サブネットのホストをDNS逆引きデータベースへ登録する方法

総合情報システム運用センター　曽根 秀昭
sone@tains.tohoku.ac.jp

SuperTAINSでは，標準的なサブネットの大きさがネットマスク長26になり，**TAINS88**も含めてネットマスク長が24より長い，小さなサブネットが増えています。このような小さいサブネットの逆引きデータの管理は，ドメイン名管理(DNSデータベース管理)の担当者にとって難しい問題です。つまり，バイト単位ごとに構成することになっている，逆引き用データベースの*.34.130.in-addr.arpaが複数のサブネットにまたがるために，サブネットごとに独立して管理できないからです。現在は，**SuperTAINS**や**TAINS88**で25ビット以上のネットマスク長のサブネットを割当てたケースでは，サブネット内のホストを逆引きデータベースへ登録する作業を総合情報システム運用センターが行なっています。

この問題は，建物や部局全体に対して大きいブロックの割当を受けたものをローカルで再分割して研究室などへ割当てるときにも，同じようにあてはまります。これについて，一つの解決方法を紹介します。

この技術の要点は，逆引きのドメインがサブネットと一致するように，サブネット専用の階層を逆引き用ドメインの中間に追加したところです。例えば，130.34.xx.yから130.34.xx.zまでを割り当てられた小さいサブネットならば，y-z.xx.34.130.in-addr.arpaを作り，これをそのサブネットで独自に管理します。その中に130.34.xx.wがあれば，逆引きのw.xx.34.130.in-addr.arpaのデータはw.y-z.xx.34.130.in-addr.arpaとして管理されます。もし，別に130.34.xx.aから130.34.xx.bを割り当てられたサブネットがあれば，そちらではa-b.xx.34.130.in-addr.arpaを使います。

設定は，まず，上位(34.130.in-addr.arpa)のネームサーバで，便宜的に，小さいサブネットに分割するバイト単位のアドレス(130.34.xx.0/24)の逆引き(xx.34.130.in-addr.arpa)のためのネームサーバを登録します。このネームサーバは，どこにあっても構いません。ここで登録した便宜的なネームサーバで，すべてのアドレスについて逆引きデータ(*.xx.34.130.in-addr.arpa)のCNAMEを定義して，それぞれのサブネットの逆引きのための新しいドメインにマッピングしておきます。それと別に，小さいサブネットごとに逆引きドメインのネームサーバを用意します。逆引きの具体的なデータはこちらのネームサーバがもち

ます。このネームサーバは，もちろん，そのサブネットの中でも外部のものでも構いません。他のサブネットのネームサーバと兼用しても構いません。

具体的な数値で例を書いておきます。

Case 1:

130.34.208.64-127 を dept.tohoku.ac.jp のサブネットに割当てたとします。(その前後は別の部局。)

208.34.130.in-addr.arpa のネームサーバの登録内容

```
; ORIGIN=208.34.130.in-addr.arpa.
0-63                    NS      ns.other.tohoku.ac.jp.
0                       CNAME   0.0-63
1                       CNAME   1.0-63
                        ......（途中も，ぜんぶ書いておく）
63                      CNAME   63.0-63
;
64-127                  NS      ns.dept.tohoku.ac.jp.
64                      CNAME   64.64-127
                        ......（途中も，ぜんぶ書いておく）
127                     CNAME   127.64-127
;
128-255                 NS      ns.another.tohoku.ac.jp.
128                     CNAME   128.128-255
                        ......（途中も，ぜんぶ書いておく）
255                     CNAME   255.128-255
```

ns における 64-127.208.34.130.in-addr.arpa のネームサーバの登録内容

```
; ORIGIN=64-127.208.34.130.in-addr.arpa.
64                      PTR     subnet-1.dept.tohoku.ac.jp.
                        A       255.255.255.192.
65                      PTR     gateway.dept.tohoku.ac.jp.
66                      PTR     ns.dept.tohoku.ac.jp.
67                      PTR     someone.dept.tohoku.ac.jp.
                        ......（途中は，存在するものを書いておく）
127                     PTR     broadcast.subnet-1.dept.tohoku.ac.jp.
;
```

Case 2:

130.34.208-209.* を dept.tohoku.ac.jp に割当て，そのうち 130.34.209.128-143 を lab.dept.tohoku.ac.jp のサブネットに割当てたとします。(部局内でのブロック再割当)

209.34.130.in-addr.arpa のネームサーバの登録内容

```
; ORIGIN=209.34.130.in-addr.arpa.
128-143                 NS      ns.lab.dept.tohoku.ac.jp.
128                     CNAME   128.128-143
129                     CNAME   129.128-143
130                     CNAME   130.128-143
                        ......（*.209 のぜんぶを書く）（*.208 も同様に）
143                     CNAME   143.128-143
;
```

ns で 128-143.209.34.130.in-addr.arpa のネームサーバの登録内容

```
; ORIGIN=128-143.209.34.130.in-addr.arpa.
128                     PTR     subnet.lab.dept.tohoku.ac.jp.
                        A       255.255.255.240.
129                     PTR     gateway.lab.dept.tohoku.ac.jp.
130                     PTR     ns.lab.dept.tohoku.ac.jp.
131                     PTR     someone.lab.dept.tohoku.ac.jp.
                        ......（途中は，存在するものを書いておく）
143                     PTR     broadcast.subnet.lab.dept.tohoku.ac.jp.
;
```

この方法が，世界的に広く使われるようになりつつあります。ただし，不完全な DNS サーバプログラム (ネームサーバ) では，ここで示した方法で登録したデータを処理できないものもありますが， UNIX では不都合の例がないようです。同様に，検索するときに，不完全な検索プログラム (リゾルバ) では，正しい結果が得られなかったり，プログラムが異常終了することもありますが， Mac 以外ではトラブルの例がないようです。

また，かなりの割合の UNIX では，テスト版の検索プログラム (リゾルバ) が入っているために，ここで示した方法で登録したデータを処理するときに動作確認用メッセージをコンソール画面に表示しますが，実害はありません。このメッセージを止めるには，別なバージョンのプログラムと入れ換えます。

ここで紹介した技術は，以下の文書に準じたものです。

INTERNET-DRAFT “Classless IN-ADDR.ARPA delegation”
(draft-ietf-cidrd-classless-inaddr-02.txt),
Network Working Group (November 1996).