多田研における Private Network の導入について

1996 年 6 月 26 日

多田研究室　林 隆広

lannet@spa.is.uec.ac.jp

Abstract

この文書は多田研における Private Network の導入について述べたものである。最初に背景となった環境を説明し、導入の理由や経緯、問題への対処方法に触れる。そして具体的なネットワークの構成や各設定について述べ、最後にその後の運用形態と問題点などについてまとめる。

1　従来の状況について

多田研 (spa) は 130.153.166.0/24 という外部と IP 接続可能 (public) なサブネットアドレスを取得している [1]。そこに十数台のホストがぶら下がるありがちな構成であった (図 1)。各種サーバはすべて同一セグメント上のマシンで動いていた。またセグメントの一部を 10Base-T ケーブルで延長して輪講室に HUB を置き、輪講中にメールを読むことができるようになっていた。

電通大の通常のマシンはルータの吐く経路情報を全部受け取るが [2]、spa のゲートウェイは経路を一切受け取らず全てのマシンは defaultroute を持つ設定になっていた。これは単に、定期的に流される RIP が Network のバンド幅を消費するだけなので嫌がられたという理由によるものだった。このため全てのマシンは外部からの直接の IP 接続が可能だった。

さて、このような構成の中で次のような問題が浮き上がってきた:

- 輪講室問題
  輪講室は多田研だけが使うものではないのでセキュリティ的には非常に危険であることが考えられる。例えばケーブルを接続するだけで NFS パケットや login コネクションのパケットを盗聴できる。
- 管理の分散
  マシンのうち、主要でないいくつかは管理者以外の者に管理させている。これは研究に必要であるという理由と勉強してもらうという意味を兼ねているが、主管理者の負担を軽減するという意味あいもあった。だが外部への IP 接続が可能ということは原則として外部からの IP-connection を許していると言えるので、初心者に管理させるのは手抜きや落度、技術不足などの点で不安だという考えがあった。

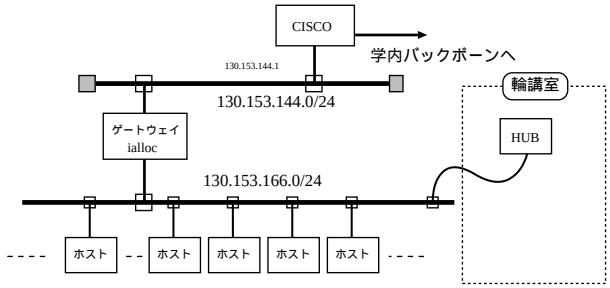

図 1: 1996 年 4 月までのネットワーク構成

2　動機

Private Network を使用することは面倒なことだがそれにも関わらず導入に踏み切った主な理由は次の通り:

- セキュリティ
  原則として組織外から直接 IP パケットは到達できないので、少々管理上の問題のあるホストがいても安心していられる。また輪講室の HUB については別セグメントになるので研究室内のパケットが流れていくことはない。

- ほかのサイトにまねをしてもらう
  IPv6[3] への移行にはかなり時間がかかると思われるので、それまでのつなぎとして Private Network を利用して public アドレスの消費を抑える。

反対意見もあった。

- めんどうだ
  これは管理者の意見。余計なことをしたくない。動かなくなるアプリケーションが出てくる可能性もある。手間がかかる。NFS パケットを遮断するならブリッジや EtherSwitch でも使い、内を外に見せたくないならフィルター (IP filter) で切れば良いではないか。
- 利便性の悪化
  利用者側の意見。学外へ到達できないので、Proxy サーバ、SOCKS などの導入が必要。`ping` や `traceroute` ができないなど。

結局、輪講室の HUB を独立させることはフィルターでは無理なので、仕方無く金はかからぬが手間暇かかる Private Network を使うことに決定したのである。

3 Private Network について

Private Network については RFC1597[4] で規定されている。日本語訳については UNIX マガジン [5] に載っているのでそちらを参照されたい。

Private Network は一般のネットワークと同様に扱えるが次の点で大きく異なる:

- 組織外と接続されない
  組織外との IP の接続性がない。また対外ルータは Private Network アドレスに関する経路情報を無視する。
- 外部組織に公表しない
  DNS に登録されない。外部組織はこのアドレスを逆引きできない。メールアドレス中に現われてもいけない。

このような性質のために、次のような長所がある:

- IP アドレス枯渇問題の緩和
  組織外にパケットが流さないので、各組織間では重複したアドレスを使える。
- セキュリティの向上
  原則として組織外からの直接の攻撃を受けにくい。

RFC1597 では、

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

のアドレスが Private Network のアドレスとして割り当てられている。電通大ではすでに 172.21.0.0/16 がサークル棟や PPP の受け口などで実際に運用されている (1996 年 6 月 1 日現在)。

4 導入の方法

Private だからといって即時導入可能というわけではない。なぜなら電通大内では Private Network 上のマシンも学内と通信できるようにするためにアドレス割当と経路制御に関する規定があるからである。したがって通常のサブネットアドレスと同様に ip-alloc[1] から割当てを受けるが、public な subnet ほど条件は厳しくない。

192.168.0.0/20[2] については真の意味での Private Network として扱われ、ip-alloc に問い合わせる必要は無く今すぐ使える。しかしこの経路情報を学内には絶対に流してはいけない。よって学内にも到達できない。

経路情報
: 経路に関しては該当ネットワークの経路を RIP にて定期的に流すことにより認識される。これによって学内との通信は可能となる。ただし学外への経路はないので通常の方法では学外には到達できない。

[1] ip-alloc@uec.ac.jp
[2] 昔のクラス C で 192.168.0. ~ 192.168.15.255

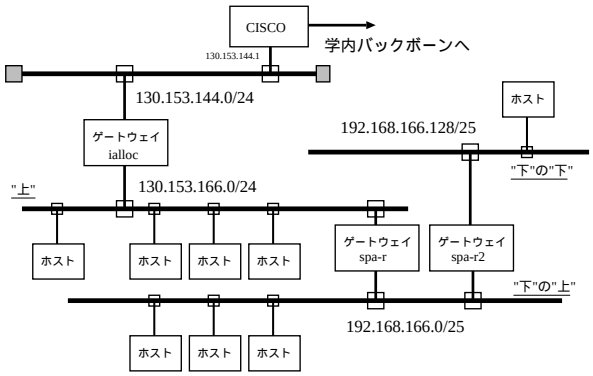

図 2: 現在の spa

DNS

学外の組織が Private Network 上のホスト名を逆引きした時に Private Address が見えてはいけない。このために学内からは見えるが学外からは見えないような工夫が必要だ。これがやっかいな問題で、一般に次の 2 つの解法が考えられる [4][6]。

- ホスト名に.private をつけて登録
  これは電通大で採られている方法である。正式なホスト名の最後に.private をつけて DNS のレコードとする。private は正式なドメインでないので学外から参照されることはない。そのかわり学内のトップドメインのサーバでこれを管理する。
- 内向けと外向けの 2 系統のサーバを用意
  名前は*.uec.ac.jp で統一されるが、正式なレコードを登録し authorize されたサーバと、そのデータと内部だけの情報を合わせた authorize されないサーバを別個に用意する必要がある。

電通大では前者を採用している。

ip-alloc から subnet をもらい (わりと簡単だろう)、DNS に名前を登録してもらえば運用可能となる。RIP で経路を流せば少したつと実際に使えるようになる。

5 設計例: 多田研ネットワークの上下の切り分け

ここでは多田研に導入してみた例について述べる。

説明のため、130.153.166.0/24 の public なアドレスを用いているネットワークを “上”、192.168.166.0/24 の private なアドレスを用いているネットワークを “下” と呼ぶことにする。多田研ではさらに図 5のように下側のネットワークを半分に分け、研究室 (192.168.166.0/25) と輪講室 (192.168.166.128/25) に割り当てた (“下” の “上” と “下” の “下”)。

上側は学外組織への IP 到達性があるのでセキュリティに気を配らねばならない。よって上には必要最小限のサーバを置き、それ以外は下側 (下の上) に置いた。各設定については次の通り:

- 経路
  各ゲートウェイには gated を入れた。spa へのゲートウェイ ialloc は 130.153.166.0/24 と 192.168.166.0/24 に関する情報を RIP で 130.153.144.0/24 に流す。spa-r は 192.168.166.0/24 に関する経路情報を 130.153.166.0/24 に流す。spa-r2 は 192.168.166.128/25 に関する経路情報を 192.168.166.0/25 に流す。
  上側の各マシンは defaultroute を ialloc に向け、下側への経路については spa-r の流す経路情報を聞くようになっている。下の上側の各マシンは defaultroute を spa-r に向け、下の下側への経路については spa-r2 の流す経路情報を聞くようになっている。下の下側の各マシンは defaultroute を spa-r2 に向ける。ialloc は SunOS-4.1.4 であるが、spa-r では両方のインターフェイスのネットマスクの幅が違うので SunOS4.x ではうまく働かず、Solaris2.5 を使用した。spa-r2 ではネットマスク幅が同じなので SunOS-4.1.4 を使用できる。
- DNS
  DNS デーモン named は外部と直接通信するので上側に置いた。Private hosts の登録については.private を補完して登録するが、各ホストの hostname は従来通り.private を補完しない。これによりホスト名

を直接見るようなアプリケーション (MH など) が.private 付きのホスト名を使用することを防ぐ。ただし.private がつかないと他のホストと通信できなくなる恐れがあるので、次のように/etc/resolv.conf の search オプション行に.private を補完するように書いておかねばならない:

```
search  spa.is.uec.ac.jp spa.is.uec.ac.jp.private
```

Solaris2.5、IRIX5.3、NetBSD、FreeBSD はこの search 行を認識するようだが、SunOS-4.1.4 に付属の resolver は古いため search 行を認識できない。そこで resolv+2.1.1 を入れ、/etc/resolv.conf の search 行を認識させた。これに伴い、libresolv をリンクしたいくつかのアプリケーション (GNU finger) などは再コンパイルが必要だった。

- NIS&NFS
  home や local の NFS サーバは下側 (下の上) に置くことにした。これにより学外からの NFS アクセスはできなくなる (学内からはできる)。NIS のマスタサーバは上側にいるので学外からアクセス可能の筈。
- sendmail
  sendmail は外部と直接通信するので上側ネットワークのみが使えることになる。幸いにも spa ではメールの配送は spool ホストに集中させているので、このホストが上側にいれば良いことになる (MX レコードもこちらを向かせる)。したがって、外部からのメールは spool ホストに溜り、内部からのメールは spool ホストを経由して出て行く。その他のホストは spool ホストのディレクトリを NFS マウントしてメールを読む設定になっている。
- NetNews
  Private Host からのアクセスは逆引きすると.private がついてくるのではねられる。News サーバの管理者に相談するのも手だが、とりあえず proxy により解決した。
- NTP
  各棟に置かれたルータは NTP パケットをブロードキャストしているので [7]、各サイトはこれを受信し自分の subnet に broadcast すればよい。spa では各ゲートウェイは内側のネットワークに NTPbroadcast を吐く設定になっている。これにより各マシンの時刻誤差は 100ms 以下に抑えられる。
- web proxy
  Private Network から外に出られないのは当然だが利便性が悪いので、web に関しては proxy server を立ち上げた。www.uec.ac.jp:8080 を利用することもできる。
- SOCKS
  Private Network から外に出られないのは当然だが利便性が悪いので、ftp, telnet, finger に関しては SOCKS を入れて使えるようにした。
- その他
  web などのサーバに関しては外部から内部に直接 TCPconnection を張られる必要があるので上においた。NAT を使えばこれらの問題は回避できるが今回は見送った。

6 その後の運用と今後の課題

2 か月ほど実際に使ってみて、気付いた点などをあげる。

- マシンの利用のされ方
  当初気にしていたほど、ユーザやプロセスの負荷は上側のマシンに集中してはいないように見える。
- NTP の誤差
  SPARC LX・Classic 以外での運用上の誤差は 100ms 以下。全く問題なし。
- 利便性に関する結果
  現在のところ、外部と直接通信するアプリケーション (`ping`, `traceroute`, `archie`, `nslookup`, `whois` など) は使えないのだが、日常的な作業に関してはあまり問題がないように思える。その他の SOCKS や proxy なども初期投資はやや大きいが、動いてしまえばあとは管理の手間もそう大きくないだろう。
- WWW-Proxy の利用率について
  あまり使われていないようなので、近いうちにやめるかもしれない。その場合はうまくごまかして proxy ホストを http://www.uec.ac.jp:8080 に向ける。

今後の課題としては、2 系統の DNS サーバを用意する構成や、ゲートウェイだけを組織外との IP の接続性を持たせ、内部はすべて Private Network とするネットワークの構成などがある。

参考文献

[1] 学内のアドレス割当, gopher://gopher.cc.uec.ac.jp:70/00/net-doc/allocate.txt.

[2] 学内の経路に関する規約, gopher://gopher.cc.uec.ac.jp:70/00/net-doc/route.

[3] 次世代 IP の実装状況, http://playground.sun.com/pub/ipng/html/ipng-implementations.html.

[4] RFC1597, ftp://ftp.uec.ac.jp/pub/wwfs/RFC/rfc1597.txt.

[5] 最近の IP アドレス事情, 加藤 朗, UNIX Magazine, 株式会社アスキー, pp.70-81, 6 月号, 1994.

[6] Private Network Address に於ける DNS 環境の構築, 楯岡 孝通, http://www.uec.ac.jp:8081/club/mma/mma/h_9504_dns.html.

[7] 学内の NTP に関する規約, gopher://gopher.cc.uec.ac.jp:70/00/net-doc/ntp.