



DNS 伺服器

1-1 名稱伺服器概念

我們設定我們的主機名稱是 flash.aasir.com 而主要 DNS 為 168.95.1.1，主機名稱是向網址公司所購買。

位址:61.218.29.3(由中華電信提供)

網路遮罩:255.255.255.248(由中華電信提供)

主機名稱:FLASH.AASIR.COM(這是 NAME.080.NET 網址公司提供)

開道位址:61.218.29.1(為固定式 IP 的第一個 IP)為 ATU-R 的 IP

主要名稱伺服器 DNS:168.95.1.1(由中華電信提供)

我們網站的名稱 HOSTNAME，是向網址管理公司購買，國內的網址(.TW)通常都是向 TWNIC 台灣網路資訊中心所申請並且購買，兩年的費用為 2000 元。

台灣網路資訊中心網址是 WWW.TWNIC.NET。

這是在 sysinstall->configure->Network 中設定網路組態設定。

flash.aasir.com 就是我們的網站名稱。

Network Configuration

Host: flash.aasir.com Domain: aasir.com

IPv4 Gateway: 61.218.29.1 Name server: 168.95.1.1

Configuration for Interface rl0

IPv4 Address: 61.218.29.3 Netmask: 255.255.255.248

Extra options to ifconfig:

OK CANCEL

網域的命名空間。

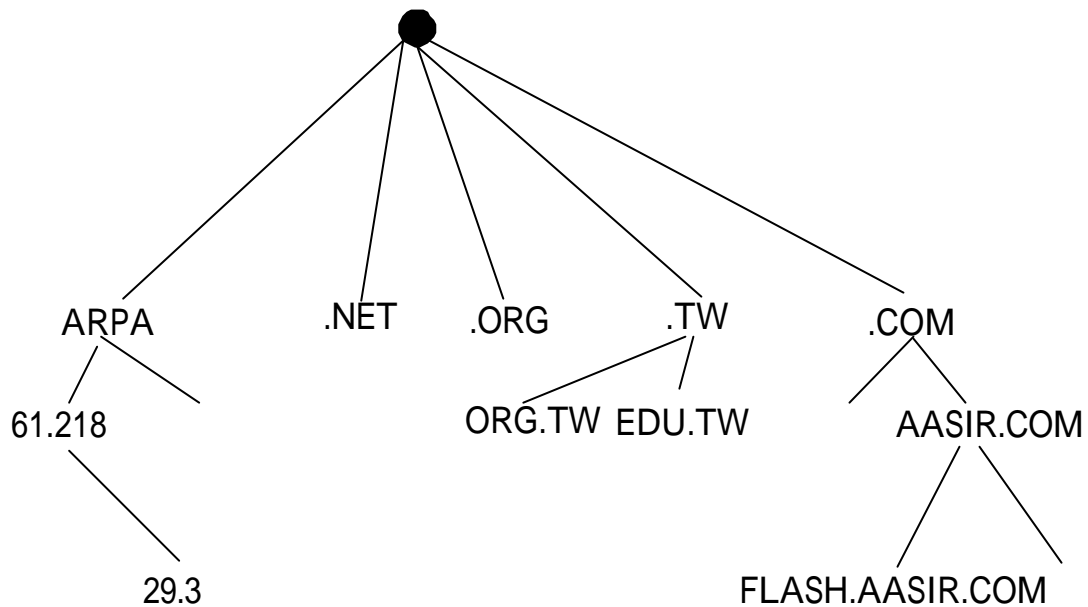
我們郵寄信件時會指定收件人的地址和姓名，也同時會有我們寄件人的地址，這就像我們網路系統的命名。

網域的命名空間，就像一根倒長的樹，這是由我們的 Arpanet 國際組織所設定。當我們在瀏覽器上打上 FLASH.AASIR.COM 時，它會先到大黑點去(根 ROOT 的名稱伺服器)，再到 .COM 的名稱伺服器(DNS) AASIR.COM(名稱伺服器 DNS)

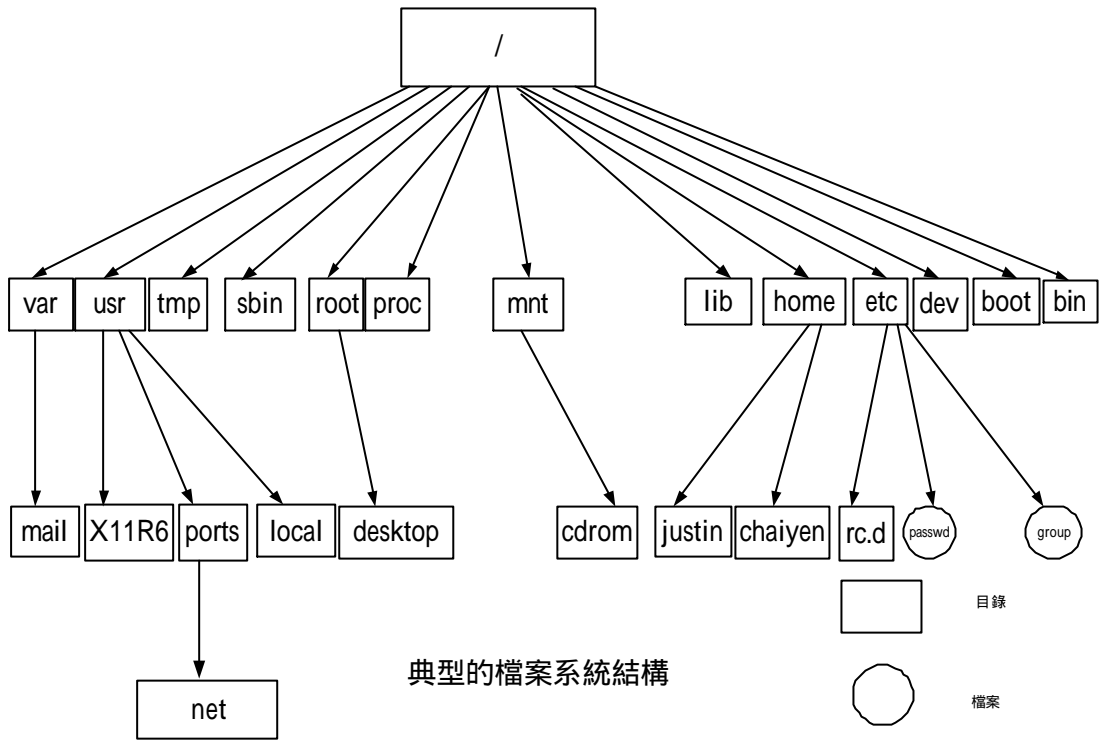
FLASH.AASIR.COM(名稱伺服器)，到了 FLASH.AASIR.COM，它會解析我們的 IP 為 61.218.29.3。

如果我們在瀏覽器上打上 61.218.29.3 時，它也會到大黑點去(根 ROOT)，再到 APRA(名稱伺服器)，再到 61 的網域，再到 61.218 的網域，再到 61.218.29 的網域，最後才找到我們 61.218.29.3 的網站。

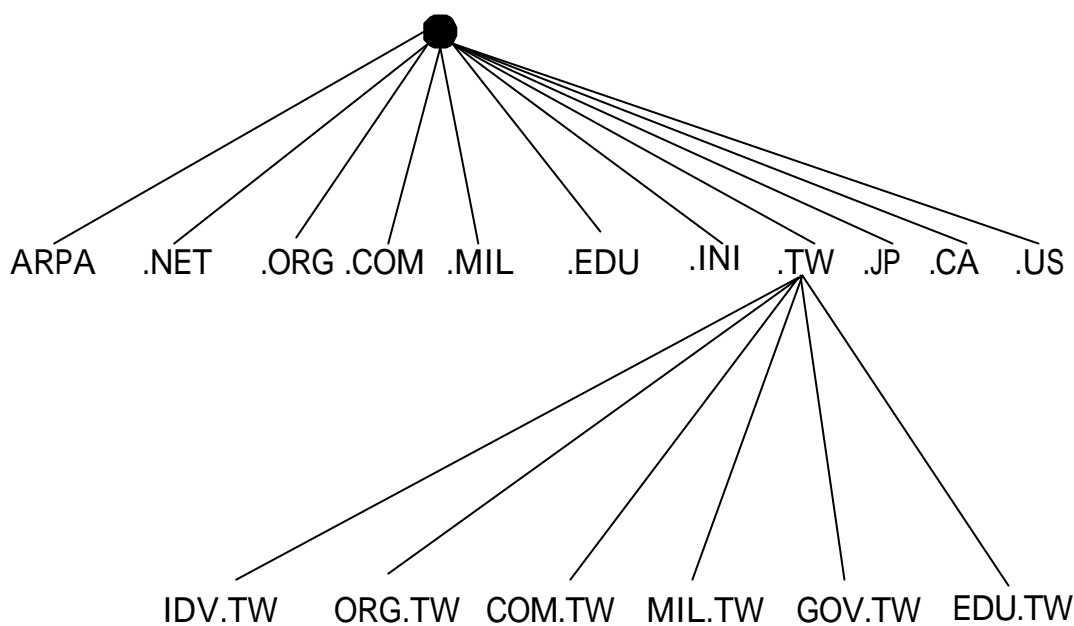
我們了解網域的命名及使用方法後，對我們之後的架設網站將有很大的幫助。



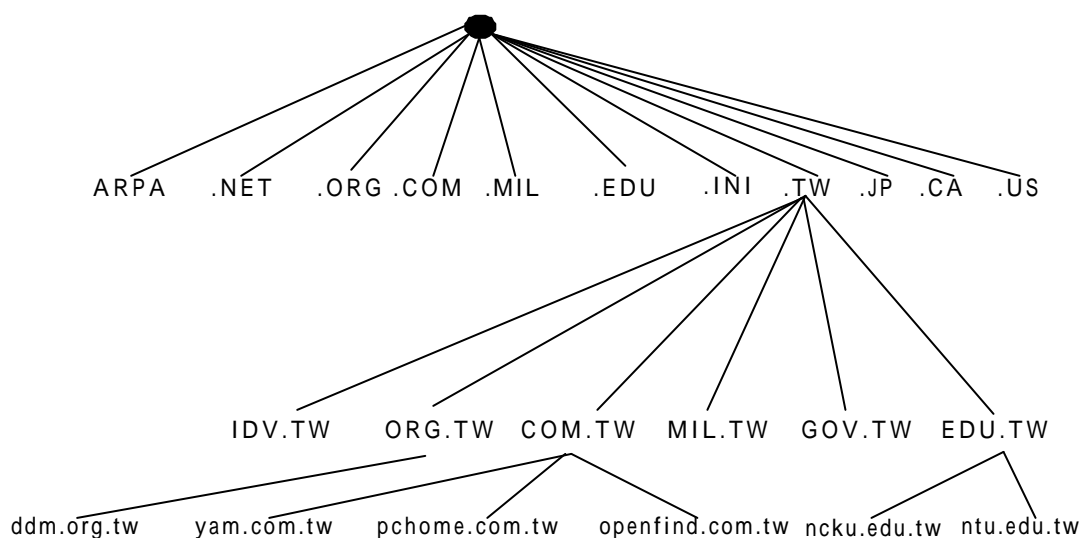
這是在 FreeBSD 上的樹檔案系統，長得就像是 DNS 資料庫。



網域的頂層領域分為一般領域與國家領域。一般領域為 com(commercial 商業使用)、edu(education 教育機構)、gov(government 政府組織)、ini(國際組織)、mil(military 軍事組織)、net(網路供應商)和 org(非營利組織)等。國家領域為 tw(台灣)、jp(日本)、kr(韓國)、us(美國)、cn(中國大陸)、hk(香港)、ca(加拿大)....。在台灣 tw 的下一層領域可分為 com.tw(commercial 台灣的商業公司)、edu.tw(education 台灣的教育機構)、gov.tw(government 台灣政府組織)、mil.tw(military 台灣的軍事組織)、idv.tw(台灣的個人使用者)和 org.tw(台灣的非營利組織)等。



在 tw 底下又可以細分成很多網域，而每個子網域又可細分成很多網站。com.tw 網域底下有很多網站，如 pchome.com.tw、yam.com.tw 蕃薯藤、openfind.com.tw 網擎....。

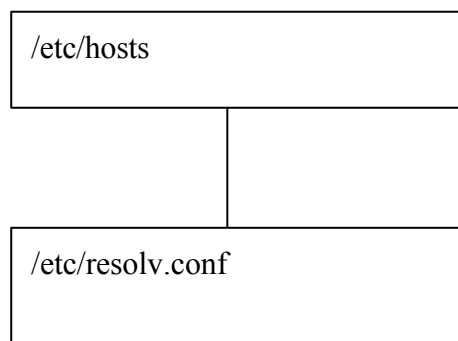


我們使用 ifconfig 來觀看網路,由這裏我們可以看到網路卡是 RTL8139 也就是螃蟹卡,為第一片網路卡 r10,而類型是 Ethernet 乙太網路,狀態 status 是可用 active

```
[ju@flash/]# ifconfig
r10: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    inet 61.218.29.3 netmask 0xffffffff broadcast 61.218.29.7
    inet6 fe80::290:ccff:fe0d:a05e%r10 prefixlen 64 scopeid 0x1
    ether 00:90:cc:0d:a0:5e
    media: Ethernet autoselect (10baseT/UTP)
    status: active
lp0: flags=8810<POINTOPOINT,SIMPLEX,MULTICAST> mtu 1500
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x3
    inet 127.0.0.1 netmask 0xff000000
tun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1500
    Opened by PID 207
```

FREEBSD 名稱解析的順序

上面所設定的就是這兩個檔案的內容。hosts 為設定網站的名稱與對應的 IP , resolv.conf 為設定我們網站的解析名稱伺服器。



我們使用 vi /etc/hosts 來編輯 hosts 檔。

```
#vi /etc/hosts
```

這裏顯示我們的 IP 61.218.29.3 和所對應的 FLASH.AAISR.COM 網站名稱。

```
127.0.0.1          localhost.aasir.com localhost
61.218.29.3       flash.aasir.com flash
61.218.29.3       flash.aasir.com.
```

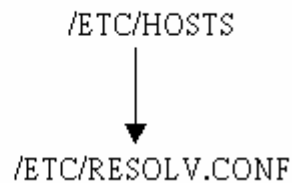
再來就是設定解析名稱伺服器 resolv.conf，這時 nameserver 為 168.95.1.1，這是由中華電信所提供。

```
domain aasir.com
nameserver 168.95.1.1
```

在 FREEBSD 上的名稱解析

在 FREEBSD 上面，我們網站簡易名稱的解析是由兩個檔所組成，分別是 /ETC/HOSTS、/ETC/RESOLV.CONF 兩個檔所組成。

FREEBSD 名稱解析的順序是：



```
61.218.29.3 flash.aasir.com flash
```

61.218.29.3 是我們主機的 IP。

flash.aasir.com 是我們主機的名稱。

flash 是我們主機的別名。

```
127.0.0.1 localhost.aasir.com localhost
61.218.29.3 flash.aasir.com flash
61.218.29.3 flash.aasir.com.
```

resolv.conf 是定義哪一些是解析我們主機的 DNS(DOMAIN NAME SERVER)。

```
#vi /etc/resolv.conf
```

nameserver 168.95.1.1, 則是名稱伺服器的 IP。

```
domain aasir.com
nameserver 168.95.1.1
```

如果我們這部機器是當 DNS SERVER 則應該寫成：

```
DOMAIN FLASH.AASIR.COM
```

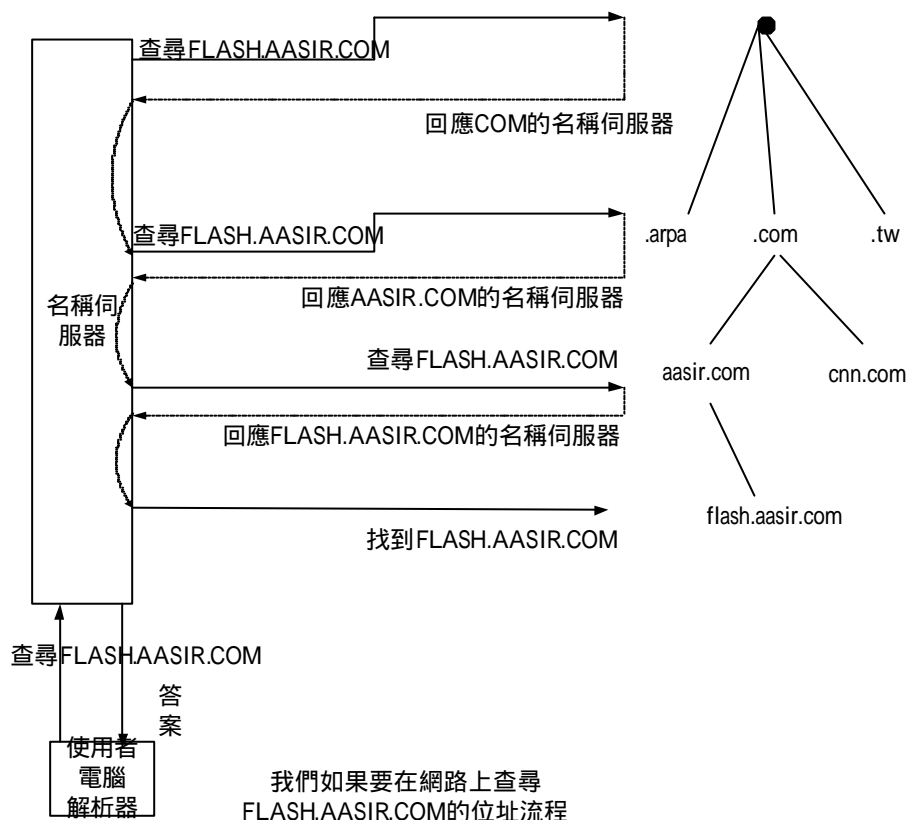
```
NAMESERVER 61.218.29.2
```

```
NAMESERVER 168.95.1.1
```

我們可以看出我們這部機器可以使用圖形介面來設定組態,也可以由文字模式來設定組態。

1-1-1 INTERNET 上解析 FLASH.AASIR.COM 的過程

當使用者在瀏覽器上打上 FLASH.AASIR.COM 時，它會先到使用者所指定的 DNS(名稱伺服器去找尋)，如果有找到對應的名稱就會回應網站的 IP，如果沒有找到，它會往根(ROOT)去尋找，因為筆者的網址是國際網址，所以它會再下去找 .COM 的名稱伺服器，找到 .COM 的名稱伺服器後，它會再往下找 AASIR.COM 的名稱伺服器，再找到 FLASH.AASIR.COM 所對應的 IP。當找到 IP 時，它就會反向去 ARPA 去尋找我們 IP 的位址，最後就找到我們網站了。



我們使用超級使用者，打上 ifconfig 之後，就可以看到我們主機的網路情況，我們第一張網路卡 rlo 的 IP 是 61.218.29.3 遮罩是 255.255.255.248。

我們 local 端的 IP 是 127.0.0.1。

```
[ju@flash/]# ifconfig
rlo: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    inet 61.218.29.3 netmask 0xfffffff8 broadcast 61.218.29.7
    inet6 fe80::290:ccff:fe0d:a05e%rlo prefixlen 64 scopeid 0x1
    ether 00:90:cc:0d:a0:5e
    media: Ethernet autoselect (10baseT/UTP)
    status: active
lp0: flags=8810<POINTOPOINT,SIMPLEX,MULTICAST> mtu 1500
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    inet6 ::1 prefixlen 128
    inet6 fe80::1%lo0 prefixlen 64 scopeid 0x3
    inet 127.0.0.1 netmask 0xff000000
tun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1500
    Opened by PID 207
```

我們使用 PING 這個指令可以看看網路是否暢通，我們 ping tw.yahoo.com 而封包都沒有遺失(0% packet loss)，表示暢通。

```
[ju@flash/]# ping tw.yahoo.com
PING tw.yahoo.com (202.1.237.21): 56 data bytes
64 bytes from 202.1.237.21: icmp_seq=0 ttl=249 time=43.460 ms
64 bytes from 202.1.237.21: icmp_seq=1 ttl=249 time=44.607 ms
64 bytes from 202.1.237.21: icmp_seq=2 ttl=249 time=44.019 ms
滌C
--- tw.yahoo.com ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 43.460/44.029/44.607/0.468 ms
```

我們可以使用 NSLOOKUP 指令來查看我們名稱伺服器的情況。

進入 NSLOOKUP 後我們設定 SET TYPE=NS，再輸入 AASIR.COM 則會出現我們的中華電信 DNS SERVER 為 168.95.1.1，而解析我們名稱的伺服器為 DNS.INTERGROUP.NET 和 DNS2.INTERGROUP.NET 兩台名稱伺服器。

```
[ju@flash/]# nslookup
Default Server:  dns.hinet.net
Address:  168.95.1.1

> set type=ns
> aasir.com
Server:  dns.hinet.net
Address:  168.95.1.1

Non-authoritative answer:
aasir.com      nameserver = dns.intergroup.net
aasir.com      nameserver = dns2.intergroup.net
aasir.com      nameserver = ns.5168.com
aasir.com      nameserver = dns.080.net

Authoritative answers can be found from:
dns.intergroup.net      internet address = 202.168.200.110
dns2.intergroup.net     internet address = 216.40.250.18
ns.5168.com             internet address = 202.168.200.110
dns.080.net             internet address = 216.40.250.18
```

如果網址是向 TWNIC 所申請的，則 NAMESERVER 為 NS2.WS300.NET 和 NS.WS300.NET 兩台。這兩部 DOMAIN NAME SERVER 掌管了台灣大部份網站的網址名稱。

1-1-2 網路位址的分配

我們解釋了整個網路的查詢名稱流程。我們在這要解說網路網路上資料傳送的協定 TCP/IP。

IP61.218.29.2

每一個 IP 都有四個位元組，每一個位元組為 0 到 255，例如我們的 IP 第一個位元組為 61、第二個位元組為 218、第三個位元組為 29、第四個位元組為 3

61.218.29.2

因為組織的大小不同，而有使用不同數量的 IP，因此我們將 IP 分成三類：CLASS A、CLASS B、CLASS C。

CLASS A 為國際大型企業或組織所使用，IP 的第一個位元組是由國際網域組織所指定，而後面三個位元組則可自行使用，因此可使用的 IP 數量為 $255*255*255=16777215$ 。

CLASS B:IP 的第一個和第二個位元組是由國際網域組織所指定，後面的二個位元組則可自行應用，因此有 $255*255=65535$ 個 IP 可供使用。

CLASS C:IP 的前三個位元組是由網域組織所指定，後面的一個位元組則可自行應用，所以總共有 255 個 IP 可以使用。

遮罩的目的地是為了讓我們切割網路所使用。

61.218.29.0 當網路遮罩為 255.255.255.0 時，我們可使用的 IP 為 255 個之多。

網址從 61.218.29.0 到 61.218.29.255 有 255 個 IP。

61.218.29.0 當網路遮罩為 255.255.255.248 時，我們可使用的 IP 為 8 個。

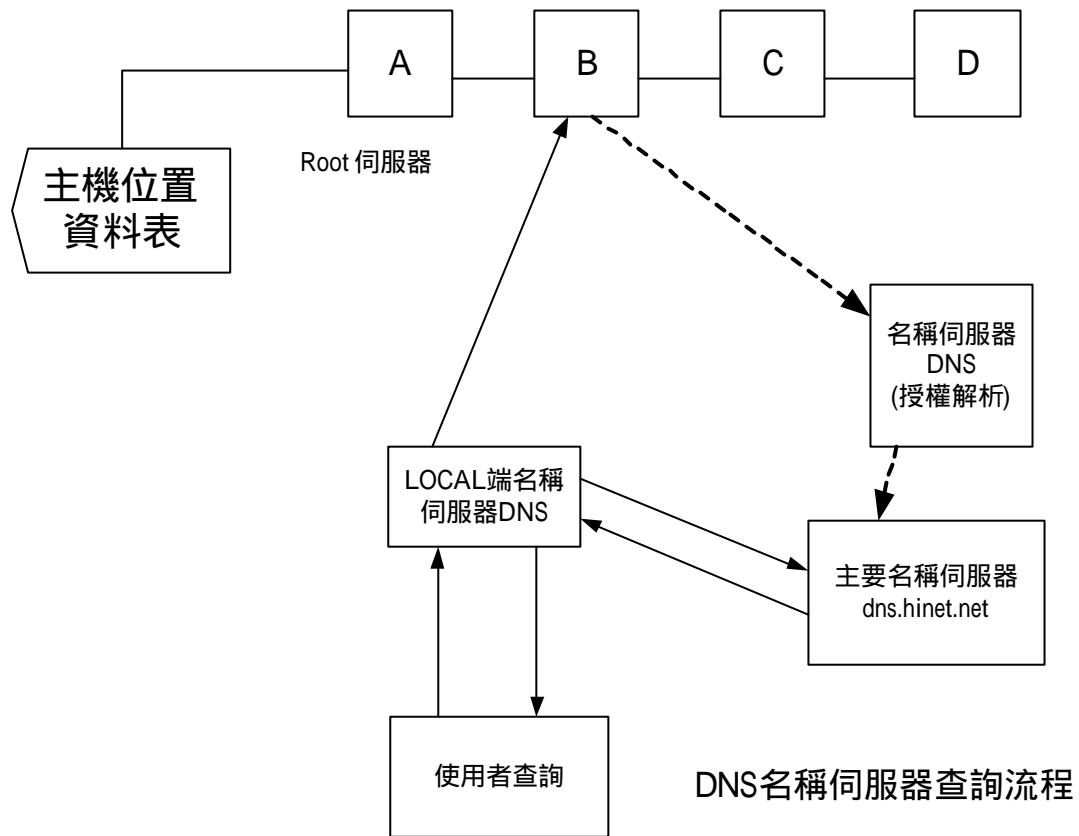
網址從 61.218.29.0 到 61.218.29.7 八個 IP。

1-1-3/etc/namedb/named.root

假如我們自己的電腦無法解析 DNS 需求查詢，則會查詢 root 的 DNS 名稱伺服器(在/etc/namedb/named.root)。

#vi /etc/namedb/named.root

我們的主要名稱伺服器是中華電信 DNS SERVER 為 168.95.1.1(dns.hinet.net)，而解析我們名稱的伺服器為 DNS.INTERGROUP.NET 和 DNS2.INTERGROUP.NET 兩台授權解析名稱伺服器。



1- 2 管理名稱伺服器

我們可以開機自動啟動名稱伺服器 bind，我們可以編輯/etc/rc.conf的檔案。

```
named_enable="YES"
```

我們也可以使用 named 指令來啟動名稱伺服器。

```
#named
```

我們也可以使用 ndc 來啟動名稱伺服器。這裏顯示新的名稱伺服器行程編號 process id 為 962。

```
#ndc start
```

```
new pid is 962
```

我們可以使用 ndc stop 來停止名稱伺服器。

```
#ndc stop
```

我們使用 ndc reload 來重新啟動名稱伺服器。

```
# ndc reload
```

我們也可以使用 killall -HUP named 來重新啟動名稱伺服器

```
#killall -HUP named
```

我們可以使用/etc/namedb/named.conf 來編輯名稱伺服器組態檔。

```
#vi /etc/namedb/named.conf
```

1-2-1 以特定目錄執行名稱伺服器

我們可以在特定的目錄 `sandbox` 執行特定的服務，所以我們在 `/etc/named` 名稱伺服器目錄下新增 `sandbox` 目錄。

```
# mkdir sandbox
```

一般在 `sandbox` 組態都有一個目錄，在名稱伺服器 `bind` 中，它是放置在 `/etc/namedb/sandbox` 的目錄下。我們將 `/etc/namedb/sandbox` 的使用者與使用者群組改為 `bind`，並且將其使用者權限修改成 `750`。

```
# chown -R bind:bind /etc/namedb/sandbox/
```

```
# chmod -R 750 /etc/namedb/sandbox
```

我們然後建立 `sandbox` 子目錄 `/etc/namedb/sandbox/etc` 和 `/etc/namedb/sandbox/var/run`，名稱伺服器將會將執行過程寫到 `/etc/namedb/sandbox/var/run` 目錄下。名稱伺服器會記錄本地端的時間然後和記錄檔寫到 `/etc/namedb/sandbox/var/run` 目錄下。

```
# mkdir /etc/namedb/sandbox/etc
```

```
# cp /etc/localtime /etc/namedb/sandbox/etc
```

```
# mkdir -p /etc/namedb/sandbox/var/run
```

我們為了開機啟動 `sandbox` 的組態目錄，我們編輯 `/etc/rc.conf` 的目錄。

```
#vi /etc/rc.conf
```

```
named_flags="-u bind -g bind -t /etc/namedb/sandbox"
```

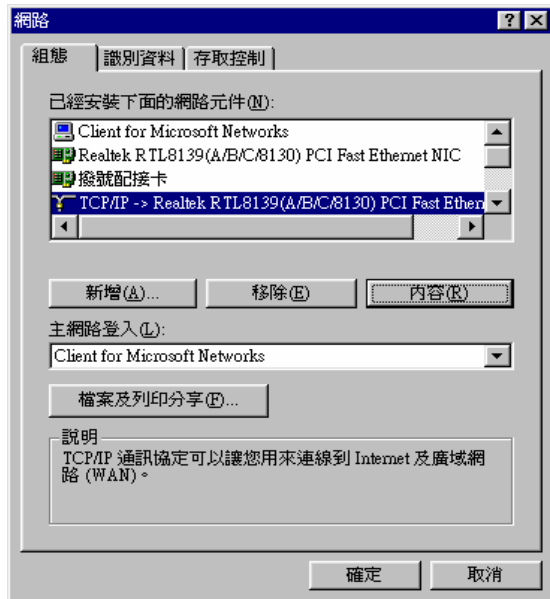
假如我們要記錄名稱伺服器的記錄，我們一定要將它記錄到

`/etc/namedb/sandbox/var/run` 目錄下。假如我們使用 `ndc` 來控制名稱伺服器而且在 `sandbox` 執行名稱伺服器，我們一定要使用 `-c` 的選項。

```
#ndc -c /etc/namedb/sandbox/var/run/ndc start
```

1-3 使用者端設定 DNS 組態

因為我們電腦使用都是使用微軟的 Window 作業系統，所以我們要到 TCP/IP 的內容來設定 DNS 組態。因為我們的電腦要能夠解析網路上的地址，就需要指定 DNS 伺服器來解析我們所要的網路位址。通常我們使用中華電信的網路都會設定 168.95.1.1 的名稱伺服器，因為我們現在也已經有名稱伺服器，所以也可以設定上我們名稱伺服器的位址。我們選取網路，再選取網路卡的 TCP/IP，再選取內容。



我們這時選取 DNS 組態,並且在 DNS 伺服器搜尋順序輸入我們自己設定的 DNS 伺服器位址 61.218.29.2。我們再按下新增,這樣就在使用者端設定好了。當使用者端上網時,就會使用我們的 DNS 名稱伺服器去搜尋網路的位址。



1- 4 名稱伺服器的組態設定

名稱伺服器的組態檔就是 `named.conf`，這是放在 `/etc` 的目錄下。當我們要設定名稱伺服器時，除了組態檔 `named.conf` 外也要設定主機區域的正反解檔才能讓 DNS 伺服器運行。正解區域檔內定是放在 `/etc/namedb` 的目錄下，正解就是作用領域名稱對應到 IP 位址的轉換。反解區域檔也是放在 `/etc/namedb` 的目錄下，反解就是將 IP 位址對應到領域名稱的轉換。

我們編輯名稱伺服器的組態檔 `vi /etc/namedb/named.conf`。

```
# vi /etc/namedb/named.conf
```

第十行是定義宣告和定義正反解區域檔的放置目錄。預設是 `/etc/namedb`。

第九行的 `options` 是控制通用的伺服器組態和設定其它選項。

第十一行的 `pid-file` 是名稱伺服器行程編號所放置的地方。

```
1 #/ $FreeBSD: src/etc/namedb/named.conf,v 1.14 2003/02/07 20:58:38 keramida Exp $
2 //
3 // Refer to the named.conf(5) and named(8) man pages for details. If
4 // you are ever going to set up a primary server, make sure you
5 // understand the hairy details of how DNS works. Even with
6 // simple mistakes, you can break connectivity for affected parties,
7 // or cause huge amounts of useless Internet traffic.
8
9 options {
10     directory "/etc/namedb";
11     pid-file "/var/run/named/pid";
12
13 // In addition to the "forwarders" clause, you can force your name
14 // server to never initiate queries of its own, but always ask its
15 // forwarders only, by enabling the following line:
16 //
17 //     forward only;
18
19 // If you've got a DNS server around at your upstream provider, enter
20 // its IP address here, and enable the line below. This will make you
21 // benefit from its cache, thus reduce overall DNS traffic in the Internet.
22 /*
23     forwarders {
24         127.0.0.1;
25     };
26 */
27 /*
28     * If there is a firewall between you and nameservers you want
29     * to talk to, you might need to uncomment the query-source
```

我們在 `named.root` 上設定轉向 `forwarders`，當在 LOCAL 端主機找不到主機時，它會轉向到 `dns.hinet.net` 去查詢。

```
forwarders{
    dns.hinet.net;
};
```

第四十二行的 include “/etc/rndc.key”是表示將參照/etc/rndc.key的內容。
第四十三行是設定正解區域名稱 aasir.com。第四十三行是設定正解區域型態。第
四十五行是設定正解區域檔名/var/named/aasir.com.hosts。

```
24 };
25 zone "." IN {
26     type hint;
27     file "named.ca";
28 };
29
30 zone "localhost" IN {
31     type master;
32     file "localhost.zone";
33     allow-update { none; };
34 };
35
36 zone "0.0.127.in-addr.arpa" IN {
37     type master;
38     file "named.local";
39     allow-update { none; };
40 };
41
42 include "/etc/rndc.key";
43 zone "aasir.com" {
44     type master;
45     file "/var/named/aasir.com.hosts";
46     };
```

zone 是宣告我們名稱伺服器的反解區域名稱為 61.218.29。第四十九行是宣告反
解區域型態為 master 主要伺服器。第五十行是設定反解區域檔名為
/var/named/61.218.29.2.rev。

```
zone "29.218.61.in-addr.arpa" {
    type master;
    file "/var/named/61.218.29.2.rev";
};
```

每一個 zone 區塊定義我們 FreeBSD 機器所管理的網路區域或子網路區域。一個
zone 定義我們的網站區域 aasir.com。

```
zone "aasir.com" {
    type master;
    file "/var/named/aasir.com.hosts";
};
```

這個 type 類型可以是 master、slave、stub、forward 或是 hint。我們經常使用的是
master 和 slave，其它的則是在特別的領域。一個 master zone 主要區域指示這
個伺服器授權這整個區域。它擁有整個區域的複製檔案，定義名稱到位置的對應。

一個 slave zone 複製區域是主要區域的複製，它也是從 mater zone 主要區域作衍生。Slave zone 複製區域可以提供 DNS 查詢授權回答。一個複製區域就像下列的情況，type 是 slave，而它的主要區域為 192.168.1.1。

zone 是設定正解區域名稱為 domain.com。type 是設定正解區域型態為 slave。file 是設定正解區域檔名為/var/named/aasir.com.bak，而這我們也可以設在別的檔案上或目錄。

```
zone "domain.com" {
    type slave;
    file "/var/named/domain.com.bak";
    masters {
        192.168.1.1;
    };
};
```

我們可以有其它區域的三種型態區塊。

stub : stub zone 區域除了傳送 NS 記錄外，其它就和 slave zone 區域一樣。

forward : 我們可以使用 forward 區域型態來轉接所有對於這個區域的要求到其它它伺服器。

hint : 這是給名稱伺服器的建議列表，列表一般設在 root 伺服器上 (/etc/namedb/named.root)。

1-4-1 領域正解區域的宣告檔

我們在/etc/namedb/named.conf 檔中已經設定好了領域正解區域的檔案,在這裏我們編輯我們所設定的正解區域 aasir.com.hosts。

```
zone "aasir.com" {  
    type master;  
    file "/var/named/aasir.com.hosts";  
};
```

```
#vi /var/named/aasir.com.hosts
```

這是我們正解區域宣告的內容。

```
$TTL      3600
```

```
aasir.com.      IN      SOA      aasir.com. "wu\chaiyen@msa\hinet\.net\" (
                @date@ ; Serial
                3600   ; Refresh
                900    ; Retry
                3600000 ; Expire
                3600 ) ; Minimum

aasir.com.      IN      NS       aasir.com.
aasir.com.      IN      A        61.218.29.2
good.aasir.com. IN      A        61.218.29.6
```

SOA : 設定這個轄區(Zone)資料的權威來源。也就是上一層 DNS 伺服器的名稱。aasir.com.這個名稱必需從檔案中的第一行開始。這個名稱以點號(.)號結尾。IN 是指網路的意義。指的是轄區資料所屬的類別。SOA 後面的 aasir.com.是指管理這轄區資料的主要名稱伺服器 Wu\chaiyen@msa\hinet\.net 就是我們管理者的電子郵件。其它的規則為更新時間(設定區域內更新網域名稱資料的時間,預設是 36000 秒)、傳輸重試時間(重試傳輸給區域的時間。預設是 900 秒)、過期時間(設定區域記錄的過期時間,預設是 3600000 秒)、預設的存活區間(區域內的名稱伺服器存活期間,預設是 3600 秒)。

NS : 列出這個轄區權威伺服器的名稱。NS 就是(名稱伺服器)資源記錄。轄區內的每一部名稱伺服器都要為它新增一個 NS 記錄 在 aasir.com.轄區內有一部 aasir 名稱伺服器。

A : 設定名稱映設到位址的對映關係,把主機名稱轉換成 IP 位址。每一筆資源記錄會將一個名稱對應到一個位址。當查詢 good.aasir.com 時就會傳回 61.218.29.6 的位址。

CNAME : 為主機的正式名稱定義別名。

1-4-2 領域反解區域的宣告檔

我們在/etc/namedb/named.conf 檔中已經設定好了領域反解區域的檔案,在這裏我們編輯我們所設定的反解區域 61.218.29.2.rev。 29.218.61.in.addr.arpa.是反解區域 61.218.29。 file /var/named/61.218.29.2.rev 是設定反解區域的檔案。

```
zone "29.218.61.in-addr.arpa" {
    type master;
    file "/var/named/61.218.29.2.rev";
};
```

我們可以編輯反解區域。

```
#vi /var/named/61.218.29.2.rev
```

```
$TTL      38400
```

```
29.218.61.in-addr.arpa. IN      SOA      aasir.com.
"wu.chaiyen@msa.hinet.net". (
                                @date@  ; Serial
                                3600    ; Refresh
                                900     ; Retry
                                3600000 ; Expire
                                3600   ) ; Minimum
29.218.61.in-addr.arpa.      IN      NS       aasir.com.
6.29.218.61.in-addr.arpa.   IN      ptr      good.aasir.com.
```

SOA : 設定這個轄區(Zone)資料的權威來源。也就是上一層 DNS 伺服器的名稱。aasir.com.這個名稱必需從檔案中的第一行開始。這個名稱以點號(.)號結尾。IN 是指網路的意義。指的是轄區資料所屬的類別。SOA 後面的 aasir.com.是指管理這轄區資料的主要名稱伺服器。Wu.chaiyen.msa.hinet.net 就是我們管理者的電子郵件。其它的則為更新時間(設定區域內更新網域名稱資料的時間,預設是 10800 秒)、傳輸重試時間(重試傳輸給區域的時間。預設是 3600 秒)、過期時間(設定區域記錄的過期時間,預設是 604800 秒)、預設的存活區間(區域內的名稱伺服器存活期間,預設是 38400 秒)。

NS : 列出這個轄區權威伺服器的名稱。NS 就是(名稱伺服器)資源記錄。轄區內的每一部名稱伺服器都要為它新增一個 NS 記錄。在 29.218.61.in-addr.arpa.轄區內有一部 aasir 名稱伺服器。

PTR : 設定位址映設到名稱的對應關係,把 IP 位址轉換成主機名稱。我們使用 6.29.218.61.in-addr.arpa 來把 IP 位址 61.218.29.6 轉換成主機名稱 good.aasir.com。

CNAME : 為主機的正式名稱定義別名。

1-5DNS 存取限制

我們在/etc/namedb/named.conf 中限制 DNS 的存取，我們使用 acl 敘述。這些可以包含 any、none、localhost 和 localnets。

Any : 允許任何主機存取。

None : 拒決任何主機存取。

localhost : 允許在這系統上任何介面的 IP 位址存取。

localnets : 允許在這網路上的任何主機存取。

因為 named.conf 名稱伺服器的組態執行是由上到下，因此一般將 acl 敘述放到組態設定的前面。!61.218.29.9 是禁止 61.218.29.9 的位址來存取我們名稱伺服器。

```
acl "aasir_list" {  
    Localhost;  
    Localhost;  
    Another_list;  
    !61.218.29.9;  
    61.218.29/24;  
};
```

allow_query{address_list_elements;...};指定什麼主機才能執行一般 DNS 的查詢。Allow-query 也可以在 zone 敘述中使用，它會覆寫在 options 中的設定。假如沒有指定，預設是允許所有的主機查詢。

allow_transfer{address_list_element;...};指定可以從主要名稱伺服器接收轉接的 slave 名稱伺服器。

Allow-recrsion{address_list_elements;...};指定可以遞迴查詢的主機。如果沒有指定，預設是允許所有主機都可以遞迴查詢。

blackhole{address_list_elements};指定不可以接授查詢的主機。

我們可以限制全域 acl `aasir_list` 的查詢。我們在 `options` 中使用 `allow-query {aasir_list}` 設定限制名稱伺服器的存取為 `aasir_list`。

```
options {  
    directory "/etc/namedb";  
    allow-query {aasir_list};  
};
```

我們也可以在 `aasir.com` 區域中設定其 acl 的存取為 `aasir_list` 和 `61.218.29/24` 的區域。我們也允許轉到 slave 的伺服器（位置 `61.218.29.2`）存取。

```
zone "aasir.com" {  
    type master;  
    file "aasir.com";  
    allow-query {aasir_list;61.218.29/24};  
    allow-transfer {61.218.29.2};  
};
```

1-6 測試 DNS 的名稱解析

Ping 使用 ICMP 協定對遠端主機發出要求來引出遠端主機或開道的 ICMP 的回應，這樣可以讓我們了解我們網路的通道是否暢通。

語法：

指令：ping 參數 ip 位址(或領域名稱)

說明：

-a：ping 時發出聲音

-b：允許 ping 廣播的位址。

-c 數目：發出要求的數目。

-d：使用 Socket 的 SO_DEBUG 選項。

-i 間隔秒數：每隔幾秒發出要求。

-n：只有數值輸出。

-q：只顯示執行結果。

-r：直接送到遠端主機，而繞過 Routing table。

-R：記錄路由過程。

-s 封包大小：指定送出資料的大小。預設為 56bytes，如果加上標頭檔 8bytes 則為 64bytes。

-t ttl：設定封包的存活時間。

-v：顯示詳細的輸出。

我們使用 ping -q aasir.com 來顯示執行的結果。在這裏顯示我們所 ping 的 aasir.com 網址是 61.218.29.2。總共有 18 個封包傳送，0 個封包遺失。我們可以按下 <CTRL+c> 來中斷。

```
# ping -q aasir.com
```

```
[root@good chaiyen]# ping -q aasir.com
PING aasir.com (61.218.29.2) from 61.218.29.6 : 56(84) bytes of data.
```

```
--- aasir.com ping statistics ---
```

```
18 packets transmitted, 18 received, 0% loss, time 21215ms
rtt min/avg/max/mdev = 0.236/0.251/0.348/0.031 ms
```

我們可以使用 ping 61.218.29.2 來測試網址 61.218.29.2 是否暢通。

```
# ping 61.218.29.2
```

```
[root@good chaiyen]# ping 61.218.29.2
PING 61.218.29.2 (61.218.29.2) from 61.218.29.6 : 56(84) bytes of data.
64 bytes from 61.218.29.2: icmp_seq=1 ttl=255 time=0.264 ms
64 bytes from 61.218.29.2: icmp_seq=2 ttl=255 time=0.240 ms
```

```
--- 61.218.29.2 ping statistics ---
```

```
2 packets transmitted, 2 received, 0% loss, time 999ms
rtt min/avg/max/mdev = 0.240/0.252/0.264/0.012 ms
```

我們使用 traceroute 來探測使用者與指定位址間的詳細路徑。

語法：

指令：traceroute 參數 ip 位址(或領域名稱)

說明：

- f：設定第一個封包存活的時間。
- d：使用 Socket 層級的除錯。
- g：指定一個疏鬆來源的路由閘道。
- i：指定網路介面來獲的路由位址。
- l：使用 ICMP 取代 UDP(使用者資料協定)
- m：設定封包最大的存活時間。
- n：使用 IP 位址而不使用主機名稱。
- p：探測時，使用 UDP 連接號碼(預設是 33434)。
- r：將封包直接送給主機，而繞過 Routing table。
- s：設定本地主機的 IP 位址。
- t：設定偵測封包服務的型態。
- v：顯示詳細指令執行的過程。
- w：設定探測回應的等待時間。
- x：開啟或關閉 IP 檢查。

我們使用 traceroute 來探測使用者與指定網址 aasir.com 間的詳細路徑。

```
# traceroute aasir.com
```

```
[root@good root]# traceroute aasir.com
traceroute to aasir.com (61.218.29.2), 30 hops max, 38 byte packets
 1 www (61.218.29.2) 0.587 ms 0.344 ms 0.216 ms
[root@good root]# traceroute tw.yahoo.com
traceroute to tw.yahoo.com (202.1.237.21), 30 hops max, 38 byte packets
 1 61-218-29-1.HINET-IP.hinet.net (61.218.29.1) 1.009 ms 0.987 ms 0.
 2 10.218.29.254 (10.218.29.254) 55.303 ms 43.444 ms 46.349 ms
 3 h210.s80.ts.hinet.net (168.95.80.210) 46.262 ms 47.086 ms 46.246
 4 tp-s2-c12r1.router.hinet.net (168.95.207.6) 47.241 ms 50.286 ms 4
 5 211.22.35.57 (211.22.35.57) 46.506 ms 52.869 ms 52.859 ms
 6 211.22.41.89 (211.22.41.89) 45.529 ms 51.059 ms 45.509 ms
 7 alteon6.tpe.yahoo.com (202.1.237.253) 47.012 ms 51.204 ms 51.919
```

我們使用 traceroute 來探測使用者與指定位址 168.95.1.1 間的詳細路徑。

```
# traceroute 168.95.1.1
```

```
[root@good root]# traceroute 168.95.1.1
traceroute to 168.95.1.1 (168.95.1.1), 30 hops max, 38 byte packets
 1 61-218-29-1.HINET-IP.hinet.net (61.218.29.1) 3.881 ms 1.009 ms 0.958 ms
 2 10.218.29.254 (10.218.29.254) 45.201 ms 48.380 ms 45.695 ms
 3 h210.s80.ts.hinet.net (168.95.80.210) 53.735 ms 49.547 ms 46.498 ms
 4 tp-s2-c12r1.router.hinet.net (168.95.207.6) 46.978 ms 48.772 ms 46.756 ms
 5 211.22.35.1 (211.22.35.1) 46.464 ms 45.686 ms 47.005 ms
 6 tp-b-c6r2.router.hinet.net (168.95.1.61) 53.749 ms 50.217 ms 46.480 ms
```

TCP 為傳輸控制協定。

UDP 為使用者資料傳輸協定。

ICMP 為網路控制訊息協定。

我們可以使用 nslookup 來查詢網域領域名稱與 IP 對應的偵錯模式。Nslookup 有交談式模式和非交談式模式。

語法：

指令：nslookup

nslookup 領域名稱

我們輸入 nslookup 來進入交談式模式。我們輸入 aasir.com 就可以查出我們的名稱伺服器為 168.95.1.1。

```
#nslookup
```

```
[root@aasir /]# nslookup
Note: nslookup is deprecated and may be removed from future releases.
Consider using the `dig' or `host' programs instead. Run nslookup with
the `-sil[ent]' option to prevent this message from appearing.
> aasir.com
Server:          168.95.1.1
Address:         168.95.1.1#53

Non-authoritative answer:
Name:   aasir.com
Address: 61.218.29.2
```

這是非交談模式，我們直接輸入我們的網址 aasir.com。

```
# nslookup aasir.com
```

```
[root@aasir /]# nslookup aasir.com
Note: nslookup is deprecated and may be removed from future releases.
Consider using the `dig' or `host' programs instead. Run nslookup with
the `-sil[ent]' option to prevent this message from appearing.

Server:          168.95.1.1
Address:         168.95.1.1#53

Non-authoritative answer:
Name:   aasir.com
Address: 61.218.29.2
```

我們使用 set all 來作完整的查詢資料。我們離開 nslookup 可以在交談模式輸入 exit。

```
> set all
Default server: 168.95.1.1
Address: 168.95.1.1#53
Default server: 61.218.29.2
Address: 61.218.29.2#53

Set options:
  novc                nodebug            nod2
  search              recurse
  timeout = 0         retry = 2          port = 53
  querytype = A       class = IN
  srchlist = aasir.com
> exit
```

假如我們要從(.)領域開始追蹤到我們的領域是由哪一些領域階層提供名稱伺服器的服務，我們可以先輸入 set type=any，再輸入我們要查尋的領域。我們輸(.)就可以得到最上層的領域。。

```
> set type=any
> .
Server:          168.95.1.1
Address:         168.95.1.1#53
```

我們輸入 tw.就可以得到台灣最上層的網路領域。

```
> tw.
Server:          168.95.1.1
Address:         168.95.1.1#53

Non-authoritative answer:
tw      nameserver = NS.TWNIC.NET.
tw      nameserver = B.DNS.tw.
tw      nameserver = A.DNS.tw.
tw      nameserver = C.DNS.tw.
tw      nameserver = D.DNS.tw.
tw      nameserver = F.DNS.tw.
Name:    tw
Address: 192.83.166.11
tw
```