Contents

[hide]

目的

- 瞭解 host name 的資源 and its 影響 on networked systems organization
- 使用通用的工具，探索和驗證 DNS server operation
- 描述 Domain Name System (DNS)
- 設置一台 BIND DNS configuration
- DHCP Overview
- DHCP Configuration

Host Name Resolution

主機名稱解析

- 一些命名服務提供機制翻譯主機名稱方便電腦可溝通

1. Example: Name --> MAC address (link layer)
2. Example: Name --> IP address (network layer) --> MAC address (link layer)

- 通用的檔案名稱服務

1. Files (/etc/hosts and /etc/networks)
2. DNS

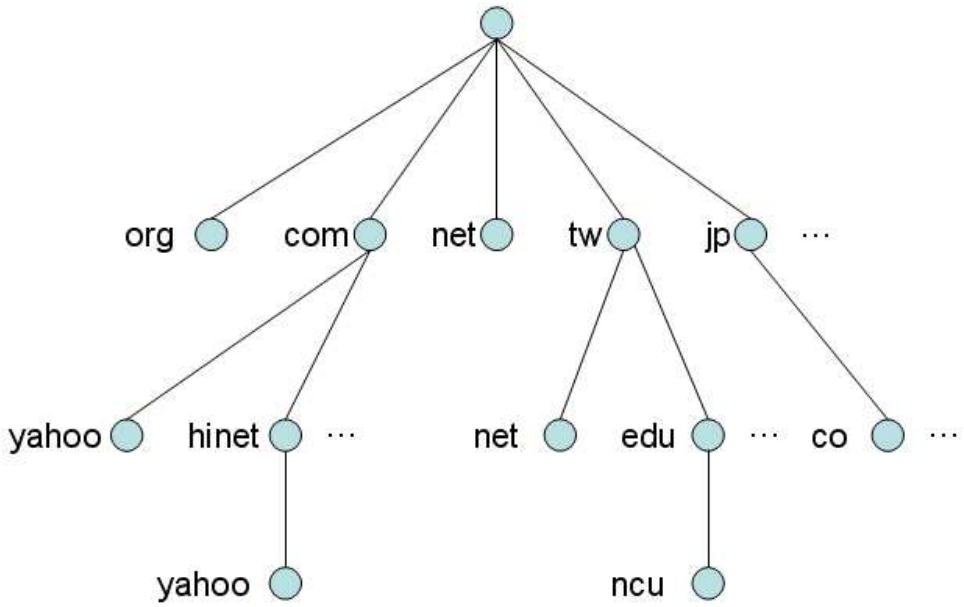
3. NIS

- 多客戶端的解析: "stub"

1. dig
2. host
3. nslookup

- FQDN(Fully Qualified Domain Name)是由「主機名稱」與「網域名稱所組成」
- DNS 有分為正解(forward) 及反解(reverse)。

1. 正解就是把Domain Name 轉成IP
2. 反解是將IP 轉成Domain Name。



The Stub Resolver

- 產生反解(resolver) 的資料庫提供給所有的應用程式使用

1. 透過 gethostbyname() 何其他的 glibc functions 存取

2. 沒有復雜能力的存取控制 access controls, 像是信號及加密的行為
3. 能查詢任何支援 glibc 的 name service

- 讀取 /etc/nsswitch.conf 來決定查詢 name services 的順序，通常順序是 hosts: files dns
- The NIS domain name and the DNS domain name should usually be different 避免命名碰撞。

DNS-Specific Resolvers

- host

1. 不會讀取 /etc/nsswitch.conf
2. 預設以 /etc/resolv.conf 的 nameserver 為查詢 server
3. 最小輸出畫面

- dig

1. 不會讀取 /etc/nsswitch.conf
2. 預設以 /etc/resolv.conf 的 nameserver 為查詢 server
3. 輸出以 RFC-standard zone 的檔案格式, 這個檔案格式可以使用在 DNS servers

- host

```
[root@server1 ~]# host www.gov.tw
www.gov.tw has address 163.29.3.40
www.gov.tw mail is handled by 10 163.29.129.70.
[root@server1 ~]# host 163.29.3.40
Host 40.3.29.163.in-addr.arpa not found: 3(NXDOMAIN)
```

- dig

```
[root@server1 ~]# dig www.gov.tw

; <<>> DiG 9.3.3rc2 <<>> www.gov.tw
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29556
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;www.gov.tw.                    IN      A

;; ANSWER SECTION:
www.gov.tw.             9779    IN      A       163.29.3.40

;; AUTHORITY SECTION:
www.gov.tw.             846     IN      NS      ns1.www.gov.tw.
www.gov.tw.             846     IN      NS      ns2.www.gov.tw.

;; ADDITIONAL SECTION:
ns1.www.gov.tw.         9779    IN      A       211.79.170.24
ns2.www.gov.tw.         9779    IN      A       211.79.170.25

;; Query time: 4 msec
;; SERVER: 140.117.11.1#53(140.117.11.1)
;; WHEN: Sat Mar 22 06:18:13 2008
;; MSG SIZE  rcvd: 112
[root@server1 ~]# dig 163.29.3.40

; <<>> DiG 9.3.3rc2 <<>> 163.29.3.40
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 7189
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;163.29.3.40.                   IN      A

;; AUTHORITY SECTION:
```

```
.                       10800   IN      SOA     A.ROOT-SERVERS.NET.
NSTLD.VERISIGN-GRS.COM. 2008032001 1800 900 604800 86400

;; Query time: 128 msec
;; SERVER: 140.117.11.1#53(140.117.11.1)
;; WHEN: Sat Mar 22 06:18:39 2008
;; MSG SIZE  rcvd: 104
```

- host 指定 dns server 的用法

```
[root@sc220469 etc]# host station10.example.com 140.117.69.219
Using domain server:
Name: 140.117.69.219
Address: 140.117.69.219#53
Aliases:


station10.example.com has address 192.168.0.10
```

- dig 指定 dns server 的用法

```
[root@sc220469 etc]# dig station10.example.com @140.117.69.219

; <<>> DiG 9.3.6-P1-RedHat-9.3.6-4.P1.el5 <<>> station10.example.com @140.117.69.219
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7783
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; QUESTION SECTION:
;station10.example.com.         IN      A

;; ANSWER SECTION:
station10.example.com.  86400   IN      A       192.168.0.10

;; AUTHORITY SECTION:
example.com.            86400   IN      NS      server1.example.com.

;; ADDITIONAL SECTION:
server1.example.com.    86400   IN      A       192.168.0.254

;; Query time: 6 msec
;; SERVER: 140.117.69.219#53(140.117.69.219)
;; WHEN: Sat Jan 30 01:48:18 2010
;; MSG SIZE  rcvd: 93
```

使用 **dig** 追蹤一個**DNS**的查詢過程

- dig +trace xxx.xxx.xxx.xxx

1. 讀取 /etc/resolv.conf 來偵測 nameserver
2. 查詢從 root name servers 開始
3. 逐步參考找到的 name records (answers)

- 這是一個交談式的 query
- Initial Observations:

1. 名稱的組織在樹狀結構中 with root (.) at top
2. The name hierarchy allows DNS to cross organizational boundaries
3. 名稱在紀錄中 with a dot when fully-qualified

- 使用 dig 指令追蹤查詢 www.gov.tw 的過程

```
$ dig +trace www.gov.tw

; <<>> DiG 9.3.4-P1 <<>> +trace www.gov.tw
;; global options:  printcmd
.                       77497   IN      NS      J.ROOT-SERVERS.NET.
```

```
.                       77497   IN      NS      K.ROOT-SERVERS.NET.
.                       77497   IN      NS      L.ROOT-SERVERS.NET.
.                       77497   IN      NS      M.ROOT-SERVERS.NET.
.                       77497   IN      NS      A.ROOT-SERVERS.NET.
.                       77497   IN      NS      B.ROOT-SERVERS.NET.
.                       77497   IN      NS      C.ROOT-SERVERS.NET.
.                       77497   IN      NS      D.ROOT-SERVERS.NET.
.                       77497   IN      NS      E.ROOT-SERVERS.NET.
.                       77497   IN      NS      F.ROOT-SERVERS.NET.
.                       77497   IN      NS      G.ROOT-SERVERS.NET.
.                       77497   IN      NS      H.ROOT-SERVERS.NET.
.                       77497   IN      NS      I.ROOT-SERVERS.NET.
;; Received 392 bytes from 140.117.11.1#53(140.117.11.1) in 4 ms

tw.                     172800  IN      NS      NS.TWNIC.NET.
tw.                     172800  IN      NS      A.DNS.tw.
tw.                     172800  IN      NS      B.DNS.tw.
tw.                     172800  IN      NS      C.DNS.tw.
tw.                     172800  IN      NS      D.DNS.tw.
tw.                     172800  IN      NS      E.DNS.tw.
tw.                     172800  IN      NS      F.DNS.tw.
tw.                     172800  IN      NS      G.DNS.tw.
tw.                     172800  IN      NS      H.DNS.tw.
;; Received 414 bytes from 192.58.128.30#53(J.ROOT-SERVERS.NET) in 42 ms

gov.tw.                 86400   IN      NS      b.twnic.net.tw.
gov.tw.                 86400   IN      NS      c.twnic.net.tw.
gov.tw.                 86400   IN      NS      a.twnic.net.tw.
;; Received 162 bytes from 192.83.166.11#53(NS.TWNIC.NET) in 11085 ms

www.gov.tw.             43200   IN      NS      ns1.www.gov.tw.
www.gov.tw.             43200   IN      NS      ns2.www.gov.tw.
;; Received 96 bytes from 192.72.81.200#53(b.twnic.net.tw) in 17 ms

www.gov.tw.             43200   IN      A       163.29.3.40
www.gov.tw.             43200   IN      NS      ns1.www.gov.tw.
www.gov.tw.             43200   IN      NS      ns2.www.gov.tw.
;; Received 112 bytes from 211.79.170.24#53(ns1.www.gov.tw) in 0 ms
```

其他的觀察

- 追蹤並觀看瞭解DNS這些資源形式
- 每一個 resource record has five fields:

1. domain - 這個被查詢的網域名稱或子網域
2. ttl - 這個紀錄需要被cached 多久,有效時間以秒計算
3. class - 紀錄分類 (通常使用 IN)
4. type - 紀錄型態e, 類似 A 或 NS 之類的
5. rdata - resource data to which the domain maps

- 從概念上來說, 一次查詢這個 domain name,指的就是對應到一個答案
- 在追蹤的例子上：

1. 這個 NS (name server) 記錄指的是參考資源
2. 這個 A (address) 紀錄是完成查詢後的答案

Forward Lookups(正解查詢)

- dig www.edu.tw

1. 先嘗試遞迴, as indicated by rd (recursion desired) in the flags section of the output: 如果名稱伺服器允許遞迴查詢，這個伺服器找到答案後會回硬給提出的客戶端。
2. 如果這個名稱伺服器不允許遞迴查詢，這個伺服器將會給一個 top-level domain 的參考伺服器, which

dig 追蹤

- 觀察
- dig's default query type is A; the rdata for an A record is an IPv4 address

```
$ dig google.com
```

- Use -t AAAA to request IPv6 rdata

```
$ dig google.com -t aaaa
```

- 當完成查詢, dig 返回一個 NOERROR 狀態, 一個答案的計數, 並表達這個 nameservers are authoritative for the name

Reverse Lookups(反解查詢)

- dig -x 140.117.69.1
- 觀察

1. 這個問題一節輸出顯示的DNS反解十進位的地址和附加在in-addr.arpa。FQDN 網域的一部分記錄.
2. 答案部分表明，DNS使用PTR（指針）記錄反解查詢
3. Additionally, the rdata for a PTR record is a fully-qualified domain name

```
[root@server1 ~]# dig -x 140.117.69.1

; <<>> DiG 9.3.3rc2 <<>> -x 140.117.69.1
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 40437
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;1.69.117.140.in-addr.arpa.     IN      PTR

;; ANSWER SECTION:
1.69.117.140.in-addr.arpa. 70293 IN     PTR     cm.nsysu.edu.tw.

;; AUTHORITY SECTION:
69.117.140.in-addr.arpa. 45391  IN      NS      ns.nsysu.edu.tw.
69.117.140.in-addr.arpa. 45391  IN      NS      cc.nsysu.edu.tw.
69.117.140.in-addr.arpa. 45391  IN      NS      cm.nsysu.edu.tw.

;; ADDITIONAL SECTION:
cc.nsysu.edu.tw.        56757   IN      A       163.28.129.1
cm.nsysu.edu.tw.        40400   IN      A       140.117.69.1
ns.nsysu.edu.tw.        80245   IN      A       163.28.129.2

;; Query time: 3 msec
;; SERVER: 140.117.11.1#53(140.117.11.1)
;; WHEN: Sat Mar 22 06:33:11 2008
;; MSG SIZE  rcvd: 168
```

郵件交換紀錄查詢

- 一個 MX record 對應到一個網域郵件伺服器的 fully-qualified domain name
- dig -t mx nsysu.edu.tw
- 觀察

1. The rdata field is extended to include an additional piece of data called the priority
2. The priority can be thought of as a distance: networks prefer shorter distances

- 為了避免更多的查找，域名服務器通常提供 A 記錄額外的反應，以符合的FQDN的提供的MX記錄
- 通常會將底下的MX記錄及相關的A 記錄放一起，紀錄解析的一個網域郵件服務器.
- 查詢 nsysu.edu.tw 的 mx 紀錄

```
[root@server1 ~]# dig -t mx nsysu.edu.tw
```

```
; <<>> DiG 9.3.3rc2 <<>> -t mx nsysu.edu.tw
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42114
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; QUESTION SECTION:
;nsysu.edu.tw.                  IN      MX

;; ANSWER SECTION:
nsysu.edu.tw.           39787   IN      MX      0 barracuda.nsysu.edu.tw.

;; AUTHORITY SECTION:
nsysu.edu.tw.           60264   IN      NS      cc.nsysu.edu.tw.
nsysu.edu.tw.           60264   IN      NS      ns.nsysu.edu.tw.

;; ADDITIONAL SECTION:
barracuda.nsysu.edu.tw. 64704   IN      A       140.117.11.135
cc.nsysu.edu.tw.        56593   IN      A       163.28.129.1
ns.nsysu.edu.tw.        80081   IN      A       163.28.129.2

;; Query time: 4 msec
;; SERVER: 140.117.11.1#53(140.117.11.1)
;; WHEN: Sat Mar 22 06:35:55 2008
;; MSG SIZE  rcvd: 138
```

SOA Lookups(權威主機查詢)

- An SOA 查負責domain的權威主機及一些資訊
- dig -t soa nsysu.edu.tw
- 初步觀察：

1. 網域名稱欄位稱為 origin
2. 這個 rdata 欄位被擴充用來添加一些資料來解釋下個 slide
3. There is typically only one master nameserver for a domain; it stores the master copy of its data
4. Other authoritative nameservers for the domain or zone are referred to as slaves; they synchronize their data from the master

```
[root@cm ~]# dig -t soa nsysu.edu.tw

; <<>> DiG 9.3.4-P1 <<>> -t soa nsysu.edu.tw
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34709
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;nsysu.edu.tw.                  IN      SOA

;; ANSWER SECTION:
nsysu.edu.tw.           86400   IN      SOA     cc.nsysu.edu.tw.
 dns.cc.nsysu.edu.tw. 2008101301 21600 7200 2419200 43200

# nsysu.edu.tw 由 cc.nsysu.edu.tw 主機管理 name server
# 管理者的 email 為 dns@cc.nsysu.edu.tw
# 以上資訊符合 rfc 標準可以直接參考為設定檔

;; AUTHORITY SECTION:
nsysu.edu.tw.           85429   IN      NS      ns.nsysu.edu.tw.
nsysu.edu.tw.           85429   IN      NS      cc.nsysu.edu.tw.

# 管理此網域有兩台 dns server 分別為 ns.nsysue.edu.tw 及 cc.nsysu.edu.tw

;; ADDITIONAL SECTION:
cc.nsysu.edu.tw.        43018   IN      A       163.28.129.1
ns.nsysu.edu.tw.        73231   IN      A       163.28.129.2

# 這兩台的 dns server 的 IP
```

```
;; Query time: 2 msec
;; SERVER: 140.117.69.1#53(140.117.69.1)
;; WHEN: Mon Oct 27 02:05:06 2008
;; MSG SIZE  rcvd: 136
```

Authoritative (權威主機的存在)

- 這個 SOA record 表示原始的紀錄來源網域
- 一個伺服器如果是權威主機：

1. 代表 from the parent domain: NS record plus A record
2. 一個本地端的的複製有 domain data 並包涵 SOA record

- A nameserver that has the proper delegation but lacks domain data is called a lame server

每個紀錄的觀察

- dig -t axfr example.com. @192.168.0.254
- 觀察結果

1. 把所有的 zone 紀錄傳輸出來
2. Records reveal much inside knowledge of the network
3. Response is too big for UDP, so transfers use TCP

- 多數的伺服器限制 zone transfers的功能到幾個主機才可以使用(通常是 slave nameservers)
- 使用這個 command from a slave to test permissions on the master
- **這是各有危險的指令，可以知道別人的 DNS server的全部紀錄，所以大多會拒絕存取**

```
$ host -t axfr example.com. 192.168.3.250
Trying "example.com"
Using domain server:
Name: 192.168.3.250
Address: 192.168.3.250#53
Aliases:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63684
;; flags: qr aa ra; QUERY: 1, ANSWER: 609, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;example.com.                   IN      AXFR

;; ANSWER SECTION:
example.com.            86400   IN      SOA     server1.example.com.
root.server1.example.com. 2003040108 3600 300 604800 60
example.com.            86400   IN      NS      server1.example.com.
example.com.            86400   IN      MX      10 server1.example.com.
example.com.            86400   IN      A       192.168.0.254
domain1.example.com.    86400   IN      NS      station1.example.com.
domain10.example.com.   86400   IN      NS      station10.example.com.
domain100.example.com.  86400   IN      NS      station100.example.com.
domain11.example.com.   86400   IN      NS      station11.example.com.
domain12.example.com.   86400   IN      NS      station12.example.com.
domain13.example.com.   86400   IN      NS      station13.example.com.
domain14.example.com.   86400   IN      NS      station14.example.com.
domain15.example.com.   86400   IN      NS      station15.example.com.
....skip.....
```

使用 host 指令的探索

- 可以用於任何的查詢,加上 -v 參數可以看到 zone 檔案格式的輸出
- Trace: not available
- Delegation: host -rt ns redhat.com
- Force iterative: host -r redhat.com
- Reverse lookup: host 209.132.177.50

- Reverse lookup: host 209.132.177.50
- MX lookup: host -t mx redhat.com
- SOA lookup: host -t soa redhat.com
- Zone transfer: host -t axfr redhat.com 192.168.0.254 or

1. host -t ixfr=serial example.com. 192.168.0.254

- 使用 cm.nsysu.edu.tw 這台主機查詢 dns 紀錄

```
[root@localhost ~]# host jangmt.cm.nsysu.edu.tw cm.nsysu.edu.tw
Using domain server:
Name: cm.nsysu.edu.tw
Address: 140.117.69.1#53
Aliases:

jangmt.cm.nsysu.edu.tw has address 140.117.69.184
```

練習：確認自己PC的Domain Name

- 使用 host or dig 查詢,確認自己的 A, MX ,NS , CNAME等紀錄狀態
- 免費的DNS服務:
  - 在家裏可以使用 http://www.co.cc/ 這個免費的服務來練習。
  - co.cc 使用教學網站 http://superstanwu.blog.ithome.com.tw/post/775/30545

網域名稱服務 DNS

認識 DNS

- Bind的全名是Berkeley Internet Name Domain，最初的時候是由加州大學柏克萊分校所發展出來的BSD UNIX中的一部份，目前則由ISC組織來負責維護與發展。
- Bind是用來解決網域名稱與IP位址對應的軟體，有近九成的DNS伺服器主機都是使用Bind。

- Recursive Query：DNS client 端只丟出一個詢問給 local DNS server，然後 local DNS 就會不斷地查到答案出來為止，最後把結果傳回來給client，這種查詢稱為 Recursive Query。
- Non-Recursive Query （iterative query）：前面的介紹中，local DNS 對其它 DNS 發出的詢問，都只是知道一個更進一步的線索，然後發問者（local DNS） 根據線索再去進一步找答案， 這種詢問方式稱為 Non-Recursive Query（iterative query）。

Service Profile: DNS

- 服務型態: System V-managed service
- 套件: bind, bind-utils, bind-chroot
- 服務程式: /usr/sbin/named, /usr/sbin/rndc
- 啟動script: /etc/init.d/named
- 網路port: 53 (domain), 953(rndc)
- 設定檔: (Under /var/named/chroot/) /etc/named.conf, /var/named/*, /etc/rndc.key
- 相關的: caching-nameserver, openssl

存取控制檔案：BIND

- Netfilter: tcp/udp ports 53 and 953 incoming; tcp/udp ephemeral ports outgoing
- TCP Wrappers: N/A
  - ldd `which named` | grep libwrap
  - strings `which named` | grep hosts
- Xinetd: N/A (named is a standalone daemon)
- PAM: N/A (no configuration in /etc/pam.d/)
- SELinux: yes - see notes
- 應用程式特殊的控制: yes, 等等討論，並載 and in the ARM

- /usr/share/doc/bind-*/arm/Bv9ARM.{html,pdf}

存取控制	相關檔案及設定
應用程式	/var/named/chroot/etc/named.conf的 acl 設定
PAM	N/A (no configuration in /etc/pam.d/)
xinetd	N/A (named is a standalone daemon)
tcp_wrappers	N/A
SELinux	ensure correct file contexts; no change on boolean
Netfilter,IPv4	inbound UDP and TCP port 53 , outbound to port53 + 額外的ports (>=1024)

DNS安裝及設定

- 安裝套件

1. bind for core binaries
2. bind-chroot for security
3. caching-nameserver for an initial configuration

- 設定檔啟動

1. service named configtest
2. service named start
3. chkconfig named on

- 使用 yum 安裝 dns 套件

```
[root@server1 ~]# yum -y install bind bind-utils bind-chroot
```

- 安裝一個簡易的基礎設定檔

```
yum install -y caching-nameserver
```

- DNS server 的類型可以分為以下三種：

1. Master DNS：本身含有Domain 的資料庫（Zone），此資料庫其實就是包含正解紀錄或者是反解紀錄的文字檔（Zone File）。
2. Slave DNS：這種類型的 DNS 功能最主要為備份Master DNS 的資料庫，並提供名稱解析的功能。它本身也有網域的Zone File，不過它的Zone File 是向Master DNS 複製（Zone Transfer）而來的。
3. Caching-only DNS：Caching-Only DNS 沒有Domain 資料庫，單純僅幫助Client 端向外部的 DNS 主機要求資料，然後再保留查詢結果至快取暫存區（Cache）。則下次Client 再提出名稱查詢的需求，若TTL 還未過期，就直接檢查快取暫存區（Cache），不用再去詢問另一台DNS。

基本的 **named** 設定

- Configure the stub resolver
- 定義存取控制檔案在 /etc/named.conf
  - 宣告 client match lists

1. 伺服器聆聽介面: listen-on and listen-on-v6

- 哪些查詢(client query)可以被允許？

1. Iterative: allow-query { match-list; };
2. Recursive: allow-recursion { match-list; };
3. Transfers: allow-transfer { match-list; };
4. 透過一個合法的 zone files 加入資料

- Test!

設定根解析器

- 這個 nameserver:

1. 修改 /etc/resolv.conf 到本地端的 nameserver 127.0.0.1
2. 修改 /etc/sysconfig/network-scripts/ifcfg-* to specify PEERDNS=no

- 優點:

1. 所有應用程式保持一樣的查詢方式
2. 簡單的存取控制及除錯

- 除了 /etc/resolv.conf, 哪裡能夠有未經授權的使用者看到 DHCP 提供的名稱伺服器？

bind-chroot 套件(改變bind程式的根)

- 安裝一個 chroot 環境在 /var/named/chroot 底下
- 移動以存在的設定檔案到這個 chroot 環境，替代掉原始的檔案環境使用符號(symlinks)連結的方式
- 更新 /etc/sysconfig/named 加入下面的選項：
  - ROOTDIR=/var/named/chroot

- 技巧：
- 查看 /etc/sysconfig/named 安裝 bind-chroot 套件之後

```
[root@stationX ~]# cat /etc/sysconfig/named
# BIND named process options
# ~~~~~~~~~~~~~~~~~~~~~~~~~
# Currently, you can use the following options:
#
# ROOTDIR="/some/where"  --  will run named in a chroot environment.
#                           you must set up the chroot environment
#                           (install the bind-chroot package) before
#                           doing this.
#
# OPTIONS="whatever"     --  These additional options will be passed to named
#                           at startup. Don't add -t here, use ROOTDIR instead.
#
# ENABLE_ZONE_WRITE=yes  --  If SELinux is disabled, then allow named to write
#                           its zone files and create files in its $ROOTDIR/var/named
#                           directory, necessary for DDNS and slave zone transfers.
#                           Slave zones should reside in the $ROOTDIR/var/named/slaves
#                           directory, in which case you would not need to enable zone
#                           writes. If SELinux is enabled, you must use only the
#                           'named_write_master_zones' variable to enable zone writes.
#
# ENABLE_SDB=yes         --  This enables use of 'named_sdb', which has support
#                        --  for the ldap, pgsql and dir zone database backends
#                        --  compiled in, to be used instead of named.
#
# DISABLE_NAMED_DBUS=[1y]--  If NetworkManager is enabled in any runlevel, then
#                           the initscript will by default enable named's D-BUS
#                           support with the named -D option. This setting disables
#                           this behavior.
#
# KEYTAB_FILE="/dir/file"    --  Specify named service keytab file (for GSS-TSIG)
ROOTDIR=/var/named/chroot
```

- Run ps -ef | grep named after starting named to verify startup options

```
# ps -ef | grep named
named    14113     1  0 09:54 ?        00:00:00 /usr/sbin/named -u named -t /var/named/chroot
root     18514 18489  0 20:10 pts/0    00:00:00 grep named
```

caching-nameserver 套件

- 提供在 /var/named/chroot/ 的 var/named/ 及 etc 目錄下

1. named.caching-nameserver.conf
2. named.ca 含 root server 'hints'
3. 正解(Forward)及反解(reverse) 本機的名稱及IP 位址網域檔案

- 技巧：

1. 拷貝 named.caching-nameserver.conf to named.conf
2. 改變擁有者權限 root:named
3. 修改 named.conf

- The following slides describe essential access directives
- RFC 1912 描述 DNS 的操作 http://www.ietf.org/rfc/rfc1912.txt

位址符合列表

- 分號分隔的 IP 位址列表或子網路的使用被用來當作 host-based 的存取控制
- 格式：

1. IP address: 192.168.0.1
2. Trailing dot: 192.168.0.
3. CIDR: 192.168.0/24
4. 使用一個驚嘆號符號 (!) 代表反向選取的意思

- A match list is checked in order, stopping on first match
- 範例：

```
# { 192.168.0.1; 192.168.0.; !192.168.1.0/24; };
```

取控制列表 (ACL)

- 在一個簡單的表擔內 ACL 賦予一個名稱來替代 address match list
- 能夠產生一個地方的符合清單 (nesting is allowed!)
- 最佳Best實施預設 ACL's 是在 /etc/named.conf 這個設定檔的頂端
- 宣告範例

```
acl "trusted"     { 192.168.1.21; };
acl "classroom"   { 192.168.0.0/24; trusted; };
acl "cracker"     { 192.168.1.0/24; };
acl "mymasters"   { 192.168.0.254; };
acl "myaddresses" { 127.0.0.1; 192.168.0.1; };
```

內建的 ACL's 定義列表

- BIND 預先定義了四個 ACL's 規則列表

```
none      - No IP address matches
any       - All IP addresses match
localhost - Any IP address of the name server matches
localnets - Directly-connected networks match
```

- What is the difference between the localhost built-in ACL and the myaddresses example on the previous page (假設這個伺服器有多個家)?

伺服器介面

- 選項: listen-on port 53 { match-list; };
- Binds 名稱服務到一個指定的網路介面卡上
- 範例：

```
listen-on port 53 { myaddresses; };
listen-on-v6 port 53 { ::1; };
```

- 重新啟動及驗證

1. 重新啟動 service named restart
2. 驗證： netstat -tulpn | grep named

- 問題:

1. What if listen-on does not include 127.0.0.1?
2. How might changing listen-on-v6 to :: (all IPv6 addresses) affect IPv4?

- 預設: if listen-on is missing, named listens on all interfaces

允許查詢(Client Queries)

- 寫在 Option 區段內: allow-query { match-list; };
- 伺服器提供權威及快取答案給在符合清單內的客戶端

- 範例：

1. allow-query { classroom; cracker; };

- 預設: 如果 allow-query 不存在則預設全開

Allowing Recursion(允許遞迴查詢)

- Option: allow-recursion { match-list; };
- Server chases referrals on behalf of clients in the match-list
- Example:

1. allow-recursion { classroom; !cracker; };

- 問題：

1. What happens if 192.168.1.21 tries a recursive query?
2. What happens if 127.0.0.1 tries a recursive query?

- Default: if allow-recursion is missing, named allows all

Allowing Transfers(允許網域傳輸)

- Option: allow-transfer { match-list; };
- Clients in the match-list are allowed to act as slave servers
- Example:

1. allow-transfer { !cracker; classroom; };

- 問題：

1. What happens if 192.168.1.21 tries a slave transfer?
2. What happens if 127.0.0.1 tries a slave transfer?

- 預設：if allow-transfer is missing, named allows all
- **這選項可以讓所有的人知道你的 DNS 的所有紀錄，所以預設最好為 127.0.0.1**

修改 BIND 作用範圍

- Option: forwarders { match-list; };
- Modifier: forward first | only;
- 指示任命為遞歸查詢中指定的服務器，而不是之前遞迴式的查詢
- 範例：

1. forwarders { mymasters; };
2. forward only;

- How can you determine if forwarders is required?
- If the forward modifier is missing, named assumes first

存取控制(放在一起)

- 範本 /etc/named.conf 包括一些基本的存取控制選項:

```
// acl's make security directives easier to read
acl "myaddresses" { 127.0.0.1; 192.168.0.1; };
acl "trusted"     { 192.168.1.21; };
acl "classroom"   { 192.168.0.0/24; trusted; };
acl "cracker"     { 192.168.1.0/24; };
options {
    # bind to specific interfaces
    listen-on port 53 { myaddresses; };
    listen-on-v6 port 53 { ::1; };

    # make sure I can always query myself for troubleshooting
    allow-query { localhost; classroom; cracker; };
    allow-recursion { localhost; classroom; !cracker; };
    /* don't let cracker (even trusted) do zone transfers */
    allow-transfer { localhost; !cracker; classroom; };

    # use a recursive, upstream nameserver
    forwarders { 192.168.0.254; };

    forward only;
};
```

Cache Only DNS (不指定 Forward)

安裝修改及設定

- 先確認套件及設定，確認有 chroot

```
[root@rhel ~]# vi /etc/sysconfig/named
ROOTDIR=/var/named/chroot
```

- 修改設定檔，從 /etc/named.caching-nameserver.conf 修改，請先確定有安裝套件。

```
[root@rhel ~]# vi /etc/named.caching-nameserver.conf
# (1)在設定檔 option {} 內加入本機對外服務網卡的IP位址
# 192.168.3.250 才可以被讀取，預設的port為UDP 53
listen-on port 53 { 127.0.0.1;192.168.3.250; };

# (2)加入 any; 的選項，讓所有的client端都可以查詢此台dns server
allow-query     { localhost;any; };

view localhost_resolver {
        // (3)請加入 any; 允許任何人可以查詢,否則只有 localhost 可查詢
        match-clients      { localhost;any; };
        match-destinations { localhost;any; };
        recursion yes;
        include "/etc/named.rfc1912.zones";
};

[root@rhel ~]# service named restart
# 重新啟動 named server
Stopping named:                                            [  OK  ]
Starting named:                                            [  OK  ]

# 檢查 port 有沒有啟動
[root@rhel ~]# netstat -an | grep 53
tcp        0      0 192.168.3.250:53            0.0.0.0:*                   LISTEN
```

```
tcp        0      0 127.0.0.1:53                0.0.0.0:*                   LISTEN
```

驗證 cache only dns 設定

- 修改本機的 resolv.conf 設定檔，把 dns server 指向自己,這樣測比較準確.

```
[root@localhost etc]# vi /etc/resolv.conf
nameserver 127.0.0.1
```

- 使用 dig +trace 追蹤查詢，第一次會比較慢，第二次就會快

```
[root@mt ~]# dig +trace www.gov.tw

; <<>> DiG 9.3.4-P1 <<>> +trace www.gov.tw
;; global options:  printcmd
.                       518391  IN      NS      G.ROOT-SERVERS.NET.
.                       518391  IN      NS      H.ROOT-SERVERS.NET.
.                       518391  IN      NS      I.ROOT-SERVERS.NET.
.                       518391  IN      NS      J.ROOT-SERVERS.NET.
.                       518391  IN      NS      K.ROOT-SERVERS.NET.
.                       518391  IN      NS      L.ROOT-SERVERS.NET.
.                       518391  IN      NS      M.ROOT-SERVERS.NET.
.                       518391  IN      NS      A.ROOT-SERVERS.NET.
.                       518391  IN      NS      B.ROOT-SERVERS.NET.
.                       518391  IN      NS      C.ROOT-SERVERS.NET.
.                       518391  IN      NS      D.ROOT-SERVERS.NET.
.                       518391  IN      NS      E.ROOT-SERVERS.NET.
.                       518391  IN      NS      F.ROOT-SERVERS.NET.
;; Received 500 bytes from 140.117.69.184#53(140.117.69.184) in 0 ms

tw.                     172800  IN      NS      H.DNS.tw.
tw.                     172800  IN      NS      G.DNS.tw.
tw.                     172800  IN      NS      B.DNS.tw.
tw.                     172800  IN      NS      D.DNS.tw.
tw.                     172800  IN      NS      C.DNS.tw.
tw.                     172800  IN      NS      E.DNS.tw.
tw.                     172800  IN      NS      NS.TWNIC.NET.
tw.                     172800  IN      NS      F.DNS.tw.
tw.                     172800  IN      NS      A.DNS.tw.
;; Received 414 bytes from 192.112.36.4#53(G.ROOT-SERVERS.NET) in 336 ms

gov.tw.                 86400   IN      NS      b.twnic.net.tw.
gov.tw.                 86400   IN      NS      c.twnic.net.tw.
gov.tw.                 86400   IN      NS      a.twnic.net.tw.
;; Received 162 bytes from 61.31.216.3#53(H.DNS.tw) in 1 ms

www.gov.tw.             43200   IN      NS      ns1.www.gov.tw.
www.gov.tw.             43200   IN      NS      ns2.www.gov.tw.
;; Received 96 bytes from 192.72.81.200#53(b.twnic.net.tw) in 6 ms

www.gov.tw.             43200   IN      A       163.29.3.40
www.gov.tw.             43200   IN      NS      ns2.www.gov.tw.
www.gov.tw.             43200   IN      NS      ns1.www.gov.tw.
;; Received 112 bytes from 211.79.170.24#53(ns1.www.gov.tw) in 10 ms
```

- 觀察套件 caching-nameserver ，這些是所有相關的檔案

```
[root@localhost etc]# rpm -ql caching-nameserver
/etc/named.caching-nameserver.conf
/etc/named.rfc1912.zones
/usr/share/doc/caching-nameserver-9.3.3
/usr/share/doc/caching-nameserver-9.3.3/Copyright
/usr/share/doc/caching-nameserver-9.3.3/rfc1912.txt
/var/named/localdomain.zone
/var/named/localhost.zone
/var/named/named.broadcast
/var/named/named.ca
/var/named/named.ip6.local
/var/named/named.local
```

```
/var/named/named.zero
```

Cache Only DNS (指定 Forward)

- 所謂的forwarder，就是當某一台DNS 遇到非本機負責的Zone 之查詢請求的時候，將不直接向root Server 查詢，而把請求轉交給指定的另一台DNS 主機（forwarder）代為查詢。

修改-指定 Forward

```
[root@localhost etc]# vi /etc/named.caching-nameserver.conf
# 在 options 的選項內插入下面兩行
        forwarders {168.95.1.1;};       // 指定forward dns serevr
        forward only;                   // forward only

[root@localhost etc]# cat /etc/named.caching-nameserver.conf
// 整體而言，看起來像是這樣
// named.caching-nameserver.conf
//
// Provided by Red Hat caching-nameserver package to configure the
// ISC BIND named(8) DNS server as a caching only nameserver
// (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
// DO NOT EDIT THIS FILE - use system-config-bind or an editor
// to create named.conf - edits to this file will be lost on
// caching-nameserver package upgrade.
//
options {
        listen-on port 53 { 127.0.0.1; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        query-source    port 53;
        query-source-v6 port 53;
        // 請加入 any; 允許任何人可以查詢
        allow-query     { localhost;any; };
        allow-query-cache { localhost;any; };

        forwarders {168.95.1.1;};       // 指定forward dns serevr
        forward only;                   // forward only
};
logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};
view localhost_resolver {
        // 請加入 any; 允許任何人可以查詢
        match-clients      { localhost;any; };
        match-destinations { localhost;any; };
        recursion yes;
        include "/etc/named.rfc1912.zones";
};
[root@localhost etc]# service named restart
# 重新啟動
Stopping named:                                            [  OK  ]
Starting named:                                            [  OK  ]
```

驗證 Cache only DNS server 指定 forward

- 驗證 Cache only DNS server 指定 forward

```
[root@localhost etc]# dig www.redhat.com

; <<>> DiG 9.3.3rc2 <<>> www.redhat.com
```

```
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8379
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;www.redhat.com.                        IN      A

;; ANSWER SECTION:
www.redhat.com.         60      IN      A       209.132.177.50

;; AUTHORITY SECTION:
redhat.com.             600     IN      NS      ns1.redhat.com.
redhat.com.             600     IN      NS      ns2.redhat.com.
redhat.com.             600     IN      NS      ns3.redhat.com.

;; ADDITIONAL SECTION:
ns1.redhat.com.         600     IN      A       66.187.233.210
ns2.redhat.com.         600     IN      A       66.187.224.210
ns3.redhat.com.         600     IN      A       66.187.229.10

;; Query time: 159 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Jul 16 05:36:31 2007
;; MSG SIZE  rcvd: 150
```

Master Zone (主要dns網域空間宣告)

```
zone "example.com" {
    type master;
    file "example.com.zone";
};
```

- 網路宣告範例，描述這台機器：
- 說明這是一台具有權威性的 example.com 網域的 nameserver ，where example.com is the origin as specified in the SOA record's domain field

1. 是一個 master 網域主機
2. 讀取 master data 從 /var/named/chroot/var/named/example.com.zone 這個設定檔

- 你必須在重新啟動 named 服務前，手動建立這個 master file

Zone File (網域空間描述檔案建立)

- zone file的內容:

1. 一些紀錄的集合從 SOA record 開始描述
2. 這個 @ 符號是一個變數替代 zone's origin 在 /etc/named.conf
3. 註解使用 assembly-style (;)

- 注意事項:

1. BIND 追加原始的網域的時候任何網域名稱需要以「.」當作結尾
2. 如果網域名稱的欄位有一個遺失， BIND 使用上一個欄位紀錄的值 (Danger! What if another admin changes the record order?)
3. 修改過 zone file 後記得增加序號(serial number) 並重新載入 named

- What DNS-specific resolver puts its output in zone file format?

Zone Files小技巧

- Shortcuts:

1. Do not start from scratch - copy an existing zone file installed by the caching-nameserver package
2. To save typing, put $TTL 86400 as the first line of a zone file, then omit the TTL from individual records

3. BIND allows you to split multi-valued rdata across lines when enclosed within parentheses ()

- Choose a filename for your zone file that reflects the origin in some way

測試

- 操作:

1. Select one of dig, host, or nslookup, and use it expertly to verify the operation of your DNS server
2. Run tail -f /var/log/messages in a separate shell when restarting services

- 設定：

1. BIND will fail to start for syntax errors, so always run service named configtest after editing config files
2. configtest runs two syntax utilities against files specified in your configuration, but the utilities may be run separately against files outside your configuration

BIND 語法工具

- named-checkconf -t ROOTDIR /path/to/named.conf

1. 審查 /etc/named.conf by default (which will be the wrong file if the -t option is missing)
2. 範例：named-checkconf -t /var/named/chroot

- named-checkzone origin /path/to/zonefile

1. 審查 a specific zone configuration
2. 範例: named-checkzone redhat.com /var/named/chroot/var/named/redhat.com.zone

Master DNS 實作

先確定domain name

- 先向你的上層網域註冊一個Domain name 對應到你的IP，並且開啟A及NS紀錄，的下為課程中用的設定內容：

```
[root@station35 ~]# host -t axfr example.com 192.168.0.254 | grep server35
domain35.example.com.   86400   IN      NS      server35.example.com.
server35.example.com.   86400   IN      A       192.168.0.135
www35.example.com.      86400   IN      CNAME   server35.example.com.
```

- 並確認他可以用(**這要設定完成後才又辦法確認**,底下範例為設定完成 master dns 後才查詢的到)，我的網域名稱為 domain35.example.com. ，IP為 192.168.0.135

- 為了底下的實驗順利，**通常先申請一個 A 紀錄當作測試，測試成功後在加上 NS 紀錄即可正確查詢**。
- NS 紀錄需要花錢申請，如果真的想玩可以去買一個真實的網域來設定 https://www.godaddy.com/ 有在賣，且還很便宜。google 也有在賣更便宜且還幫你做 dns 代管，順便送你 mail 及 web 的服務全部都不用錢。缺點是沒有 NS 紀錄可以自己玩子網域。
- http://co.cc 有提供 NS 紀錄的免費申請服務. http://cz.cc 也有提供.免費的次級網域申請。

- 底下為你設定完成master dns後，測試看是否有此紀錄 A 及 NS ,請指定用 127.0.0.1測試。

```
# 先修改系統的 dns server 設定
[root@station35 ~]# cat /etc/resolv.conf
search example.com
nameserver 127.0.0.1

# 有此結果表示可以工作了
[root@station35 ~]# host domain35.example.com
```

```
domain35.example.com has address 192.168.0.135
domain35.example.com mail is handled by 10 mail.domain35.example.com.
```

設定 Master DNS 的 zone 區塊

- 設定 Master DNS 的 zone 區塊

```
[root@localhost named]# vi /etc/named.caching-nameserver.conf
# 借用剛剛的 cache only dns 設定檔
[root@station35 ~]# cat /etc/named.caching-nameserver.conf
//
// named.caching-nameserver.conf
//
// Provided by Red Hat caching-nameserver package to configure the
// ISC BIND named(8) DNS server as a caching only nameserver
// (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
// DO NOT EDIT THIS FILE - use system-config-bind or an editor
// to create named.conf - edits to this file will be lost on
// caching-nameserver package upgrade.
//
options {
        listen-on port 53 { 127.0.0.1; 192.168.0.135; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";

        // Those options should be used carefully because they disable port
        // randomization
        // query-source    port 53;
        // query-source-v6 port 53;

        allow-query     { localhost; any; };
        allow-query-cache { localhost; any; };

        // 允許本機紀錄讓其他主機作 zone transfer
        // 這是給 slave dns 使用的
        allow-transfer {
                127.0.0.1;
                192.168.0.0/16;
        };

};

logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};

// 把系統預設定的此段註解掉，並建立自己新的 view ，不建立也不會怎樣
// view localhost_resolver {
//       match-clients      { localhost; };
//       match-destinations { localhost; };
//       recursion yes;
//       include "/etc/named.rfc1912.zones";
//};


// 建立自己新的 view zone
// view 這個功能是設定在 options 裡的，它主要的目的是讓不同的
// client IP 查詢同一個 host name 時，可以回應不同的 zone file。
// 例如你只有一台 DNS server但需同時兼做 External 及 Internal DNS 時
// ，就可以使用 view 的方式。讓外面的人查到 External IP，而內部的使用者查到 Internal IP。
// --------
// 用法：
```

```
// 用法:
//     view "view_name" {
//
//         match-clients { address_match_list };
//        // 符合此 view 的 client IP，可套用 acl 的名稱
//        [ view_option; ...]
//        // view 的設定，例如說，此 view 要不要提供 recursion
//        [ zone_statement; ...]
//        // 這個 view 所使用的 zone file 及相關設定
//     };


// 只要寫下底下這段即可。
zone "domain35.example.com" {
    type master;
    file "domain35.example.com.zone";
};


zone "example.com" IN {
    type slave;
    masters {192.168.0.254; };
    file "slaves/example.com.zone";
};
```

新增網域正解Zone File

- 新增網域正解Zone File

1. 詳細請參考 http://dns-learning.twnic.net.tw/bind/intro6.html#c
2. ";" 為這解說明內容,可以不用加入 zone file , // 及 ## 也可以當作註解
3. 小心有空白的空行及不存在的字元，會造成服務設定鬼打牆的狀況。

```
[root@localhost named]# pwd
/var/named/chroot/var/named
[root@station35 ~]# cat /var/named/chroot/var/named/domain35.example.com.zone
$TTL    86400
@               IN SOA  domain35.example.com. root.domain35.example.com. (
                                        50              ; serial (d. adams)
                                        3H              ; refresh
                                        15M             ; retry
                                        1W              ; expiry
                                        1D )            ; minimum

@               IN NS           domain35.example.com.
@               IN A            192.168.0.135
localhost       IN A            127.0.0.1

dns             IN A            192.168.0.135
www             IN A            192.168.0.135
www2            IN CNAME        server35.example.com.
mail            IN A            192.168.0.35

; 把 @domain35.example.com. 的郵件寄送到 mt.cm.nsysu.edu.tw 主機
@               IN MX           10 mail.domain35.example.com.

; 自動產生 station1.domain35.example.com. IN A 192.168.0.1
; 產生到station254.domain35.example.com.
$GENERATE 1-254 station$ A 192.168.0.$
```

- NS：name server，定義某個 domain 是由哪個 name server 負責。
- A：address，定義某個主機名稱（FQDN）所對應的 IP。
- PTR：pointer，定義某個 IP 對應的主機名稱（FQDN）。
- CNAME：canonical name，定義一個別名及其真正對應到的 record。
- MX：mail exchanger，定義某部機器的 mail exchanger，所有要送往那部機器的 mail 都要經過 mail

exchanger 轉送。

錯誤修正

- 請注意在 /var/named/chroot/var/named 的檔案權限必須為 root.named 且 chmod 最少為 640 如果不正確需要修正正確，否則 named 程式不會載入設定檔。
- 你可以從 /var/log/message 看看是否有告訴你權限的問題，如果不對請用 restorecon 修正檔案屬性。

```
# 以下是正確的權限設定
[root@station35 ~]# ls /var/named/chroot/var/named/ -laZ
drwxr-x---  root  named system_u:object_r:named_zone_t   .
drwxr-x---  root  named system_u:object_r:named_conf_t   ..
drwxrwx---  named named system_u:object_r:named_cache_t  data
-rw-r--r--  root  named root:object_r:named_zone_t       domain35.example.com.zone
-rw-r-----  root  named system_u:object_r:named_zone_t   localdomain.zone
-rw-r-----  root  named system_u:object_r:named_zone_t   localhost.zone
-rw-r-----  root  named system_u:object_r:named_zone_t   named.broadcast
-rw-r-----  root  named system_u:object_r:named_conf_t   named.ca
-rw-r-----  root  named system_u:object_r:named_zone_t   named.ip6.local
-rw-r-----  root  named system_u:object_r:named_zone_t   named.local
-rw-r-----  root  named system_u:object_r:named_zone_t   named.zero
drwxrwx---  named named system_u:object_r:named_cache_t  slaves

# 如果不正確請使用 chown or chmod or restorecon 修正權限
[root@station35 ~]# chown root:named domain35.example.com.zone
[root@station35 ~]# chmod 640 domain35.example.com.zone
[root@station35 ~]# restorecon domain35.example.com.zone
```

master dns 測試

- 測試 Master DNS server 是否工作，正解是否正確。請先將本機的 dns server 設定為 127.0.0.1

```
# dns server 設定為本機
[root@station35 ~]# cat /etc/resolv.conf
search example.com
# nameserver 192.168.0.254
nameserver 127.0.0.1

# 該有的紀錄都可以查詢
[root@station35 ~]# host domain35.example.com
domain35.example.com has address 192.168.0.135
domain35.example.com mail is handled by 10 mail.domain35.example.com.
[root@station35 ~]# host www2.domain35.example.com
www2.domain35.example.com is an alias for server35.example.com.
server35.example.com has address 192.168.0.135
[root@station35 ~]# host mail.domain35.example.com
mail.domain35.example.com has address 192.168.0.35
[root@station35 ~]# host station100.domain35.example.com
station100.domain35.example.com has address 192.168.0.100

# zone transfer 可以支援 slave dns 的備份使用
[root@station35 ~]# host -t axfr domain35.example.com 127.0.0.1 |more
Trying "domain35.example.com"
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53467
;; flags: qr aa ra; QUERY: 1, ANSWER: 264, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;domain35.example.com.          IN      AXFR

;; ANSWER SECTION:
domain35.example.com.   86400   IN      SOA     domain35.example.com. root.d
omain35.example.com. 49 10800 900 604800 86400
domain35.example.com.   86400   IN      MX      10 mail.domain35.example.com
```

```
.
domain35.example.com.   86400   IN      NS      domain35.example.com.
domain35.example.com.   86400   IN      A       192.168.0.135
dns.domain35.example.com. 86400 IN      A       192.168.0.135
localhost.domain35.example.com. 86400 IN A      127.0.0.1
mail.domain35.example.com. 86400 IN     A       192.168.0.35

station1.domain35.example.com. 86400 IN A       192.168.0.1
....略 300 行....
```

- 以上是簡單的 master dns 設定範例

Slave Zone 宣告

- 在主要設定檔 named.conf 加入 slave 的 zone 宣個

```
zone "example.com" {
    type slave;
    masters { mymasters; };
    file "slaves/example.com.zone";
};
```

- Sample zone declaration directs the server to:

1. Act as an authoritative nameserver for example.com, where example.com is the origin as specified in the SOA record's domain field
2. Be a slave for this zone
3. Perform zone transfers (AXFR and IXFR) against the hosts in the masters option
4. Store the transferred data in /var/named/chroot/var/named/slaves/example.com.zone

- Reload named to automatically create the file

- 在主要設定檔 options{}內需要有 allow-transfer 的設定,才可以作 zone transfer

```
# vi /etc/named.caching-nameserver.conf
# 請在 options{} 內加入底下四行內容
        allow-transfer {
                127.0.0.1;
                192.168.0.0/16;
        };

# 重新啟動 named
[root@station35 data]# /etc/init.d/named restart

# 在本機 127.0.0.1 測試 zone transfer
[root@station35 data]# host -t axfr domain35.example.com. 127.0.0.1
```

Slave DNS 實作

- 請參考課本 LAB 10.1: Configuring a Slave Zone 有詳細的說明.
- 目的是以 example.com 伺服器為 master dns server 每台使用者的 stationX 機器都是 slave dns server 作 zone transfer 就可以完成 slave dns 的服務了.

- 先確定可以對 example.com 的 master 主機作 zone transfer

```
[root@linux ~]# host -t axfr example.com 192.168.0.254
```

- 在 /etc/named.caching-nameserver.conf 加入關於 slave 的設定檔

```
[root@station35 named]# vi /etc/named.caching-nameserver.conf
zone "example.com" IN {
    type slave;
    masters {192.168.0.254; };
    file "slaves/example.com.zone";
};

[root@station35 named]# /etc/init.d/named restart
```

```
Stopping named:                                            [  OK  ]
Starting named:                                            [  OK  ]

[root@station35 named]# ls /var/named/chroot/var/named/slaves/ -l
total 28
-rw-r--r-- 1 named named 23887 May 10 17:51 example.com.zone
```

進階的 BIND 主題

- Remote Name Daemon Control (rndc)
- Delegating Subdomains
- Views and Split DNS

Remote Name Daemon Control (rndc)

- Provides local and remote management of named
- The bind-chroot package configures rndc

1. Listens on the IPv4 and IPv6 loopbacks only
2. Reads key from /etc/rndc.key
3. If the key does not match, cannot start or stop the named service
4. No additional configuration is needed for a default, local install

- Example - flush the server's cache: rndc flush

Delegating Subdomains

- Steps

1. On the child, create a zone file to hold the subdomain's data
2. On the parent, add an NS record
3. On the parent, add an A record to complete the delegation

- Glue Records

1. If the child's canonical name is in the subdomain it manages, the A record is called a glue record

Views and Split DNS

- Answering queries differently based on who is asking
- match-clients and match-destinations
- Options and zones defined within a view
- Any view statement means that all zone definitions must be inside a view

反解的DNS設定

- 設定一個可以反解的 master dns zone 底下範例因為是在教室,所以使用 192.168.3.x 的網段作範例,所以和上面的 master dns 不相關.
- 設定反解的 zone

```
[root@localhost named]# vi /etc/named.caching-nameserver.conf
# 在 view 中加入這段 zone 建立一各反解的zone 192.168.3.x
zone "3.168.192.in-addr.arpa" IN {
        type master;
        file "192.168.3.zone";
        allow-update { none; };
        forwarders{};
};
```

- 檢查設定檔

```
[root@localhost named]# service named configtest
other/0.168.192.in-addr.arpa/IN: file not found
zone rhel.blogdns.org/IN: loaded serial 46
zone 0.168.192.in-addr.arpa/IN: loading master file 192.168.3.zone: file not found
```

- 建立反解的 zone 檔案

```
[root@localhost named]# cp named.local 192.168.3.zone
$TTL    86400
@       IN      SOA     mtchang.blogdns.com. root.mtchang.blogdns.com.  (
                                        1997022700 ; Serial
                                        28800      ; Refresh
                                        14400      ; Retry
                                        3600000    ; Expire
                                        86400 )    ; Minimum
@       IN      NS      mtchang.blogdns.com.
208     IN      PTR     dns.mtchang.blogdns.com.
150     IN      PTR     server1.mtchang.blogdns.com.
```

- 修改權限及SELINUX

```
[root@localhost named]# ls -lZ
-rw-r-----  root  root                                     192.168.3.zone
drwxrwx---  named named system_u:object_r:named_cache_t:s0 data
-rw-r-----  root  named                                    localdomain.zone
-rw-r-----  root  named                                    localhost.zone
-rw-r-----  root  named                                    named.broadcast
-rw-r-----  root  named                                    named.ca
-rw-r-----  root  named                                    named.ip6.local
-rw-r-----  root  named                                    named.local
-rw-r-----  root  named                                    named.zero
-rw-r-----  root  named                                    rhel.blogdns.org.zone
drwxrwx---  named named system_u:object_r:named_cache_t:s0 slaves
[root@localhost named]# chown root.named 192.168.0.zone
```

- 啟動及測試

```
[root@localhost named]# service named restart
Stopping named:                                            [  OK  ]
Starting named:                                            [  OK  ]
[root@localhost named]# host 192.168.3.150 192.168.3.208
Using domain server:
Name: 192.168.3.208
Address: 192.168.3.208#53
Aliases:

150.3.168.192.in-addr.arpa domain name pointer server1.mtchang.blogdns.com.
```

- 問題發現與處理

1. 記得要觀看/var/log/message 得知目前服務運作狀況

DNS參考文件

- 這兩篇文章就是課程的內容了，只是版本還是 4 版的內容。

1. http://linux.vbird.org/somepaper/20050630-dns-1.pdf
2. http://linux.vbird.org/somepaper/20050630-dns-2.pdf

- TWNIC DNS教學計劃網站 BIND教學

1. http://dns-learning.twnic.net.tw/bindFrame.html

- 外國人寫得很詳細 http://www.zytrax.com/books/dns/ch4/

DNS Server(example.com) 設定範例

- 上課用的 DNS server 設定範例
- 先安裝 dns server 及 caching-nameserver 範例

```
# yum -y install bind bind-utils bind-chroot
# yum install caching-nameserver -y
```

named.conf

- 新增加 /var/named/chroot/etc/named.conf 檔案，內容如下：

```
# /etc/named.conf
#
# This file should be used for all classes except RH320.
# Replaces: named.conf-isolated, named.conf-internet

//////////////////////////////////////////////////////////////////////
#   Define the location of the zone files, clean daily,
#   and possibly specify forwarders.
//////////////////////////////////////////////////////////////////////
// Define ACL(s) here
acl exampleNetwork { 192.168.0.0/24;140.117.69.0/24; };
acl crackerNetwork { 192.168.1.0/24; };
acl internal       { 127.0.0.1; 192.168.0.0/24; 192.168.1.0/24; 140.117.69.0/24; };
acl bogusNets      { 0.0.0.0/8;
                     1.0.0.0/8;
                     2.0.0.0/8;
                     192.0.2.0/24;
                     224.0.0.0/3;
};

options {
        listen-on port 53 { 127.0.0.1; 140.117.69.204; };

        // Where do our zone files live?
        directory "/var/named";

        cleaning-interval 1440;
        // Use the ACL to say who can query us
        allow-query { internal; };

        // Allow recursion for localnets( not really needed becauses of above )
        allow-recursion { internal; };

        // Allow zone transfers only to exampleNetwork ACL
        allow-transfer { exampleNetwork; };

        // Blackhole illegal addresses commonly used for spoofing
        // This is also redundant but we are showing off
        blackhole { bogusNets; };

        // If you're behind a firewall but have Internet access, you
        // might need to run DNS lookups through another name server
        // that can see through it, to resolve outside hosts.
        // The commented-out line below works for Meridian.
        # forwarders { 192.168.22.250; };

        // Get rid of annoying reminder of default that is, in fact, the
        // opposite of what man named.conf would have you believe.
        auth-nxdomain no;
};
// Magic to make rndc work
include "/etc/rndc.key";
controls {
        inet 127.0.0.1 allow { localhost; } keys { rndckey; };
};

//////////////////////////////////////////////////////////////////////
#   Help out root nameservers; take responsibility for localhost.
//////////////////////////////////////////////////////////////////////
// file names are arbitrary and can be anything
// RFC 1033 uses  zone in their examples and so shall we
```

```
// RFC 1035 uses ".zone" in their examples and so shall we
zone "localhost" {
        type master;
        file "localhost.zone";
};

zone "0.0.127.in-addr.arpa" {
        type master;
        file "127.0.0.zone";
};

############################################################################
#   Provide a hint to the root nameservers
############################################################################

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

############################################################################
#   Master nameserver for example.com and 192.168.0/24
############################################################################

zone "example.com" {
        type master;
        file "example.com.zone";
        forwarders {};
};

zone "0.168.192.in-addr.arpa" {
        type master;
        file "192.168.0.zone";
        forwarders {};
};

############################################################################
#    Master nameserver for cracker.org and 192.168.1/24
############################################################################

zone "cracker.org" {
        type master;
        file "cracker.org.zone";
        forwarders{};
};

zone "1.168.192.in-addr.arpa" {
        type master;
        file "192.168.1.zone";
        forwarders{};
};
```

127.0.0.zone

- 新增加 /var/named/chroot/var/named/127.0.0.zone 檔案，內容如下：

```
$TTL 86400
@ IN  SOA localhost. root.localhost. ( 2001101100 28800 14400 604800 0 )

  IN  NS  localhost.

1.0.0.127.IN-ADDR.ARPA.    IN  PTR    localhost.
```

example.com.zone

- 新增加 /var/named/chroot/var/named/example.com.zone 檔案，內容如下：

```
; Specify the time-to-live( TTL ) for the zone
$TTL 86400  ; 1 Day ( we could have used 1D )
```

```
; Begin Start Of Authority resource record
example.com. IN  SOA server1.example.com. root.server1.example.com. (
                                2003040101      ; serial number
                                1H              ; refresh slave
                                5M              ; retry query
                                1W              ; expire
                                1M              ; negative TTL
)

; Specify our name servers
; !!WARNING: You can not use CNAMEs for RDATA here !!
; owner                 TTL     CL  type                RDATA

@                               IN  NS          server1.example.com.

; Specify our mail exchangers
; !!WARNING: You can not use CNAMEs for RDATA here !!
; owner                 TTL     CL  type        RDATA
@                               IN  MX          10  server1.example.com.

; This is broken and against RFC but must be done to placate the masses
; owner                 TTL     CL  type        RDATA
example.com.                    IN  A           192.168.0.254

; List our CNAME records ( aliases ) here
; owner                 TTL     CL  type        RDATA
mail.example.com.       3600    IN  CNAME       server1.example.com.
kerberos.example.com.   3600    IN  CNAME       server1.example.com.

; List our A records ( hosts ) here
; owner                 TTL     CL  type        RDATA
station1.example.com.           IN  A           192.168.0.1
station2                        IN  A           192.168.0.2
station3                        IN  A           192.168.0.3
station4                        IN  A           192.168.0.4
station5                        IN  A           192.168.0.5
station6                        IN  A           192.168.0.6
station7                        IN  A           192.168.0.7
station8                        IN  A           192.168.0.8
station9                        IN  A           192.168.0.9
station10                       IN  A           192.168.0.10
station11                       IN  A           192.168.0.11
station12                       IN  A           192.168.0.12
station13                       IN  A           192.168.0.13
station14                       IN  A           192.168.0.14
station15                       IN  A           192.168.0.15
station16                       IN  A           192.168.0.16
station17                       IN  A           192.168.0.17
station18                       IN  A           192.168.0.18
station19                       IN  A           192.168.0.19
station20                       IN  A           192.168.0.20
server1                         IN  A           192.168.0.254

; Okay, my fingers are getting tired.  BIND 8.1 and BIND 9.1 and later supports
; a shortcut.  $GENERATE creates a record for each value in the
; numerical range specified in the first argument, replacing any $
; in the template with the current value of the iterator.

; Set up the rest of the station records.

$GENERATE 21-100 station$               A 192.168.0.$

; Set up CNAMEs for www1.example.com and so on.

$GENERATE 1-100 www$                    CNAME station$

; Delegate owner1.example.com and so on to the individual stations.

$GENERATE 1-100 domain$.example.com.    NS station$.example.com.

; The $GENERATE shortcut is normally used to simplify delegating
; subnets on a non-octet boundary.  (This is for non-traditional
```

```
; network sizes -- everything but /8, /16, and /24 subnets.)

; For the dns exam changes.
$GENERATE 101-220 server$.example.com.  A 192.168.0.$
$GENERATE 101-200 domain$.example.com.  NS server$.example.com.
$GENERATE 101-200 www$                  CNAME server$
```

cracker.org.zone

- 新增加 /var/named/chroot/var/named/cracker.org.zone 檔案，內容如下：

```
$TTL 86400
@ IN  SOA server1.cracker.org. root.server1.cracker.org. ( 6 10800 3600 604800 0 )

  IN  NS  server1.cracker.org.
  MX  10  server1.cracker.org.

cracker.org.            IN      A       192.168.1.254
server1                 IN      A       192.168.1.254

; Since most classes don't use cracker.org, crackerX is made the
; A record and stationX the CNAME record, so that when machines
; in vcracker do reverse lookups on their IPs they get crackerX
; instead of stationX.  See doczilla thread:

cracker1                IN      A       192.168.1.1
cracker2                IN      A       192.168.1.2
cracker3                IN      A       192.168.1.3
cracker4                IN      A       192.168.1.4
cracker5                IN      A       192.168.1.5
cracker6                IN      A       192.168.1.6
cracker7                IN      A       192.168.1.7
cracker8                IN      A       192.168.1.8
cracker9                IN      A       192.168.1.9
cracker10               IN      A       192.168.1.10
cracker11               IN      A       192.168.1.11
cracker12               IN      A       192.168.1.12
cracker13               IN      A       192.168.1.13
cracker14               IN      A       192.168.1.14
cracker15               IN      A       192.168.1.15
cracker16               IN      A       192.168.1.16
cracker17               IN      A       192.168.1.17
cracker18               IN      A       192.168.1.18
cracker19               IN      A       192.168.1.19
cracker20               IN      A       192.168.1.20

$GENERATE 21-253 cracker$               A 192.168.1.$

$GENERATE 1-253  station$               CNAME cracker$.cracker.org.
```

192.168.0.zone

- 新增加 /var/named/chroot/var/named/192.168.0.zone 檔案，內容如下：

```
; Specify the time-to-live( TTL ) for the zone
$TTL 86400  ; 1 Day ( we could have used 1D )

; Begin Start Of Authority resource record
0.168.192.IN-ADDR.ARPA. IN  SOA server1.example.com. root.server1.example.com.(
                                2003040101      ; serial number

                                1H              ; refresh slave
                                5M              ; retry query
                                1W              ; expire
                                1M              ; negative TTL
)

; Specify our name servers
; !!WARNING: You can not use CNAMEs for RDATA here !!
; owner                 TTL     CL  type        RDATA
```

```
@                               IN  NS          server1.example.com.

; List our PTR records ( rev lookup ) here
; owner                  TTL     CL  type        RDATA
1.0.168.192.IN-ADDR.ARPA.       IN  PTR         station1.example.com.
2                               IN  PTR         station2.example.com.
3                               IN  PTR         station3.example.com.
4                               IN  PTR         station4.example.com.
5                               IN  PTR         station5.example.com.
6                               IN  PTR         station6.example.com.
7                               IN  PTR         station7.example.com.
8                               IN  PTR         station8.example.com.
9                               IN  PTR         station9.example.com.
10                              IN  PTR         station10.example.com.
11                              IN  PTR         station11.example.com.
12                              IN  PTR         station12.example.com.
13                              IN  PTR         station13.example.com.
14                              IN  PTR         station14.example.com.
15                              IN  PTR         station15.example.com.
16                              IN  PTR         station16.example.com.
17                              IN  PTR         station17.example.com.
18                              IN  PTR         station18.example.com.
19                              IN  PTR         station19.example.com.
20                              IN  PTR         station20.example.com.

$GENERATE       21-100          $   PTR         station$.example.com.

$GENERATE       101-200         $   PTR         server$.example.com.

254                             IN  PTR         server1.example.com.

; Note that we're not actually delegating the students authority to
; manage their IP addresses...so their server and our server will
; disagree on the correct reverse lookup for their IP address, and
; we're both claiming to be authoritative.  Naughty of us.  :)  We
; have to do this, since their server won't be there most of the
; time to delegate to.  Doesn't matter for ownerXX.example.com.
```

192.168.1.zone

- 新增加 /var/named/chroot/var/named/192.168.1.zone 檔案，內容如下：

```
$TTL 86400
@ IN  SOA server1.example.com. root.server1.cracker.org. ( 5 10800 3600 604800 0 )

  IN  NS  server1.example.com.

1.1.168.192.IN-ADDR.ARPA.       IN  PTR   cracker1.cracker.org.
2       IN  PTR   cracker2.cracker.org.
3       IN  PTR   cracker3.cracker.org.
4       IN  PTR   cracker4.cracker.org.
5       IN  PTR   cracker5.cracker.org.
6       IN  PTR   cracker6.cracker.org.
7       IN  PTR   cracker7.cracker.org.
8       IN  PTR   cracker8.cracker.org.
9       IN  PTR   cracker9.cracker.org.
10      IN  PTR   cracker10.cracker.org.
11      IN  PTR   cracker11.cracker.org.
12      IN  PTR   cracker12.cracker.org.
13      IN  PTR   cracker13.cracker.org.
14      IN  PTR   cracker14.cracker.org.
15      IN  PTR   cracker15.cracker.org.
16      IN  PTR   cracker16.cracker.org.
17      IN  PTR   cracker17.cracker.org.
18      IN  PTR   cracker18.cracker.org.
19      IN  PTR   cracker19.cracker.org.
20      IN  PTR   cracker20.cracker.org.

$GENERATE       21-253          $   PTR         cracker$.cracker.org.

254     IN  PTR   server1.cracker.org.
```

cache-nameserver 套件會協助建立

- 底下列表 cache-nameserver 套件會協助建立，但仍需要檢查是否存在及權限是否正確。

```
[root@sc220469 named]# ls -l
-rw-r----- 1 root named  198 Jul 30  2009 localdomain.zone
-rw-r----- 1 root named  195 Jul 30  2009 localhost.zone
-rw-r----- 1 root named  427 Jul 30  2009 named.broadcast
-rw-r----- 1 root named 1892 Jul 30  2009 named.ca
-rw-r----- 1 root named  424 Jul 30  2009 named.ip6.local
-rw-r----- 1 root named  426 Jul 30  2009 named.local
-rw-r----- 1 root named  427 Jul 30  2009 named.zero
```

測試

- 使用 host 指令測試
- 語法：host IP/名稱 [DNS伺服器]

```
[root@sc220469 named]# host 192.168.1.24 127.0.0.1
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:

24.1.168.192.in-addr.arpa domain name pointer cracker24.cracker.org.
[root@sc220469 named]# host 192.168.0.24 127.0.0.1
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:

24.0.168.192.in-addr.arpa domain name pointer station24.example.com.
[root@sc220469 named]# host server120.example.com 127.0.0.1
Using domain server:
Name: 127.0.0.1
Address: 127.0.0.1#53
Aliases:

server120.example.com has address 192.168.0.120
```

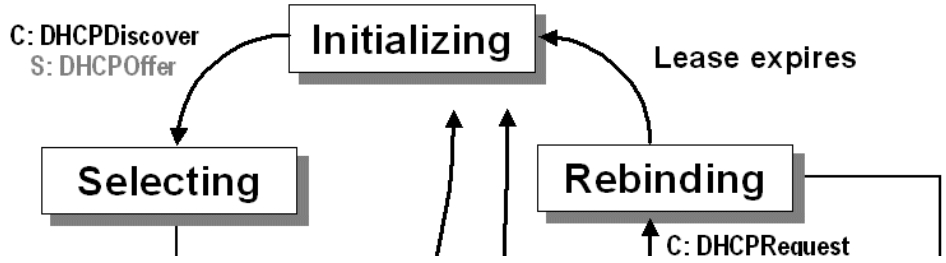
動態主機設定協定 (DHCP)

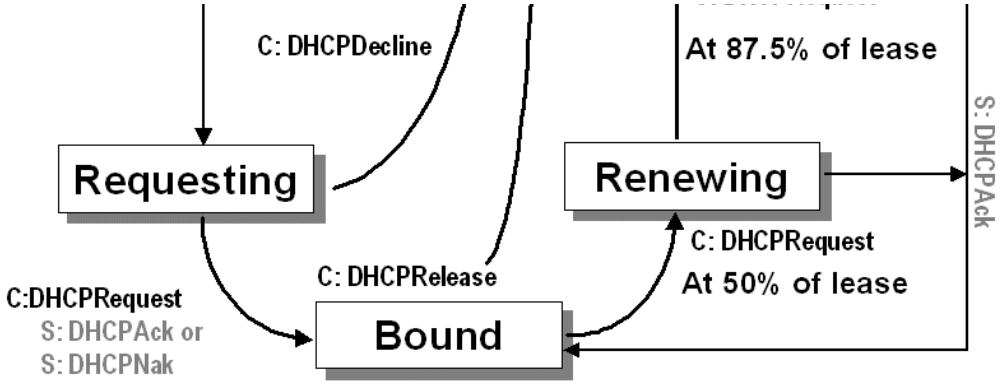
DHCP介紹

- DHCP: 動態主機設定通訊協定，實做 via dhcpd
- dhcpd 提供服務包涵 DHCP 及 BOOTP IPv4 clients

- DHCP IP發放步驟： 當Client PC網路設定使用DHCP自動抓取IP時，一開機後

1. Client to Server 發Discover 廣播訊息，一般PC不理會，但DHCP Server會回應
2. Server to Client 還有IP可用的話，發 Offer 廣播訊息
3. Client to Server 發 REQUEST，選取 Offer 當中想要的資訊，如gateway, IP, Dns...，Server收到，並記錄租約資訊
4. Server to Client 回傳確認的 ACK 訊息給 client，租約始生效





- IP定址解決方案－DHCP http://www.ascc.sinica.edu.tw/nl/86/1321/02.txt

DHCP設定

- Service Profile: DHCP
- Type: SystemV-managed service
- Package: dhcp
- Daemon: /usr/sbin/dhcpd
- Script: /etc/init.d/dhcpd
- Ports: 67 (bootps), 68 (bootpc)
- Configuration: /etc/dhcpd.conf, /var/lib/dhcpd/dhcpd.leases
- Related: dhclient, dhcpv6_client, dhcpv6

設定一個 IPv4 DHCP Server

- 設定檔 /etc/dhcpd.conf
- 樣本檔 /usr/share/doc/dhcp-version/dhcpd.conf.sample
- 最少以一個 subnet 為單位 and it must correspond with configured interfaces.
- 如錯誤請使用 dhcpd configtest to check 語法
- 安裝 dhcp server

```
[root@server1 ~]# yum install dhcp
```

- 取得設定的範例檔

```
[root@server1 ~]# cat /usr/share/doc/dhcp-3.0.5/dhcpd.conf.sample  > /etc/dhcpd.conf
```

- 設定 eth1 可以自動分發 172.24.0.1 ~ 172.24.0.200 的 IP

```
[root@server1 ~]# vi /etc/dhcpd.conf
# 是否動態更新 dns 的紀錄
ddns-update-style none;
ignore client-updates;

# 自動分配的子網路範圍，他會透過廣播封包自行找到合適的
subnet 172.24.0.0 netmask 255.255.255.0 {

# --- default gateway 預設的閘道
        option routers                  172.24.0.254;
        option subnet-mask              255.255.255.0;

#       option nis-domain               "domain.org";
       # 預設的 Domain
        option domain-name              "example.com";
       # 預設的 DNS server
        option domain-name-servers      168.95.1.1;

        option time-offset              -18000; # Eastern Standard Time
#       option ntp-servers              192.168.1.1;
#       option netbios-name-servers     192.168.1.1;
# --- Selects point-to-point node (default is hybrid). Don't change this unless
# -- you understand Netbios very well
```

```
#       option netbios-node-type 2;

        # 分配的 IP 範圍
        range dynamic-bootp 172.24.0.100 172.24.0.200;
        # 預設的租約時間，後面的時間參數預設單位為秒；
        default-lease-time 21600;
        # 最大租約時間，當用戶端超過租約時間卻尚未更新 IP 時，最長可以使用該 IP 的時間；
        max-lease-time 43200;

        # 網段固定 IP 設定
        host ns {
                next-server station1.example.com;
                hardware ethernet 12:34:56:78:AB:CD;
                fixed-address 172.24.0.1;
        }
}
[root@server1 ~]# service dhcpd restart
Shutting down dhcpd:                                       [FAILED]
Starting dhcpd:                                            [  OK  ]

[root@server1 ~]# chkconfig dhcpd on
```

- 實際設定的範例 http://blog.cm.nsysu.edu.tw/?uid-2-action-viewspace-itemid-42
- 更進階的DHCP參考

目標檢核

- Address questions
- Preparation for Lab
- Goals
- Scenario
- Deliverables
- Please ask the instructor for assistance when needed

實作

實做一個最小的 DNS server

- 安裝 dns server 相關套件
- Access Control
- 建立一個最小的設定檔案
- 改變你的網路設定，使用 localhost 測試 dns 的工作是否正常？
- 實作過程

請參考課本

加入日期到 Name Server

- 加入一個 forward lookup zone for **domainX.example.com**
- 測試你的 forward lookups
- 增加一條 reverse lookup zone
- 測試你的 reverse lookups 是否正確可以工作？
- 實作過程

請參考課本

增加 Slave DNS 的能力

- 定義一個 slave zone for example.com
- 測試 slave zone transfer 的功能
- 實作過程

實作過程

請參考課本

Challenge Projects

- 設定一個 round robin ....
- 增加一個subdomain support.domainX.example.com 去到你的 domain.
- 實作過程

請參考課本

Cleaning up

- 實作過程

請參考課本

回到索引頁 or 回到首頁