# 網域名稱伺服系統 (DNS) 規劃與建置

交 通 大 學 計 算 機 中 心
陳 昌 盛

# 1999 TANet DNS Tutorial Course

# 0. 從何處获得DNS 系統旳相關資訊？

- DNS Resource Directory

- ://dnsrd.nctu.edu.tw ( 中文)
- the O'Reilly DNS bible 'DNS and BIND'
- 第 3 版已出書, 有介紹 BIND 8.x
- DNS related RFC ( Request For Comments )
- RFC 1033, 1034, 1035, ..., 1912, ...
- Newsgroups:
- '' ( 行政管理)
- p.protocols.dns.* ( 技術)

# 1. DNS 入門

(1.0) 什麼時候會用到 DNS 系統？

往外連線時 (out-going 連線)

存取檢查, 系統記錄 (in　ing 連線)

(1.1) DNS 系統的做用

定義網域名稱

提供網域名稱查詢

(1.2) DNS 實務操作及應用

# 1.1.1 定義網域名稱

- **網域授權 (domain zone -> NS RR)**
- **網域名稱 ( domain name -> A RR)**
- **電子郵件交換 ( mail exchange -> MX RR)**
- **網址對應 (pointer -> PTR RR)**
- **常用別名 (alias naming -> AME RR)**
- **其他功能**

# 網域名稱系統(Domain Name System)

- 網域名稱系統, 按英文常簡稱 DNS 系統.
- DNS 系統, 概提成三個部份
- 網域空間 (Domain Name Space )
- 網域名稱伺服系統 (Domain Name Server)
- BIND/named, ...
- 網域名稱解譯程式 (Domain Name Resolver)
- DNS  client, agent,  server

# 網域空間(Domain Name Space)

- **分散式 與 階層式 旳組織架構**
- **tree-structure vs. DAG-structure**
- **地理區域 與 功能組織 旳分類組合方式**
- **正解網域 (forward domain zones):**
- **‘tw’, ‘edu.tw’, ...**
- **反解網域 (reverse domain zones):**
- **‘113.140.in-addr.arpa’, ‘1.113.140.in-addr.arpa.’, ...**

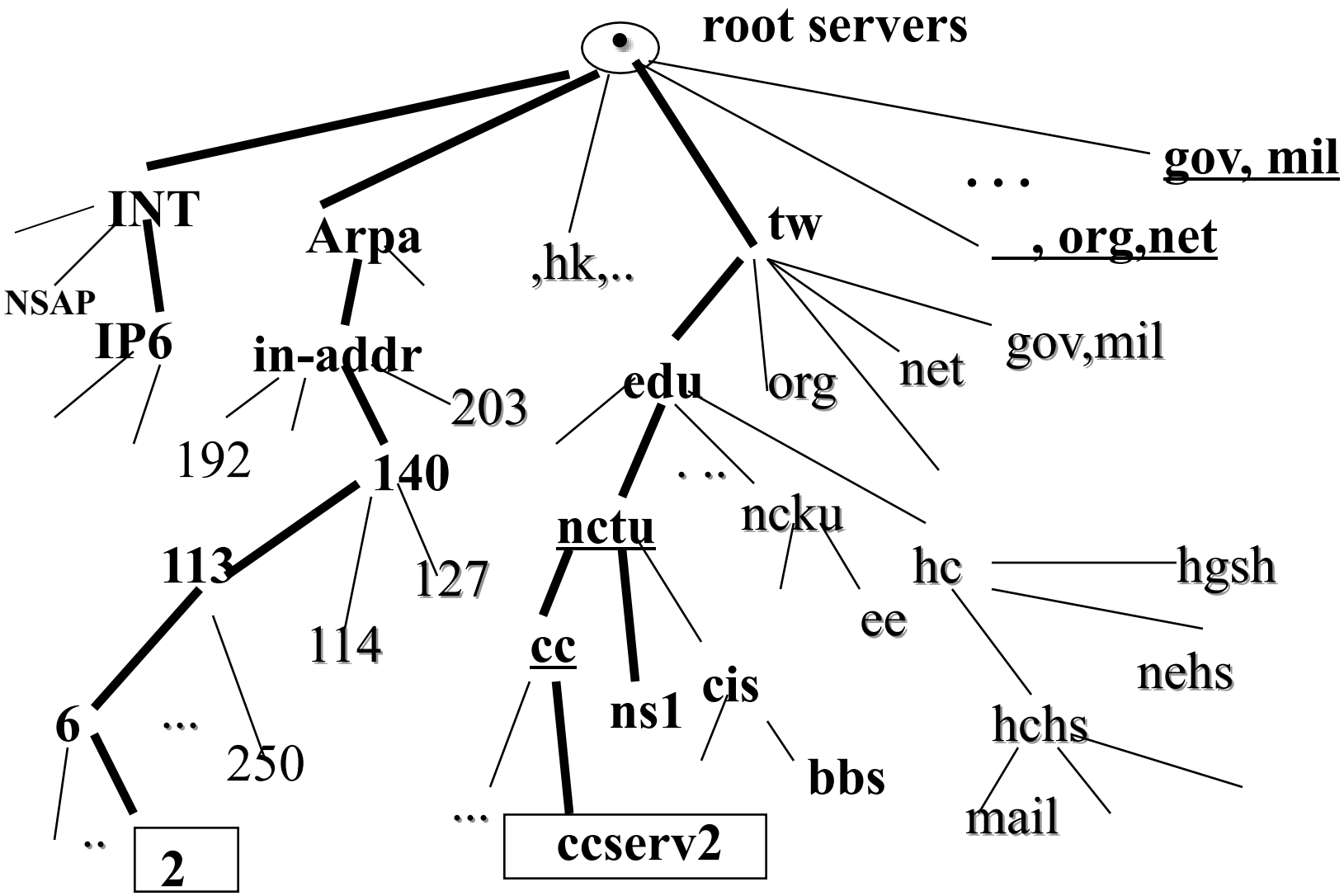


**Fig.1 DNS 運作基本架構圖**

# 1.1.2 DNS - 提供查詢

- DNS 相關程式
  - client(用戶端), agent(代理查詢), server(伺服器)
- **DNS 查詢 (query)**
  - **iterative mode (往復式 ; referral)**
  - **recursive mode (遞迴式 )**
- DNS server (伺服系統)
  - primary/master (原始資料 server) vs secondary/slave
  - caching, forwarder (查詢轉送)
- DNS caching
  - Time-To-Live (TTL; 資料有效期限)
  - positive caching(正確資料) vs negative caching

# DNS - 提供網路查詢(續)

- 資料項 round-robin mode (輪流)
- load sharing/balancing
  - round-trip-time ( RTT; 來回傳送時間)
- **reverse** pointer query (IP addr. 反解查詢)
  - **inverse** query ( 廣義反向查詢)

# 1.2 DNS 實務操作及應用

- Domain Zone 的註冊與授權
- forward / reverse domain zones
- Primary/master; Secondary/slave DNS server
- DNS 上轻易有錯誤觀念與設定的地方
- 電子郵件轉接轉送(Mail Relay)服務
- Anti-SPAM checking ( access control)
- 正反解 DNS 資料項, 必須匹配
- DNS 查詢轉送 (forwarders; 參見 3.2.2 )

# 1.2.1 正解 Domain Zone 註冊問題

- nctu.edu.tw ( 到 MOECC 登記)
- csie.nctu.edu.tw ( 到 NCTU-CC 登記)
- ck.tp.edu.tw (臺北建國高中)
  - 直接由 MOECC 負責 (edu.tw)
- thps.hc.edu.tw ( 新竹市載熙國小)
  - hc.edu.tw 目前由新竹區域網路中心負責

# 1.2.2 反解 Domain Zone 註冊問題

- 140.113 ( Class B; 透過 MOECC 向 InterNIC 註冊)
- 140.126.3 ( 由 class B 分割; 到區域網路中心註冊)
  - 140.126 (Class B; 透過 MOECC 向 InterNIC 註冊)
- 192.83.166 ( 個別 class C )
  - 透過 MOECC 到 InterNIC 註冊)
- 203.68.12 ( class C; 到 MOECC 註冊)
  - 203.68 ( 整批 class C 到 APNIC 註冊)

# 1.2.3 DNS server 的網址選定

```
$Origin     NCTU.edu.tw.
@       IN      NS      ns.nctu.edu.tw.
        IN      NS      ns1.nctu.edu.tw.
        IN      NS      ns2.nctu.edu.tw.
        IN      NS      ns3.nctu.edu.tw. ; TANet 骨幹
;

ns1     IN      A       140.113.1.1     ; 指定

ns3     IN      A       163.28.64.246   ; 高速專用道
```

# 1.2.4 轻易有錯誤觀念與設定的地方

$Origin NCTU.edu.tw.

**nctu.edu.tw.** IN **NS** ns.nctu.edu.tw.

; ***domain zone*** ==> ***dig***

**nctu.edu.tw.** 7200 IN **A**

; ***domain name*** ==> ***telnet***

**nctu.edu.tw.** IN **MX** 0 ns1.nctu.edu.tw.

; ***mail exchange*** ==> ***E-mail***

;----------

**nctu.edu.tw.** IN NS **nctu.edu.tw.**

# 1.2.5 Mail Relay 的相關設定

- DNS side :
- ; e-mail 最終目的地
- .  IN  MX  10  ccserv6.cc.nctu.edu.tw.
- ; mail relay ==> 宜善加运用, 可作為“備援與轉接”之用
- cc.nctu.edu.tw.  IN  MX  20  mx.nctu.edu.tw.
- ; 高速專用道 (MOECC)
- cc.nctu.edu.tw.  IN  MX  30

# 1.2.6 Anti-SPAM checking (DNS entry 正反解必須匹配)

- domain name 驗證流程.
- reverse
  forward
- IP addr. A ---------> domain name B ---------> IP addr. C
- Fig. 2 anti-SPAM checking 圖示
- 其中, IP addr. C (也许是一個 group), 必須包括或等於 A 才算通過 DNS 查驗.

# DNS 系統新設計的功能 (部份已完毕實作)

- New DNS RR (rfc 1183)
  - RP, AFSDB, ISDN, X25, RT
- resolver implicit search problem (rfc 1535)
- LOC (rfc 1876)
- IPv6 ( rfc 1886)
  - **AAAA** (new record type), **IP6.INT** (new domain top )
- incremental zone transfer IXFR ( rfc 1995 )
- DNS notify (rfc 1996) -> BIND_NOTIFY
- SRV (rfc 2052)
- Secure Zone
- Dynamic update ( IP/host )

# 2. DNS Server Hosts 配置與規劃

- 主機系統選擇 ( platform/OS )
- Unix , Windows NT, OS/2, ... ( 現階段, 仍以 Unix 為佳 )
- 硬體設備需求
- 重要 memory size, 原則是 named 將 90% 以上的 dns query 放在 RAM 中 caching 起來, 不需用到 swap.
- 系統軟體 ( BIND/named, ... )
- 網路位址 (多重 servers)
- primary/secondary server host 分離, 放在不一樣的網路區段, 當然假如能放在不一樣單位, 一般更好.

# 2.1 關於 BIND 的許多資訊

- 目前最新版本  8.2-P1 (1999.03.16)
- 4.9.7 ( 舊式 ); BIND 8.x ( 新式)
- 怎樣得知系統上的 named 版本 ?

- 有沒有 Windows 下的版本 ?
- 不一樣版本 BIND 之間功能差別 ?

# BIND ( Berkeley Internet Name Domain )

- Standalone Daemon ( named )
- UDP/TCP port 53
  - UDP query/response ( < 512 bytes )
  - TCP response(>512 bytes) + zone transfer
- DNS message format
  - **Question/Answer** section
  - **Authority** section
  - **Additional** section
    - example --> dig output

# 2.1.1 怎样得知系統上旳 named 版本 ?

- 一般可以這麼作.
- 1) 確定 named program 旳 pathname.
- e.g. /etc/named, /usr/sbin/in.named, ...
- 作法: 使用 which, find, ...

- -- 2) 用 what 配合 grep 找出相關字串
- % what /usr/sbin/named | grep named
- named:

# 2.1.2 不一样版本 BIND 之間功能的差別 ?

- V8.x 整套程式 , 重新改寫
- /etc/named.boot (v4) -> /etc/named.conf ( v8)
- zone transfer ( named vs named-xfer )
- no more fork for each AFXR jobs
- ( for v 8.1.X and later )
- BIND 與先前版本的重大差異
- 新的功能
- negative caching
- bind_notify, IPv6 support, RFC 1535 pliant, ...

# 2.1.3 從何處获得 BIND 原始程式?

- BIND home at  the ISC
  - ftp://ftp.isc.org/isc/bind/*
- NCTUCCCA & mirror sites
  - packages/networking/bind/*

# 2.2 BIND V8.x/4.9.x 程式的安裝

- BIND 4.9.x piling & installation
- $bind-src/README, OPTIONS
- $bind-src/conf/options.h
- check and/or update /etc/named.boot
- BIND 8.x piling & instatllation
- $bind-src/INSTALL, README
- $bind-src/port/README
- check and/or update /etc/named.conf
- DNS syslogging
- /etc/syslog.conf
- /var/adm/messages

# 3. DNS 設定範例與說明

- BIND server options
- /etc/named.boot 設定範例
- /etc/named.conf (V8.x)
- 自動轉換程式 named-bootconf.pl
- zone data files 設定範例
- /etc/resolv.conf ( resolver) 設定範例
- 參見 ://dnsrd.nctu.edu.tw 上的範例

# 3.1 DNS Server Options

- primary/master vs. secondary/slave
- caching only server
- forwarders ( slave server)
- recursive vs. non-recursive

“

# 3.2 DNS Server Options -- /etc/named.boot (v4.x)

```
; type          domain                                  source file or host
;-------------------------------------------------------------------------------
directory       /var/named
;
cache                 .                                       named.root
;
primary         localhost                                     Localhost
primary         .IN-ADDR.ARPA                 Rev-127.0
;  [ 省略 ]
primary         NCTU.edu.tw                                   Zone.NCTU
secondary       ADM.nctu.edu.tw          140.113.2.1          Zone.ADM
primary         CC.nctu.edu.tw                                Zone.CC
;   [ 省略 ]          .          .          .
primary         113.140.IN-ADDR.ARPA                          R-140.113
primary
secondary       .in-addr.arpa.
```

# DNS Server Options ( 續)
# -- /etc/named.conf (新版; v8.x)

```
options {
        check-names master fail;  check-names slave fail; //  default warn
        directory "/var/named";
        fake-iquery yes;        //  default warn
        forwarders { 163.28.1.103; 139.175.55.244; };
};
zone "." { type hint;  file "named.root"; };   // cache            root.cache
zone "localhost" { type master;  file "Localhost" };
zone "0.0.127.IN-ADDR.ARPA" { type master; file "Rev-127.0"};
zone "" {
         type slave;  file "sec/zone-HC.edu.tw";
         masters {140.113.250.135; };      };
zone "" {
        type slave;   file "sec/R-140.126.237";
        masters {140.113.250.135;};        };
```

# 3.2.1 Caching Only Server -- /etc/named.boot

```
directory       /var/named
;
cache                .                                  named.root
;
; BIND 4.9.x & later
check-names     primary         fail    ; default fail
check-names     secondary       fail    ; default warn
;check-names    response        fail    ; default ignore
; [ 省略 ]
primary         localhost                          Localhost
primary         .IN-ADDR.ARPA                  Rev-127.0
primary         0.IN-ADDR.ARPA                 Rev-0
primary         255.IN-ADDR.ARPA                       Rev-255
; [ 省略]
options         fake-iquery
;
```

# 3.2.2 DNS Server Options (2) - /etc/named.boot

```
directory       /var/named
;
cache                .                          named.root
;
    [ 省略]]

; 設定 DNS forwarders, 以轉送 DNS query ( 末端網路節點適用 )
;-------------------------------------------------------------------------
forwarders      140.113.1.1
;
; options       forward-only

;
bogusns         203.74.66.1
```

# 3.2.3 DNS Server Options (3) - /etc/named.boot

**directory** /var/named
;
**cache** **.** named.root
;
**.** **.[ 省略 ]**

**options** **fake-iquery**
; options **non-recursion**
**;** options **forwarder-only**
**;** options **query-log**

# 3.3 Domain Zone files 設定

- **Basic DNS Resource Record Types**
- **SOA, NS, A, PTR,　AME, MX**
- **TXT, WKS, HINFO**
- **RP, AFSDB, AAAA ( IPv6) , LOC, SRV, ...**

# 3.3.1 Special Symbols on DNS database

- **Special Symbols for defining the DNS database**
- **“@”,  current origin**
- **“*,” wildcard ( only for some of the types )**
- **“ . ” , root domain & domain separator**
- **“ ; ” , for  ment lines**
- **“( )”, grouping data which crossing a line**
- **--> only work for SOA RR (now)**
- **“\X”,  --> escape character ;  “\@”**
- **“\DDD”, octal number ; ->  “\345”**

# 3.3.2 SOA ( Start Of Authority ) RR

- **;;** for forward/reverse **Domain Zones**.
- **;;**----------
  ----------
- **@** IN **SOA** **ns.NCTU.edu.tw.** **hostmaster..** **(**
- 1997090200 **; Serial number**
- 86400 ; **Refresh** - 1 days
- 1800 ; **Retry**
- 1728000 ; **Expire** - 20 days
- 259200 **)** ; **Minimum TTL** - 3 days
- ;;----------
  ----------
- IN **NS** NCTU.edu.tw.
- IN **NS** **ns.NCTU.edu.tw.** **; primary / master**
- IN **NS** ns2.nctu.edu.tw.
- ;
- **localhosts.** IN **A** ; **forward** case
- ;; 1 IN **PTR** **localhost.** ; **reverse** case

# 3.3.3 Domain Zone delegation (授權) -- NS (Name Server) RR

```
; forward domain zones (正解)
;-------------------------------------------------------------
;  上下兩層 “NCTU.edu.tw” & “CSIE.NCTU.edu.tw” 的
    設定檔,
;  都應該有對應的 Name Server 記錄項目 ( NS RR )
;-------------------------------------------------------------
$ORIGIN        CSIE.NCTU.edu.tw.
@              IN     NS     .     ; FQDN
               IN     NS     operator
               IN     NS     ccsun7                ; hostname
;; Glued Records
.          IN     A
                          IN     A
operator                  IN     A
ccsun7                    IN     A
```