13:02:50 cent6x64 named[32227]: found 2 CPUs, using 2 worker threads
Dec 11 13:02:50 cent6x64 named[32227]: using up to 4096 sockets
Dec 11 13:02:50 cent6x64 named[32227]: loading configuration from '/etc/named.conf'
Dec 11 13:02:50 cent6x64 named[32227]: using default UDP/IPv4 port range: [1024, 65535]
Dec 11 13:02:50 cent6x64 named[32227]: using default UDP/IPv6 port range: [1024, 65535]
Dec 11 13:02:50 cent6x64 named[32227]: listening on IPv6 interfaces, port 53
Dec 11 13:02:50 cent6x64 named[32227]: listening on IPv4 interface lo, 127.0.0.1#53
Dec 11 13:02:50 cent6x64 named[32227]: listening on IPv4 interface eth0, 163.32.119.175#53
Dec 11 13:02:50 cent6x64 named[32227]: generating session key for dynamic DNS
Dec 11 13:02:50 cent6x64 named[32227]: sizing zone task pool based on 15 zones
Dec 11 13:02:50 cent6x64 named[32227]: set up managed keys zone for view localhost_resolver, file 'dynamic/03641f096ea0ceb02e407a63ea6d9e42d7ceafabd8156336551aee23ee060ed.mkeys'
```

DNS Server 成功啟動。

```
# cd /var/named/chroot/  
# cd var/named/slaves/  
# ls -al  
總計 20  
drwxr-xr-x  2 named named 4096 11月 3 14:33 .  
drwxr-x---  3 root  named 4096 11月 3 14:27 ..  
-rw-----  1 named named  687 11月 3 14:33 named.rev  
-rw-----  1 named named 1487 11月 3 14:33 named.rev.ipv6  
-rw-----  1 named named  796 11月 3 14:33 named.host
```

8. 若以上一切正常，則恭喜您，您已完成 Secondary DNS Server 的設定了。

陸、防火牆(NAT)環境中，建置內外網段不同解析的 DNS Server

在防火牆環境架構中，為了保護內部專用的Server，不至受到無謂的攻擊或騷擾；或是在NAT網路架構中，為了避免同時服務內外部的Server DNS解析不一致的情況下，可以以查詢的來源網段為單位，設定成內外部不同解析表(DNS Table)的DNS Server。當內部網段查詢DNS時，DNS Server就回應內部專用的IP，當外部網段查詢DNS時，DNS Server就回應外部專用的IP；如此，便可避免同時要架設兩台DNS Server的困擾，也可以增進內部網路的安全性。

1. 請下載 <http://ftp.kh.edu.tw/APPL/dns-config/dualview-dns-conf.tar.bz2>，並解壓縮至/var/named/chroot/

```
# wget http://ftp.kh.edu.tw/APPL/dns-config/dualview-dns-conf.tar.bz2
--2014-12-10 15:29:25-- http://ftp.kh.edu.tw/APPL/dns-config/dualview-dns-conf.tar.bz2
正在查找主機 ftp.kh.edu.tw... 163.28.136.5
正在連接 ftp.kh.edu.tw|163.28.136.5|:80... 連上了。
已送出 HTTP 要求，正在等候回應... 200 OK
長度: 10677 (10K) [application/x-bzip2]
Saving to: `dualview-dns-conf.tar.bz2'

100%[=====] 10,677
--.-K/s in 0s

2014-12-10 15:29:25 (366 MB/s) - `dualview-dns-conf.tar.bz2' saved [10677/10677]

# tar jxvf dualview-dns-conf.tar.bz2 -C /var/named/chroot/
./
./etc/
./etc/named.root.hints
./etc/named.zones.master.in
./etc/named.rfc1912.zones
./etc/named.zones.master.out
./etc/named.zones.slave.out
./etc/named.conf
./etc/named.zones.out
./etc/malice.zones
./etc/named.zones.in
./etc/named.caching-nameserver.conf
./etc/named.zones.slave.in
./var/
./var/named/
./var/named/localhost.zone
./var/named/malice.host
./var/named/named.broadcast
./var/named/named.ca
./var/named/localdomain.zone
./var/named/named.ip6.local
./var/named/named.local
./var/named/named.zero
./var/named/data/
./var/named/master/
./var/named/master/named.host.in
./var/named/master/named.host
./var/named/master/named.rev.ipv6
./var/named/master/named.natxxx.rev
./var/named/master/named.rev.in
./var/named/master/named.rev
./var/named/master/named.rev.ipv6.in
./var/named/slaves/

# restorcon -R /var/named/chroot
```

2. 檢查一下/var/named/chroot/etc/named.conf 中 internal、external 兩個 view 引入的正反解設定檔，是否分成兩個不同的設定檔。

```
view "internal"
{
    //內部正反解表設定檔引入
    include "/etc/named.zones.in";
};
view "external"
{
    //外部正反解表設定檔引入
    include "/etc/named.zones.out";
};
```

3. named.zones.in：內部網段專用的 DNS table 設定檔，內含一個 domain 的正解設定及內部幾個網段的反解表設定。

```
//貴單位網域之正查資料設定([domain]字串請換成貴校核定之Domain Name)
zone "[domain].kh.edu.tw"{
    type master;
    file "master/named.host.in";
};

//貴單位IPv4反查資料設定(xxx字串請換成貴校核定網段之第三碼，如核定網段為163.32.36.0，則須表示成36.32.163.in-addr.arpa)
zone "xxx.32.163.in-addr.arpa"{
    type master;
    file "master/named.rev.in";
};

//貴單位內部網段IPv4反查資料設定(xxx字串請換成貴校核定網段之第三碼，如核定網段為192.168.33.0，則須表示成33.168.192.in-addr.arpa)
zone "xxx.168.192.in-addr.arpa"{
    type master;
    file "master/named.natxxx.rev";
};

//貴單位內部網段IPv4反查資料設定(xxx字串請換成貴校核定網段之第三碼，如核定網段為192.168.54.0，則須表示成54.168.192.in-addr.arpa)
zone "xxx.168.192.in-addr.arpa"{
    type master;
    file "master/named.natxxx.rev";
};

//貴單位IPv6反查資料設定(xx字串請換成貴校核定IPv6 /48之最末兩碼，如核定網段為2001:288:8234::/48，則須表示成4.3.2.8.8.2.0.1.0.0.2.ip6.arpa)
zone "x.x.2.8.8.2.0.1.0.0.2.ip6.arpa" {
    type master;
    file "master/named.rev.ipv6.in";
};
```

正查之資料表：(master/named.host.in)

```
$TTL 86400
@      IN      SOA  [domain].kh.edu.tw. root.[domain].kh.edu.tw. (
                        2010101201 ; serial
                        1H ; refresh
                        15 ; retry
                        14D ; expire
                        12H ; Minimum
                        )

@      IN      MX   5      mail.[domain].kh.edu.tw.
@      IN      NS   [domain].kh.edu.tw.
@      IN      NS   dns.[domain].kh.edu.tw.
@      IN      A    163.32.xxx.1
dns     IN      CNAME [domain].kh.edu.tw.
proxy  IN      A    163.32.xxx.2
mail    IN      A    163.32.xxx.3
        IN      AAAA 2001:288:82xx:1::3
        IN      MX   0      mail.[domain].kh.edu.tw.
www     IN      A    163.32.xxx.4
ftp     IN      CNAME www

;; Windows 7/Vista KMS register record
```



```

4.1.0.0      IN    PTR    pdns.[domain].kh.edu.tw.
5.1.0.0      IN    PTR    pdns1.[domain].kh.edu.tw.
1.2.0.0      IN    PTR    mail.[domain].kh.edu.tw.
;
; for 2001:288:82xx:3::/64
$ORIGIN 0.0.0.0.0.0.0.0.0.0.0.0.3.0.0.0.x.x.2.8.8.8.2.0.1.0.0.2.ip6.arpa.
9.0.2.0      IN    PTR    pbx.[domain].kh.edu.tw.

```

4. named.zones.out：供外部網段(含 INTERNET)使用的 DNS table 設定檔，內含一個 domain 的正解設定及對外 IPv4/IPv6 網段的反解表設定。

```

//貴單位網域之正查資料設定([domain]字串請換成貴校核定之Domain Name)
zone "[domain].kh.edu.tw"{
    type master;
    file "master/named.host";
};

//貴單位IPv4反查資料設定(yyy字串請換成貴校核定網段之第三碼，如核定網段為163.32.36.0，則須表示
成36.32.163.in-addr.arpa)
zone "xxx.32.163.in-addr.arpa"{
    type master;
    file "master/named.rev";
};

//貴單位IPv6反查資料設定(xx字串請換成貴校核定IPv6 /48之最末兩碼，如核定網段為
2001:288:8234::/48，則須表示成4.3.2.8.8.8.2.0.1.0.0.2.ip6.arpa)
zone "x.x.2.8.8.8.2.0.1.0.0.2.ip6.arpa" {
    type master;
    file "master/named.rev.ipv6";
};

```

正查之資料表：(master/named.host)

```

$TTL 86400
@      IN    SOA    [domain].kh.edu.tw. root.[domain].kh.edu.tw. (
                2010101201 ; serial
                1H ; refresh
                15 ; retry
                14D ; expire
                12H ; Minimum
                )

@      IN    MX     5      mail.[domain].kh.edu.tw.
@      IN    NS     [domain].kh.edu.tw.
@      IN    NS     dns.[domain].kh.edu.tw.
@      IN    A      163.32.xxx.1
dns     IN    CNAME   [domain].kh.edu.tw.
proxy  IN    A      192.168.xxx.2
mail    IN    A      163.32.xxx.3
        IN    AAAA   2001:288:82xx:1::3
        IN    MX     0      mail.[domain].kh.edu.tw.
www     IN    A      163.32.xxx.4
ftp     IN    CNAME   www

;; Windows 7/Vista KMS register record
;; Windows 7/Vista KMS 啟動方式之服務紀錄，有了這筆紀錄，全市授權之 Windows 7/Vista 企業版便可
找到這筆紀錄後，自動向中心登錄主機啟用 Windows 7/Vitsa 及 office 2010
vlmcs._tcp      IN    SRV     0 0 1688      ap24.kh.edu.tw.

```

IPv4 網段反查之資料表：(master/named.rev)

```

$TTL 86400
@      IN    SOA    [domain].kh.edu.tw. root.[domain].kh.edu.tw. (
                2001101201 ; serial
                1H ; refresh
                15 ; retry
                14D ; expire
                12H ; Minimum
                )

@      IN    NS     [domain].kh.edu.tw.
@      IN    NS     dns.[domain].kh.edu.tw.
1      IN    PTR     [domain].kh.edu.tw.

```

```
2          IN      PTR    proxy.[domain].kh.edu.tw.
3          IN      PTR    mail.[domain].kh.edu.tw.
4          IN      PTR    www.[domain].kh.edu.tw.
; 使用變數作大範圍反解
$GENERATE 60-220 $ PTR    nat???-pc$.[domain].kh.edu.tw.
```

IPv6 網段反查之資料表：(master/named.rev.ipv6)

```
; IPv6 reverse lookup zone for 2001:288:82xx::/48
$TTL 86400
@           IN      SOA   dns.[domain].kh.edu.tw.  root.[domain].kh.edu.tw. (
                        2010102101 ; serial
                        28800 ; refresh
                        7200 ; retry
                        129600 ; expire
                        86400 ; default_ttl
                        )
@           IN      NS    dns.[domain].kh.edu.tw.
;
; for 2001:288:82xx::/48
$ORIGIN x.x.2.8.8.2.0.1.0.0.2.ip6.arpa.
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0          IN      PTR    [domain].kh.edu.tw.
;
; for 2001:288:82xx:1::/64
$ORIGIN 0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.x.x.2.8.8.2.0.1.0.0.2.ip6.arpa.
2.0.0.0            IN      PTR    dns1.[domain].kh.edu.tw.
5.0.0.0            IN      PTR    ftp.[domain].kh.edu.tw.
5.0.0.0            IN      PTR    ftp.ipv6.[domain].kh.edu.tw.
0.1.0.0            IN      PTR    dns2.[domain].kh.edu.tw.
4.1.0.0            IN      PTR    dns.[domain].kh.edu.tw.
;
; for 2001:288:82xx:2::/64
$ORIGIN 0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.0.0.x.x.2.8.8.2.0.1.0.0.2.ip6.arpa.
1.1.0.0            IN      PTR    www.[domain].kh.edu.tw.
1.1.0.0            IN      PTR    www.ipv6.[domain].kh.edu.tw.
2.1.0.0            IN      PTR    kiecc.[domain].kh.edu.tw.
4.1.0.0            IN      PTR    pdns.[domain].kh.edu.tw.
5.1.0.0            IN      PTR    pdns1.[domain].kh.edu.tw.
1.2.0.0            IN      PTR    mail.[domain].kh.edu.tw.
;
; for 2001:288:82xx:3::/64
$ORIGIN 0.0.0.0.0.0.0.0.0.0.0.0.0.3.0.0.0.x.x.2.8.8.2.0.1.0.0.2.ip6.arpa.
9.0.2.0            IN      PTR    pbx.[domain].kh.edu.tw.
```

5. 檢查設定是否正確：

named-checkconf 是用來檢查 named.conf 設定是否正確，若設定正確，則不會有任何訊息

```
[root@ldap named]# named-checkconf -t /var/named/chroot etc/named.conf
```

6. 啟動 DNS 服務：

```
[root@ldap named]# /etc/rc.d/init.d/named start
```

7. 檢查系統之 log 檔，看看 DNS 是否正常執行：

vi /etc/log/messages

```
May 29 09:19:05 localhost named[2612]: starting BIND 9.5.0b2 -u named -t /var/named/chroot
May 29 09:19:05 localhost named[2612]: found 1 CPU, using 1 worker thread
May 29 09:19:05 localhost named[2612]: loading configuration from '/etc/named.conf'
May 29 09:19:05 localhost named[2612]: the working directory is not writable
May 29 09:19:05 localhost named[2612]: listening on IPv4 interface lo, 127.0.0.1#53
May 29 09:19:05 localhost named[2612]: listening on IPv4 interface eth0, 192.168.3.39#53
May 29 09:19:05 localhost named[2612]: default max-cache-size (33554432) applies: view
localhost_resolver
May 29 09:19:05 localhost named[2612]: automatic empty zone: view localhost_resolver: 127.IN-
ADDR.ARPA
May 29 09:19:05 localhost named[2612]: automatic empty zone: view localhost_resolver:
254.169.IN-ADDR.ARPA
May 29 09:19:05 localhost named[2612]: automatic empty zone: view localhost_resolver:
2.0.192.IN-ADDR.ARPA
```

```
May 29 09:19:05 localhost named[2612]: automatic empty zone: view localhost_resolver:
255.255.255.255.IN-ADDR.ARPA
May 29 09:19:05 localhost named[2612]: automatic empty zone: view localhost_resolver:
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.IP6.ARPA
May 29 09:19:05 localhost named[2612]: automatic empty zone: view localhost_resolver:
D.F.IP6.ARPA
May 29 09:19:05 localhost named[2612]: automatic empty zone: view localhost_resolver:
8.E.F.IP6.ARPA
May 29 09:19:05 localhost named[2612]: automatic empty zone: view localhost_resolver:
9.E.F.IP6.ARPA
May 29 09:19:05 localhost named[2612]: automatic empty zone: view localhost_resolver:
A.E.F.IP6.ARPA
May 29 09:19:05 localhost named[2612]: automatic empty zone: view localhost_resolver:
B.E.F.IP6.ARPA
May 29 09:19:05 localhost named[2612]: default max-cache-size (33554432) applies: view internal
May 29 09:19:05 localhost named[2612]: automatic empty zone: view internal: 0.IN-ADDR.ARPA
May 29 09:19:05 localhost named[2612]: automatic empty zone: view internal: 127.IN-ADDR.ARPA
May 29 09:19:05 localhost named[2612]: automatic empty zone: view internal: 254.169.IN-ADDR.ARPA
May 29 09:19:05 localhost named[2612]: automatic empty zone: view internal: 2.0.192.IN-ADDR.ARPA
May 29 09:19:05 localhost named[2612]: automatic empty zone: view internal: 255.255.255.255.IN-
ADDR.ARPA
May 29 09:19:05 localhost named[2612]: automatic empty zone: view internal:
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.IP6.ARPA
May 29 09:19:05 localhost named[2612]: automatic empty zone: view internal:
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.IP6.ARPA
May 29 09:19:05 localhost named[2612]: automatic empty zone: view internal: D.F.IP6.ARPA
May 29 09:19:05 localhost named[2612]: automatic empty zone: view internal: 8.E.F.IP6.ARPA
May 29 09:19:05 localhost named[2612]: automatic empty zone: view internal: 9.E.F.IP6.ARPA
May 29 09:19:05 localhost named[2612]: automatic empty zone: view internal: A.E.F.IP6.ARPA
May 29 09:19:05 localhost named[2612]: automatic empty zone: view internal: B.E.F.IP6.ARPA
May 29 09:19:05 localhost named[2612]: default max-cache-size (33554432) applies: view external
May 29 09:19:05 localhost named[2612]: default max-cache-size (33554432) applies: view tighten-
chaos
May 29 09:19:05 localhost named[2612]: default max-cache-size (33554432) applies: view _bind
May 29 09:19:05 localhost named[2612]: command channel listening on 127.0.0.1#953
May 29 09:19:05 localhost named[2612]: command channel listening on ::1#953
May 29 09:19:05 localhost named[2612]: zone 0.in-addr.arpa/IN/localhost_resolver: NS '0.in-
addr.arpa' has no address records (A or AAAA)
May 29 09:19:05 localhost named[2612]: zone 0.in-addr.arpa/IN/localhost_resolver: loaded serial
0
May 29 09:19:05 localhost named[2612]: zone 1.0.0.127.in-addr.arpa/IN/localhost_resolver: NS
'1.0.0.127.in-addr.arpa' has no address records (A or AAAA)
May 29 09:19:05 localhost named[2612]: zone 1.0.0.127.in-addr.arpa/IN/localhost_resolver: loaded
serial 0
May 29 09:19:05 localhost named[2612]: zone
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa/IN/localhost_resolver:
NS '1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa' has no address
records (A or AAAA)
May 29 09:19:05 localhost named[2612]: zone
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa/IN/localhost_resolver:
loaded serial 0
May 29 09:19:05 localhost named[2612]: zone localhost.localdomain/IN/localhost_resolver: loaded
serial 0
May 29 09:19:05 localhost named[2612]: zone localhost/IN/localhost_resolver: loaded serial 0
May 29 09:19:05 localhost named[2612]: zone 225.32.163.in-addr.arpa/IN/internal: loaded serial
2003120301
May 29 09:19:05 localhost named[2612]: zone 100.168.192.in-addr.arpa/IN/internal: loaded serial
2007103102
May 29 09:19:05 localhost named[2612]: zone 101.168.192.in-addr.arpa/IN/internal: loaded serial
2002040801
May 29 09:19:05 localhost named[2612]: zone hmes.kh.edu.tw/IN/internal: NS 'hmes.kh.edu.tw' has
no address records (A or AAAA)
May 29 09:19:05 localhost named[2612]: zone hmes.kh.edu.tw/IN/internal: loaded serial 2007103101
May 29 09:19:05 localhost named[2612]: zone 225.32.163.in-addr.arpa/IN/external: loaded serial
2003120301
May 29 09:19:05 localhost named[2612]: zone hmes.kh.edu.tw/IN/external: NS 'dns.hmes.kh.edu.tw'
is a CNAME (illegal)
May 29 09:19:05 localhost named[2612]: zone hmes.kh.edu.tw/IN/external: loaded serial 2007011001
May 29 09:19:05 localhost named[2612]: zone bind/CH/tighten-chaos: loaded serial 1
May 29 09:19:05 localhost named[2612]: running
May 29 09:19:05 localhost named[2612]: zone hmes.kh.edu.tw/IN/internal: sending notifies (serial
2007103101)
May 29 09:19:05 localhost named[2612]: zone 225.32.163.in-addr.arpa/IN/internal: sending
notifies (serial 2003120301)
May 29 09:19:05 localhost named[2612]: zone 100.168.192.in-addr.arpa/IN/internal: sending
notifies (serial 2007103102)
May 29 09:19:05 localhost named[2612]: zone 101.168.192.in-addr.arpa/IN/internal: sending
notifies (serial 2002040801)
```

```
May 29 09:19:05 localhost named[2612]: zone hmes.kh.edu.tw/IN/external: sending notifies (serial 2007011001)
May 29 09:19:05 localhost named[2612]: zone 225.32.163.in-addr.arpa/IN/external: sending notifies (serial 2003120301)
```

DNS Server 成功啟動。

8. 若以上一切正常，則恭喜您，您已完成外網段不同解析的 DNS Server 的設定了。

柒、測試 DNS 系統

1. 啟動 DNS 服務：

```
/etc/rc.d/init.d/named start
```

2. 停止 DNS 服務：

```
/etc/rc.d/init.d/named stop
```

3. 設定/etc/resolv.conf檔，增加這台 DNS Server 的描述：

```
nameserver 163.32.???.1
```

4. 利用 dig 命令測試 DNS table 是否正確無誤：

```
dig [@server] [-b address] [-c class] [-f filename] [-k filename] [-m] [-p port#] [-t type] [-x addr] [-y name:key] [-4] [-6] [name] [type] [class] [queryopt...]
```

a	T_A	network address
any	T_ANY	all/any information about specified domain
mx	T_MX	mail exchanger for the domain
ns	T_NS	name servers
soa	T_SOA	zone of authority record
hinfo	T_HINFO	host information
axfr	T_AXFR	zone transfer (must ask an authoritative server)
txt	T_TXT	arbitrary number of strings

```
# dig @dns.hmes.kh.edu.tw mail.hmes.kh.edu.tw a

; <<>> DiG 9.3.6-P1-RedHat-9.3.6-4.P1.el5_4.2 <<>> @dns.hmes.kh.edu.tw mail.hmes.kh.edu.tw a
; (2 servers found)
;; global options: printcmd
;; Got answer:
;; -->HEADER<<- opcode: QUERY, status: NOERROR, id: 33991
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;mail.hmes.kh.edu.tw.      IN      A

;; ANSWER SECTION:
mail.hmes.kh.edu.tw.      86400   IN      A      163.32.225.4

;; AUTHORITY SECTION:
hmes.kh.edu.tw.           86400   IN      NS      dns.hmes.kh.edu.tw.
hmes.kh.edu.tw.           86400   IN      NS      hmes.kh.edu.tw.

;; ADDITIONAL SECTION:
hmes.kh.edu.tw.           86400   IN      A      163.32.225.1
hmes.kh.edu.tw.           86400   IN      AAAA    2001:288:829f:1::1

;; Query time: 2 msec
;; SERVER: 2001:288:829f:1::1#53(2001:288:829f:1::1)
;; WHEN: Wed Oct 6 22:23:24 2010
;; MSG SIZE rcvd: 129

# dig @dns.hmes.kh.edu.tw mail.hmes.kh.edu.tw aaaa

; <<>> DiG 9.3.6-P1-RedHat-9.3.6-4.P1.el5_4.2 <<>> @dns.hmes.kh.edu.tw mail.hmes.kh.edu.tw aaaa
; (2 servers found)
```

```

;; global options: printcmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 54522
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;mail.hmes.kh.edu.tw.          IN      AAAA

;; ANSWER SECTION:
mail.hmes.kh.edu.tw.  86400   IN      AAAA    2001:288:829f:1::4

;; AUTHORITY SECTION:
hmes.kh.edu.tw.       86400   IN      NS       hmes.kh.edu.tw.
hmes.kh.edu.tw.       86400   IN      NS       dns.hmes.kh.edu.tw.

;; ADDITIONAL SECTION:
hmes.kh.edu.tw.       86400   IN      A        163.32.225.1
hmes.kh.edu.tw.       86400   IN      AAAA    2001:288:829f:1::1

;; Query time: 2 msec
;; SERVER: 2001:288:829f:1::1#53(2001:288:829f:1::1)
;; WHEN: Wed Oct 6 22:29:43 2010
;; MSG SIZE rcvd: 141

# dig @dns.hmes.kh.edu.tw hmes.kh.edu.tw axfr

; <<>> DiG 9.3.6-P1-RedHat-9.3.6-4.P1.el5_4.2 <<>> @dns.hmes.kh.edu.tw hmes.kh.edu.tw axfr
; (2 servers found)
;; global options: printcmd
hmes.kh.edu.tw.      86400   IN      SOA      hmes.kh.edu.tw. root.hmes.kh.edu.tw. 2010042102
28800 14400 3600000 86400
hmes.kh.edu.tw.      86400   IN      NS       dns.hmes.kh.edu.tw.
hmes.kh.edu.tw.      86400   IN      NS       hmes.kh.edu.tw.
hmes.kh.edu.tw.      86400   IN      MX       5 mail.hmes.kh.edu.tw.
hmes.kh.edu.tw.      86400   IN      A        163.32.225.1
hmes.kh.edu.tw.      86400   IN      AAAA    2001:288:829f:1::1
admin.hmes.kh.edu.tw. 86400   IN      A        163.32.225.5
bbs.hmes.kh.edu.tw.  86400   IN      CNAME    hmes.kh.edu.tw.
blog.hmes.kh.edu.tw. 86400   IN      A        163.32.225.6
blog.hmes.kh.edu.tw. 86400   IN      AAAA    2001:288:829f:5::6
chat.hmes.kh.edu.tw. 86400   IN      CNAME    sql.hmes.kh.edu.tw.
dns.hmes.kh.edu.tw.  86400   IN      CNAME    hmes.kh.edu.tw.
docs.hmes.kh.edu.tw. 86400   IN      A        163.32.225.81
ftp.hmes.kh.edu.tw.  86400   IN      CNAME    mail.hmes.kh.edu.tw.
impmail.hmes.kh.edu.tw. 86400   IN      CNAME    mail.hmes.kh.edu.tw.
jonasvr.hmes.kh.edu.tw. 86400   IN      A        163.32.225.82
mail.hmes.kh.edu.tw. 86400   IN      MX       0 mail.hmes.kh.edu.tw.
mail.hmes.kh.edu.tw. 86400   IN      A        163.32.225.4
mail.hmes.kh.edu.tw. 86400   IN      AAAA    2001:288:829f:1::4
manager.hmes.kh.edu.tw. 86400   IN      A        163.32.225.3
mrtg.hmes.kh.edu.tw. 86400   IN      CNAME    hmes.kh.edu.tw.
ms.hmes.kh.edu.tw.   86400   IN      A        163.16.8.100
mysql.hmes.kh.edu.tw. 86400   IN      CNAME    sql.hmes.kh.edu.tw.
proxy.hmes.kh.edu.tw. 86400   IN      A        163.32.225.2
router.hmes.kh.edu.tw. 86400   IN      A        163.32.225.254
smail.hmes.kh.edu.tw. 86400   IN      CNAME    student.hmes.kh.edu.tw.
sql.hmes.kh.edu.tw.  86400   IN      A        163.32.225.15
sql.hmes.kh.edu.tw.  86400   IN      AAAA    2001:288:829f:5::15
student.hmes.kh.edu.tw. 86400   IN      A        163.32.225.7
student.hmes.kh.edu.tw. 86400   IN      AAAA    2001:288:829f:5::7
stumail.hmes.kh.edu.tw. 86400   IN      CNAME    student.hmes.kh.edu.tw.
vdn.hmes.kh.edu.tw.  86400   IN      A        163.32.225.2
web.hmes.kh.edu.tw.  86400   IN      A        163.32.225.14
work.hmes.kh.edu.tw. 86400   IN      CNAME    mail.hmes.kh.edu.tw.

```

```

www.hmes.kh.edu.tw.      86400   IN      CNAME   mail.hmes.kh.edu.tw.
x-world.hmes.kh.edu.tw. 86400   IN      A       192.192.128.6
hmes.kh.edu.tw.         86400   IN      SOA     hmes.kh.edu.tw. root.hmes.kh.edu.tw. 2010042102
28800 14400 3600000 86400
;; Query time: 11 msec
;; SERVER: 2001:288:829f:1::1#53(2001:288:829f:1::1)
;; WHEN: Wed Oct 6 22:19:20 2010
;; XFR size: 37 records (messages 1)

```

5. 利用 nslookup 命令：

```

# nslookup
Default Server: hmes.kh.edu.tw
Address: 163.32.225.1

> help
$Id: nslookup.help,v 8.5 2000/03/30 23:25:35 vixie Exp $

Commands:      (identifiers are shown in uppercase, [] means optional)
NAME           - print info about the host/domain NAME using default server
NAME1 NAME2    - as above, but use NAME2 as server
help or ?      - print info on common commands; see nslookup(1) for details
set OPTION     - set an option
    all         - print options, current server and host
    [no]debug   - print debugging information
    [no]d2      - print exhaustive debugging information
    [no]defname - append domain name to each query
    [no]recurse - ask for recursive answer to query
    [no]vc      - always use a virtual circuit
    domain=NAME - set default domain name to NAME
    srchlist=N1[/N2/.../N6] - set domain to N1 and search list to N1,N2, etc.
    root=NAME   - set root server to NAME
    retry=X     - set number of retries to X
    timeout=X   - set initial time-out interval to X seconds
    querytype=X - set query type, e.g., A,ANY,CNAME,HINFO,MX,PX,NS,PTR,SOA,TXT,WKS,SRV,NAPTR
    port=X      - set port number to send query on
    type=X      - synonym for querytype
    class=X     - set query class to one of IN (Internet), CHAOS, HESIOD or ANY
server NAME    - set default server to NAME, using current default server
lserver NAME   - set default server to NAME, using initial server
finger [USER]  - finger the optional USER at the current default host
root           - set current default server to the root
ls [opt] DOMAIN [> FILE] - list addresses in DOMAIN (optional: output to FILE)
    -a         - list canonical names and aliases
    -h         - list HINFO (CPU type and operating system)
    -s         - list well-known services
    -d         - list all records
    -t TYPE    - list records of the given type (e.g., A,CNAME,MX, etc.)
exit           - exit the program, ^D also exits

> www.hmes.kh.edu.tw
Server: hmes.kh.edu.tw
Address: 163.32.225.1

Name: mail.hmes.kh.edu.tw
Address: 163.32.225.4
Aliases: www.hmes.kh.edu.tw

Name: mail.hmes.kh.edu.tw
Address: 163.32.225.4
Aliases: www.hmes.kh.edu.tw

> www.kh.edu.tw

```

```
Server: hmes.kh.edu.tw  
Address: 163.18.225.1
```

```
Non-authoritative answer:  
Name: www.kh.edu.tw  
Address: 163.32.250.11
```

```
> www.kh.edu.tw
```

```
Server: 163.18.250.14  
Address: 163.18.250.14#53
```

```
Name: www.kh.edu.tw  
Address: 163.32.250.11
```

```
> 163.28.136.13
```

```
Server: 163.18.250.14  
Address: 163.18.250.14#53
```

```
13.136.28.163.in-addr.arpa name = proxy13.kh.edu.tw.
```


柒、DNS 記錄的更新與維護

在日常的維護與管理中，Server 及服務會隨著時間逐漸增加而有所變動或增加，這時就會去更新 DNS 的記錄了。DNS 記錄的更動，管理者常常會忽略了幾個小地方，而導致外界其他的 DNS Server 都不知道您的記錄更新了，而一直沿用 **cache** 在自己 DNS 上的記錄，造成不同步的結果。因此，一般更新 DNS 記錄的程序如下：

1. 更動 DNS 記錄時，要記得正解及反解表均同時要更動；常常有人記得改正解表，卻忘了改反解表。
2. 更改正解表及反解表的狀況是一樣的，在此我們以修改正解表為例。
3. 開啟自己 domain 的正解表：(/var/named/chroot/var/named/named.host)

```
$TTL      86400
@         IN      SOA    [domain].kh.edu.tw. root.[domain].kh.edu.tw. (
                2001101201 ; serial
                1H ; refresh
                15 ; retry
                14D ; expire
                12H ; Minimum
        )

@         IN      MX     5      mail.[domain].kh.edu.tw.
@         IN      NS     [domain].kh.edu.tw.
@         IN      NS     dns.[domain].kh.edu.tw.
@         IN      A      163.32.???1
dns       IN      CNAME   [domain].kh.edu.tw.
proxy    IN      A      163.32.???2
mail     IN      A      163.32.???3
         IN      MX     0      mail.[domain].kh.edu.tw.
www      IN      A      163.32.???4
ftp      IN      CNAME   www
```

4. 首先，記得先更改正解表的版本序號(serial)

```
2004111201 ; serial
```

說明：因為 bind 9 的版本序最多可以有 10 個數字組成，一般的習慣，我們會設成日期序號。(西元記元 4 碼+月 2 碼+日 2 碼+2 碼版次號碼，只 10 碼)

5. 再來才是更動主機名稱與 IP 的記錄。
6. 完成後，記得存檔。
7. 記得也要更改反解表。
8. 最後記得要重新啟動 DNS 服務或重新載入新的 DNS 記錄。

重新載入 DNS 記錄

```
[root@ldap named]# /etc/init.d/named reload
```

重新啟動 DNS 服務

```
[root@ldap named]# /etc/init.d/named restart
```

9. 查看一下系統記錄檔，沒問題的話，就是更新記錄成功了！

參考資料：

1. 高健智、賴阿福（民 90）。隨裝即用 Linux7 中文版。知城數位。
2. http://www.study-area.net/linux/servers/linux_dns.htm。
3. <http://www.isc.org/downloads/bind/doc/bind-9-8/>。